BERGISCHE
UNIVERSITÄT
WUPPERTAL

Konzeption und Evaluierung eines Prozesses zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen

Dissertation
zur Erlangung eines Doktorgrades
(Dr.-Ing.)

in der
Fakultät für Maschinenbau und Sicherheitstechnik

der
Bergischen Universität Wuppertal

vorgelegt von
Arne Schwerdtfeger
aus Hildesheim

Erstgutachter: Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf
Zweitgutachter: Prof. Dr.-Ing. Jan Pelzl

Tag der Einreichung: 06.12.2017
Tag der mündlichen Prüfung: 08.05.2018

Wuppertal 2018

Die Dissertation kann wie folgt zitiert werden:

urn:nbn:de:hbz:468-20180615-104709-7
[http://nbn-resolving.de/urn/resolver.pl?urn=urn%3Anbn%3Ade%3Ahbz%3A468-20180615-104709-7]

Vorwort der Gutachter

Die fortschreitende Digitalisierung bringt Informationstechnik in Bereiche der Industrie und des alltäglichen Lebens, welche bisher wenig oder nur kaum mit Vernetzung und Datenverarbeitung konfrontiert waren. So steht z.B. eine allgegenwärtige Nutzung von Mobiltelefonen oder Smartphones mit ihren technologischen Freiheitsgraden in engem Zusammenhang mit der Entstehung einer neuen Kategorie von Geschäftsmodellen, die im Wesentlichen einen Mehrwert aus der Sammlung und Auswertung von Nutzerdaten generieren sollen. Dabei steht einem Komfortgewinn des Nutzers oft die Preisgabe persönlicher Daten gegenüber, deren Erhebung und Handhabung auch vor dem Hintergrund zunehmend restriktiverer Gesetzesvorgaben im Bereich des Datenschutzes ernsthaft hinterfragt werden muss. Wenn der Marktwert personenbezogener Daten als Asset in eine Risikobewertung einfließt, müssen die Technologien, die die Grundlagen für solche Geschäfte bilden, als besonders interessant für Angriffe durch Dritte angenommen und in der Konsequenz einer besonders gründlichen Analyse der Sicherheit und Vulnerabilität unterzogen werden. Die neue Datenschutzgrundverordnung (DSGVO) beispielsweise fordert explizit „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung" von Nutzerdaten, wobei die Risikoanalyse und -abwägung weitgehend an rechtsunterworfene Unternehmen delegiert wird.

Die Schloss- und Beschlagindustrie steht aktuell vor der Aufgabe, Anwendungsfälle, Technologien und Geschäftsmodelle zu digitalisieren. Das so entstehende Ökosystem zur Administration und Entwicklung derartiger Technologien sollte zum sicheren Umgang auch ein Mindestmaß an Standards voraussetzen. Jüngste Angriffe auf die Informationstechnik haben das Vertrauen der Nutzer nachhaltig negativ beeinflusst; die Effektivität und der Sicherheitswert effizienter automatisierter Mechanismen der IT-Security rücken immer mehr in den Fokus. Aufgrund des hohen Grads an Komplexität und vielfach unterschiedlicher Rahmenbedingungen lässt sich eine einfache Aussage zur Qualität der IT-Security meist nicht treffen. Unternehmen und Kunden empfinden die Bewertung von Sicherheit oft als sehr komplex und unübersichtlich; Vorgaben in Form von Standards sowie Handlungsempfehlungen existieren nur wenige.

Hier setzt die vorliegende Arbeit von Herrn Schwerdtfeger an. Sie befasst sich mit der ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen, welche eine sehr flexible Administration und Nutzung von Zutrittsberechtigungen über das Smartphone ermöglichen. Dabei können die z. B. an Türen in Gebäuden angebrachten elektronischen Schließsysteme über diverse vorhandene Schnittstellen eines Smartphones adressiert und somit der Zutritt mit der richtigen elektronischen Zutrittsberechtigung ermöglicht werden. Ganz ähnliche Systeme können im Automobilbereich für den Zutritt zu und auch das Starten und Nutzen von Kraftfahrzeugen eingesetzt werden. Zumindest den deutschen Markt betreffend muss festgestellt werden, dass die Systeme noch keine flächendeckende Verbreitung gefunden haben, obwohl alle technologischen Voraussetzungen gegeben sind. Ähnlich wie bei Mobile-Payment-Systemen, die beispielsweise in den USA und Asien schon weiter verbreitet sind, erfolgt die Rezeption dieser Technologien in Deutschland recht zögerlich, was sicher auch auf eine hohe Risikowahrnehmung zurückzuführen ist.

Damit trifft die vorliegende Arbeit einen Nerv der gegenwärtigen Entwicklung, indem sie, ganz an der Durchführbarkeit orientiert, systematisch aufzeigt, welche Anforderungen aus bestehenden Sicherheitsstandards existieren, und wie ein Produkt in einem kontinuierlichen und transparenten Prozess zur Risikominimierung anhand dieser Standards bewertet werden kann.

Velbert, im Mai 2018

J. Pelzl und K.-D. Wolf

Danksagung

„Sich selbst besiegen ist der schwerste Sieg."

(Sophokles)

Die Erstellung einer Dissertation bedeutet stets eine große Herausforderung – nicht nur für den Promovierenden selbst, sondern auch für die Personen, die ihn auf diesem Weg begleiten.

Aus diesem Grund möchte ich als erstes meinem Doktorvater Herrn Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf (Leiter des Instituts für Sicherungssysteme der Bergischen Universität Wuppertal) danken, der mein Promotionsvorhaben persönlich und wissenschaftlich betreut hat und stets zum angeregten wissenschaftlichen Austausch zur Verfügung stand.

Ein weiterer Dank gilt auch meinem zweiten Betreuer, Herrn Prof. Dr.-Ing. Jan Pelzl von der Hochschule Hamm-Lippstadt, der zu allen fachspezifischen Themen der IT-Security für anregende Diskussionen zur Verfügung stand und stets auch aus seiner persönlichen Promotionserfahrung aufmunternde und motivierende Worte an mich richtete.

Ebenfalls bedanken möchte ich mich bei Herrn Dipl.-Ing. Richard Rackl, Geschäftsführer der C.Ed. Schulte GmbH Zylinderschlossfabrik, der mein Promotionsvorhaben auch finanziell ermöglicht hat, so dass diese Promotion am Institut für Sicherungssysteme und im Unternehmen CES zu gleichen Teilen durchgeführt werden konnte. Ich hatte stets die Möglichkeit, meinen Arbeitsschwerpunkt variabel zu gestalten und konnte somit meine Ressourcen als wissenschaftlicher Mitarbeiter im Institut und als Leiter des Industrial Engineering (IE) bei CES optimal einsetzen.

Weiterer Dank gilt meinen Arbeitskollegen und Freunden in meiner Abteilung bei CES: Mara Schulte, Peter Teubler und Kathrin Rackl. Sie haben mir in der Zeit größter Anstrengungen für die Promotion mit hilfreicher Unterstützung zur Seite gestanden und mich stets motiviert, den eingeschlagenen Weg weiter zu gehen.

Bedanken möchte ich mich auch bei meinen Kollegen am Institut, insbesondere bei Sabine Kranz (Assistenz am Institut für Sicherungssysteme) für die sehr guten und hilfreichen Ratschläge zu der sprachlichen Ausformulierung meiner Gedankengänge und das Lektorat.

Zusätzlich gilt ein besonderer Dank meiner Freundin, die mir in zahlreichen Gesprächen motivierend zur Seite stand und mich immer unterstützt und in meinem Vorhaben bestärkt hat.

Ein besonderes und herzliches Dankeschön gilt meinen Eltern, die mich während meiner gesamten Ausbildung, insbesondere auch während der Zeit der Promotion, finanziell und emotional unterstützt haben, so dass ich auch schwierige Phasen mit ihrer Hilfe und Unterstützung bewältigen konnte.

Arne Schwerdtfeger

Zusammenfassung

Der zunehmende Einsatz von digital vernetzten Produkten macht das Leben für den Endnutzer in vielen Fällen einfacher und leichter. Dennoch stellt er die Anbieter solcher Technologien vor große Herausforderungen, so müssen sie im Stande sein, ihre Produkte zeitgemäß zu digitalisieren. Dies bedeutet insbesondere für die Hersteller konventioneller Produkte wie beispielsweise die Schloss- und Beschlagindustrie die Entwicklung komplett neuer Geschäftsmodelle. Zukünftig werden hier keine physischen Schlüssel mehr benötigt; eine digitale Berechtigung auf dem Smartphone verschafft den Zugang. Das entstehende Ökosystem zur Administration und Entwicklung einer solchen Technologie sollte zum sicheren Umgang auch ein Maß an Standards voraussetzen. Gerade Angriffe auf die IT-Security haben in jüngster Zeit das Vertrauen der Nutzer nachhaltig negativ beeinflusst. Deshalb sollten gerade hier sichere Standards und Bewertungsverfahren den vertrauensvollen Umgang mit innovativen Technologien bestärken und vertrauensbildend wirken.

Leider sind die Produktzertifizierungen im Bereich der Schließsysteme stark der Mechanik unterworfen und lassen einen gewichtigen Einfluss der IT-Security vermissen. Aufgrund der Historie entstanden elektronische Schließsysteme erst in jüngerer Zeit; diese werden jedoch in zu vielen Punkten am technischen Standard der mechanischen Schließzylinder gemessen. Es fehlt somit an einer ganzheitlichen Sicherheitsbewertung, die sowohl mechanische als auch IT-Security-Kriterien in einem sinnvollen Maße aufstellt.

Ziel der Sicherheitsbewertung im Bereich der mobilen Zugangslösung war eine holistische Betrachtung mechanischer Voraussetzungen und IT-Security-Kriterien des gesamten Systems aus Hersteller- und Kundensicht. Dies beinhaltet sowohl den mechatronischen Schließzylinder wie auch teilweise das Ökosystem. Dazu wurden im Sinne eines kontinuierlichen Verbesserungsprozesses in Anlehnung an PDCA-Schritte einzelne Arbeitsschritte für eine Sicherheitsbewertung entwickelt. Dabei orientierte sich die Bewertung an einem zuvor aufgestellten theoretischen Sicherheitsprofil, welches den Rahmen für den Detaillierungsgrad und die Qualität der Sicherheitsbewertung schafft. Dafür wurde das System abstrakt modelliert, um es anschließend im Analyseteil mithilfe eines Leitfragenkataloges, der sich an etablierten Werken des Bundesamtes für Sicherheit in der Informationstechnik und an den Common Criteria anlehnt, einem differenzierten Soll-Ist-Vergleich zu unterziehen. Das semi-quantitative Ergebnis der Sicherheitsbewertung steht immer in Relation zu den zuvor aufgestellten Rahmenbedingungen und schafft eine adäquate Positionierung der Sicherheit im Vergleich zur Einsatzbestimmung.

Abstract

The increasing application of digitally networked products simplifies the end user's life in many aspects. However, it challenges providers of such technologies enormously as they have to digitalise their products according to the fast moving state of the art.

This implies especially for producers of conventional products as i.e. the lock and fitting industry the development of completely new business models. In future, physical keys are no longer needed; a digital bunch will enable the user to unlock a system. The resulting ecosystem to administer and develop such technologies should presuppose an appropriate measure of standards. Especially recent attacks on IT-security infrastructures have negatively influenced the users' confidence. This is the reason why secure standards and evaluation measures should enhance the confidential trusting interaction with innovative technologies and will generate confidence.

Unfortunately, product certifications in the field of locking systems are often based on mechanics and lack the important influence of IT-security. Electronic locking systems have only been developed in recent times; however, they are assessed according to the technical standard of mechanical locking cylinders in many aspects. A holistic security evaluation which considers mechanical as well as IT-security criteria is still missing.

The final objective of evaluating security in the field of mobile access was the holistic inspection of mechanic requirements and IT-security criteria of the whole system - evaluated from either the customer's and the producer's perspective. This comprises mechatronic locking cylinders as well as parts of the ecosystem. In the course of a continuous improvement process following the PDCA measures single steps for a holistic security evaluation have been developed. The evaluation is based on a theoretical security profile which designs the framework for a detailed and qualified security profile. Therefore, the system has been modelled on an abstract level in order to study it afterwards under nominal and actual conditions with the help of a catalogue of central questions in the analytic part. The catalogue references to established publications of the BSI (Bundesamt für Sicherheit in der Informationstechnik) and to the Common Criteria. The semi-quantitative result of the security evaluation always relates to the conditions previously set and allows an adequate assessment of security compared to the intended use.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Die fortschreitende Digitalisierung ist zu einem konstanten Bestandteil der heutigen Gesellschaft geworden. Eine schleichende und kontinuierliche Vernetzung elektronischer Komponenten hat zu einem gesteigerten Komfortgewinn beim Umgang mit klassischen Systembestandteilen geführt. Gerade im industriellen Umfeld ist die Vernetzung von z.B. industriellen Produktionsanlagen unter dem Begriff „Fabrik 4.0" hinlänglich bekannt; hier steht im Wesentlichen die Entwicklung neuer Geschäftsmodelle im Vordergrund. So ist beispielsweise im Bereich der kommerziellen Endanwendungen ein offensichtlicher Mehrwert durch vereinfachtes Handling zu verzeichnen. Vordergründig sind die zyklischen Technikentwicklungen als Treiber innovativer Anwendungen im Technologiebereich zu sehen. Jedoch werden gerade durch die stärkere Verzahnung unterschiedlichster Anwendungen, wie z. B. die Einbindung des Smartphones in den Bereichen Bezahlung (Payment) oder Zutritt (Access) völlig neue Marktverhältnisse geschaffen. Parallel zur gewöhnlichen Produktentwicklung müssen auch die etablierten Geschäftsmodelle an die neuen Anforderungen angepasst werden.

Hier waren besonders die Anbieter von konventioneller Technik wie z.B. die Schloss- und Beschlagindustrie in der Vergangenheit wenig von der Umstrukturierung ihres bestehenden Marktes betroffen. Insbesondere die Sicherheitsbranche, speziell im Bereich der mechanischen Zutrittslösungen (mechanische Schließzylinder), hatte durch stark normierte und zertifizierte Produkte den bestehenden Markt professionell bedienen können. Dabei sind alle Anbieter historisch gewachsen und namentlich bestens etabliert. Feine Unterschiede im Produktportfolio bedienten bedarfsgerechte Produktanforderungen und gewährleisteten so eine gute Separierung des Marktes für jeden Hersteller. Die voranschreitende Digitalisierung führt nun zu einem Umbruch im Bereich der Marktverhältnisse. Bestehende Unternehmungen müssen sich gegen neu in den Markt eintretende Unternehmen behaupten. Es entsteht ein Konkurrenzkampf, der nicht nur auf der Ebene des besten Produktes ausgetragen wird sondern auch im intelligenten Aufsetzen der Geschäftsmodelle. In vergangenen (mechanischen) Zeiten sicherten die Nachschlüsselgeschäfte gute Erträge z. B. durch Erweiterungen der mechanischen Schließanlagen. Dieses Geschäft dürfte in der nahen Zukunft immer mehr ausbleiben, da die Komfortvorteile für den Benutzer bei einer mechatronischen Schließanlage wesentlich höher sind. Ist das Schließgeheimnis nun nicht mehr als mechanischer Code im Schlüssel sichtbar hinterlegt sondern elektronisch auf einem Transponder oder auf dem Smartphone abgespeichert, können die Berechtigungen einfach an zusätzliche Personen übertragen werden. Der Hersteller könnte somit nicht mehr die Hoheit über das Erweiterungsgeschäft haben.

Um dieser Folgeerscheinung entgegenzuwirken, müssen sich die Produzenten frühzeitig mit den neuen Technologien auseinandersetzen. Doch gerade hier werden historische Barrieren sichtbar. Eine starke Fokussierung auf den Zwischenhandel, das Sicherheitsfachgeschäft, erlaubt per se keinen direkten Endkundenkontakt. Die Bedürfnisse und Erwartungen werden also in den meisten Fällen durch den Zwischenhandel widergespiegelt und beeinflusst. Wie bereits eingangs angedeutet kommt eine starke mechanische Prägung hinzu, die, in Approximation auf die neue digitale Welt, dem Produkt nicht gerecht wird. Im Umkehrschluss müssen auch Entwicklungsleistungen im eigenen Unternehmen abgedeckt werden, da historisch bedingt oftmals kundenspezifische Anpassungen im traditionellen (mechanischen) Geschäft forciert wurden. Dadurch wird auch ein Teil der Beratungsleistung durch den Hersteller abgedeckt, der wiederum hierfür weitere Leistungen und Anstrengungen aufwenden muss, um sein Produkt bestmöglich zu bewerben. Diese Konstellationen führen unter anderem in der Konsequenz zu einer stark fokussierten Sicht, ein marktfähiges Produkt zu etablieren. Begleitet wird diese Art des Definitionsprozesses von der Ungewissheit, wie das ursprüngliche Geschäftsmodell auf die neuen Gegebenheiten angepasst oder gar revolutioniert werden kann und wie einheitliche Produktspezifika der vernetzten Systeme wie z. B. Schließgerät und Smartphone normenspezifisch zu erfassen wären. So ergeben sich auch hier völlig neue Disziplinen im Umgang mit den mobilen Zutrittslösungen. Aufgrund der Einbindung von elektronischen Komponenten erlangen z. B. die Themen Datenschutz, Cyberkriminalität und

IT-Sicherheit hohe Brisanz[1]. Vor allem in der angesprochenen Kundenberatung werden verstärkt Themen zum Schutz der persönlichen Daten diskutiert. Die IT-Sicherheit hat nicht zuletzt durch die mediale Präsenz einen enormen Einfluss auf die Meinungsbildung der potenziellen Käufer. Immer wieder wird über Fahrzeuge oder Computersysteme berichtet, die Opfer eines Cyberangriffes werden. So steigt die Verunsicherung von Kunden, Nutzern und Endverbrauchern. Die wachsenden Ansprüche an die IT-Sicherheit eifern im Wettlauf mit den Angreifern auf IT-Strukturen; oftmals nicht aus wirtschaftlichen oder persönlichen Motiven, sondern um die Medien als Instrument zu nutzen, die Hersteller nachbessern zu lassen. Leider geben die einschlägigen Normen oder Richtlinien kein umfassendes Werk dafür an die Hand, wie im Detail mit diesen Fragestellungen im Bereich der mobilen Zutrittskontrollsysteme umzugehen ist. So werden wichtige Erkenntnisse erst im Feld beim Kunden gesammelt, wenn Sicherheitslücken aufgedeckt werden. Negativ schlagen so Imageverluste und steigende Hemmnisse für Produkte der digitalen Vernetzung zu Buche.

1.2 Ausgangslage – kurzer Status-quo

1.2.1 Digitalisierung, die gesellschaftliche Triebfeder

Die Schloss- und Beschlagindustrie wird in letzter Zeit immer stärker mit den Anforderungen der Digitalisierung konfrontiert. Mechanische Systeme leisten zwar immer noch einen wichtigen Anteil des gewöhnlichen Geschäftsumsatzes, jedoch kann auch ein traditioneller Geschäftsbereich die Zeichen der Zeit nicht unbeschadet übergehen. So haben in jüngster Vergangenheit die Hersteller das Produktportfolio zunächst mit Gerätesystemen auf Basis von RFID-Transpondern, in Form von Karten oder sogenannten Tags, erweitert. Hiermit war zunächst eine berührungslose Anwendung von Geheimnisträgern, den digitalen Schlüsseln, möglich und eine vereinfachte Organisation der Schließberechtigungen. Erstmalig wurden so die nicht sichtbaren Schließmerkmale vom Anwender selbst digital auf Transponder übertragbar, speicherbar und so zu verwalten. Insbesondere bei großen Organisationseinheiten erweisen sich die elektronischen Anlagen in der Handhabung des Berechtigungsmanagements als vorteilhaft. So kann die Zutrittsverwaltung sich nahezu komplett am Geschäftsbetrieb orientieren, indem der Zutritt z.B. nur zu den Bürozeiten möglich ist oder auch Reinigungskräften nur für ein bestimmtes Zeitfenster den Zugang erlaubt. Der Verlust früherer mechanischer Schlüssel führte oft auch zum Austausch der gesamten Schließanlage; für den Betreiber war dies mit hohen Kosten verbunden und teils sehr aufwändig. Bei Hotelanlagen oder in Organisationen mit starker personeller Fluktuation wurde dieses Sicherheitsdefizit über Jahre hinweg stillschweigend geduldet. Auch die in jüngerer Vergangenheit zunehmende Berichterstattung seitens der Medien bezüglich allgemeiner Sicherheitsaspekte hat dazu geführt, dass die Sensibilität für dieses Thema stark erhöht worden ist. Selbst Polizei und Behörden reagieren darauf mit Kampagnen, wie z. B. „Zuhause sicher“[2].

Ein weiterer Aspekt der fortschreitenden Digitalisierung stellt die vermehrte Nutzung von Smartphones im privaten und auch beruflichen Bereich dar. Ausgehend von der reinen Telefonie sind mittlerweile viele weitere Dienste integriert worden. Selbst günstige Geräte können Termine organisieren, E-Mails verschicken, Routen berechnen etc. die Vielfalt scheint schier unerschöpflich. Die Unternehmung HID wirbt zum Thema Mobile Access mit dem Hinweis: „Ein komfortables und motivierendes Erlebnis für Ihre Mitarbeiter“[3]. Das Smartphone ist somit das zentrale Element in der privaten Digitalisierung. Dies bestätigt auch die hohe Zahl von 49 Millionen Nutzern in Deutschland, die sich seit 2012 mehr als verdoppelt hat[4]. Mit einer prognostizierten Wachstumsrate in 2017 von 8,2% dürfte der Trend auch weiter anhalten, wenn auch bis zum Jahre 2019 auf 2,6% Wachstum im Vorjahr zurückgehen[5]. Bei einer kürzlich durchgeführten repräsentativen Umfrage von 633 Personen besaßen 21% der Nutzer sogar zwei Smartphones, wobei die separierten Daten von geschäftlich und privat zu diesem relativ hohen Prozentsatz führen dürften[6]. Auswirkungen auf den Smart Home-Bereich betreffen somit auch weltweit den Absatzmarkt. Hier wird in 2017 eine

[1] Vgl. HID Global Corporation/ASSA ABLOY AB, Was Sie über Mobile Access wissen sollten, Teil 1, 2016, S. 1.
[2] Vgl. Polizei-Initiative, Abrufbar im Internet, http://www.zuhause-sicher.de/einbruchschutz-und-brandschutz/, 2017.
[3] Vgl. HID Global Corporation/ASSA ABLOY AB, Was Sie über Mobile Access wissen sollten, Teil 1, 2016, S. 6.
[4] comScore MobiLens, In: Statista, 2017.
[5] eMarketer, In: Statista, 2017.
[6] SevenOne Media, In: Statista, 2017.

Umsatzveränderung von 50,85% auf 22,854 Mio. Euro angenommen [7]. Generell werden im Bereich Smart Home große Wachstumschancen gesehen, die u. a. durch den demografischen Wandel bedingt sind, für die mit Assisted-Living ein eigener Absatzmarkt entsteht.

Parallel zu den wachsenden Dienstleistungen im Bereich E-Commerce können sich auch die definierten und standardisierten Schnittstellen weiter etablieren. Bei den Datenschnittstellen zählt Bluetooth zu den meistgenutzten mit einem Anteil von rund 30%[8]. Für nicht sicherheitsrelevante Dienste eignet sich die Verbindung aufgrund ihrer guten Übertragungsreichweite von bis zu 10 m. Werden allerdings sicherheitsrelevante Informationen übertragen, die per se schon eine kürzere Distanz fordern, um ein Belauschen oder Abhören der Verbindung zu unterbinden, sind in der Vergangenheit, insbesondere vom Sektor „Payment" große Hoffnungen in die NFC-Datenschnittstelle gelegt worden. Hier liegt die Distanz zur Übertragung von Daten bei circa 10 cm. Das prognostizierte Marktvolumen in 2017 von 191 Mrd. US-Dollar bestätigt diesen Eindruck[9]. Insgesamt sehen über 80% der Einzelhändler NFC als die potentiell beste Bezahltechnik; die Anwendung Bluetooth bewerten nur rund 27% der Befragten als optimal[10].

Mit den konkurrierenden Zielen, ob nun der Komfort- oder Sicherheitsgedanke im Vordergrund steht, mussten sich auch die Hersteller der Schloss- und Beschlagtechnik auseinandersetzen. Zunächst wurde im Spannungsfeld die NFC-Technologie forciert. Da hier aber der große Durchbruch über das Ausrollen des Payments ausblieb, war die Resonanz und Technikverbreitung einfach zu gering. Ein weiteres K.-o.-Kriterium für die branchenweite Nutzung ist die fehlende Unterstützung respektive vollständige Offenlegung der Schnittstelle von Apple bei seinen iPhone-Geräten (nur lesend)[11]. Da knapp 16% des Absatzes über das iOS-Betriebssystem generiert werden, würde ein respektabler Anteil an Käufern unberücksichtigt bleiben, zumal insbesondere Führungskräfte und Beschäftigte in gehobenen Positionen Nutzer von Apple-Geräten darstellen[12].

In letzter Zeit finden sich vermehrt auch Bluetooth-Anwendungen für das Bedienen eines Schließzylinders, die einer potentiellen Komforterweiterung Rechnung tragen sollten. Hierbei kann aus der Entfernung, bei Herantreten an die Tür, schon ein Öffnungssignal an den Zylinder gesendet werden, ohne das Smartphone in die Hand nehmen zu müssen. Eine NFC-Variante bietet diesen Komfort nicht, da das Smartphone mindestens bis auf die angesprochene Distanz von 10 cm an die Öffnungseinheit der Tür herangeführt werden muss. Begleitet werden die Technologien von einer Vielfalt an Funktionalitäten der erforderlichen Applikation. Digitale Berechtigungen können von Smartphone zu Smartphone übertragen werden und zeichnen sich durch ein dezentrales Berechtigungsmanagement mit z. B. limitierten Zeitfenstern, individuellen Nutzergruppen, Blacklist- und Whitelistfunktionen etc. aus.

Es ist zu erwarten, dass der Wettbewerb im digitalisierten Schloss- und Beschlagmarkt mit steigender Produktvielfalt noch zunehmen wird.

1.2.2 Normen, Richtlinien und Zertifizierungen

Wie eingangs erwähnt, finden sich für die mechanischen Schließzylinder eine große Anzahl von branchenspezifischen Informationen aus den verschiedensten Quellen. Insbesondere die normativen Verweise können eine ganze Reihe von vorgegebenen Abmessungen, Kennzeichnungen, Einsatzgebieten, Eigenschaften usw. vorgeben. Da es sich um ein nicht vernetztes System handelt, bewegen sich die Kriterien auf einem relativ simplen und nachvollziehbaren Niveau. Es sind nahezu alle möglichen Kombinationen von Produkttypen und deren Verwendung genauestens beschrieben. Als Grundlage für den mechanischen Schließzylinder zählt die EN 1303[13], die im Wesentlichen die Anforderungen und Prüfverfahren für Schließzylinder in Schlössern wiedergibt. Alle aufbauenden oder angrenzenden Normen referenzieren auf diesen

[7] Huhn, Philipp, SMART HOME, In: Statista, 2017.
[8] IfD Allensbach (ACTA 2015), In: Statista, 2017.
[9] ABI Research, In: Statista, 2017.
[10] EHI Retail Institute, In: Statista, 2017.
[11] Vgl. Apple Inc., Core NFC, Abrufbar im Internet, https://developer.apple.com/documentation/corenfc#overview, 2017.
[12] Kantar Worldpanel, In: Statista, 2017.
[13] DIN EN 1303, Baubeschläge - Schließzylinder für Schlösser, 2005.

Standard. Weiterführend sind für den Profilzylinder in Türschlössern die Begriffe, Maße, Anforderung und Kennzeichnung in der DIN 18252[14] wiederzufinden. Für ein erhöhtes Sicherheitsempfinden empfehlen sich die Richtlinien der VdS Schadenverhütung GmbH, die zum Gesamtverband der Deutschen Versicherungswirtschaft e.V. gehört. Hier sollte u. a. die VdS 2156-1[15] für Schließzylinder mit Einzelsperrschließung, die Anforderungen und Prüfmethoden vorgibt, Erwähnung finden.

Auch für die elektromechanischen respektive elektronischen Anlagen existieren zahlreiche Normen und Richtlinien. Zu nennen wäre z. B. die EN 15684[16] der mechatronischen Schließzylinder mit Anforderungen und Prüfverfahren im Bereich der Schlösser und Baubeschläge. Der VdS Schadenverhütung GmbH geht bei den Anforderungen für Schließzylinder mit Einzelsperrschließung bei den Anforderungen und Prüfmethoden mit der VdS 2156-2[17] noch etwas stärker ins Detail. Zusätzlich hat das Bundesamt für Sicherheit in der Informationstechnik eine technische Leitlinie für Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme entwickelt (TL 03405)[18].

Weiterhin lassen sich auch für Schließsysteme und Schließanlagen, die sowohl mechanisch als auch elektromechanisch oder elektronisch sein können, Normen oder Richtlinien benennen, wie z. B. die VdS 2215[19] oder VdS 2386[20]. Die Bezeichnung „Schließsystem" stellt im einfachsten Fall eine komplette Ausstattung einer Tür dar; dies bedeutet den Einsatz von Schließzylinder, Schloss und Beschlag. Bei der Schließanlage, explizit der VdS 2386[21], wird die Eignung des Schließzylinders in der Schließanlage überprüft und gilt nur in Verbindung mit der VdS 2156-1[22] und VdS 2156-2[23].

Insgesamt lassen sich in diesem Bereich sehr viele Normen und Richtlinien aufzählen, die es für Hersteller und Errichter im Bereich der Produktgestaltung zu berücksichtigen gilt. Damit verbundene Zertifizierungsverfahren sind zum Teil sehr kostspielig. Grundsätzlich lässt sich aber festhalten, dass alle Hersteller bemüht sind, die anwendbaren Systeme zertifizieren zu lassen. Bei den effektiv verkauften Produktgruppen, die schlussendlich an den Kunden (Händler) verkauft werden, sieht die Bereitschaft jedoch wieder ganz anders aus. In der Regel enthalten entsprechende Ausschreibungen immer den Hinweis auf Zertifizierungen oder Richtlinien. Hier macht es Sinn, dass der Hersteller auch die geforderten Rahmenbedingungen der Ausschreibung erfüllt, um sein Produkt anbieten zu können. Der Kunde jedoch wählt nicht selten eine kostengünstigere Version ohne Zertifizierung. In Anbetracht der geschilderten Sachlage werden die Produzenten regelmäßig mit dem Problem konfrontiert, einen gangbaren Weg zwischen theoretischen Anforderungen und praktischer Realität zu finden.

Wenn auch die Auswahl der Normen und Richtlinien für elektromechanische und elektronische Schließzylinder für jeden erdenklichen Anwendungsfall schier unerschöpflich erscheint, so decken diese doch nicht die gestiegenen Anforderungen an digitalisierte Produkte ab. Die gestiegenen Ansprüche für die Vernetzung mithilfe der Digitalisierung verkürzen verstärkt die Produktlebenszyklen, so dass Standards über Normen und Richtlinien kaum noch von adäquaten bestehenden Richtlinien erfasst werden. Mit den erwähnten Regelwerken kann die Realität nur noch schwer abgebildet werden, die sich selbst noch in der Definition und Aufteilung der neuen Märkte befindet. In Zukunft müssen weitere Technologiekomponenten, wie Smartphones und dezentrale Datenverwaltung, über Serverorganisation auf ihre Sicherheitsarchitektur hin überprüft werden. Doch gerade in dieser Übergangsphase sehen sich die Hersteller mit dem Problem konfrontiert, dem Markt gerecht werden zu müssen. Durch die Mitgliedschaft in Interessengemeinschaften, die

[14] DIN 18252, Profilzylinder für Türschlösser, 2006.
[15] VdS 2156-1, Schließzylinder mit Sperrschließung, 2012.
[16] DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013.
[17] VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013.
[18] BSI – TL 03405, Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme, 2010.
[19] VdS 2215, Schließsysteme, 2005.
[20] VdS 2386, Schließanlagen, 2012.
[21] Ebd.
[22] VdS 2156-1, Schließzylinder mit Sperrschließung, 2012.
[23] VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013.

außerhalb der Kooperationsbestrebungen für neue Dienstleistungen liegen, verpassen die Hersteller so den Aufbau eines gemeinsamen Verständnisses zum Thema Sicherheit. Dabei spielt die sukzessive Begleitung der Sicherheitsforschung eine entscheidende Rolle, denn Sicherheit entsteht schon während der Produktentwicklungsphase sowie dem anschließenden Erfolg oder Misserfolg einer daraus resultierenden Dienstleistung; dem Mehrwert für den Kunden.

Für die Betrachtung weiterer Bewertungsmöglichkeiten, nicht nur die überwiegend mechanische Produktnormung, sollte auch die Organisation oder Dienstleistung stärker in den Fokus rücken. Daher können die IT-Grundschutzkataloge vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Common Criteria (CC) eine geeignete Wahl sein.

Der IT-Grundschutz-Standard bezeichnet eine vom BSI standardisierte Methode zum systematischen Beheben von Schwachstellen in einem IT-System. Dabei werden für wesentliche IT-Komponenten vordefinierte Schutzmaßnahmen angegeben. Durch eine sukzessive Angleichung der Vorgehensweise innerhalb des Regelwerkes an die internationale Norm ISO/IEC 27001[24] ist eine Zertifizierung möglich. Der Aufbau zu einem ganzheitlichen Informations-Sicherheits-Management-System (ISMS) wurde im Zuge der Angleichung vom IT-Grundschutz angestrebt und in vier Teile zerlegt, den heutigen IT-Grundschutz-Standard. Dabei kann sich das BSI als unabhängiges Bundesamt präsentieren, welches auch Produktzertifizierungen nach ITSEC (Information Technology Security Evaluation Criteria) und CC in den beispielhaften Bereichen Smartcard, Verschlüsselungssoftware, Server usw. durchführt.

Eine Zertifizierung nach CC kann nur durch eine vom BSI anerkannte Prüfstelle durchgeführt werden, hier kann als ein Beispiel die TÜV Informationstechnik GmbH genannt werden. Generell wird mit einer CC-Zertifizierung nicht bestätigt, ob ein Produkt sicher oder unsicher ist, sondern es wird ausschließlich die Vertrauenswürdigkeit eines IT-Produktes evaluiert. In diesem Fall werden die Anforderungen an das Produkt anhand von sieben verschiedenen Stufen der Vertrauenswürdigkeit definiert. Der Vorteil der Methodik liegt in der Möglichkeit zur internationalen Anerkennung von CC-Zertifizierungen. Das bereitgestellte Wissen wird im Wesentlichen auch durch das BSI angeboten und in Schulungen vermittelt. Der Bedarf an diesem spezifischen Know-how lässt sich aus der Dringlichkeit der durchgeführten Schulungen sowie der dauerhaft erforderlichen Erhöhung der Schulungskapazitäten ableiten. Als Unterstützung präsentiert sich u.a. hier die Telekom als Schulungspartner zur Durchführung von Workshops der CC.

In der heutigen Informationsgesellschaft ist es durchaus eine zentrale Aufgabe der öffentlichen Verwaltung, Anforderungen und Aufgaben zur IT-Sicherheit in den Bereichen Prävention, Reaktion und Nachhaltigkeit zu beantworten[25].

Sollen eine holistische Sicherheitsbetrachtung mit Einbezug branchenspezifischer Normen und Richtlinien sowie Aspekte der IT-Sicherheit Anwendung finden, müssen diese Themen auch miteinander in Bezug gebracht werden. Beide Bereiche sind somit unabdingbar für eine vollumfängliche Betrachtung.

1.3 Problemstellung

Resultierend aus den Regelwerken lässt sich keine geeignete Norm heranziehen, die eine umfängliche Sicherheitsbewertung für mobile Zutrittskontrollsysteme ermöglicht. Grundsätzlich sind die Normungen im mechanischen Bereich sehr ausgeprägt und detailliert. Was hier aber an geeigneter Stelle fehlt, ist der Bereich der IT-Security. Es werden z. B. nicht ausreichend Verschlüsselungen oder eine schlussendliche Organisation des Berechtigungsmanagements abgefragt. Separiert können dies nur die angesprochenen Common Criteria und der BSI-Grundschutzkatalog. Wenn neue Technologien um die Erweiterung einer besonderen Dienstleistung zur Sicherung der gewöhnlichen Geschäftstätigkeit angepasst werden, sollten frühzeitig Richtlinien oder Methoden angewandt werden, die eine solide Überprüfung des Produktes ermöglichen. Am erwähnten Beispiel des Nachschlüsselgeschäftes wird die Dringlichkeit neuer Geschäftsmodelle sichtbar. Doch auch die Sensibilisierung des Kunden in Bezug auf die Vertrauenswürdigkeit der

[24] DIN ISO/IEC 27001, Informationstechnik – IT-Sicherheitsverfahren, 2015.
[25] Vgl. BSI, Workshop Common Criteria 3.1, 2015, Kap. 1.

Sicherheitsprodukte muss gewährleistet sein. Damit die mobilen Zutrittslösungen eine respektable Resonanz und Akzeptanz für ein nachhaltiges Geschäft sichern, müssen die Produkte nachvollziehbare Standards in der Produktqualität erfüllen. Hier fehlt es bisher an einer systematischen Vorgehensweise, und es eröffnet sich eine wissenschaftliche Fragestellung zur Konzeption und Evaluierung eines Prozesses zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen.

1.4 Ziel / Ergebnisse

Ziel der Arbeit ist es, eine Systematik zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen unter Einbezug von geltenden Normen, Richtlinien und Methoden zu entwickeln. Hierbei stellen den Rahmen die etablierten Werke des BSI-Grundschutzkataloges und die der Common Criteria. Für weitere mechanische respektive konstruktive Bereiche werden die begründeten Normen und Richtlinien der EN, der DIN, des VdS und die BSI-TL herangezogen.

Somit kann sichergestellt werden, dass die Bewertung der mechanischen Eigenschaften um diejenigen erweitert wird, die in der jetzigen Form nicht ausreichend betrachtet werden. Ergebnis soll die Entwicklung einer semi-quantitativen Sicherheitsbewertung sein, die durch eine holistische Betrachtungsweise differenzierte Analyseergebnisse zum gegenwärtigen Stand von mobilen Zutrittskontrollsystemen liefern kann. Dabei soll die Sicherheitsbewertung sowohl die Sichtweise des Herstellers als auch die des Kunden gleichermaßen berücksichtigen.

Ausgehend von Kapitel 2 wird der Rahmen zum Status quo der Forschung beschrieben, an dem sich die Sicherheitsbewertung orientiert. Dazu werden insbesondere die Grundlagen der allgemeinen Risikobewertung erläutert, um die Basis zur Differenzierung einer quantitativen und qualitativen Bewertung zu legen. Weitere Unterkapitel orientieren sich an der Risikobewertung mithilfe von Modellen und Methoden, die z. B. in der Identifikation von Risiken in Organisationseinheiten dienen. Aufbauend für spätere Betrachtungen des Lösungsansatzes steht der allgemeine KVP-Prozess für eine originäre Vorgehensweise bei der Erarbeitung der Sicherheitsbewertung von Mobile-Access-Systemen. Um die Evaluierung der Methodik auf betrachtete technologische Komponenten zu konzentrieren, findet die Unified-Modelling-Language hier speziell Anwendung. Begründete Teilelemente oder extrahierte Schritte der angesprochenen Themen finden sich zur weiteren Vorgehensweise in der Zusammenfassung wieder.

Zur Darstellung und Erläuterung der Technologien werden die mechanischen und mechatronischen Schließsysteme in Kapitel 3 differenziert nach prinzipiellen und konstruktiven Merkmalen für unterschiedliche Anwendungen im Bereich der Zugangslösungen beschrieben. Dies erläutert die generellen Funktionsweisen gleicher Systematiken jedoch mit unterschiedlicher Umsetzung in Betrieb, Handhabung und Aufbau. Anschließend können die Beispielsysteme auf Basis der Kommunikation mithilfe von Near-Field-Communication und Bluetooth-Low-Energie im Einsatz mobiler Anwendungen in einen sinnvollen Kontext gebracht und verstanden werden.

In Kapitel 4 wird ausführlich auf die gegenwärtigen Normen, Richtlinien und Methoden eingegangen, die eine Grundlage für die vorliegende Arbeit bilden. Die Eingruppierung in IT-Security und branchenspezifische Normen/Richtlinien stellt den Rahmen für die Grundlage der inhaltlichen Bewertung. Dabei werden sowohl branchenspezifische Normen und Richtlinien wie auch die praktische IT-Security beschrieben.

Das Kapitel 5 enthält sowohl das Konzept der allgemeinen Sicherheitsbewertung als auch die konkrete Vorgehensweise bei der Anwendung der Sicherheitsbewertung auf die zu evaluierenden Systeme. Im Kern beschreibt es einen sogenannten „PDCA-Problemzyklus“, der auf übliche Problem- oder Verbesserungsstrategien aufsetzt. Im Ergebnis bildet es die Konzeption der Sicherheitsarchitektur mit den spezifischen Anforderungen sowohl der Hersteller wie auch der Kunden.

Das Kapitel 6 dient der Beschreibung der Anwendung und Ergebnisdarstellung der Sicherheitsbewertung fiktiver Beispielsysteme. Es illustriert die möglichen Anwendungsfälle und

gibt Aufschluss darüber, ob die neu entwickelte Sicherheitsbewertung auf mobile Zutrittskontrollsysteme anwendbar ist.

Abschließend wird in Kapitel 7 retrospektiv eine Reflektion der durchgeführten Arbeit und der gewonnenen Arbeitsergebnisse dargestellt. Es werden sich anschließende Forschungsfragen, die über den abgegrenzten Forschungsschwerpunkt hinausgehen, skizziert, um potentielles Verbesserungspotenzial aufzuzeigen.

2 Sicherheitsmanagement / Informationssicherheit

Wie der Titel dieser Dissertation schon andeutet, ist der Begriff der Sicherheit ein zentrales Element der Arbeit. Dabei geht es um die maßvolle Anwendung einer Beurteilung zum Thema Sicherheit. Da es sich bei dem Sachverhalt um eine sehr subjektive Einschätzung handelt, was und in welchem Maße sicher oder unsicher ist, die nicht zuletzt auch auf Erfahrungswerten sowie subjektiver persönlicher Einschätzung beruht[26], sollte im Ergebnis eine situativ-gerechte Beurteilung die realistischen Tatsachen widerspiegeln. Es schließt sich die Erkenntnis an, dass keine totale Sicherheit angeboten werden kann respektive keine Technologie zu 100% sicher ist[27].

Um sich dem sehr breiten und komplexen Themenfeld der Sicherheit nähern zu können, finden sich im Englischen drei eindeutige Begriffe, die nach der Übersetzung in die deutsche Sprache nicht mehr klar getrennt werden können, weil sie alle mit „Sicherheit" übersetzt werden. Hauptsächlich sind hier die Begriffe safety und security zu unterscheiden, wobei safety, die Sicherheit von Maschinen (z. B. gegenüber Personen) und security, die Sicherheit in der Informationstechnik beschreibt, wie z. B. den Schutz von persönlichen Daten[28]. Die englische Sprache verwendet des Weiteren den Begriff „certainty", welcher Sicherheit im Sinne der Verlässlichkeit und Vertrauenswürdigkeit bezeichnet[29].

Eine gesellschaftsspezifische Brisanz kann dem Thema generell zugeordnet werden. Aufgrund vielfältiger, aktueller Diskussionen um Zuwanderung oder auch gehackte Autoschlüssel, nimmt mittlerweile die Bevölkerung diese Themen sehr sensibel war. Aufgrund sich häufender Medienpräsenz zu Themen der Digitalisierung kann ein sich wandelnder Bedarf an neuen Technologien festgestellt werden. So reicht es nicht mehr aus, nur den Drang nach der Vernetzung verschiedener Geräte zu befriedigen, sondern auch das Bedürfnis nach Schutz vor unberechtigten Angriffen. Der Forderung nach Hilfestellungen beim „Schutz vor Internetkriminalität beziehungsweise das Thema Mediensicherheit ist bereits seit Jahren Schwerpunkt der Präventionsarbeit […]"[30] verschiedener öffentlicher Einrichtungen. An diesen Bemühungen kann erkannt werden, dass es eine erhöhte Unsicherheit in der Bevölkerung gibt, die nicht genau einzuschätzen weiß, wie vermieden werden kann, dass der Umgang mit neuen Technologien in die unverschuldete Opferrolle führt. Dabei kann sich die gesunkene Computerkriminalität von 2015 um 5,2 %[31] durchaus sehen lassen. Jedoch ist die Gefahr von Angriffen auf digitale Systeme im privaten Bereich ungleich gestiegen. Noch vor ein paar Jahren war die Anzahl der vernetzten Geräte, die im privaten Bereich Anwendung fanden, überschaubar. Doch mit steigender Anwendung von digitalen Produkten und Geräten insbesondere im Bereich Smart Home sind auch die Privathaushalte mittlerweile immer mehr potenziellen Angriffen ausgesetzt. Die Anzahl von Delikten im Bereich der digitalen Systeme ist zwar nicht angestiegen, der tatsächliche potenzielle Schaden kann sehr wohl im Einzelfall beträchtlich hoch sein.

Ein weiteres Beispiel für ein gestiegenes Problembewusstsein sind die sehr kontroversen Diskussionen über den Zusammenhang von Zuwanderung und Kriminalität. So weist die polizeiliche Kriminalstatistik von 2015 genau in diesem Bereich ein Schwerpunktthema aus, allerdings mit dem Hinweis, dass „[…] bei der Opfererfassung keine Angaben zum Aufenthaltsanlass vorgesehen sind […]"[32] und daher auch keine genauen Aussagen über einen direkten Zusammenhang von Zuwanderung und Kriminalität gegeben werden kann. Gegensätzlich zur subjektiven Wahrnehmung kann in einigen Fällen ein Rückgang der Straftatdelikte attestiert werden[33]. Diese Beispiele illustrieren die Differenz der subjektiven Wahrnehmung und der objektiven Beweislasst zum mannigfaltigen Thema der Sicherheit. Es ist im Detail keine selbsterklärende Wirkungskette, die

[26] Vgl. Frevel, Bernhard, Sicherheit, 2016, S. 11.
[27] Vgl. Kersten, Heinrich / Klett, Gerhard, Der IT Security Manager, 2008, S. 5.
[28] Vgl. ebd., S. 55.
[29] Vgl. Frevel, Bernhard, Sicherheit, 2016, S. 4.
[30] Bundesministerium des Innern, Polizeiliche Kriminalstatistik 2015, 2016, S. 14.
[31] Ebd., S. 9.
[32] Ebd., S. 64.
[33] Vgl. Walburg, Christian, Migration und Kriminalität, 2016, S. 29.

einfach abgespult werden kann. Vielmehr müssen alle Aspekte und Standpunkte mit in die Entscheidungsfindung einbezogen werden oder Berücksichtigung finden.

Da sich die folgenden Kapitel mehr mit den Themen der Informationssicherheit auseinandersetzen, kommt dem Begriff der (IT-)Security eine besondere Bedeutung zu.

Das zweite Kapitel beinhaltet in der eigenen Durchführung der Arbeit alle relevanten Themenbereiche, die in Bezug auf die Sicherheitsbewertung eine entscheidende Rolle gespielt haben. Sie stellen somit die Fundamente für die weitere Arbeit dar, aus denen im weiteren Verlauf zu verschiedenen Arbeitsschritten unterschiedliche Ergebnisse erarbeitet werden sollen oder als Vorbetrachtung wesentliche Erkenntnisse liefern. Um die Sicherheitsbewertung an mobilen Zutrittssystemen aufzustellen, entscheidet für die strukturierte Vorgehensweise ein methodischer Rahmen. Hier kann auf die allgemeinen Erfahrungen im Bereich der Risikobewertung eines IT-Managementsystems zurückgegriffen werden. Genaue Definitionen und Anforderungen für eine Risikobetrachtung geben den richtigen Kontext zum Verständnis der Dringlichkeit. Bestehende Modelle und Methoden der Risikoanalysen fokussieren weiterführend Bestandteile im speziellen Anforderungsfeld der mobilen Zutrittssysteme. Für den adäquaten Rahmen der Durchführung sind einzelne Arbeitsschritte erforderlich, die im Rahmen des KVP-Prozesses eine Strukturverbesserung findet. Bei der Bearbeitung von komplexen Ökosystemen mit unterschiedlichen Technologien müssen bei der Überführung in ein konkretes Schema Teilsysteme extrahiert und Systemgrenzen besser festgelegt werden. Hier wurde in der Umsetzung die Unified Modeling Language (UML) als Hilfestellung benutzt. Erst in diesem Rahmen ist es möglich, wesentliche Anforderungen an ein schlüssiges Sicherheitskonzept zu bestimmen.

2.1 Definition Risiko

Um eine genaue Definition des Risikos zu verstehen, eignet sich als verständliches Mittel das Beschreiben der einzelnen Risikofaktoren, indem „Das Risiko abhängig vom Schadensausmaß und der Wahrscheinlichkeit des Schadenseintritts“[34] ist. Diese gängige Definition hat sich aufgrund bestimmter Umweltereignisse als ein mächtiges Instrument im Prozess des Risikomanagements etabliert. In vielen Bereichen ist es heute üblich, eine Schadensabwehr in einen Managementprozess zu integrieren. Dabei findet diese Definition sich in vielen technischen und organisatorischen Prozessen wieder. So ist beispielsweise die Finanzbranche verpflichtet, nach den Basel-II Anforderungen besondere Risiken in ihren eigenen organisatorischen Abläufen zu berücksichtigen[35]. Für technische Prozesse wie z. B. das Entwickeln von Maschinen gilt das für Deutschland verbindliche Produktsicherheitsgesetz (ProdSG) in der 9. Verordnung, dessen gesetzlicher Rahmen die Durchführung einer Risikobeurteilung vorsieht[36]. Somit ist die strategische Einbindung des Risikomanagements zu einer Selbstverständlichkeit geworden, was sich in der Praxis allerdings nicht immer so einfach darstellt. Gemeinsam haben alle Ansätze, dass frühzeitig Risiken gemindert werden sollen, um Schäden auf ein zuvor aufgestelltes Sicherheitsziel zu begrenzen[37], was auch die Aussage der Nichterreichbarkeit der 100%igen Sicherheit unterstützt[38].

Abbildung 1 verdeutlicht nachfolgend die allgemeinen Bemühungen zur Risikominimierung:

[34] DIN 820-12, Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen, 2014, S. 13.
[35] Vgl. Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, 2008, S. 1.
[36] Vgl. Mössner, Thomas, Risikobeurteilung im Maschinenbau, 2012, S. 7 f.
[37] Vgl. Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, 2008, S. 4.
[38] Vgl. Frevel, Bernhard, Sicherheit, 2016, S. 11.

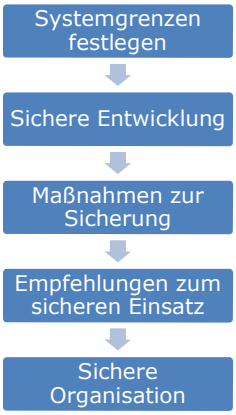


Abbildung 1: Allgemeine Risikominimierung[39]

Aus der Darstellung heraus lassen sich die einzelnen Elemente zur Risikominimierung als iterativer Prozess verstehen, um der Komplexität innerhalb eines Systems gerecht zu werden. Bewusst wird dies durch die Verbindung verschiedener Disziplinen, die in einem System integriert sind[40]. Besonders die neuen Technologien beflügeln eine Verschmelzung bekannter und unbekannter Disziplinen miteinander.

So werden derartige Systeme schnell vielschichtig und verwoben, da sie nicht mehr nur auf eine Disziplin beschränkt sind, um gewünschte Funktionsweisen interaktiv auszuführen. „Es geht also um funktionelle Koppelungen von Systemteilen, die nicht auf die Eigenschaft der einzelnen Elemente selbst rückführbar sind.“[41] Dabei sind Safety-Aspekte in Form von konstruktiven Bedingungen zu berücksichtigen, die zum Beispiel in der DIN 820-12 als „Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen“ Hilfestellung leisten soll[42]. Wird die Unterscheidung in Bezug der Security-Aspekte getroffen, geht es um das Risiko in der Informationssicherheit. Konkret beschreibt es die Angreifbarkeit eines Assets, d. h. Vermögensgegenstände einer Organisation zu gefährden oder zu kompromittieren[43]. In der Ausführung und zur Wahrung der Unternehmensziele wird ein sogenanntes Informations-Sicherheits-Management-System eingesetzt[44]. Mit dessen Hilfe können die IT-Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit gewahrt werden[45]. Das IT- Managementsystem zeugt längst vom hohen Einfluss der Software im alltäglichen Leben[46]. Hier werden persönliche Daten, Verkaufsinformationen, Finanzwerte etc. für den zwingenden geschäftlichen Betrieb analysiert, gespeichert und verarbeitet. Dies sichert in einigen Fällen die Existenz der Geschäftsmodelle.

Für eine erfolgreiche Implementierung in ein ISMS sollte der Top-Down-Ansatz als adäquates Mittel Anwendung finden. Dies bestätigt ein kontrolliertes Herunterbrechen von Zielen für ein effizientes und effektives Vorgehen.

Abbildung 2 verdeutlicht diesen Ansatz nochmals.

[39] Modifiziert nach: DIN EN ISO 12100, Sicherheit von Maschinen, 2011, S. 17.
[40] Vgl. Schließmann, Christoph, Das Konzept Interdependency, 2014, S. 25.
[41] Ebd., S. 27 f.
[42] DIN 820-12, Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen, 2014, S. 10.
[43] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 45.
[44] Kersten, Heinrich / Klett, Gerhard / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 5.
[45] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 17.
[46] Vgl. Ebert, Christof, Risikomanagement kompakt, 2013, S. 1.

Abbildung 2: Top-Down-Ansatz[47]

Für eine sinnvolle Zielformulierung können sich ganz unterschiedliche Kriterien eignen. Bei einer eher allgemeingültigen Aufstellung sollten Ziele immer „SMART" formuliert sein, wobei jeder Buchstabe für ein Muss-Kriterium steht: spezifisch, messbar, anforderungsgerecht, realistisch und terminiert[48]. Orientiert an den genannten Bedingungen besteht so Eindeutigkeit im Hinblick auf deren tatsächliche Erfüllung. Generell ist darauf zu achten, dass alle Personen die aufgestellten Ziele selbst erarbeiten und deren Sinnhaftigkeit verstehen. Gelten entsprechende Ziele oder Zielvorgaben immer für weitreichende Unternehmensteile oder gar für das gesamte Unternehmen, sollte die Geschäftsführung die Kommunikation initiieren und diese Top-Down weitergeben. Da es sich hier im Speziellen um den informationstechnischen Bereich handelt, sind die Ziele an den oben genannten allgemeinen IT-Sicherheitszielen auszurichten: Verfügbarkeit, Integrität und Vertraulichkeit[49]. In der mittleren Schicht, dem operativen Vorgehen bzw. der gewählten Methodik, findet eine Umsetzung der Vorgaben respektive der Ziele in die operative Praxis statt. Hier finden sich die Begrifflichkeiten der Risikobeurteilung und Risikobehandlung wieder[50]. Zusammengefasst kann vereinfacht von einer Risikoanalyse ausgegangen werden, die z. B. in der Ausführung einer FMEA (Fehler-Möglichkeits-Einfluss-Analyse) verbreitet Anwendung findet[51]. Vorteile der FMEA-Methode sind die angesprochene Risikobehandlung und Risikobeurteilung aufgrund der quantitativen Erfassung über teilweise auch subjektive Einschätzungen. Insgesamt umfasst die Risikoanalyse drei Möglichkeiten der Analyse von Risiken[52]:

- Qualitativ: Hier gilt es, eine effiziente Aufnahme von Risiken zu gewährleisten, die sich im einfachsten Fall in die Kategorien „Gering" und „Hoch" aufteilt. Aufgrund des schnellen Vorgehens wird hier meistens auf eine genaue Analyse verzichtet und subjektive Bewertungen bilden die referenzierten Einschätzungen.

- Quantitativ: Mit messbaren Größen kann hier eine genaue Datengrundlage zur Bewertung geschaffen werden. Eine exakte und klare Metrik sowie präzise Messgrößen eliminieren den schwammigen Interpretationsspielraum und ermöglichen auch Dritten die Nachvollziehbarkeit.

- Semi-quantitativ: Hier werden eigens angelegte Messgrößen zur Bewertung ermittelt. Es erfolgt also z. B. eine Festlegung quantitativer Messgrößen, die qualitativ ermittelt wurden. Häufig erfolgt eine Kombination der ersten beiden aufgezählten Grundtypen.

In der Praxis erfreuen sich die qualitativen Möglichkeiten großer Beliebtheit, da es eine Vielzahl an Methoden für deren Einsatz gibt[53]. Außerdem können sich Anwender auch ohne umfangreiche Erfahrung Themengebieten strukturiert nähern. Welche Analysemöglichkeit schlussendlich

[47] Modifiziert nach: Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, 2008, S. 11.
[48] Vgl. Hruschka, Peter, Requirements Engineering, In: Tiemeyer, Ernst, IT-Projektmanagement, 2014, S. 440.
[49] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 17.
[50] Vgl. Kersten, Heinrich / Klett, Gerhard / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 5.
[51] Vgl. Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, 2008, S. 41 f.
[52] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 34.
[53] Vgl. Lichte, Daniel, Ein analytischer Ansatz zur szenarioübergreifenden Modellierung der Verwundbarkeit von Infrastrukturen, 2015, S. 12.

Anwendung findet, ist im Einzelfall zu entscheiden und sollte individuell abgewogen werden. Können hieraus nun Maßnahmen oder konkrete Arbeitspakete ermittelt werden, stellen diese die Basis für operative Tätigkeiten zur Risikominimierung dar.

Die vereinfachten Wirkzusammenhänge des Risikomanagement in einem ISMS stellt Abbildung 3 dar.

Abbildung 3: Risikomanagement (vereinfacht)[54]

2.2 Modelle und Methoden der Risikoanalyse

Wie im Eingangskapitel verdeutlicht nimmt die Wichtigkeit von Unternehmensprozessen und deren Inhalten zu. Durch eine konsequente Kundenorientierung der Geschäftsprozesse können ohne Probleme gesamte Wertschöpfungsketten digitalisiert werden. Was im Umkehrschluss eine exorbitante Zunahme an Informationen impliziert, die Geschäftsgrundlage und Risiko zugleich darstellen![55] Dieser Sachverhalt deckt sich mit der subjektiven Wahrnehmung aufgrund vermehrter Cyberattacken und Spionageangriffen in den letzten Jahren[56]. Auf diesen negativen Trend haben die Firmen reagiert. So planten 2016 40% der Unternehmen, einen Teil des Budgets im Bereich der Informations- und Telekommunikationstechnik für IT-Security auszugeben[57]. Gleichwohl ist das Interesse der Unternehmen an diesem Thema mit 92% deutlich höher und liegt noch vor den Belangen All-IP[58], Kundenzufriedenheit und Verfügbarkeit mit jeweils 90%[59]. Jedoch existieren die Bemühungen meist nur rein theoretisch und können von den nötigen Fachabteilungen nur mäßig umgesetzt werden[60]. Mit oberster Priorität hat besonders die Aufrechterhaltung der gewöhnlichen Geschäftstätigkeit Vorrang, was in vielen Abteilungen dazu führt, dass IT-Security nicht prioritäres Thema ist. Hinzu kommt insbesondere bei produzierenden Unternehmen eine notorische Ressourcenknappheit, da die Geschäftsergebnisse nicht von der EDV-Abteilung generiert werden und daher der Fokus auf der Verfügbarkeit sowie dem Ausbau der Infrastruktur liegt. Müssen im Ernstfall aber die IT-Sicherheitseinrichtungen greifen, bleibt nur die Hoffnung, präventiv genügend finanzielle und personelle Ressourcen dafür bereitgestellt zu haben.

Wie bei allen Strategien, so auch hier in der IT-Security, sollte es ein Top-Down-Prinzip geben, das von der Geschäftsführung ausgeht und die Nachhaltigkeit und Glaubwürdigkeit erheblich stärkt. Diese Kaskadierung sollte von der organisatorischen Ebene bis auf die technische Ebene heruntergebrochen werden.

Zur Verdeutlichung der Abwehrebenen dient die nachfolgende Abbildung 4.

[54] Modifiziert nach: Klipper, Sebastian, Information Security Risk Management, 2015, S. 61.
[55] Vgl. Peltier, Thomas R., Facilitated Risk Analysis Process (FRAP), 2000, S. 1 f.
[56] Vgl. Pudar, Srdjan/ Manimaram, Govindarasu / Liu, Chen-Ching, PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, In: Computers & Security, 2009, S. 754.
[57] euromicron AG, Im Bereich welcher ITK-Trendthemen planen Sie im Jahr 2016 Investitionen zu tätigen?, In: Statista, 2017.
[58] Unter All-IP wird die komplette Umstellung von verschiedenen Kommunikationsprotokollen, wie z. B. von Telefon, Fernseher etc. auf das Internetprotokoll (IP) verstanden.
[59] euromicron AG, Anteil von deutschen Unternehmen, die sich für folgende ITK-Trendthemen interessieren, In: Statista, 2017.
[60] Vgl. Ebert, Christof, Risikomanagement kompakt, 2013, S. 36 f.

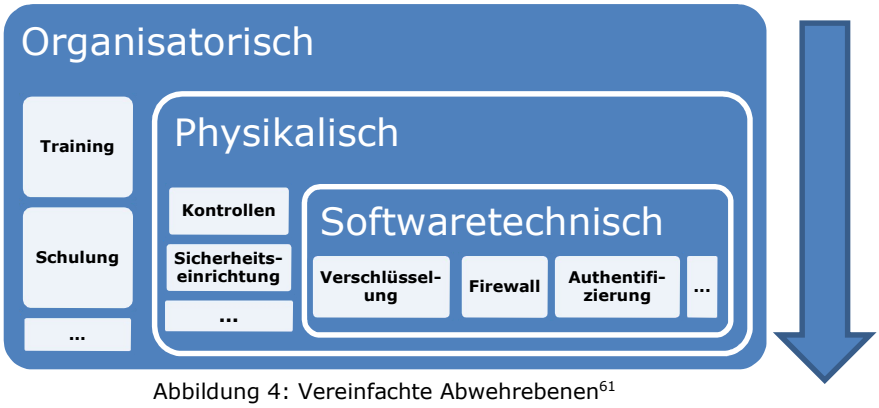


Abbildung 4: Vereinfachte Abwehrebenen[61]

Bei der Betrachtung der Abbildung wird schnell deutlich, dass eine holistische Betrachtung der Disziplinen angezeigt ist und eine punktuelle Vorbereitung nicht sinnvoll erscheint. Verglichen mit einer privaten Vorsorge würde die einfache Installation einer Firewall und der Antiviren-Software nicht ausreichen, um das Unternehmen gegen Angriffe von außen zu schützen[62]. Auch die physikalische Absicherung kann sehr vielfältig in der Umsetzung sein; dies geht von Sicherheitseinrichtungen für Serverräume für das Stammpersonal bis hin zu speziellen Kontrollen für eingesetzte Freelancer. Die organisatorischen Belange initiieren den Top-Down-Prozess und schaffen den nötigen Akzeptanzrahmen, indem Schulungen und Trainings angeboten werden.

Für die Identifikation des bestehenden Risikos ist eine maßvolle Ziel-Mittel-Relation ratsam. Dafür sollten die Begrifflichkeiten, in Bezug auf einen Angriff in Folge eines bestehenden Risikos näher betrachtet werden.

Die Abbildung 5 gibt einen Überblick zu den bestehenden Abhängigkeiten.

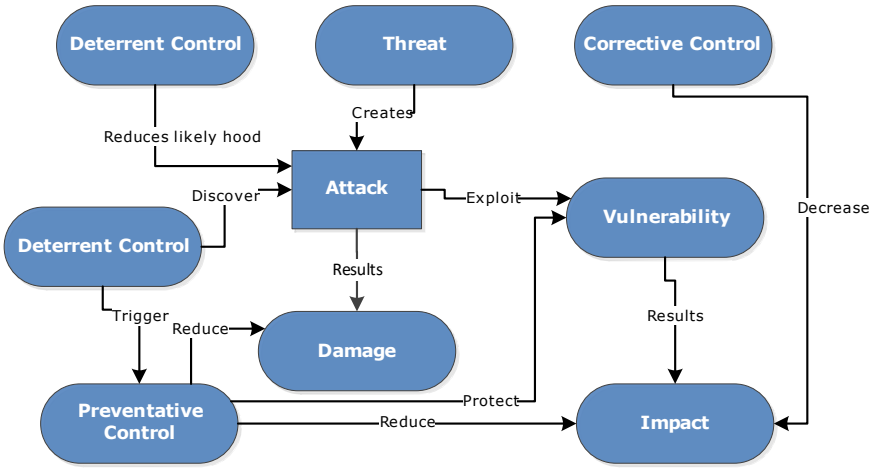


Abbildung 5: Abhängigkeiten Schwachstelle, Bedrohung und Angriff[63]

Ersichtlich wird hier eine gegenseitige Abhängigkeit und Beeinflussung von Ereignissen. So sind die Einwirkungen durch einen Angriff sehr unterschiedlich und lassen sich nicht auf einzelne Abwehrmaßnahmen reduzieren. Für die quantitative Bemessung der Schadenshöhe im Falle eines Angriffes können präventive Einrichtungen einen übermäßigen Schaden im Vorfeld eindämmen. Sinn der präventiven Maßnahmen ist es natürlich nicht nur, den Schaden zu begrenzen, sondern auch einen möglichst schnellen Schutz nach dem Angriff wieder herzustellen[64]. Möglich wird dieses

[61] Modifiziert nach: Pyka, Marek / Januszkiewicz, Paulina, The Octave methology as a risk analysis tool for business resources, In: Proceedings of the International Multiconference on Computer Science and Technology, 2006, S. 486.
[62] Vgl. ebd., S. 485.
[63] Modifiziert nach: Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, 2012, S. 80.
[64] Vgl. Frevel, Bernhard, Sicherheit, 2016, S. 29.

aber in jedem Falle erst durch die dezidierte Analyse des Modus Operandi, der einen Angriff mit Schadensauswirkung zulässt. Das gesammelte Wissen kann nicht nur zum Verständnis der Vorgehensweise genutzt werden, sondern auch für die frühzeitige Identifizierung und das gelenkte Schadensausmaß. Besonders letzteres wird in der Technik eingesetzt, um beispielsweise Cyberangriffe frühzeitig zu detektieren und intelligente Abwehrmaßnahmen einzuleiten. Damit eine adäquate Handlung auf ein Ereignis folgen kann, spielt die Risikoabschätzung eine entscheidende Rolle. Hierbei lassen sich die in nachfolgenden Kapiteln angeführten Varianten der qualitativen, quantitativen und semi-quantitativen Risikoanalysen unterscheiden.

2.2.1 Qualitative Risikoanalysen

Da sich die qualitative Risikoanalyse an subjektiven Messgrößen orientiert, lässt sich für nahezu jedes beliebige System eine eigene Metrik zur Risikobestimmung aufstellen. Hier kann eine leichte und schnelle Abschätzung des Risikos getroffen werden, ohne präzise Angaben aus dem zu bewertenden System zu kennen oder ermitteln zu können[65]. Gerne werden für einen schnellen Überblick komplexer Systeme „[…]simple Ja-Nein-Entscheidungen[…]"[66] eingefordert, um sich dann detaillierter den neuralgischen Punkten nähern zu können. Da es sich aber häufig um die Abbildung von Zwischenstadien handelt, die mit Unsicherheiten behaftet sind, eignet sich die Anwendung einer Farbskala im Ampelprinzip, d. h. die obere rote Skala mit hohem Risiko und die untere grüne Skala mit einem geringen Risiko[67]. Der Vorteil liegt hier auch in der leichten Visualisierbarkeit. In diesem Zusammenhang wird in der Technik gerne von dem ALARP-Prinzip (As Low As Reasonably Practicable) gesprochen, das einen gelben Bereich beschreibt, der ein optimales Verhältnis zwischen Aufwand und Nutzen von eingeleiteten Maßnahmen zur Risikoreduzierung erläutert[68].

Die Abbildung 6 verdeutlicht nochmal den optimalen Bereich im Sinne der Farbskala.

Abbildung 6: ALARP-Prinzip[69]

Um die Präzision der qualitativen Risikoanalyse zu heben, kommt den Grenzbetrachtungen eine wichtige Bedeutung zu. Da sich aber die Ergebnisse vielfach auf die Erfahrung und die analytischen Fähigkeiten von Personen stützt, sollte eine genaue Auswahl des Personenkreises erfolgen, der die Beurteilung durchführt. Schlussendlich kommt es auf die Fähigkeiten jeder einzelnen Person an, da der Rahmen zur Beurteilung per se noch keine selbständige Entscheidung herbeiführen kann. Aufgrund steigender Komplexitäten und Abhängigkeiten gibt es eine steigende Anzahl von systemimmanenten nicht zu beurteilenden Unsicherheiten, die eine sinnvolle Bewertung fast unmöglich erscheinen lassen. Abhilfe können hier in erster Linie die regulatorischen Vorgaben im Unternehmen schaffen, die z. B. die Organisation der IT-Landschaft regeln. Zweck des Vorgehens ist die Standardisierung, um die „unkontrollierte" Vielfältigkeit von Systemen einer handhabbaren Systematik zu unterwerfen. Je nachdem, wie stringent die Vorgaben gestaltet sind, ist ein Ausschluss bestimmter Systeme möglich, da sie sich nicht in ein generelles Schema einordnen lassen. Genau hier können die qualitativen Risikoanalysen ansetzen, wenn die vorher angesprochenen Rahmenbedingungen zur Organisation der Bestimmung von Risiken eingehalten werden. Die vorteilige Umsetzbarkeit kann allerdings nur in der Erstmaligkeit attestiert werden, da

[65] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 72 f.
[66] Klipper, Sebastian, Information Security Risk Management, 2015, S. 34.
[67] Vgl. Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, 2008, S. 32.
[68] Vgl. Health and Safety Executive, Reducing risks, protecting people, 2001, S. 43.
[69] Modifiziert nach: Preiss, Reinhard, Methoden der Risikoanalyse in der Technik, 2009, S. 74.

bei wiederholten Analysen z. B. die Reproduzierbarkeit nicht garantiert werden kann. Somit liegt der kritische Punkt in der Auswahl der Methodik jedoch nicht in der angesprochenen Durchführung.

Für die generelle Abgrenzung der qualitativen Risikoanalysen beruhen die subjektiven Einschätzungen häufig auf der Kombination der folgenden drei Faktoren: der Verwundbarkeit (vulnerability) in Folge einer akuten Bedrohung (threat) und der entgegneten Kontrolle (control) für eine mögliche Abwehr oder Eindämmung[70]. Diese Merkmale liefern im Rahmen einer qualitativen Risikoanalyse wesentliche Ansätze zur Identifizierung von Schwachstellen oder zeigen Verbesserungspotenziale auf.

Eine Verteilung zur Anwendungshäufigkeit der wichtigsten qualitativen Risikomethoden für Informationssicherheitsanalysen zeigt die nachfolgende Abbildung 7.

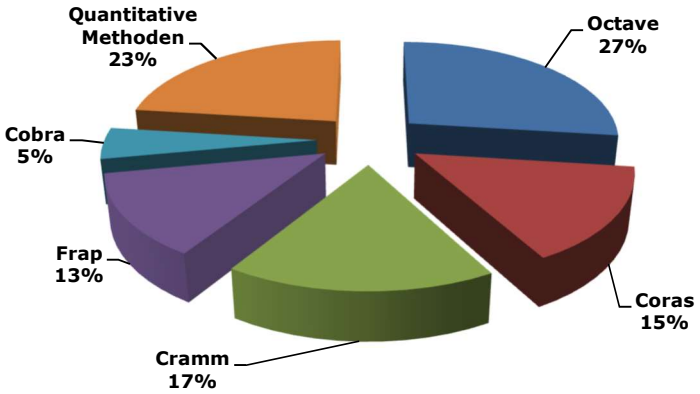


Abbildung 7: Qualitative Risikomethoden[71]

Für eine weitere Unterscheidung innerhalb der qualitativen Risikoanalysen lassen sich, je nach Perspektive, eine Reihe von Separierungen vornehmen. Damit ein Überblick zu den wesentlichen Methoden in Technik und Organisation gegeben werden kann, dienen die folgenden Unterkapitel.

Eine Essenz der Vor- und Nachteile von qualitativen Risikoanalysen ist nachfolgend in Tabelle 1 aufgelistet.

Vorteile	Nachteile
- Leichter Analysetypus - Schneller Überblick von Risikoquellen - Effiziente Beurteilung komplexer Systeme	- Keine Wahrscheinlichkeiten von Auswirkungen in Folge von Risiken darstellbar - Keine monetären Ergebnisse - Ergebnisse nicht exakt

Tabelle 1: Vor- und Nachteile der qualitativen Risikoanalyse (vereinfacht)[72]

2.2.1.1 Auswahl qualitativer Risikoanalysen in der Technik

Eine artverwandte Methode zur bekannten FMEA (Fehler-Möglichkeits-Einflussanalyse) ist die **HAZOP** (HAZard and OPerability analysis). Hier werden auf der Basis von HAZOP-Workshops Störungen und Ausfälle auf ein System ermittelt und anhand verschiedener Kriterien beschrieben. Im Fokus steht dabei immer das gesamte System und nicht nur einzelne Teilsysteme wie bei der Durchführung der FMEA. In der Durchführung wird mit Synonymen gearbeitet, die eine

[70] Vgl. Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, 2012, S. 80 f.
[71] Modifiziert nach: ebd., S. 83.
[72] Vgl. Lee, Ming-Chang, Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, In: International Journal of Computer Science & Information Technology (IJCSIT), 2014, S. 30.

entsprechende Gleichbedeutung haben; so kann in klassischer Weise eine Ergebnistabelle mit den beschreibenden Kriterien wie z. B. Störung, Effekt und Abstellmaßnahme erarbeitet werden.[73]

Für mannigfaltige Anwendungsszenarien eignet sich die **Fehlerbaumanalyse FTA** (Fault Tree Analysis). Hierbei kann ein Hauptereignis aufgeführt werden, von dem sich verschiedene Kausalitäten ableiten lassen, die in Folge z. B. einen unerwünschten Zustand bewirken. Dabei gleicht die visuelle Darstellung einem „Baum", der von oben nach unten wächst.[74]

Über eine entsprechende Notation lassen sich die Zustände weiter präzisieren und detaillieren. In der Erweiterung der Methode können Wahrscheinlichkeiten der abgeleiteten Zustände quantitativ erfasst werden, deshalb kann diese den semi-quantitativen Analysen zugeordnet werden - je nach Ausprägung und Detaillierungsgrad.

Eine kreative Methode zur Identifizierung von Störungen ist die **What-If-Analyse.** Sie eruiert mithilfe eines Brainstorming-Ansatzes Auswirkungen auf ein Ereignis. Entscheidend ist auch hier die Expertise des Teilnehmerkreises, da sich nur brauchbare Ergebnisse einstellen, wenn der Ablauf des zu untersuchendenden Objektes fachlich bekannt ist. Das Ergebnis stellt eine Tabelle mit der aufgelisteten Wirkungskette von Ausgangszustand, mögliche Störungen, Auswirkungen und Maßnahmen dar.[75]

Alle beschriebenen Methoden sind in Umfang und Aufwand schnell zu verwirklichen. Grundsätzlich empfiehlt sich aber bei qualitativen Risikoanalysen eine formale Struktur und visuell eindringliche Charakteristiken. Nur so kann eine strukturierte Vorgehensweise mit entsprechender Ergebnisdarstellung sichergestellt werden.

2.2.1.2 Auswahl qualitativer Risikoanalysen in der Organisation

Wie in Abbildung 7 veranschaulicht, kristallisiert sich für die organisatorische Risikoanalyse die Methode **Octave** mit 27%-Anteil als die meist verwendete heraus. Aufgrund ihrer relativ einfachen und selbstorganisierenden Umsetzung ist sie für Unternehmen ein guter Ansatz, um deren IT-Geschäftsprozesse zu analysieren. Vorteil hierbei ist die Selbstbestimmung im Vorgehen innerhalb eines gegebenen Rahmens; diese trägt dazu bei, erste Erfahrungen im Umgang mit Risikomanagement im Unternehmen aufzubauen. Gleichzeitig kann sich so ein interner Kreis von Experten etablieren, der den regelmäßigen Zyklus der IT-Richtlinien stetig ausbauen und pflegen kann. Charakterisiert ist das Vorgehensmodell durch das Aufstellen der kritischen Vermögenswerte, dem Identifizieren der Schwachstellen in den Geschäftsprozessen und dem Entwickeln der Sicherheitsstrategie. Innerhalb der drei Phasen, in denen die Octave-Risikoanalyse durchzuführen ist, werden explizite Aufgabenpakete mit definierten Ergebniserwartungen beschrieben. Gerade für die jüngste Digitalisierungswelle ist sie ein adäquates Mittel, um die Informationsdichte im Unternehmen auf allen Ebenen eigenständig zu evaluieren.[76]

Das **CRAMM**-Model orientiert sich, ähnlich dem Octave-Modell, an den drei Stufen der Identifizierung der Vermögenswerte: resultierende Bedrohungen und Schwachstellen, sowie den Gegenmaßnahmen. Zusätzlich findet eine Priorisierung und Ordnung der Ergebnisse innerhalb der Methode statt, so dass konkrete Handlungsweisen kondensiert werden können. Weiterhin gilt natürlich das gleiche Prozedere für ein abgeleitetes Notfallmanagement, was auch Bestandteil der Analyse sein kann. Trotz der expliziten Entwicklung in den 1980er Jahren zur Prüfung von IT-Systemen könnte es durch mehrere Revisionsstände aktuell gehalten werden.[77] Bei der

[73] Vgl. Preiss, Reinhard, Methoden der Risikoanalyse in der Technik, 2009, S. 52 ff.
[74] Vgl. Edler, Frank / Soden, Michael / Hankammer, René, Fehlerbaumanalyse in Theorie und Praxis, 2015, S. 17 ff.
[75] Vgl. Preiss, Reinhard, Methoden der Risikoanalyse in der Technik, 2009, S. 166 f.
[76] Vgl. Pyka, Marek / Januszkiewicz, Paulina, The Octave methology as a risk analysis tool for business resources, In: Proceedings of the International Multiconference on Computer Science and Technology, 2006, S. 487 ff.
[77] Vgl. Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, 2012, S. 84.

Durchführung ist auf ein hohes fachliches Know-how der Evaluierungspersonen zu achten. So kann im Bedarf ein etwas höheres Abstraktionsniveau erzielt werden.[78]

Das modellbasierte Risikomanagementsystem **CORAS** basiert auf der Kombination der Risikoanalyse, der objektorientierten Modellierung und der computergestützten Verfahren. Dabei identifiziert die Einbindung der Unified Modeling Language (UML) den Prozess, welche Objekte oder Personen welche Informationen generieren oder mit ihnen im Zusammenhang stehen. Hierbei kann die Abhängigkeit bestimmter Verfahren definiert werden, was im Umkehrschluss alle kritischen Prozesse zur weiteren Risikoanalyse bereitstellt. Die einzelnen Analyseschritte sind in der Grundidee den weiteren qualitativen Analysen sehr ähnlich. Sie teilen sich in fünf Einzelaspekte auf: Identifizieren von Zusammenhängen, Formulieren von Risiken, Risikoanalyse, Risikoevaluierung und Risikobehandlung/-umsetzung.[79]

2.2.2 Quantitative Risikoanalysen

Für eine genaue Bemessung der Risikoanalyse mit Zahlenwerten müssen quantitative Methoden eingesetzt werden. Sie können aufgrund ihrer Struktur den genauen Risikowert ausweisen und eignen sich immer dann, wenn die Anwendungsszenarien die Ermittlung von Zahlenwerten zulassen. Einhergehende Unsicherheiten in der Datenbasis sind von vornherein zu berücksichtigen. So kann dieses Risiko mit in die Risikoanalyse integriert und entsprechend bewertet werden[80]. Der Prozess der quantitativen Risikoanalyse baut im einfachsten Fall auf der simplen Multiplizierung der Eintrittswahrscheinlichkeiten und der Auswirkung eines unerwünschten Ereignisses auf[81]. Je nach betrachtetem System ist dies nicht so leicht zu ermitteln. Im Unterschied zur qualitativen Analyse ist die Festlegung auf einen bestimmten Wert innerhalb einer Datenbasis nicht immer exakt und häufig müssen bestimmte Grenzwerte festgelegt werden, die in Kausalität stehen sollten. Demnach ist die Durchführung dieser Methode nicht in allen Fachdisziplinen gleich beliebt. Nach Ebert ist es in der Finanzwelt üblich, auch Unschärfen in einem System zu bewerten, gleichwohl sich die Naturwissenschaften schwer mit der exakten Quantifizierung unter Unsicherheiten tun[82].

Das Prozedere zur Risikoanalyse ist in vier Phasen in Abbildung 8 aufgezeigt:

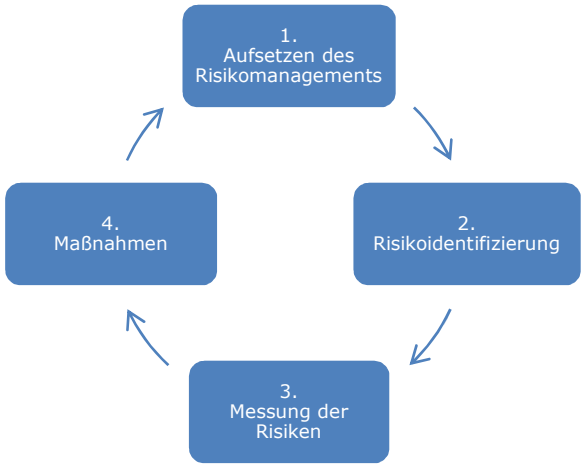


Abbildung 8: Prozess der Risikoanalyse (im Finanzwesen)[83]

Ersichtlich ist die simultane Vorgehensweise, die auch schon in vorherigen Kapiteln der allgemeinen oder speziellen Risikobestimmung erkennbar ist. Dem mathematischen Teil zur Berechnung des

[78] Vgl. Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, 2012, S. 88.
[79] Vgl. Fredriksen, Rune / Kristiansen, Monica / Gran, Bjørn Axel / Stølen, Ketil / Opperud, Tom Arthur / Dimitrakos, Theo, The CORAS Framework for a Model-Based Risk Management Process, In: Anderson S. et al. (Eds.), Safecomp 2002, 2002, S. 94 ff.
[80] Vgl. Klipper, Sebastian, Information Security Risk Management, 2015, S. 34.
[81] Vgl. Pudar, Srdjan/ Manimaram, Govindarasu / Liu, Chen-Ching, PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, In: Computers & Security, 2009, S. 756.
[82] Vgl. Ebert, Christof, Risikomanagement kompakt, 2013, S. 55.
[83] Vgl. Cottin, Claudia / Döhler, Sebastian, Risikoanalyse, 2013, S. 21.

Risikos aus der Eintrittswahrscheinlichkeit und deren Auswirkung in Folge eines unerwünschten Ereignisses kommt in Phase 3 *„Messung der Risiken"* eine besondere Bedeutung zu. Hier sind die zwei genannten Faktoren für das Produkt „Risiko" entscheidend. Die Eintrittswahrscheinlichkeit beschreibt innerhalb eines definierten Zeitintervalls das Eintreten eines unerwünschten Ereignisses. Eine darauf erzeugte Reaktion innerhalb eines Systems oder Teilsystems beschreibt die Auswirkung. In diesem Fall wird auch von dem Schadensausmaß gesprochen, da es sich um ein unerwünschtes Ereignis handelt. Der dabei auftretende Schaden kann also monetär bewertet bzw. abgeschätzt werden. Wird für ein geeignetes System vom Aspekt der Sicherheit gesprochen, können hier die ersten Unsicherheiten plastisch sichtbar gemacht werden. Wie wahrscheinlich ist es, dass ein Airbag nicht auslöst oder welcher Schaden ist in einem Fall eines defekten Airbags zu beziffern? Auch die Nachvollziehbarkeit ist unter den entsprechenden und vor allem änderbaren Umständen nur schwer definierbar und kann häufig nicht auf andere Systeme approximiert werden, gleichwohl die reine Berechnung bei gleichem Ereigniszustand reproduzierbar ist. Bei weiterer Betrachtung detailliert sich die Quantifizierung des Risikos nach Ebert, wie folgt[84]:

$$Risiko\ [R] = Auswirkung[A] x\ Wahrscheinlichkeit\ [W] \qquad (1)$$

$$Wahrscheinlichkeit\ [W] = Eintritt\ [WE]\ x\ Kontrollierbarkeit\ [WK]\ x\ Integrität\ [WI] \qquad (2)$$

Hierbei teilt sich die Wahrscheinlichkeit in drei Faktoren auf, was im Zweifel eine genauere Aussage zulässt. Zur Erklärung beschreibt die Wahrscheinlichkeit den Eintritt eines ungewünschten Ereignisses wie gehabt. Neue Faktoren sind die Kontrollierbarkeit, die den genauen Zustand des unerwünschten Ereignisses beschreibt, und die Integrität, welche Gegenmaßnahmen zur Eindämmung des unerwünschten Ereignisses definiert.

Die qualitative Risikoanalyse ist mit der subjektiven Einschätzung durch Experten beschrieben. Entscheidend bei der quantitativen Vorgehensweise ist aber die Bestimmung der einzelnen Faktoren, was wiederum auf die Befragung von Experten zurückführen ist. Somit bestätigt es die Tatsache der unmittelbaren Herkunft und absoluten Vertrauenswürdigkeit der Datengrundlage zur Berechnung des Risikos. Ohne diese zwingende Vorgabe kann die sichere Berechnung des Risikos nicht gewährleistet werden.

Zusammenfassend sind die Vor- und Nachteile nochmal in der folgenden Tabelle 2 aufgelistet:

Vorteile	Nachteile
- Exaktere Risikobestimmung - Erfassung und Auswertung über einen längeren Zeitraum, bzw. Trendbeobachtung, Analyse etc. - Gute Reproduzierbarkeit - Gute Akzeptanz der Ergebnisse	- Berechnung beruht auf zwingend-exakter Datenbasis - Im Detail sehr komplex - Fachwissen erforderlich - Exakte Ergebnisse können die Realität nicht immer korrekt abbilden

Tabelle 2: Vor- und Nachteile der quantitativen Risikoanalyse (vereinfacht)[85]

In vielen Fällen kann allerdings eine so scharfe Trennung wie in Tabelle 2 gezeigt nicht vorgenommen werden. Oftmals vermischen sich die harten Grenzen innerhalb dieser Klassifikation; quantitative und semi-quantitative Risikoanalyse. Wobei speziell bei der semi-quantitativen Risikoanalyse (Grenze zwischen quantitativ und qualitativ) einer qualitativen Basis fiktive Zahlenwerte zugeordnet werden. Zur besseren Übersicht sind hier die semi-quantitativen Ansätze im Kapitel der quantitativen Risikoanalysen beschrieben. Prinzipiell dient es nur zur groben Orientierung, um eine bedarfsgerechte Klassifikation auszuwählen. Generell eignen sich verschiedene Ansätze nur bei vorheriger sorgfältiger (individueller) Prüfung, um optimale Arbeitsergebnisse erzielen zu können[86].

[84] Vgl. Ebert, Christof, Risikomanagement kompakt, 2013, S. 10.
[85] Vgl. Hasso Plattner Institut, Studie zur Messbarkeit von Sicherheiten in SOA, 2010, S. 39.
[86] Vgl. Campbell, Philip L. / Stamp, Jason E., A Classification Scheme for Risk Assessment Methods, 2004, S. 25.

2.2.2.1 Auswahl quantitativer Risikoanalysen in der Technik

Die Auswahl von quantitativen Risikoanalysen beruht auf der Bildung von Wahrscheinlichkeiten, die je nach Anwendungsfall und Detaillierung gleichermaßen auch zu den semi-quantitativen Risikoanalysen gezählt werden können.

Nach eigener Ansicht handelt es sich bei der klassischen (und vielseitigen) **Fehler-Möglichkeits-Einfluss-Analyse** (FMEA, engl. Failure Mode and Effects Analysis) um eine semi-quantitative Risikobestimmung, da auch nach DIN EN 60812 beide Möglichkeiten der qualitativen oder quantitativen Bestimmung der Kritizität erwähnt werden[87]. In der Produktneuentwicklung von Qualitätsleitlinien ist die FMEA eine akzeptierte Methode zur strukturierten Verbesserung der Produktqualität. Dabei werden bei einer Konstruktions-FMEA systematisch mögliche Fehlerquellen identifiziert. Zur effektiven Vorgehensweise eignet sich die Durchführung im Team mit einem Moderator, um ein möglichst breites Fehlerspektrum einzufangen. Als Hilfestellung zur Dokumentation gibt es vielfältige frei verfügbare Varianten an Vordrucken und Arbeitsdokumenten, die es dem Team angenehmer machen, einen strukturierten Nachweis zum Ablauf anzufertigen. Jegliche Sammlungen von Fehlern und Störungen werden anfänglich ohne eine Quantifizierung durchgeführt. Elemente wie Durchführung im Team oder Ideensammlung zu Fehlern sind schon aus den Bereichen der qualitativen Risikoanalyse bekannt. In einem weiteren Schritt sind die eruierten Fehler respektive Störungen hinsichtlich der Wahrscheinlichkeiten von Ursache, Bedeutung und Entdeckung zu bewerten. Bewährt hat sich dabei in der Praxis eine entsprechende Einordnung der nummerischen Skala von 1 bis 10. Im Anschluss kann durch einfache Multiplikation eine Risikoprioritätszahl (RPZ) berechnet werden. Im Ergebnis werden die einzelnen Fehler mithilfe der Bewertung priorisiert dargestellt.[88] Direkte Vergleiche über die Zahlenwerte innerhalb der priorisierten Fehler sind dabei nicht möglich. Somit können auch die einzelnen Fehler nicht zu einem Gesamtrisiko summiert werden. In jedem Fall sollten aber die Ergebnisse sehr vorsichtig und nur mit fachlichem Hintergrund interpretiert werden, da sich durch die Vorgehensweise sowie die schlussendlich vermeintliche Genauigkeit der Ergebnisse, eindeutige Schwächen der FMEA offenbaren[89,90].

Bei der **Layer of Protection-Analyse** (LOPA) handelt es sich um eine etwas aufwändigere Risikoanalyse für die Anlagensicherheit, die auf Ergebnissen vorangegangener Analysen in Anbetracht von verschiedenen Szenarien, basiert. Strukturell baut sie auf einem Schichtenmodell auf, das verschiedene Barrieren symbolisiert, die einen Schadenseintritt verhindern können. Abhängig von den einzelnen Szenarien werden die jeweiligen Auswirkungen eines begrenzten oder massiven Ausfalls anhand eines Ablaufschemas modelliert. Das quantifizierbare Risiko wird mit Bezug zu einem tolerierbaren Wert eingeordnet und spiegelt eine Einordnung innerhalb des Restrisikos wider. Vorteile dieser Methode sind die entsprechende Nachvollziehbarkeit der Risikobewertung von Einzelszenarien sowie die konkrete Abbildung und Beschreibung von Schutzebenen.[91]

In Ergänzung zu den qualitativen Möglichkeiten einer Risikobewertung in der Technik kann die Methode der **Fehlerbäume** quantifiziert werden. Somit ergibt sich, wie schon erwähnt, eine Wahrscheinlichkeitsbewertung von abgeleiteten Fehlern. Praxistaugliche Berechnungen von festen Wahrscheinlichkeiten zur Analyse von Verfügbarkeiten eines Systems lassen sich dabei besonders hervorheben.[92]

[87] Vgl. DIN EN 60812, Analysetechniken für die Funktionsfähigkeit von Systemen, 2006, S. 18.
[88] Vgl. Blohm, Hans / Beer, Thomas / Seidenberg, Ulrich / Silber, Herwig, Produktionswirtschaft, 2008, S. 230 ff.
[89] Vgl. Bowles, John B., An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis, In: Proceedings Annual Reliability and Maintainability Symposium, 2003, S. 385 f.
[90] Vgl. DIN EN 60812, Analysetechniken für die Funktionsfähigkeit von Systemen, 2006, S. 31.
[91] Vgl. Reinhard, Preiss, Methoden der Risikoanalyse in der Technik, 2009, S. 148 ff.
[92] Vgl. Edler, Frank / Soden, Michael / Hankammer, René, Fehlerbaumanalyse in Theorie und Praxis, 2015, S. 32 ff.

2.2.2.2 Auswahl quantitativer Risikoanalysen in der Organisation

Wie in der Abbildung 7 aufgezeigt repräsentieren nur etwa 23% der bekannten Methoden den Part der quantitativen Risikoanalysen in der Organisation. Dies ist ein Indiz für die meist erschwerte Anwendbarkeit in der Praxis und auch fehlender Expertise, diesen Methodentypus qualifiziert anzugehen. Auch hier kann in Form von Unschärfe die Einordnung zu semi-quantifizierbaren Analysen sinnvoll erscheinen.

Am häufigsten unter den (semi-)quantitativen Risikoanalysen wird die **ISRAM**-Methode benutzt, da sie eine relativ leicht zu verstehende Vorgehensweise offeriert, die nicht von komplizierten mathematischen Formeln geprägt ist. Dabei wurde bei der Entwicklung Wert auf die Nähe zum operativen Geschäft von Unternehmen gelegt, so dass eine schnelle Akzeptanz auch bei Führungskräften oder Managern erreicht werden kann. Basierend auf der allgemeinen Risikodefinition, die auf der Multiplikation von Eintrittswahrscheinlichkeiten und der Folge von Sicherheitsverletzungen beruht, werden in der Durchführung zwei unabhängige Umfrageteile erhoben. Das Analyseergebnis wird über eine relative Risikoskala festgelegt, die eine Einordnung in nummerischen Stufen zulässt. Innerhalb der Abfolge der Methode gibt es sieben Stufen zur Risikoanalyse, die jeweils für die Wahrscheinlichkeit und Folge der Sicherheitsverletzungen getrennt modelliert werden. Vorteilhaft ist ein anpassungsfähiger Verlauf der Analyse, um problemorientiert ein abgestimmtes Ergebnis zu erhalten. Im Detail bedeutet das, dass alle Durchführungshilfen wie Tabellen oder Skalen individuell angepasst werden können, ohne die Struktur zu verfälschen. Aufgrund der generalistischen Vorgehensweise und Adaptierbarkeit lassen sich besonders organisatorische Sicherheitslücken damit bearbeiten und analysieren. Aber auch komplexe IT-Infrastrukturprobleme sind mögliche Anwendungsfelder.[93]

Als weitere Möglichkeit kann der **CORA**-Ansatz für eine quantitative Berechnung von Verlusten in Folge von Bedrohungen und deren Häufigkeit verwendet werden. Als Grundlage werden die Datensammlungen bekannter Definitionen bemüht, wie Schwachstellen und folgende Angriffsmöglichkeiten auf schützenswerte Objekte. In einem zweistufigen Vorgehen sind die Auswirkungen in quantitativer Darstellung berechenbar. Dies erfolgt über die Ermittlung von einzelnen Verlusten von Angriffsmöglichkeiten mit der Multiplikation von Häufigkeiten in Auswirkung der Eintrittsverluste.[94] Dieses setzt eine genaue Erhebung der gesamten Verlustmöglichkeiten auf schützenswerte bzw. kritische Objekte voraus. Auch hier ist die Datenerhebung in einem definierten Rahmen mithilfe einer Expertengruppe anzuraten.

Aufgrund der geringen Verbreitung spielt die **IS Risk Analysis Based on a Business Model** eine eher untergeordnete Rolle und sei hier nur der Vollständigkeit halber benannt. In diesem Modell werden einige Schwachstellen aus den üblichen Ansätzen zur Risikoanalyse verbessert. Berücksichtigt wird nicht nur der reine kritische Unternehmenswert sondern auch der Wert für die operative Geschäftstüchtigkeit des Unternehmens. Dies bedeutet einen konkreten Mehrwert für die Auswahl an Informationen (kritischer Prozesse) in den Unternehmen zum Fortgang der Geschäftstüchtigkeit. Das Ergebnis wird monetär beziffert und aufgrund komplexerer mathematischer Berechnungen ermittelt.[95]

2.3 Kontinuierlicher-Verbesserungs-Prozess (KVP)

Seitdem sich Unternehmen immer mehr dem nationalen aber auch internationalen Wettbewerb ausgeliefert sehen, wurde sukzessive die sogenannte Lean-Philosophie implementiert, um die eigene Leistungsfähigkeit zu steigern. Anfänglich stand nur die Produktion im Fokus jeglicher Effizienzsteigerung, was im Detail die plakative Devise: „Mehr Output bei weniger Personaleinsatz", bedeutete. Im ganzheitlichen Lean-Ansatz geht es allerdings um die Verkürzung der Gesamtdurchlaufzeit von Rampe zu Rampe, d. h. vom Auftragseingang bis hin zum Versand der

[93] Vgl. Karabacak, Bilge / Sogukpinar, Ibrahim, ISRAM: information security risk analysis method, In: Computers & Security, 2004, S. 1 ff.
[94] Vgl. Vorster, Anita / Labuschagne, Les, A Framework for Comparing Different Information Security Risk Analysis, In: Proceedings of SAICSIT 2005, 2005, S. 97.
[95] Vgl. Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, 2012, S. 85.

Ware. Dies impliziert auch Administration und Supportprozesse. Hierbei stellt der kontinuierliche Verbesserungsprozess eine fundamentale Strategie innerhalb der Lean-Philosophie dar. Sie hilft dabei, den Wettbewerbsvorteil stetig auszubauen und grundlegende Denkweisen im Unternehmen zu verankern. Heutzutage finden sich weitreichende Triebfedern zur Verbesserung mithilfe des KVPs.

Eine diesbezügliche Übersicht unterschiedlicher Motivationen gibt die Abbildung 9 wieder.

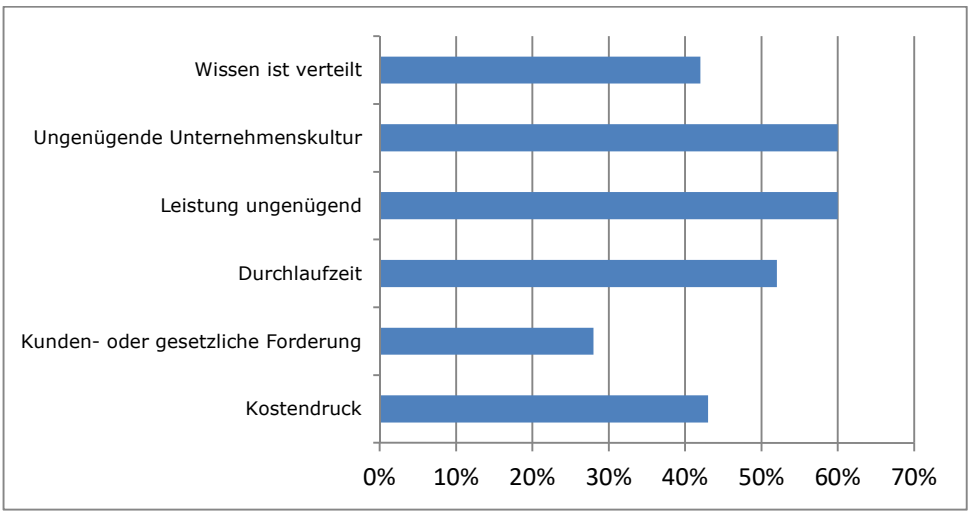


Abbildung 9: Triebfeder für den Einsatz von KVP[96]

Wichtigstes Kernelement des KVP's ist die Identifizierung und Beseitigung von Verschwendungen, die einen Prozess unnötig behindern bzw. die nicht wertschöpfend im Sinne des Kunden sind. Mit diesem Ansatz findet keine Leistungsverdichtung im Sinne der Wertschöpfung statt sondern eine Reduzierung respektive Eliminierung von nicht-wertsteigernden Tätigkeiten. Demnach gibt es eine ganze Reihe von anwendungsorientierten Methoden. Aus diesem KVP-Fundus existiert der eher generalistische Ansatz des PDCA-Zyklus, der einen strategischen Mehrwert für Aufgaben aufgrund der logischen Verknüpfung von Erfahrung, vernetztem Denken und Schlussfolgerungen generiert[97]. Die wiederkehrende Abfolge der einzelnen Plan-Do-Check-Act Schritte hilft, das vorliegende Problem strukturiert und systematisch abzuarbeiten. Den Zusammenhang von KVP und PDCA beschreibt die Abbildung 10.

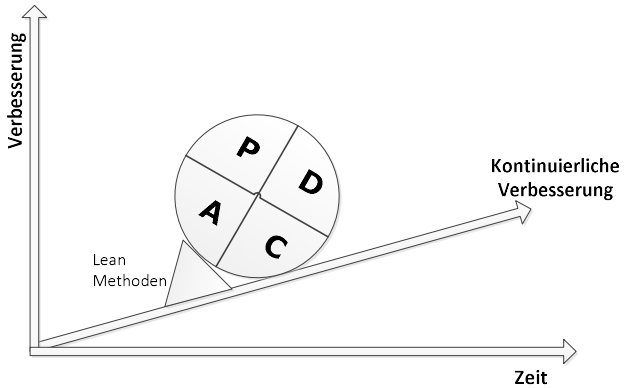


Abbildung 10: Kontinuierlicher Verbesserungsprozess[98]

[96] Modifiziert nach: Deutsche Gesellschaft für Qualität, KVP-Der Kontinuierliche Verbesserungsprozess, 2014, S. 7.
[97] Vgl. Bronner, Albert, Handbuch der Rationalisierung, 2003, S. 213.
[98] Modifiziert nach: Gastl, René, Kontinuierliche Verbesserung von Umweltmanagementsystem und Umweltleistung, 2005, S. 14.

Im Kontext der einzelnen Arbeitsschritte des PDCA-Zyklus beschreibt jeder Einzelschritt eine Aktivität zur Bearbeitung eines Problems. Dabei kann in einigen Fällen auch der Zyklus durch nur einen einmaligen Durchlauf gekennzeichnet sein. Nachfolgend die vier Schritte in der Übersicht und Formulierung[99]:

1. **Plan:**
    a. Formulierungen der genauen Problembeschreibung anhand verschiedener Kennzahlen, um einen IST-Zustand zu beschreiben. Als Orientierung hat sich die Ermittlung verschiedener Kennzahlen in Bezug auf den Sachverhalt als vorteilhaft erwiesen.

    b. Genaue Vorstellung vom Zielzustand entwickeln und beschreiben. Als Maßgabe eines realistischen Zieles müssen zwingend Minimum-Vorgaben an Zeit und Zustand getroffen werden.

2. **Do:**
    Definition und Umsetzung geplanter Aktivitäten. Die Ergebnisse sind zu dokumentieren und in einer adäquaten Art und Weise für weitere Zwecke aufzubereiten.

3. **Check:**
    Interpretation der Ergebnisse aus den durchgeführten Maßnahmen und Überprüfung, ob die festgelegten Parameter auch eine Zielerreichung ermöglichen. Bei aufbauenden Maßnahmen sind die Teilergebnisse ebenfalls auf Kausalität und Richtigkeit zu prüfen.

4. **Act:**
    Abgleich Ist-Zustand mit aufgestelltem Plan-Vorhaben. Sollten sich Differenzen eingestellt haben, die ein erneutes Durchlaufen der einzelnen Schritte nötig machen, kann hier eine erneute Einleitung des Zyklus erfolgen. Dies bedeutet konkret eine detailliertere Abstimmung der Zieldefinition, damit sukzessiv eine Annäherung erfolgen kann. Hat sich der gewünschte Zielzustand eingestellt, sollten Maßnahmen zur Standardisierung getroffen werden.

    Sollte sich nach einiger Zeit der Zustand wieder verschlechtern, kann durch Aufrechterhaltung der PDCA-Schritte ein immerwährender Verbesserungszyklus etablieren.

Die Initiierung von Optimierungs- oder Verbesserungsprozessen sollte immer von der obersten Ebene eingeleitet und auch forciert werden. Erst durch Vermittlung der nötigen Dringlichkeit und durch die Präsenz von Führungskräften entsteht bei allen Beteiligten eine gewisse Verbindlichkeit. Oftmals erfahren wichtige strategische Projekte schon in der Definitionsphase starken Widerstand und werden nicht realisiert. Problematisch sind dabei die langfristigen Auswirkungen, weil sich daraus entstehende Konsequenzen erst viel später manifestieren. Für eine potenzielle Projektdurchführung bedeutet dies, die Implizierung von möglichen Verhaltensveränderungen bei Projektmitarbeitern: Sie werden sich bei allen zukünftigen Projekten an einer gewissen Unverbindlichkeit der Zielvereinbarung orientieren. Doch gerade in der Lean-Philosophie wird jeder einzelne Mitarbeiter in die eigenständige Verantwortung genommen. Erst mit immer wiederkehrenden Schulungen und durch das Antrainieren von Verhaltensmustern kann ein Paradigmenwechsel in der Belegschaft realisiert werden.

Methoden der Lean-Philosophie erlauben eine individuelle Anwendbarkeit in verschiedensten Bereichen, die aus einer flexiblen Vorgehensweise und der Nutzung eines weitreichenden

[99] Vgl. Koch, Susanne, Einführung in das Management von Geschäftsprozessen, 2015, S. 119.

Methodenpools resultieren[100]. Durch die nachweislich guten Erfolge der Lean-Philosophie profitieren mittlerweile auch andere Bereiche von der Denkweise. Auch ein stark informationslastiges Themenfeld, wie die kontinuierliche Analyse der IT-Sicherheit im Unternehmen, eignet sich für die Anwendung des PDCA-Kreislaufes, beispielsweise für die Implementierung eines Informations-Sicherheits-Management-Systems[101]. Gerade kritische und weitreichende Problemstellungen, die mit der Einrichtung eines interdisziplinär arbeitenden Teams einhergehen, erfordern auf der einen Seite ein gutes Projektmanagement sowie fundiertes Fachwissen, zum anderen aber auch eine gute Methodenkompetenz für die logische Abarbeitung innerhalb der Aufgabenstellungen; wie eben am Beispiel von PDCA.

2.4 Unified-Modeling-Language (UML)

Für die Durchführung von Softwareprojekten hat sich für verschiedene Entwicklungsphasen die Unified-Modeling-Language (UML) etabliert. Hier können eine Vielzahl von Entwicklungsergebnissen dokumentiert und strukturiert bearbeitet werden. Dabei wird auf eine einheitliche Notation und Vorgangsweise geachtet. Die UML-Systematik ist somit standardisiert respektive formalisiert gemäß geltender Konventionen.[102]

Für diese sogenannte Modellierungssprache wurde 1990 der erste Grundstein in einer Vorläuferversion gelegt. Die erste offizielle Version, im heutigen Verständnis von UML, wurde 1997 von der Object Management Group (OMG) veröffentlicht[103]. Über die nachfolgenden Jahre sind weitere Versionen entwickelt und erprobt worden, sodass ein mächtiges Instrument mit vielen Eigenschaften zur Abbildung von modellbasierter Softwareentwicklung entstanden ist. Bei der Realisierung werden grundsätzlich zwei Vorgehensweisen unterschieden[104]:

1. Ein durchgängiges Modell, welches modellbasiert nur Änderungen oder Entwicklungen erlaubt, die kausal zum Gesamtmodell sind, d. h. jede Ergänzung im Modell wird auf Plausibilität zu ggf. darin enthaltenen Systemteilen überprüft.
2. Ein begrenztes Modell, welches dokumentenorientiert nur begrenzt die Plausibilität auf das beschriebene Modell oder dessen Systemteil erlaubt, d. h. das Gesamtmodell kann Verständnislücken aufweisen, die aufgrund fehlender Durchgängigkeit entstehen.

Vorteilhaft bei dieser Modellierungssprache ist die sinnhafte Überführung der rein natürlichen Wahrnehmung eines technischen Systemteiles in die softwaremäßige Abbildung respektive Realisierung über ein Werkzeug. Somit sind direkte Schnittstellen dafür verantwortlich, schon während eines frühen Stadiums des Produktentwicklungsprozesses die Gedanken programmtechnisch korrekt abzubilden und zu modellieren, um eine korrekte Programmierung (z. B. Java) anschließen zu können, ohne verschiedene Entwicklungsprozesse parallel zu forcieren[105]. Die einschlägige Literatur hält ein relativ großes Repertoire an Vorgehensweisen für die Durchführung in Theorie und Praxis von UML bereit. Es kann als Hilfsmittel für einen Modellierungsprozess Ansätze liefern, um z. B. Dienstleistungen, Geschäftsprozesse, Entwicklungen etc. transparent und verständlich darzustellen. Weitere Werkzeuge, die schon im Bereich KVP beschrieben wurden, ordnet UML in einen strukturierten Entwicklungsprozess ein, der u. a. die klassischen Werkzeuge eines Lasten- und Pflichtenheftes fordert. Der Einsatz von UML erfordert die Berücksichtigung etlicher Randparameter, die in einem hohen Maß individuell sind. Kern der UML-Systematik sind die UML-Diagramme, die es aufgrund des breiten Angebotes erlauben, eine Vielzahl von abbildbaren Eigenschaften zu dokumentieren und zu visualisieren. Hierbei folgen die eingeordneten Diagrammtypen in zwei Schemata den Grundsätzen der Darstellung der anwendbaren Funktionen und der eigentlichen technischen Umsetzung[106].

[100] Vgl. Bronner, Albert, Handbuch der Rationalisierung, 2003, S. 103.
[101] Vgl. Kersten, Heinrich / Klett, Gerhard, Der IT Security Manager, 2008, S. 8.
[102] Vgl. Kleuker, Stephan, Grundkurs Software-Engineering mit UML, 2013, S. 3 f.
[103] Vgl. Czuchra, Waldemar, UML in logistischen Prozessen, 2010, S. 21.
[104] Vgl. Rumpe, Bernhard, Modellierung mit UML, 2011, S. 9 f.
[105] Vgl. Czuchra, Waldemar,UML in logistischen Prozessen, 2010, S. 23.
[106] Vgl. ebd., S. 25.

Beispielhaft sind im Folgenden ein paar wichtige UML-Diagramme aufgelistet[107]:

- **Use Case-Diagramme** (Anwendungsfalldiagramme) dienen zur Abbildung der eigentlichen und einzelnen Anwendungsfunktionen und nehmen die Sicht des Benutzers ein. Vorteil ist hier der schnelle Überblick über grundlegende Funktionen, die durch den Benutzer ausgeführt werden können. Meistens stellt ein solches Diagramm einen der ersten Schritte in der weiteren Anwendung von UML dar und ist auch für dritte (evtl. Auftraggeber) leicht lesbar.

- **Aktivitätsdiagramme** stellen die Aktivitäten und innere Abfolge von Funktionen in einer Software dar. Somit werden die Anwendungen aus dem Use Case-Diagramm hier im inneren der Programmierung weiter aufgelöst.

- **Klassendiagramme** stellen die Beziehungen von Klassen und damit den Kern der objektorientierten Programmierung dar. Denn aus Klassen lassen sich Objekte ableiten, die somit eine genaue Beschreibung dessen enthalten, wofür eine Klasse verantwortlich ist.

- **Sequenzdiagramme** ergänzen die Klassendiagramme um die Beziehungen von Objekten. Die Aktivitäten jedes einzelnen Objektes und zwischen einzelnen Objekten liefern genaue Aktionen zur Ausführung der Funktionsumfänge.

Ziel der Diagramme war und ist die Separierung der unterschiedlichen Visualisierungen aufgrund der kausalen Zusammenhänge in der Durchführung von UML und der programmtechnischen Umsetzung[108].

Durch diese systematische Trennung ergeben sich weitere Anwendungsfelder. So kann die UML-Spezifikation auch speziell für die Integration von Security-Aspekten genutzt werden[109]. Wenige Publikationen versuchen sich an der Entwicklung von entsprechenden Modellierungen in UML für eine sichere Software-Entwicklung. Konkret um die Notation erweiterte UML-Spezifikationen sind die SecureUML und die UMLsec. Dabei stehen diese nicht in direkter Konkurrenz zueinander, sondern ergänzen sich in den verschiedenen Aspekten (oder Diagrammtypen) der sicheren Softwareentwicklung. Wobei SecureUML mehr die Modellierung über die statischen Klassendiagramme nutzt und UMLsec stärker die dynamischen Aktivitätsdiagramme zur Lösungsidentifikation heranzieht[110].

Die Forschungsfelder für eine sicherheitsorientierte Softwareentwicklung mittels UML sind unter der weiteren Zunahme an Komplexität in Softwarestrukturen in der Praxis noch relativ unbekannt. Sie sollten aber in Anbetracht der Dringlichkeit weiter erforscht und ausgebaut werden.

[107] Vgl. Kleuker, Stephan, Grundkurs Software-Engineering mit UML, 2013, S. 383 f.
[108] Vgl. Rumpe, Bernhard, Modellierung mit UML, 2011, S. 6.
[109] Vgl. Mouheb, Djedjiga / Debbabi, Mourad / Pourzandi, Makan / u. a., Aspect-Oriented Security Hardening of UML Design Models, 2015, S. 215 f.
[110] Vgl. Matulevičius, Raimundas / Dumas, Marlon, A Comparison of SecureUML and UMLsec for Role-based Access Control, Abrufbar im Internet, http://courses.cs.ut.ee/2010/is/uploads/Main/RBAC-for-UML.pdf, 2010, S. 13.

3 Technologie Schließsysteme

Die historische Betrachtung von Schließsystemen führt sehr schnell in die Schlüsselregion Velbert / Heiligenhaus. Hier findet sich seit Jahrhunderten eine konzentrierte Ansammlung verschiedener Hersteller im Bereich Schloss und Beschlag sowohl für den immobilen wie auch den mobilen Anwendungsfall. Aufgrund verschiedener geografischer, historischer und gesellschaftstypischer Entwicklungen konnte die Region ein Alleinstellungsmerkmal in Deutschland etablieren. Viele bekannte Schloss und Beschlaghersteller produzieren in dieser Region ihre Produkte aus dem Bereich der Sicherheitstechnik. Namhafte Vertreter sind z. B. BKS, CES, Wilka, Witte etc.

Die Entwicklung der Sicherheitstechnik war historisch betrachtet auch stets ein Abbild der herrschenden Lebensumstände. So reichte die Sicherung von Häusern und Siedlungen von einem gänzlichen Verzicht auf jegliche Sicherheitsmaßnahmen (da es nicht üblich war, das eigene Leben zu sichern) bis hin zur rein autoritären Versiegelung mit Knoten und Seilen.[111] Jedoch gilt das 19. Jahrhundert mit dem Beginn der Industrialisierung als das Jahrhundert mit den entscheidenden technologischen Entwicklungen, die sich auch noch heute in den Funktionalitäten der Schließzylinder widerspiegeln[112].

In Deutschland ist die gängige Form des mechanischen Schließzylinders der Profilzylinder in Tropfenform, siehe Abbildung 11.

Abbildung 11: Profilzylinder[113]

3.1 Mechanische Schließsysteme

3.1.1 Funktion

Für die in der Region Velbert / Heiligenhaus verortete Schloss- und Beschlagindustrie stellt die Herstellung und der Vertrieb konventionellen (mechanischen) Schließzylinder immer noch das Kerngeschäft dar. Es besteht allerdings das sich zunehmende manifestierende Risiko, dass die digitale Transformation zunehmend eine Herausforderung für konventionelle Sicherungssysteme darstellt.
Unabhängig von den verschiedenen Abwandlungen und Auslegungen eines mechanischen Schließzylinders verfügen diese eine gleichgeartete Funktionsweise. Dabei sitzen im Inneren des Gehäuses gefederte Stifte, die hintereinander in einer Reihe stehen. Durch die Trennung innerhalb der Stiftreihe in Kern- und Gehäusestifte kann mit dem passenden eingeschnittenen Schlüssel der Kern rotatorisch die Schließnase freigeben und das Schloss zur Entriegelung betätigen. Für die produktionstechnische Umsetzung in der Automation ist die Stiftreihe durchnummeriert. Mit dem Einführen des Schlüssels in den Schließkanal (Kern) werden die Stifte entgegen der Federkraft in das Gehäuse gedrückt. Sind nun die Trennungen der Kern- und Gehäusestifte genau an der Trennebene zwischen Kern und Gehäuse angebracht, ist der Formschluss aufgehoben und der Schließzylinder entsperrt. Die formschlüssige Verbindung des Kerns zur Schließnase ermöglicht nun eine Betätigung des Schlosses, was wiederum den Riegel respektive die Falle zurückzieht. In Folge ist die Tür entsperrt und kann geöffnet werden. In umgekehrter Reihenfolge werden mit dem Herausziehen des Schlüssels die Stifte wieder in den Kern gedrückt und hindern mit einem Formschluss die Rotation des Kernes im Gehäuse. Zum leichteren Verständnis ist in der Abbildung 12 ein nummeriertes Schnittmodell dargestellt.

[111] Vgl. Morgenroth, Ulrich, Sternstunden der Schlossgeschichte, 2008, S. 12 ff.
[112] Vgl. Morgenroth, Ulrich, Vierhundert Jahre und mehr…, 2002, S. 23 ff.
[113] Bildersammlung C.Ed. Schulte GmbH Zylinderschlossfabrik, Mechanische Konstruktion, 2017.

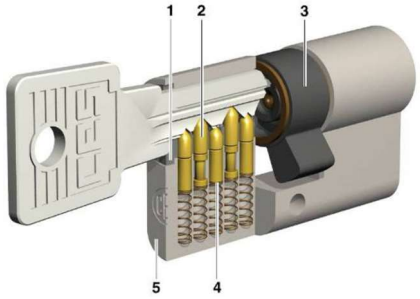


Abbildung 12: Schnittmodell 5-stiftiger Profilzylinder[114]

(1. Kern, 2. Kernstifte, 3. Schließnase, 4. Gehäusestift, 5. Gehäuse)

Die Unterschiedlichkeiten der Einschnitte vom Schlüssel, den Längen der Stifte und dem Profil (Schlüssel und Eingang Schließkanal) erlauben die verschiedenartigsten Permutationen, die eine Überschneidung von z. B. einem Schlüssel in eine nicht zugehörige Schließanlage verhindern sollen. Zur Umsetzung weiterer Permutationen kommen zusätzliche Sperrmerkmale wie z. B. Bohrungen im Schlüssel zum Einsatz. Handelt es sich um eine Schließanlage mit gewünschter Schließhierarchie, so werden durch das Hinzufügen von kleinen Plättchen in die Trennebene von Kern- und Gehäusestift weitere Trennebenen realisiert.

Als weitere Gruppe der Profilvarianten hat sich zusätzlich zum konventionellen Schließprofil das Wendeschlüsselprinzip durchgesetzt, welches dem Anwender erlaubt, den Schlüssel in zwei Positionen (180° gedreht) in den Kern einzuführen. Dabei wird nicht über die Einschnitte der Schlüssel die Permutationen erzeugt, sondern über die Bohrungen im Schlüssel. Als Materialen kommen Messing (Kupfer und Zink) bei den Profilzylindern und Neusilber (Kupfer, Nickel und Zink) bei den Schlüsseln in den meisten Fällen zum Einsatz. Unabhängig von den geltenden Normen können die Profilzylinder so konstruiert werden, dass es Unbefugten erschwert wird, einen Schlüssel für eine Schließanlage nachzumachen. Im Wesentlichen sind dieses der technische Kopierschutz und der markenrechtliche Schutz. Der technische Kopierschutz beinhaltet eine möglichst komplexe Schlüsselgeometrie, so dass mit handelsüblichen Maschinen keine Nachschlüssel reproduziert werden können, wie z. B. der Hinterschnitt von CES[115] und bewegliche Elemente im Schlüssel von DOM[116]. Beim markenrechtlichen Schutz kann z. B. die CES-Bildmarke[117] in der Profilkontur des Schlüssels geschützt werden. Was natürlich im Zweifel den Einbrecher nicht davon abhält, über den Schließzylinder seinen Einbruchversuch zu unternehmen. Gängige Methoden sind hierbei das Picking, das Aufbohren des Profilzylinders, das Kernziehen oder das Herausbrechen des Profilzylinders. Abgeleitet davon werden folglich konstruktive Gegenmaßnahmen zum Schutz entwickelt. In der Tabelle 3 sind nochmal die Vor- und Nachteile exemplarisch zusammengefasst.

Vorteile	Nachteile
- Gewohnte Bedienung - Leichte Installation - Kaum Wartung - Kostengünstig	- Schlüsselverlust - Nachträgliche Anpassung der Schließhierarchie - Erweiterungen

Tabelle 3: Vor- und Nachteile mechanischer Schließanlagen[118]

[114] Bildersammlung C.Ed. Schulte GmbH Zylinderschlossfabrik, Mechanische Konstruktion, 2017.
[115] Schutzrecht, DE 10 2010 017 166 B4, C.Ed. Schulte Gesellschaft mit beschränkter Haftung Zylinderschlossfabrik, 07.03.2013.
[116] Schutzrecht, DE 10 2015 111 914 A1, DOM-Sicherheitstechnik GmbH & Co. KG, 28.07.2016.
[117] Schutzrecht, 398 35 630, C. Ed. Schulte GmbH Zylinderschloßfabrik, 03.09.1998.
[118] Eigene Darstellung.

3.1.2 Anwendung

In den letzten Jahrzehnten wurden die mechanischen Schließprodukte äußerst vielfältig variiert, welche unterschiedlichsten Anforderungen gerecht werden können. Dabei kann fast alles gesichert werden, was irgendwie verschlossen werden kann. Angefangen von der einfachen ordinären Haustür über Anwendungen in der Industrie sowie im Möbelbereich bis hin zur einzelnen Sonderlösungen von Schalteinrichtungen, die über einen Schlüssel betätigt werden sollen. Marktbegleitet hat jeder Hersteller seinen eigenen Weg gefunden, der Partner für das Massengeschäft zu sein und spezielle Lösungen für Kunden entwickelt, so dass schlussendlich viele hundert Einzelprodukte hervorgebracht wurden. Der Eindruck, es handele sich bei der Schloss- und Beschlagindustrie um schlicht konfektionierte Sicherheitstechnik, wird schnell bei der Sondierung des Marktes widerlegt. Da es sich um ein Produkt handelt, was täglich in Benutzung ist, wird leicht das hohe Maß an Know-How und die weitreichende Bedeutung dieses Gebrauchsgegenstandes unterschätzt.

3.2 Mechatronische Schließsysteme

3.2.1 Funktion

Die Auswahl an zur Verfügung stehenden mechatronischen Schließsystemen ist sehr groß. So versucht mittlerweile eine ganze Reihe von Herstellern am Marktpotenzial neuer Technologien zu partizipieren. Interessant ist dabei, dass auch seit geraumer Zeit Firmen ihre Produkte anbieten, die nicht aus dem klassischen Schloss- und Beschlagbereich stammen. Hier steht der Ansatz im Vordergrund, unter neuem Namen ein innovatives und neues Produkt anbieten zu können. Dies lässt aufgrund der vermutlich gleichmäßigen Aufteilung des Marktes bei den mechanischen Schließsystemen eine wohlüberlegte Strategie vermuten. Mit den einhergehenden wechselnden Anforderungen in der Zutrittsverwaltung größerer Objekte kommen die mechanischen Anlagen immer häufiger an ihre Grenzen. Der stete Ruf nach einer dynamischen Berechtigungsverteilung geht einher mit den gestiegenen Anforderungen an das Arbeitsumfeld. Weiter wird der Markt vom angesprochenen Preisverfall bei den mechanischen Anlagen und im Nachrüstgeschäft beflügelt. Auf dem Weg in das digitale Zeitalter stellen somit die mechatronischen Schließanlagen den ersten logischen Folgeschritt innerhalb einer ganzheitlichen Digitalisierungsstrategie dar. Entscheidend hierbei ist jedoch der globale Wettbewerb, der durch die Etablierung innovativer und vernetzter Produkte ausgerufen wird. Diese Entwicklung führt zu einem sich stetig vollziehenden Wandel bei derzeitig etablierten Geschäftsmodellen der klassischen Branchen[119]. Grundlage dieses Wandels sind die umfangreichen Produktinnovationen, die in einem Zwischenstadium über den reinen Technologiefortschritt dem Kunden einen Mehrwert bieten sollen; dies lediglich, um in weiteren Innovationssprüngen die kompletten Ressourcen des Unternehmens auf andere Art und Weise mit neuen Geschäftsmodellen zu verknüpfen[120]. Vor diesem Hintergrund werden die Tragweite der mechatronischen Schließsysteme und deren Markterschließung zur entscheidenden Wegbereitung der erfolgreichen Geschäftstüchtigkeit im 21. Jahrhundert. Diese Ausgangsbasis lässt das Angebot an Hersteller von mechatronischen Schließsystemen seit Jahren steigen. Bei der Marktsichtung lassen sich mittlerweile mindestens 98 Anbieter mit 207 Lesegeräten für Zutrittskontrollsysteme ermitteln[121]. Trotz der jüngeren Marktbearbeitung sind auch hier wieder viele Lösungen für ganz spezielle Anforderungen entstanden, ähnlich der Systematik bei den mechanischen Systemen.

Vorteile der angesprochenen mechatronischen Anlagen sind im Wesentlichen in Tabelle 4 dargestellt:

[119] Vgl. Wittpahl, Volker, Digitalisierung, 2017, S. 179.
[120] Vgl. Mast, Clemens, Neuerfindung einer Industrie, 2017, S. 21.
[121] Vgl. Lesegeräte für Zutrittskontrolle, In: Protector&WIK, 03.2017, S. 30.

Vorteile	Nachteile
- Schlüsselverlust (einfache Sperrung) - Veränderung d. Schließberechtigung - Erweiterungen - Interaktiv (Protokollierung, Zeitfunktionen,…)	- Kosten - Wartung - Anwender müssen geschult sein/werden - Affinität zur Elektronik sollte bestehen

Tabelle 4: Vor- und Nachteile mechatronischer Schließanlagen[122]

Die Komponenten eines mechatronischen Schließsystems sind im Vergleich zu einem mechanischen System, das die Verwendung eines mechanischen Schlüssels vorsieht, ein aktiver Transponder (mit Energieversorgung) oder ein passiver Transponder (ohne Energieversorgung). In der Tür ist dann z. B. ein sogenannter Knaufzylinder montiert. Einige Grundkomponenten sind in der Abbildung 13 aufgeführt.

Abbildung 13: Mechatronische Komponenten[123]

(v. l. n. r.: Smartcard, Transponder, mechatronischer Knaufzylinder, Beschlag, eingebauter Beschlag)

Die Freigabe des Schließzylinders funktioniert über die Näherung des Transponders an die integrierte Leseeinheit. Die positive Rückmeldung wird in der Regel über das Aufleuchten einer grünen Leuchte signalisiert, welches daraufhin die Sperrmechanik entriegelt und der Knauf rotatorisch bewegt werden kann, was wiederum den Riegel respektive die Falle im Schloss betätigt.

Die Funkkommunikation zwischen den elektronischen Komponenten verläuft, je nach Übertragungsreichweite und System, in 125 kHz-Langwellenfrequenzen von EM410x und hitag™-Systemen oder in 13,56 MHz-Kurzwellenfrequenzen von mifare® und Legic® Systemen.

3.2.2 Anwendung

Die Anwendungsmöglichkeiten der mechatronischen Schließanlagen sind durch die softwarewaretechnische Abbildung der Bedienungsmöglichkeiten gut in den organisatorischen Ablauf integrierbar. Bei großen Zutrittsanlagen lassen sich weitere Schließgeräte, wie z. B. mechatronische Beschläge oder Transponder-Lesegeräte, leicht in die Anwendung integrieren. Die Programmierung der Zutrittssysteme kann entweder voll vernetzt über eine Online-Anlage funktionieren, oder es müssen einzeln alle Transponder und elektronischen Komponenten offline angelernt werden.

Flexible Schlüsselverwaltungen erlauben nun einen minimalen Aufwand, so dass bei hoher Fluktuation der Anwender, die Berechtigungen einfach zentral am Rechner zu verwalten sind. Auch lassen sich bestimmte Zeitfenster für den Zutritt freischalten, die es z. B. Reinigungskräften erlauben, erst nach üblichen Bürozeiten das Gebäude zu betreten. Dies ist nur ein Beispiel für die optimale Anpassung der Anlage an die Erfordernisse einer Organisation.

Generell ist die Beratung und Installation bei mechatronischen Schließanlagen deutlich umfangreicher und erfordert daher mehr Beratungsleistung. Auch sollten frühzeitig die Benutzer respektive die Verwalter der Anlage in die Entscheidungen mit eingebunden werden. Es ist nicht zu unterschätzen, dass in vielen Fällen die nötige technologische Akzeptanz fehlt. Ein jahrzehntelanger Einsatz von mechanischen Anlagen hat zu bestimmten Verhaltensmustern und Routinen geführt.

[122] Vgl. BHE, Zutrittsregelung und Mechanische Sicherungstechnik, 2007.
[123] Bildersammlung C.Ed. Schulte GmbH Zylinderschlossfabrik, Mechanische Konstruktion, 2017.

Sie lassen sich nicht ohne weiteres auf eine mechatronische Anlage überführen. Mitentscheidend ist das Hinzuziehen eines geeigneten Handelspartners vor Ort, der auch im Notfall entsprechenden Support leisten kann. Hierbei können Checklisten zur Planung einer mechatronischen Anlage helfen[124]. Die Anforderungen sind hochgradig individuell und werden somit auch bedarfsgerecht vom Hersteller für den Kunden angepasst und konzipiert. Reicht das schmale Leistungsspektrum von einem Hersteller nicht aus, werden schnell künstliche Restriktionen geschaffen, die bei einer Erweiterung erst Jahre später sichtbar werden. Auch Handelspartner können nicht immer einen Vor-Ort-Service leisten, so ist auch ein entsprechendes Serviceangebot des Herstellers ein wichtiger Punkt bei der Produktentscheidung.

3.3 Mobile Schließsysteme

3.3.1 Einleitung

Das dritte Unterkapitel beschreibt die zukünftig größte Herausforderung der Schloss- und Beschlagindustrie in den kommenden Jahren. Parallel zu den Entwicklungen im Payment-Bereich, wo die Bezahlung mit Bargeld weiter zurückgeht und die EC-Karte mittlerweile berührungsloses Bezahlen ermöglicht, verschwinden auch sukzessive die Berechtigungsmedien für mechatronische Schließzylinder. Generell wird der Bereich des Payments als Vorreiter und Treiber für die Bündelung von Servicedienstleistungen auf dem Smartphone gesehen. Durch den Kommunikationsstandard NFC konnten kritische Transaktionen sicherer im Nahfeldbereich abgewickelt werden. Zusätzlich war die Trendentwicklung der NFC-Technologie einem starken Hype ausgesetzt, was die Marktdurchdringung beflügeln sollte (Abbildung 14).

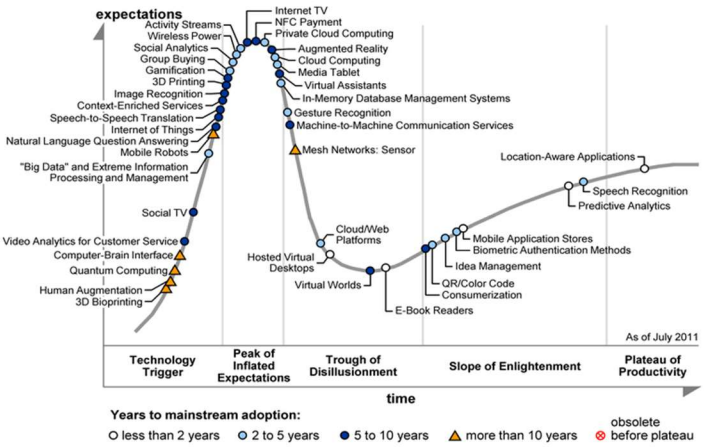


Abbildung 14: Hype-Cycle NFC-Payment 2011[125]

Auch der klassische Automobilsektor versucht, mit neuen Geschäftsmodellen seine marktbeherrschende Stellung zu wahren. Längst hat sich beim Kunden das Interesse durchgesetzt, dass im Automotive-Bereich nicht mehr die reinen Leistungsdaten der angebotenen Verbrennungsmotoren von enormer Wichtigkeit sind sondern die Konnektivität der Bordsysteme. Die Interoperabilität des Automobils gilt auch als Chance für neue und unbekannte Player im Automobilsektor. Da sich über die Konnektivität weitere Mehrwertdienste ergeben, wird speziell der Nutzung des Fahrzeuges bei Bedarf, dem sogenannten Carsharing, besonderes Interesse beigemessen. Entsprechende Patente für den schlüssellosen Zugang zu Fahrzeugen[126] wurden nicht nur von den klassischen Automobilherstellern initiiert sondern auch von der Zulieferindustrie, wie z. B. Continental. Getragen wird dieses vor allem durch die Entkopplung traditioneller Statussymbole wie z. B. besonders hochpreisige Autos von der gesellschaftlich-sozialen Stellung. Zukünftige elitäre Gesellschaften werden sich durch differente Statussymbole definieren. Auch in der Vergangenheit hat es schon disruptive Entwicklungen gegeben. Die Herausforderungen der Zukunft

[124] Vgl. Jeschke, Hartwig, Elektronische Schließanlagen, In: Sicherheitsmarkt, 2003, S. 6.
[125] Gartner's Hype cycle places NFC at 'Peak of Inflated Expectations', Abrufbar im Internet, https://www.nfcworld.com/2011/08/11/39008/gartner-hype-cycle-places-nfc-at-peak-of-inflated-expectations/, 2011.
[126] Schutzrecht, DE 10 2016 204 807 A1, Continental Automotive GmbH, 09.03.2017.

aber liegen in der enormen Geschwindigkeit. Bei keiner Entwicklung der Vergangenheit gab es derartige Umsetzungsgeschwindigkeiten zeitgleich in allen Branchen. Damit bestehende Märkte nicht an Marktbegleiter oder Newcomer verloren werden, sind die Unternehmen auf die Expertise von neuen Kooperationspartnern angewiesen[127]. Auch aus diesem Spannungsfeld resultiert ein weiterer Paradigmenwechsel zur gewöhnlichen Geschäftstätigkeit und damit zu Veränderungen in der gesamten Arbeitswelt. Dies sind zwei repräsentative Beispiele aus dem Automobil- und Bankensektor, die belegen, mit welchen essentiellen Fragestellungen die regionale Industrie im Zuge der Neuausrichtung konfrontiert ist, um durch eine entsprechende Vernetzung existenzsichernde Produkte und Dienstleistungen hervor zu bringen[128].

Mittlerweile haben Vertreter der unterschiedlichsten Branchen kreatives Gedankengut patentrechtlich schützen lassen. Im Bereich der Schloss- und Beschlagindustrie sind einige Patentrechte für ein mobiles Ökosystem angemeldet worden. Beispielhaft lassen sich spezielle Patente von Assa Abloy erwähnen, wie z. B. die Schlüsselverwaltung auf dem Smartphone[129] oder eine mobile Schließgeräteprogrammierung[130] sowie ein allgemeiner gehaltenes Patent von BKS zum Zugang mittels einer elektronischen Schließeinrichtung mit NFC[131]. Aber auch Dienstleistungsunternehmen wie die Post überdenken ihren klassischen Paketversand. Mit einer direkten Kommunikationsverbindung könnte zukünftig der intelligente Briefkasten direkt von der Post beliefert werden, der anschließend eine Information mit dem Berechtigungscode an das Smartphone des Empfängers sendet[132].

3.3.2 Mobiles Ökosystem (Beispiel)

Die Vernetzung verschiedener Akteure kann Synergieeffekte hervorrufen, um mögliche Bedarfe in einem Testbetrieb zu ermitteln. Damit unternehmerische Kooperationen ein innovatives Vorhaben realisieren können, bedarf es für alle Beteiligten einer sinnhaften Akzeptanz der Aktivität. In diesem Vorstadium der Marktreife befinden sich eine Reihe von Patenten aus den unterschiedlichsten Bereichen von Technik und Organisation. Abbildung 15 zeigt einen Zusammenschluss verschiedener Akteure im Bereich Mobile Access. Positiver Effekt der Kooperationen ist die entstehende Vielfalt des Dienstleistungsangebotes für den Endnutzer im Bereich der mobilen Zutrittslösungen und gleichzeitig Basis neuer Geschäftsmodelle für die beteiligten Akteure.

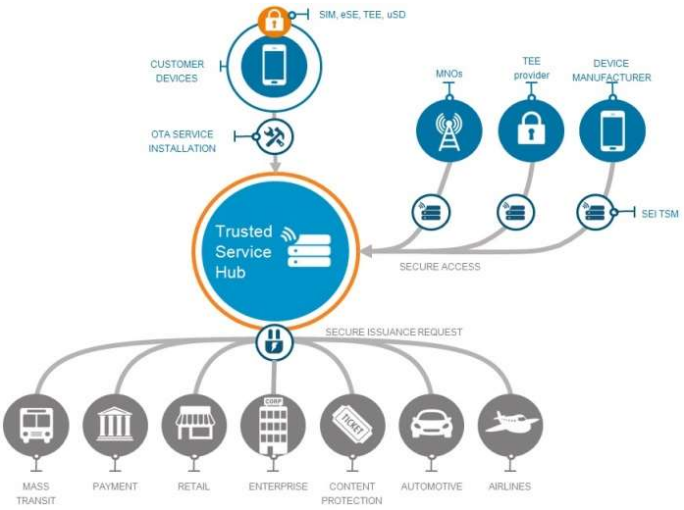


Abbildung 15: TSM-Plattform[133]

[127] Vgl. Dunker, Hilmar, Lockruf des Geldes, In: business impact, S. 34, 01.2017.
[128] Vgl. Bretting, Ralf, Lockruf des Geldes, In: business impact, S. 34, 01.2017.
[129] Schutzrecht, WO 2016/177667 A1, Assa Abloy AB, 10.11.2016.
[130] Schutzrecht, WO 2016/185283 A1, Assa Abloy AB, 24.11.2016.
[131] Schutzrecht, DE 20 2015 003 163 U1, BKS GmbH, 08.09.2016.
[132] Schutzrecht, EP 3 121 795 A1, Deutsche Post AG, Pr.: 20.07.2015 DE 102015111711.
[133] Dominique Brulé, Gemalto, What`s behind the acceleration of NFC mobile payments?, Abrufbar im Internet, https://blog.gemalto.com/blog/2014/09/30/whats-behind-the-acceleration-of-nfc-mobile-payments/, 2014.

Über eine Trusted Service Management Plattform werden für verschiedene Akteure, sogenannte Service Provider, Dienstleistungen administriert. Wie in der Abbildung 15 auszugsweise dargestellt, handelt es sich dabei um Dienstleistungen aus den Bereichen öffentlicher Nahverkehr, Finanzwesen, Einzelhandel, Gebäudemanagement, Sicherheit, Automotive und Flugverkehr. Damit das komplexe Wechselspiel von Service-Providern, Mobilfunkanbietern (mobile network operators), Geräteherstellern (secure elements issuers), TSM-Anbietern und den Endnutzern funktioniert, laufen alle Hard- und Softwarefunktionalitäten bei einem vertrauenswürdigen und sicheren Vermittler, der TSM-Plattform zusammen. Ausgehend von dieser Organisationsstruktur kann eine jederzeit sichere Übermittlung und Verwaltung der Daten gewährleistet werden. Im Gegensatz dazu steht die komplette Datenhoheit beim Service-Provider selbst, wo die Administration von nur einer Stelle geleistet wird. Gerade im Payment-Bereich sind die Ansprüche an die Datensicherheit sehr hoch, so dass hier frühzeitig entsprechende Kooperationen mit Know How-Trägern forciert wurden. Ein weiterer wichtiger Systembaustein im Bereich der Sicherheit ist das sogenannte Secure Element. Hierbei handelt es sich um einen physischen Speicher für die Berechtigung (Credential), der in drei Bauformen vorkommen kann, die wiederum abhängig von den Besitzansprüchen der Berechtigung sind. Somit kann das Secure Element in der SIM-Karte, der Speicherkarte oder direkt im Smartphone integriert sein. Die gesamte Kommunikation und lokale gespeicherte Daten der Kooperationspartner im NFC-Ökosystem sind mit einer End-to-End-Verschlüsselung gesichert. In der Umsetzung beschreibt das Secure Element eine sichere Umgebung innerhalb des Trusted Execution Environment, für welche spezifische Aufgaben und Rollen der Akteure festgelegt sind[134]. Vorteil dieser Sicherheitsarchitektur ist die diversifizierte Behandlung von sensiblen Endbenutzerdaten innerhalb eines solchen Ökosystems. An einem einfachen fiktiven Beispiel „Mobile Access" lässt sich dieser Sachverhalt vergegenwärtigen. Für die erstmalige Einrichtung des Dienstes separiert der TSM-Anbieter auf dem Secure Element einen Speicherbereich. Für den direkten SE-Zugriff wird mithilfe des MNOs (mobile network operator) der Datenverkehr über das Mobilfunknetz durchgeführt. Gleichzeitig ist der Speicherplatz durch eine Verschlüsselung zusätzlich abgesichert; der Schlüssel dafür ist je nach SE-Besitzzustand beim MNO oder TSM-Anbieter hinterlegt. Mit der Autorisierung des Endbenutzers beim SP, dem Schließanlagenhersteller, kann die jeweilige Zutrittsberechtigung organisiert durch den TSM-Anbieter vom SP abgerufen und an den Endbenutzer durchgereicht werden. Dabei wird dieses Datenpaket nochmal durch den TSM-Anbieter mehrfach verschlüsselt und im geschützten Bereich auf dem SE im Smartphone abgelegt. Der eigentliche digitale Schlüssel zur Zutrittsberechtigung ist dem TSM-Anbieter nicht bekannt. Im Anschluss kann der Anwender mithilfe des Smartphones als Träger der geschützten Daten sich an einer Tür berechtigten Zutritt verschaffen. Aufgrund dieser verteilten Eigentumsrechte wie Verschlüsselung, Kommunikationsweg, Schließgeheimnis und sichererem Speicherort (SE) kann ein sehr hohes Maß an Sicherheit gewährleistet werden. Innerhalb dieses Konzeptes können über die TSM-Plattform mehrere Dienstleistungen für den Anwender orchestriert werden. In einigen pilothaften Anwendungen wurde versucht, die Akzeptanz und das Verständnis in diesem Bereich zu fördern. Jedoch hat in einigen Fällen die Sicherheitsarchitektur bei den SP für „Überforderung" gesorgt, weil sie nicht mit dem traditionellen Sicherheitsgedanken der Schloss- und Beschlagindustrie deckungsgleich ist[135]. Dieser folgt eher herstellerspezifisch proprietären Ansätzen ohne Beteiligung von Global Playern.

3.3.3 Anwendung Mobile-Access

Nach den eher globalen Möglichkeiten im Bereich des Mobile Access sind mittlerweile kleinere Anwendungen mit bestehenden Erfahrungen konzipiert und in den Markt eingeführt. Nach anfänglicher Skepsis und zögerlicher Marktbearbeitung konnten auch kleinere Start-Ups zusammen mit der traditionellen Schloss- und Beschlagindustrie Kooperationen eingehen. Zusätzlich hat sich der Kommunikationsstandard NFC als Nahfeldkommunikation als nicht ausreichend und praxistauglich herausgestellt. Der Übertragungsweg von Sender und Empfänger musste in einigen Fällen als zu gering attestiert werden, wie z. B. bei der Berechtigung aus dem Auto heraus eine

[134] Entscheidend für die Standardisierung ist ein Industrieverband aus verschiedenen Herstellern zur Umsetzung einer sicheren Umgebung für sensible (mobile) Aktionen, wie z. B. dem Mobile-Payment. Weitere Informationen sind auf der Global-Platform-Seite, unter: https://www.globalplatform.org/, abrufbar.

[135] Vgl. Banse, Gerhard, Techniksicherheit und Sicherheitskulturen, In: Bach, Friedrich-Wilhelm / Schnieder, Eckehard / Winzer, Petra, Sicherheitsforschung, 2010, S. 199.

Schrankenanlage zu öffnen oder zu schließen. Weiterhin bewahren viele Benutzer ihre Smartphones in der Hosentasche auf und müssen bei allen Aktivitäten zur Berechtigung das Gerät extra in die Hand nehmen. Einen deutlichen Komfortgewinn erzielt die Bluetooth Low Energy-Schnittstelle (BLE). Ihre Übertragungsreichweite ist fühlbar größer und hat noch den positiven Nebeneffekt der reellen Akzeptanz beim Endnutzer. Abbildung 16 zeigt eine mögliche Mobile Access-Anwendung.

Abbildung 16: Mobile-Access-Anwendung[136]

Die Mobile Access-Anwendungen in Abbildung 16 stellen zwei Möglichkeiten des mobilen Zutrittsmanagements dar. Auf der linken Hälfte der Abbildung wird mit dem Smartphone ein motorisierter Schließzylinder per Bluetooth Low Energy angesteuert. Vorteil für den Kunden ist der geringe Umbauaufwand, da der Motor an den mechanischen Schließzylinder angeflanscht wird. Auffällig ist hierbei die etwas voluminöse Konstruktion, was aber auf die integrierte Stromversorgung mit handelsüblichen Batterien zurückzuführen ist. Für eine im Handel verfügbare Nachrüstlösung eignet sich diese Variante jedoch am besten.

Auf der rechten Seite der Abbildung befindet sich ein nicht-motorisierter Knaufzylinder, welcher per NFC angesteuert werden kann. Dabei wird durch die Annäherung mit dem Smartphone die Schließnase eingekuppelt, und das Türschloss kann manuell über den Knauf betätigt werden. Für eine Installation an der Tür muss unter Umständen der Handelspartner vor Ort unterstützen, da die Einrichtung nicht immer selbsterklärend ist.

Die digitale Transformation vom mechanischen Schlüssel zum digitalen Berechtigungsmanagement über das Smartphone bringt für den Endnutzer eine Menge Vorteile. Simultan fügt es sich in die gesellschaftliche Orientierung der allgegenwärtigen Vernetzung durch die Etablierung des neuen Technikverständnisses im Konzept der Mensch-Maschine-Interaktion ein[137].

In der folgenden Tabelle 5 sind die Vor- und Nachteile eines solchen Systems nochmal zusammengefasst.

Vorteile	Nachteile
- Dezentrale Schlüsselverwaltung - Keine zusätzlichen Medien - Unkomplizierte Erweiterung - Gute Anpassung an organisatorische Betriebsabläufe	- Kosten - Umfangreichere Beratung nötig - Oft nicht klassisches Geschäftsmodell aus Sicht der Schließanlagenhersteller - Smartphone nötig (Affinität)

Tabelle 5: Vor- und Nachteile Mobile-Access

3.4 Kommunikationstechnologien

Für einen berührungslosen Datenaustausch werden geeignete Kommunikationstechnologien benötigt. Dabei spielen die Einsatzumgebung und der Zweck eine entscheidende Rolle bei der

[136] Vgl. Bildersammlung C.Ed. Schulte GmbH Zylinderschlossfabrik, Marketing, 2017.
[137] Vgl. Banse, Gerhard, Techniksicherheit und Sicherheitskulturen, In: Bach, Friedrich-Wilhelm / Schnieder, Eckehard / Winzer, Petra, Sicherheitsforschung, 2010, S. 192.

richtigen Auswahl. Nach dem Hype von NFC als „Alleskönner" qualifizierten sich daraufhin auch bestimmte Aufgaben für den BLE-Einsatz.

3.4.1 Near Field Communication (NFC)

Die NFC-Schnittstelle eignet sich generell für den Nahfeld-Bereich innerhalb einer theoretischen Distanz von maximal 20 cm mit der RFID-üblichen Frequenz von 13,56 MHz, so dass auch eine Interaktion mit RFID-Lesegeräten und -Transpondern (nach ISO/IEC 14443) durchgeführt werden kann[138]. Durch die Anwendungsfälle, die in der Regel keine sehr großen Datenmengen beinhalten wie in den Bereichen der Bezahlfunktionalitäten oder Ticketing, reichen die Datenübertragungsgeschwindigkeiten von 424 kbit/s vollkommen aus[139]. Für die Kommunikation werden jeweils ein „NFC-Master" und ein „NFC-Slave" benötigt, die im gegenseitigen magnetischen Wechselfeld liegen und in folgenden Betriebsarten funktionieren[140]:

- Peer-to-Peer-Modus
- Reader/Writer-Modus
- Card-Emulation-Mode

Bei direkter Kommunikation mit NFC-Geräten ist der Peer-to-Peer-Modus üblich. Für die Übertragung mit passiven Transpondern kann im Reader-/Writer-Modus gearbeitet werden, der, wie angesprochen, auch mit den klassischen RFID-Standards größtenteils kompatibel ist. Bei dem Card-Emulation-Mode verhält sich das NFC-Gerät wie eine Smardcard und kann über ein RFID-Lesegerät kommunizieren.

Aus Konsumentensicht ist es bisher unverständlich, warum die Schnittstelle nicht bei Apple-Geräten aber sehr wohl bei Android-Geräten frei genutzt werden kann. Sicherlich möchte Apple seinem eigenen Bezahldienst Apple Pay damit die Exklusivität sichern, jedoch werden hier im Vorlauf entscheidende negative Signale gesendet, die sich im Nachhinein nachteilig auswirken könnten. Im Gegensatz dazu müssen natürlich noch keine teuren Werbemaßnahmen für die Nutzung des Dienstes getroffen werden, solange die Marktdurchdringung beim Benutzer noch nicht abgeschlossen ist.

Trotz steigendem Bekanntheitsgrad und dem kontinuierlichen Ausbau der Akzeptanzstellen in Deutschland, ist die Beliebtheit von Bargeld noch deutlich größer[141]. Gerade hier, wo das anonyme Bezahlen mit Bargeld einen sehr hohen Stellenwert genießt, sollte für den Ausbau von Mobile Payment mit NFC eine ähnliche Anonymität gewährleistet werden können, um den Verbreitungsgrad nachhaltig zu stärken[142]. Parallel dazu ist auf entsprechend implementierte kryptografische Verfahren zu achten, die insbesondere bei Payment, Ticketing oder Zugangssystemen für sicherheitsrelevante Funktionen eine unverzichtbare Funktionalität darstellen[143].

3.4.2 Bluetooth Low Energy (BLE)

Der Bluetooth-Standard ist die wohl meist genutzte drahtlose Kommunikation zur Verbindung der Freisprecheinrichtung im Auto mit dem Smartphone oder dem Streaming von Audiodateien. Die Möglichkeiten der Anwendungen sind so groß, dass diese in fast allen technischen Geräten schon standardmäßig integriert sind, wie z. B. in Notebooks, Lautsprechern, Smartphones, Tablets, Funktastaturen/-mäusen etc. Ein Vorteil gegenüber NFC ist die viel größere Verbreitung und Akzeptanz von Bluetooth, die frühzeitig nicht nur technologische Entwicklungen beflügelte.

[138] Vgl. Finkenzeller, Klaus, RFID Handbuch, 2015, S. 73 ff.
[139] Vgl. Langer, Josef / Roland, Michael, Anwendungen und Technik von Near Field Communication, 2010, S. 87.
[140] Vgl. ebd., S. 90.
[141] Vgl. Dietz, Ulrich, Die Zukunft des Bezahlens, Abrufbar im Internet, https://www.bitkom.org/noindex/Publikationen/2015/Sonstiges/PK-Zukunft-des-Bezahlens/BITKOM-PK-Zukunft-des-Bezahlens-Praesentation-10-06-2015-final.pdf, 2015, Folie 3.
[142] Vgl. Kaymaz, Feyyat, User-Anonymität in Mobile Payment Systemen, 2011, S. 222 f.
[143] Vgl. Finkenzeller, Klaus, RFID Handbuch, 2015, S. 316.

Werbemaßnahmen für Dienstleistungsangebote, wie z. B. dem Bluetooth-Marketing zur Umsetzung von mobilen Kampagnen, sollten eine direkte Kontaktaufnahme mit dem Kunden sicherstellen[144].

Für den noch energiesparenderen Einsatz in kleinen Geräten mit einem reduzierten Energieverbrauch hat sich der Bluetooth Low Energy-Standard durchgesetzt, der in den letzten Jahren verschiedene Entwicklungsstufen durchlaufen hat[145]. Da jede Version eine Leistungserweiterung erfahren hat, sind die Übertragungsraten und Reichweiten von der jeweiligen Version abhängig. Eine Übersicht zur groben Einordnung ist in Abbildung 17 dargestellt.

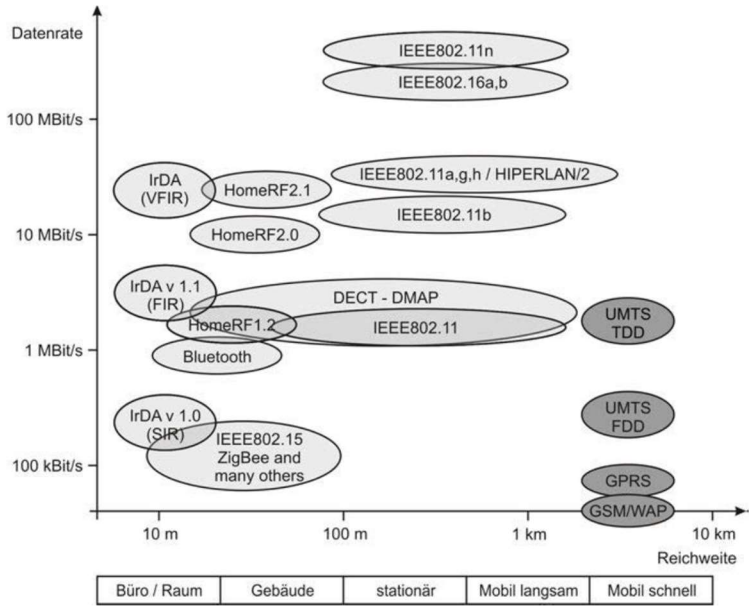


Abbildung 17: Drahtlose Kommunikationsstandards im Vergleich[146]

Das benötigte Frequenzband von 2,4 GHz teilt sich Bluetooth mit weiteren Funktechnologien (u. a. Wireless LAN), so dass es auf keiner festen Bandbreite sendet sondern verschiedene nutzt bzw. diese wechselt[147]. Da Bluetooth auch in vielen kleinen Geräten verbaut ist, die eine begrenzte Energieversorgung gewährleisten, existieren drei Leistungsklassen[148]:

- Klasse 3: 1 mW (Ausgangsleistung) und 10 m Reichweite,

- Klasse 2: 2,5 mW und 10 m Reichweite und

- Klasse 1: 100 mW und 100 m.

Durch die generell größeren Reichweiten von Bluetooth eignet es sich für Anwendungsfelder die nicht unbedingt einen Sichtkontakt voraussetzen, wie es z. B. bei NFC im Nahfeldbereich der Fall ist. Daher müssen auch hier besondere Sicherheitsvorkehrungen in Abhängigkeit zur Anwendung beachtet werden. Das Koppeln der Freisprecheinrichtung mit dem Smartphone setzt im Zweifel geringere Schutzmaßnahmen voraus als z. B. das Koppeln des Smartphones mit der Türschließanlage. So kann es ausreichend sein, dass im Fall der Freisprecheinrichtung eine einmalige Sicherheitsvorkehrung mit dem Eingeben eines Zahlenschlüssels zum Koppeln ausreichend ist. Im Fall der Steuerung einer Türschließanlage sollte aber auch die ständige Kommunikation verschlüsselt werden. Hier stellt Bluetooth ein umfassendes Sicherheitspaket mit bis zu 128 Bit-Schlüsseln in der Sicherungsschicht zur Verfügung[149].

[144] Vgl. Eickemeyer, Danny, Bluetooth-Marketing, 2010, S. 1 f.
[145] Vgl. Sauter, Martin, Grundkurs Mobile Kommunikationssysteme, 2013, S. 356.
[146] Vgl. Gessler, Ralf / Krause, Thomas, Wireless-Netzwerke für den Nahbereich, 2015, S. 202.
[147] Vgl. Sauter, Martin, Grundkurs Mobile Kommunikationssysteme, 2013, S. 358.
[148] Vgl. Gessler, Ralf / Krause, Thomas, Wireless-Netzwerke für den Nahbereich, 2015, S. 204.
[149] Vgl. ebd., S. 209.

4 Standards, Normen und Richtlinien

Das Kapitel 4 soll einen Einblick in die wichtigsten Arbeitsunterlagen der bestehenden Standards, Normen und Richtlinien geben. Dabei wird auf Standards der praktischen IT-Security zurückgegriffen, die sich auch im realen Einsatz bei Systemkomponenten befinden. Besonders entscheidend sind die entsprechenden kryptografischen Implementierungen zur Verschlüsselung von Informationen. Bei den Normen und Richtlinien sind insbesondere jene, die aus dem Schloss- und Beschlagbereich stammen, für eine thematische Annäherung an übliche Zertifizierungen hilfreich. Gängige Interessensverbünde sind dort die Europäischen Normen (EN), das Deutsche Institut für Normung (DIN) und der Verband der Schadenversicherer (VdS). Interessante Richtlinien im Bereich der IT-Security stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Common Criteria (CC) zur Verfügung.

Für einen verständlicheren Einblick sind die Standards, Normen und Richtlinien den Bereichen IT-Security und in die der branchenspezifischen Unterlagen einsortiert.

4.1.1 IT-Security

Im Zuge der fortschreitenden Umsetzung der Digitalisierung, sollten auch Fragen zur sicheren Umsetzung en détail gestellt und beantwortet werden; leider können aus der Summe von Einzelmaßnahmen zur Absicherung von Komponenten keine Rückschlüsse auf die Sicherheit des gesamten Systems gezogen werden. „Die Voraussetzung heißt in diesem Fall Beherrschbarkeit der Komplexität und auch der Sicherheit."[150] Dies wird unter dem Gesichtspunkt „Internet der Dinge (IoT)" zu einer globalen und umfassenden Herausforderung[151], die gleichermaßen von der Gesellschaft, den Herstellern und der Politik getragen werden muss. Da sich durch die Vernetzung der Geräte die physische Verortung egalisiert, steht Sicherheit an erster Stelle. Es ist die Aufgabe aller Benutzer oder Inhaber eines intelligenten Gerätes darauf zu achten, die Einbindung in das Internet mit einem Mindestmaß an Sicherheit vorzunehmen. Für die entsprechenden Funktionalitäten im Gerät und deren sichere Implementierung trägt der Hersteller die Verantwortung, damit nicht Fernwartungszugänge oder unverschlüsselte Kommunikation für einen manipulativen Zugriff (Cyber-Kriminalität) benutzt werden können. Gleichermaßen muss ein politischer und gesetzlicher Rahmen geschaffen werden, damit ein sicherer Raum entsteht, in dem Gesetze auf nationaler und internationaler Ebene bindende und praktikable Gültigkeit haben. Hier stehen insbesondere Fragen zum Schutz persönlicher Daten in besonderem Fokus.

Nur unter der Voraussetzung eines erfolgreichen Zusammenspiels von Benutzern, Herstellern und Politikvertretern kann Komplexität reduziert und Sicherheit erhöht werden; daraus resultiert im idealen Fall, dass auch der einfache Anwender und Benutzer IT-Security anwenden kann und wird[152]. Da die Hersteller aber in der Regel nicht nach dem Maximum-Prinzip arbeiten sondern nach der Input-Output-Relation und Gewinnmaximierung vorgehen, ist eine exakte Anforderung an die zu leistende Informationssicherheit zu formulieren[153].

In diesem Zusammenhang ist immer wieder die Rede von kryptographischen Maßnahmen, gleichwohl es sich um die Chiffrierung zur Speicherung, Kommunikation oder Verarbeitung von Daten handelt. Im einfachsten Sinne wird eine Nachricht dabei so unverständlich abgeändert, dass es einem Außenstehenden nicht möglich ist, aus der Nachricht noch einen sinnvollen Inhalt zu ermitteln. Zur Entschlüsselung wird ein geheimer Schlüssel benötigt. Wichtiges Unterscheidungsmerkmal ist auch der Schlüssel zur Identifizierung eines symmetrischen Verfahrens, d. h. ein gemeinsamer Schlüssel zur Ver- und Entschlüsselung oder ein asymmetrisches Verfahren, d. h. ein Schlüssel zur Verschlüsselung und ein Schlüssel zur Entschlüsselung[154]. Für die Entscheidung, ob eine kryptographische Maßnahme sicher oder unsicher

[150] Pelzl, Jan, Aus dem smarten Leben gegriffen, In: Bub, Udo / Deleski, Viktor / Wolfenstetter, Klaus-Dieter, Sicherheit im Wandel von Technologien und Märkten, 2015, S. 28.
[151] Vgl. Pelzl, Jan, Motivationsvortrag: Das Internet der Dinge, Hochschule Hamm-Lippstadt, 2017.
[152] Vgl. Abolhassan, Ferri, Security Einfach Machen, 2017, S. 130 f.
[153] Vgl. Gadatsch, Andreas / Mangiapane, Markus, IT-Sicherheit, 2017, S. 23.
[154] Vgl. Beutelspacher, Albrecht / Schwenk, Jörg / Wolfenstetter, Klaus-Dieter, Moderne Verfahren der Kryptographie, 2015, S. 1 f.

ist, entscheidet die Kryptoanalyse (Abbildung 18). Mit diesem gegenseitigen Wechselspiel von neuen und vermeintlich sicheren Verschlüsselungen (Chiffren) und den Codebrechern der Kryptoanalyse entsteht eine Symbiose zur stetigen Weiterentwicklung sicherer Verschlüsselungen.

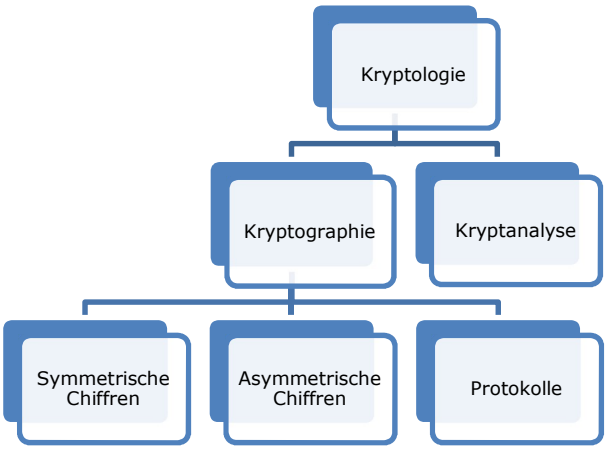


Abbildung 18: Kryptologie[155]

Im derzeitigen Stand der sicheren Verschlüsselungen befinden sich die folgenden Chiffren:

- **DES (Data Encryption Standard):** Dieser symmetrische Standard galt lange als sehr sicher und fand sich daher in vielen Systemen wieder. Dabei wird die zu verschlüsselnde Nachricht in 64 Bit Blöcke zerlegt und mit einem Schlüssel von 56 Stellen chiffriert. Grundsätzlich verschlüsselt der Standard in einer Abfolge von 16 Runden mit verschiedenen Funktionen, wobei die Klartextblöcke in eine linke und rechte Einheit getrennt werden. Bei jedem Durchlauf der Runden wird aus dem DES-Schlüssel ein Rundenschlüssel abgeleitet. Die Entschlüsselung funktioniert in umgekehrter Reihenfolge der zuvor durchlaufenden einzelnen Runden.[156]

- **3DES (Triple-DES):** Da der beschriebene Stand eines einfachen DES-Verfahrens mit seinem 2^{56} Schlüsselraum heutzutage nicht mehr ausreichend ist, wurde das Verfahren durch eine Mehrfachverschlüsselung an die gegenwärtigen Anforderungen an eine sichere Chiffre angepasst. Bei dem 3DES werden drei Schlüssel zur Ver- und Entschlüsselung erzeugt. Aufgrund technischer Gegebenheiten erhöht sich der Schlüsselraum aber nur auf 2^{112}. Im Gegensatz zum einfachen DES stellt dies bereits eine deutliche Erhöhung der Sicherheit dar, die den sicheren Einsatz des DES-Verfahrens weiter gewährleistet.[157]

- **AES (Advanced Encryption Standards):** Um der erhöhten Rechenleistung gerecht zu werden, wurde mit dem AES-Standard der Schlüsselraum variabel in drei Stufen auf 128, 192 und 256 Bit erhöht. Im Unterschied zum DES-Standard wirken die internen Verschlüsselungsfunktionen in Form einer Matrix. Die Anzahl der jeweiligen Runden ist dabei vom Schlüssel abhängig. Da der AES als offizieller Nachfolger vom einfachen DES eingesetzt wird, gilt der AES als „sehr sicher". Insbesondere sensible Operationen, wie im Payment-Bereich, setzen auf diesen neueren Standard.[158]

- **RSA (Rivest-Shamir-Adleman-Verfahren):** Im Gegensatz zu den bereits erwähnten Verschlüsselungen handelt es sich hierbei um ein asymmetrisches Verfahren. Aufgrund des erhöhten Rechenaufwandes wird RSA bevorzugt für kleine Datenmengen und den Schlüsseltransport eingesetzt. Im Wesentlichen geht die Funktionsweise auf das Faktorisierungsproblem großer Zahlen zurück (Einwegfunktion). In der Praxis wird dieses Verfahren

[155] Paar, Christof / Pelzl, Jan, Kryptografie verständlich, 2016, S. 3.
[156] Vgl. Swoboda, Joachim / Spitz, Stephan / Pramateftakis, Michael, Kryptographie und IT-Sicherheit, 2008, S. 52 f.
[157] Vgl. Eckert, Claudia, IT-Sicherheit, 2012, S. 340 ff.
[158] Vgl. Beutelspacher, Albrecht / Schwenk, Jörg / Wolfenstetter, Klaus-Dieter, Moderne Verfahren der Kryptographie, 2015, S. 12.

häufig in Kombination mit einer symmetrischen Chiffre zum gemeinsamen Schlüsselaustausch eingesetzt.[159]

Zusätzlich gibt es viele weitere eingesetzte Verfahren, die in Abhängigkeit zum Einsatzfeld auch proprietär sein können. In letzter Zeit erlangen aber auch sehr komplexe Verfahren weitere Popularität, wie z. B. die der Elliptischen-Kurven-Kryptographie[160].

Wichtig bei der IT-Sicherheit ist jedoch die frühzeitige Einbindung dieser eher theoretischen Disziplin in einen Gebrauchsgegenstand. Es sollte rechtzeitig ein gemeinsames Verständnis gefunden werden, wie und in welchem Umfang die Implementierung einer sicheren Kryptographie das System gegen potenzielle Angreifer widerstandsfähig machen kann[161].

4.1.2 Common Criteria (CC)

Die Common Criteria erhalten aufgrund erhöhter IT-Bedrohungen mehr und mehr Relevanz. Sowohl die Hersteller wollen sich gegenüber dem Kunden als „sicherer" Partner authentifizieren, aber auch die Kunden möchten das Thema Datensicherheit in verantwortungsvolle Hände legen. Das Bundesamt für Sicherheit in der Informationstechnik zertifiziert in einem Anerkennungsverfahren Prüfstellen, die das CC-Verfahren offiziell durchführen dürfen[162]. Geprüft werden die Produkte nach Gesichtspunkten der IT-Sicherheit anhand eines einheitlichen Kriterienkatalogs. Als Ergebnis eines langen Evaluationsprozesses wird die Vertrauenswürdigkeitsstufe der Evaluierung dargestellt. Vorteile für die Hersteller sind die Standardisierung (ISO), eine direkte Vergleichbarkeit der Evaluierungsergebnisse (international begrenzt) und die stetige Steigerung von evaluierten (erstklassigen) Produkten nach IT-Security Aspekten[163]. Da dieses internationale Regelwerk über übliche Standards hinausgeht, wird es in Zukunft an Relevanz zunehmen. Nationale Bestrebungen von Interessensverbänden im Bereich der Normierung und Richtlinien können allerdings keinen alleinigen Anspruch auf Vollständigkeit erheben. In der Entwicklungsphase gab es intensive internationale Mitwirkung. In die einzelnen Versionen der CC sind auch immer wieder praktische Erfahrungen eingeflossen, so dass die Kriterien immer Praxisbezug aufweisen. Wie in einem Kriterienwerk üblich ist der Rahmen der Evaluierung formalisiert und dokumentiert. Die CC ist dreigeteilt (siehe Abbildung 19) und wird durch eine Evaluationsmethodologie ergänzt.

Abbildung 19: Teile der Common Criteria[164]

Die Teile 1 bis 3 der CC geben den Rahmen dessen vor, was geprüft werden soll. Ergänzt werden die Dokumente von der Evaluationsmethodologie (CEM), die eine Aussage darüber trifft, wie geprüft wird. Die Einarbeitung in die CC ist nicht trivial und kann daher nur von gut ausgebildeten

[159] Vgl. Paar, Christof / Pelzl, Jan, Kryptografie verständlich, 2016, S. 199 ff.
[160] Vgl. ebd., S. 238.
[161] Vgl. Wolf, Marko, Security Engineering for Vehicular IT Systems, 2009, S. 173 f.
[162] Vgl. BSI Magazin, „Das Deutsche Prüfschema genießt weltweit einen exzellenten Ruf", In: Mit Sicherheit, Abrufbar im Internet, https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2016_02.pdf?__blob=publicationFile&v=7, 2016/02, S. 18.
[163] Vgl. BSI, Workshop Common Criteria 3.1, 2015, Kap. 1, Folie 20.
[164] Modifiziert nach: ebd., Folie 23.

Fachkräften mit einer speziellen Schulung durchgeführt werden. Somit werden alle Vorgaben an die Zertifizierungsstelle und den Evaluierenden vom BSI genauestens nachverfolgt.

Für eine detaillierte Annäherung an das CC-Verfahren sind im ersten Teil die Grundlagen inklusive der Philosophie mit zugehöriger Terminologie beschrieben. Hier werden die Wechselbeziehungen der unterschiedlichen Akteure zueinander innerhalb der CC-Evaluierung sichtbar. Das Ziel der Evaluierung ist nicht, eine Aussage darüber zu treffen, ob ein Produkt sicher oder unsicher ist, sondern ob die gewünschte Vertrauenswürdigkeitsstufe (EAL) erreicht wird[165]. Der Evaluierungsprozess auf abstrakter Ebene ist in der Abbildung 20 dargestellt.

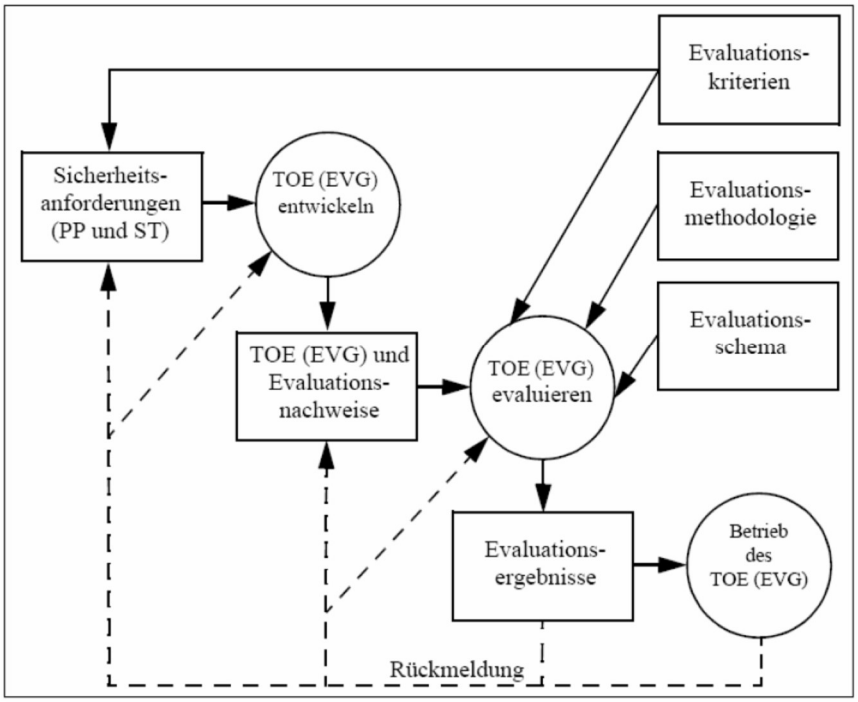


Abbildung 20: Prozess nach Common Criteria[166]

Wie in Abbildung 20 aufgezeigt sind insbesondere Protection Profile (PP), Security Target (ST) und Target of Evaluation (TOE) von besonderer Bedeutung. Eine bedingte Abhängigkeit besteht bei den PP und den ST. Dabei beschreibt das PP den benötigten Sicherheitsbedarf und das ST den zu bietenden (konkreten) Sicherheitsbedarf. Somit baut das ST auf dem PP auf. Beim TOE handelt es sich um das zu evaluierende Objekt, wobei es sich dabei im weitesten Sinne um ein IT-System handelt. Viele weitere Begrifflichkeiten und prinzipielle Handlungsweisen sind im Teil 1 der CC beschrieben und in Abhängigkeit von einander dargestellt.

Teil 2 der CC stellt funktionale Anforderungen an die Sicherheitsfunktionalitäten in Form eines Kataloges dar. Dabei ist der Katalog streng hierarchisch aufgebaut und wird von Klassen, der höchsten Ebene, über Familien, Komponenten und zuletzt bis auf die kleinste Ebene der Elemente herunter gebrochen. Beispiele für Klassen sind z. B. Kommunikation, Identifikation und Authentifikation.[167]

Im Teil 3 der CC werden die Sicherheitsanforderungen an die Vertrauenswürdigkeit dargestellt. Somit gewährt ein evaluiertes TOE das Vertrauen, die gestellten Sicherheitsanforderungen auch tatsächlich zu erfüllen. Je größer somit das Vertrauen, desto größer ist auch die Prüftiefe und somit

[165] Vgl. Fox, Dirk, Schutzprofile – Protection Profiles, In: Datenschutz und Datensicherheit, Abrufbar im Internet, https://www.secorvo.de/publikationen/schutzprofile-protection-profiles-fox-2011.pdf8/2011, S. 570.
[166] Stumpf, Michael, Toolunterstützte Zertifizierung auf Basis der Common Criteria, Abrufbar im Internet, http://www.petrastumpf.de/michael/Wissen/CommonCriteria.pdf, 2005, S. 17.
[167] Vgl. Herrmann, Debra S., Using the common criteria for IT security evaluation, 2003, S. 12 ff.

der Prüfaufwand. Bewertet wird nach Vertrauenswürdigkeitsstufen von EAL (Evaluation Assurance Levels) 1-7 mit aufsteigender Tendenz.[168]

Für die standardisierte Vorgabe von gleichen Voraussetzungen ist es auch möglich, die funktionalen Sicherheitsanforderungen für eine ganze Produktvariante zu erstellen, da die PP nicht konkret für implementierte Sicherheitsfunktionen in einem IT-Produkt gelten. Für eine internationale CC-Anerkennung ist die ISO/IEC 15408 verabschiedet worden, die so einen akzeptierten und anerkannten Status erreicht.

Bei der CEM (Common Methodology for Information Technology Security Evaluation) handelt es sich vereinfacht um eine Art „Prüfanweisung". Hier ist festgelegt, wie geprüft werden sollte. Ziel ist es hierbei, u. a. die Evaluierungen mit einem koordinierten Vorgehen durchführen zu können. Zusätzlich ist sie Vorgabe für die internationale Anerkennung von CC-Ergebnissen.[169] Die mit einer CC-Evaluierung einhergehenden Kosten sind nicht unerheblich. Es sind hier für eine hohe Vertrauenswürdigkeit entsprechende Prüftiefen und Aufwände zu kalkulieren. Besonders kleinere Unternehmen mit eingeschränkter Liquidität, in welchen der finanzielle Rückfluss über das Produkt nicht eindeutig ist, sehen die CC nur beschränkt als eine Alternative üblicher Zertifizierungsverfahren.[170]

4.1.3 BSI-Grundschutzkatalog

Das Bundesamt für Sicherheit in der Informationstechnik hat mit der Herausgabe der IT-Grundschutzkataloge ein umfassendes Werk zum Schutz von IT-Infrastrukturen geliefert. Über die letzten Jahre hinweg konnte sich so das BSI zu einer unabhängigen Stelle für Fragen in der Informationstechnik etablieren und wird in der Bevölkerung auch als seriös und kompetent wahrgenommen. Für den praktischen Gebrauch liefert der Grundschutzkatalog sinnvolle und angemessene Vorgehensweisen für den Schutz von Informationstechnik. Die Erklärungen des Grundschutzkataloges sind in der umfangreichen BSI Standard-100-Reihe aufgeführt[171]:

-**BSI-Standard 100-1:** Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS); stellt die grundsätzlichen Prinzipien eines ISMS dar und erläutert deren Wirkungsweise auf ein Gesamtsystem.

-**BSI-Standard 100-2:** Vorgehensweise des IT-Grundschutzes; die logische Anwendung der Methodik in Kombination mit der Abbildung des IT-Systems, den daraus resultierenden Gefährdungen und nötigen Maßnahmen. In Folge wird hier der schrittweise Aufbau einer IT-Sicherheitsarchitektur nach dem BSI erläutert.

-**BSI-Standard 100-3:** Risikoanalyse auf Basis des IT-Grundschutzes; die Risikoanalyse baut auf vordefinierte Gefährdungen und Maßnahmen aus dem Grundschutzkatalog des BSI auf.

-**BSI-Standard 100-4:** Notfallmanagement: Ergänzt um den kontinuierlichen und sicheren Betrieb eines Notfallmanagements. Prinzipien aus den schon genannten Standards werden berücksichtigt und stellen eine folgerichtige Ergänzung im Sinne des betrieblichen Kontinuitätsmanagements bei.

In Anwendung des Grundschutzhandbuches folgt das Sicherheitsmanagement dem in Abbildung 21 dargestellten Prozess.

[168] Vgl. BSI, Workshop Common Criteria 3.1, 2015, Kap. 5, Folie 4 ff.
[169] Vgl. ebd., Kap. 8, Folie 2.
[170] Vgl. Stumpf, Michael, Toolunterstützte Zertifizierung auf Basis der Common Criteria, Abrufbar im Internet, http://www.petrastumpf.de/michael/Wissen/CommonCriteria.pdf, 2005, S. 56.
[171] Vgl. Müller, Klaus-Rainer, IT-Sicherheit mit System, 2014, S. 45 ff.

Abbildung 21: Sicherheitsmanagement nach Grundschutz[172]

Ein wesentlicher Vorteil der Grundschutzkataloge ist die u. a. vereinfachte Form der Risikoanalyse, da hier keine Wahrscheinlichkeiten festgelegt werden müssen, sondern diese schon im Vorfeld bewertet sind[173]. Dadurch können innerhalb der Use Cases schon sinnvolle Gefährdungen und Maßnahmen angenommen werden; was für die generalistische Bearbeitung und Umsetzung für alle Branchen und Unternehmensgrößen, insbesondere kleine und mittlere Unternehmen mit wenig Ressourcen, vorteilhaft ist[174]. Zur Nachbildung des IT-Systems bestehen folgende fünf Bausteine (B): Übergreifende Aspekte der Informationssicherheit (B1), Sicherheit der Infrastruktur (B2), Sicherheit der IT-Systeme (B3), Sicherheit in Netzen (B4) und Sicherheit in Anwendungen (B5) [175]. Resultierend daraus ergeben sich die Gefährdungskataloge mit sechs Kategorien: elementare Gefährdungen (G0), höhere Gewalt (G1), organisatorische Mängel (G2), menschliche Fehlhandlungen (G3), technisches Versagen (G4) und vorsätzliche Handlungen (G5)[176]. Im Abschluss werden die empfohlenen Maßnahmen in sechs Kategorien eingeteilt: Infrastruktur (M1), Organisation (M2), Personal (M3), Hard- und Software (M4), Kommunikation (M5) und Notfallvorsorge (M6)[177]. Jede angeführte Hauptkategorie der Kataloge enthält eine große Anzahl an Unterkategorien, die an die jeweiligen Anwendungsszenarien angepasst sind. Auf diesem Wege ergeben sich schnelle und relativ leichte Abhängigkeiten, die mit konkreten Handlungsempfehlungen für die Praxis hinterlegt sind.

Für eine nationale Anerkennung und Zertifizierung nach den Grundprinzipien des Grundschutzkatalogs besteht eine entsprechende Nähe zur ISO 27001[178]. Für die internationale Reputation des Modells entstand die ISO/IEC 27001[179].

In regelmäßigen Überarbeitungen wird der Grundschutzkatalog an die gegenwärtigen technischen Bedingungen angepasst und erweitert. So sind die Kataloge (Bausteine, Gefährdungen und Maßnahmen) mit einer entsprechenden Reaktionszeit aktuell und relevant.

4.1.4 Kurze Gegenüberstellung CC und 27001 Basis-BSI-Grundschutz

Für eine kurze Zusammenfassung der erläuterten Eckpunkte von CC und der ISO 27001 auf Basis des BSI-Grundschutzes dient die nachfolgende Tabelle 6.

[172] Vgl. Federrath, Hannes, IT-Sicherheitsmanagement nach ISO 17799 und nach BSI-Grundschutzhandbuch, Abrufbar im Internet, https://epub.uni-regensburg.de/7472/1/2004-06-23IT-Security-Messe.pdf, 2004, Folie 4.
[173] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014, S. 69.
[174] Vgl. Kardel, Danilo, IT-Sicherheitsmanagement in KMU, Abrufbar im Internet, https://link.springer.com/content/pdf/10.1007%2FBF03340623.pdf, 2011, S. 48.
[175] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014, S. 70.
[176] Vgl. ebd., S. 71.
[177] Vgl. ebd., S. 70.
[178] Vgl. Kersten, Heinrich / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 2013, S. 15.
[179] Vgl. Maier, Joern, Zeit für Erneuerung, In: kes, 08/2015, S. 5.

	ISO 27001 (mit/ohne Basis-BSI-Grundschutz)	Common Criteria
Anwendung	Komplettes Unternehmen	Begrenzt auf technische Produkte, kein Management-System.
Aufwand	Umfangreicher Aufwand für die Modellierung und das Hinzuziehen von externen Beratern erscheint sinnvoll.	Hoher formaler und zeitlicher Aufwand.
Reputation	In Deutschland hoch.	Hohe Anerkennung auch international, Anerkennung höherer EAL-Stufen international schwierig.
Nutzen	Erfüllt Forderungen aus Basel II/III, international eher eingeschränkt (mit Basis-BSI-Grundschutz).	Zunehmende Forderung bei Beschaffungen, setzt Standards und senkt dadurch eigene Analyseaufwände.
Kosten	20.000<x<100.000 € (Zertifizierung)	20.000<x>100.000 € (+ Zertifizierung)

Tabelle 6: Übersicht CC und ISO 27001 Basis BSI Grundschutz[180]

Sinnvoller erscheint eine Zertifizierung nach ISO 27001 ohne Basis BSI-Grundschutz, da sich hier ohne Referenz des nationalen Hinweises eine international höhere Anerkennung ergibt. Aus diesem Grund (u. a.) scheinen Zertifizierungen auf Basis des BSI-Grundschutzes nicht mehr sinnvoll und zweckdienlich.

4.2 Branchenspezifische Normen und Richtlinien

Die gängigen Normen aus dem Bereich der Schloss- und Beschlagindustrie haben großen Einfluss auf die zukünftigen Entwicklungen. Durch die starke Normung und Reglementierung in diesem Bereich haben sich feste Routinen verstetigt, die die Etablierung von neuen Technologien schwierig macht respektive den bewährten Anbietern erschwert, ihre „ausgefahrenen" Wege zu verlassen. Ein Auszug der Normen und Richtlinien, die als Gegenstand zur Analyse herangezogen wurden, sind in den kommenden Unterkapiteln erläutert.

4.2.1 Auszug deutscher / europäischer Normen und Richtlinien für mechanische Schließzylinder

Im mechanischen Bereich der Schließzylinder gilt die DIN EN 1303[181] als die Basisnorm. Sie stellt die grundlegendsten Anforderungen an einen mechanischen Türschließzylinder. Hier finden sich die Kategorien Anforderungen, Verschlusssicherheit, Angriffswiderstand, Prüfverfahren und Klassifikation wieder. Weiterhin eignet sich die besagte Norm für einen weiteren Einblick in Mindestanforderungen an Türschließzylinder. Als Beispiel müssen Höchstdrehmomente beim Betätigen des eingeführten Schlüssels erreicht werden, Dauerhaftigkeiten für Schließzyklen, Temperaturbeständigkeiten, Widerstandsangaben für mechanische Angriffe etc. Für reproduzierbare Prüfergebnisse sind auch die Prüfanforderungen und Prüfaufbauten genauestens beschrieben.

Auf die Grundlage der DIN EN 1303[182] setzt die DIN 18252[183] für Profilzylinder in Türschlössern auf. Nähere Spezifikationen zum Stiftzylinder wie beispielsweise Bauformen, Bemaßungen, Bauteilbenennungen, konkretere Schließanlagenfunktionalitäten etc. sind Gegenstand der

[180] Modifiziert nach: Vgl. Kersten, Heinrich / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 2013, S. 16 f.
[181] DIN EN 1303, Baubeschläge - Schließzylinder für Schlösser, 2005.
[182] Ebd.
[183] DIN 18252, Profilzylinder für Türschlösser, 2006.

Beschreibungen und Bedingungen. Generell wird detaillierter auf die Voraussetzungen in einer Schließanlage eingegangen.

Schließzylinder mit Einzelsperrschließung beschreibt die VdS 2156-1[184]. Unabhängig von weiteren Prüfkriterien wird genauer auf den Widerstand von Aufsperrversuchen eingegangen. Bestätigt wird sie mit den Klassen A, AZ, B und BZ. Eine hohe Sicherheit, so schreibt es die Richtlinie vor, kann aber generell nur mit der mechanischen und elektrischen Kombination erreicht werden. Inhalte der aufgeführten Normungen und der Richtlinie sind im Anhang (Tabelle 23, Tabelle 24 und Tabelle 25) verkürzt dargestellt.

Der normative Aufbau kann vereinfacht angenommen werden (siehe Abbildung 22).

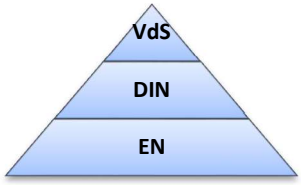


Abbildung 22: Kriterienverschärfung Normen/Richtlinien[185]

Bei Sichtung der genannten Normen und Richtlinien lassen sich starre Formalien erkennen. Es wird eine schlichte Abarbeitung der Prüfkriterien vollzogen, die keinerlei Handlungsspielraum oder Freiheiten für Anpassungen lässt. Auch erlaubt das Vorgehen keine Erweiterungen bei technologischen Entwicklungen. Lediglich die VdS-Richtlinie geht in Teilen auf die Montage vor Ort an der Tür ein. So muss z.B. ein Hinweis dem Monteur vor Ort aufzeigen, dass der zertifizierte Schließzylinder mit einem einbruchhemmenden Türschild verbaut werden muss. So bleibt es allerdings fragwürdig, ob u. a. die Auseinandersetzung mit der Montageanleitung die Erwartungen des Kunden an einen sicheren Schließzylinder befriedigt. Die Klassifizierungen, mit denen die mechanischen Schließzylinder ihren Erfüllungsgrad gegenüber der Norm oder Richtlinie bestätigen, geben keinen sofortigen Eindruck, ob der vorliegende Zylinder für den individuellen Einsatz geeignet ist. Erst mit dem Hintergrund der Normen oder Richtlinien kann die Legende aufgelöst und der optimale Einsatzzweck bestimmt werden. Die wichtigen Widerstandsfähigkeiten eines mechanischen Zylinders sind auch auf einen mechanischen Modus Operandi zurückzuführen. Sowohl in den Normen als auch in den Richtlinien sind Angriffe, wie z. B. das Aufbohren oder Abdrehen des Profilzylinders oder auch Angriffe durch Meißel bzw. mithilfe einer Bohrmaschine erwähnt. Für den Bereich der sicheren Auslegung der Konstruktion (safety) wird eine solide Basis mit den Vorgaben an Dauerhaftigkeit, Nachschließsicherheit, Feuerwiderstand etc. geliefert. Die beschriebenen Formalkriterien für einen mechanischen Schließzylinder können als ausreichend und sinnvoll erachtet werden und stellen eine gute Grundlage für weitere Betrachtungen dar.

4.2.2 Auszug deutscher / europäischer Normen und Richtlinien für mechatronische Schließzylinder

Grundlage für Zertifizierungen von mechatronischen Schließzylindern ist DIN EN 15684[186] - Mechatronische Schließzylinder - Anforderungen und Prüfverfahren. Die Norm prüft in den Bereichen Gebrauchskategorie, Umweltbeständigkeit, Verschlusssicherheit und Systemmanagement verschiedenste Ansprüche. Auffallend dabei ist der hohe mechanische Anteil, der nahezu alle einschlägigen mechanischen Normen/Richtlinien widerspiegelt. Natürlich hängt in einem wesentlichen Maße die Leistungsfähigkeit des Zylinders auch von seiner mechanischen Robustheit und Konstruktion ab. Jedoch müssen für eine ganzheitliche systemische Betrachtung auch Security-Aspekte berücksichtigt werden; und gerade geltende Normen/Richtlinien sollten zumindest ein solides Fundament liefern. Leider wird die Norm diesem Anspruch nicht gerecht. Den Verfassern genügt die Prüfung der Anforderungen hinsichtlich elektrostatischer Entladung, der Mindestanzahl der elektrischen Codes sowie verschiedener Angriffe mit überhöhter Spannung,

[184] VdS 2156-1, Schließzylinder mit Sperrschließung, 2012.
[185] Eigene Darstellung.
[186] DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013.

elektrischer Spannung/Entladung und Magnetfeldern. Es findet sich kein Hinweis, wie IT-Security in das Produkt integriert werden sollte, und konkrete Verschlüsselungsanforderungen fehlen. Die ist für eine geltende Norm im Bereich eines Sicherheitsproduktes auf elektronischer Basis absolut unzureichend.

Auch die Richtlinie des VdS 2156-2[187] Schließzylinder mit Einzelsperrschließung, Teil 2, ist hier unzureichend: Elektronische Schließzylinder geben keinen konkreten Hinweis auf Anforderungen der IT-Security. Wie schon in der DIN EN 15684[188] beschränken sich die elektronischen Voraussetzungen auf ein sehr rudimentäres Anforderungsprofil. Zwar weisen einzelne Kategorien erhöhte Anforderungen auf, jedoch nur bei den absoluten Grundlagen der elektromagnetischen Einflüsse, der physikalischen Einflüsse und bei den konstruktiven Anforderungen, wie z. B. Hintergrundspeicher, Sperrzustände, Übertragung von Codes, etc. Abschließend verbleibt auch hier der Eindruck, dass gängige IT-Security-Vorgaben oder -Hinweise fehlen.

Den richtigen Ansatz verfolgt die technische Richtlinie vom BSI (BSI - TL 03405[189]) mit den Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme. Der Verweis auf übliche IT-Security Maßnahmen ist hier gut dargestellt und konkret in verschiedenen Kategorien zu erkennen. So müssen die Codeträger benannter Systeme einen Schutz gegen Replay-Attacken aufweisen. Bei erhöhtem Schutzbedarf ist eine 3DES-Verschlüsselung respektive eine AES-Verschlüsselung gefordert sowie der Einsatz von zertifizierten Produkten nach CC mit dem Vertrauenslevel von mindestens EAL-3. Generell erfüllt die technische Richtlinie die gestellten Anforderungen: Alle relevanten Themenfelder für eine ganzheitliche Betrachtung werden abgedeckt mit dem Ziel der Vertrauensbildung; die Entwicklung eines dem Stand der Technik entsprechend zertifizierten und geprüften Produkts. Inhalte der aufgeführten Normung und der Richtlinien sind im Anhang (Tabelle 26, Tabelle 27 und Tabelle 28) verkürzt dargestellt.

Abschließend kann festgehalten werden, dass die derzeitig verfügbaren Normungen und Richtlinien in dem Bereich der mechatronischen Schließzylinder ein gutes mechanisches Anforderungsprofil bieten aber keine ausreichenden Forderungen an die IT-Security stellen und somit nicht auf die derzeitige Bedrohungslage von IT-Systemen eingehen und einen sinnvollen Beitrag zum Schutz leisten. Dies belegt Abbildung 23: Mechanische Forderungen in DIN EN 15684[190] überwiegen deutlich; VdS 2156-2[191] beschreibt nur elektrische Anforderungen aber keine IT-Security.

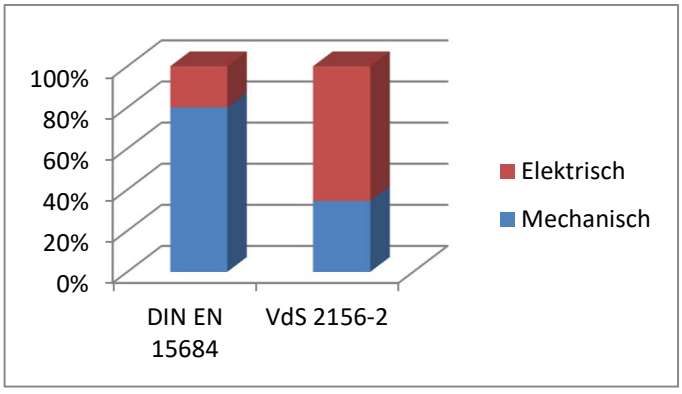


Abbildung 23: Auswertung DIN EN 15684 und VdS 2156-2[192]

[187] VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013.
[188] DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013.
[189] BSI – TL 03405, Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme, 2010.
[190] DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013.
[191] VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013.
[192] Eigene Darstellung.

5 Kreationsprozess der ganzheitlichen Sicherheitsbewertung

Das 5. Kapitel soll einen holistischen Ansatz zur Sicherheitsbewertung von Mobile Access Systemen liefern. Nachdem in den vorherigen Kapiteln die in Relation stehenden Themenbereiche behandelt wurden, soll nun mit der Darstellung einzelner Spezifika das Vorgehen der Sicherheitsbewertung erarbeitet werden. Grundlage der Sicherheitsbewertung war das vorherige Aufstellen von methodischen Zielen. Es sollte so ohne Präferenz innerhalb bestehender Methodiken und Vorgehensweisen sichergestellt werden, dass sich ein möglichst optimales Vorgehen ableiten lässt. Da die Produkte der Schloss- und Beschlagindustrie den dort geltenden Gesetzmäßigkeiten folgen, sind die bestehenden Verfahren, z. B. der Normung, zur Sicherheitsbestimmung notwendig. Gleichzeitig sind so auch inhaltliche Differenzen und Unvollständigkeiten sichtbar geworden, die wiederum ergänzend aufgenommen werden sollten. Der technologische Fortschritt wird sich auch zukünftig nicht aufhalten lassen und an Tempo zunehmen. Dies erfordert eine gewisse Flexibilität in der Sicherheitsbewertung, um das Verfahren adaptiv zu gestalten.

Hersteller und Interessensverbände sollten das gemeinsame Ziel verfolgen, ihre Sicherheitsprodukte mit einem adäquaten Bewertungsschema überprüfen zu lassen. Dies trägt auch dem geänderten Kundenverhalten Rechnung: ein blindes Vertrauen in die Expertise der Hersteller gehört längst der Vergangenheit an. Auch überprüfen immer mehr unabhängige Tester, insbesondere aus dem Bereich der IT-Security, verschiedenste Produkte überaus genau. Ein Reputationsverlust wäre hier existenzbedrohlich. Nicht nur die Produkte sollen in heutiger Zeit intelligent und „smart" sein, sondern auch die Bewertungen. Das Festhalten an starren und alt hergebrachten und unflexiblen Bewertungen kennzeichnet hier oft gestriges Gedankengut.

Die Inhalte des 5. Kapitels lassen sich aus dem Kreationsprozess, wie in Abbildung 24 dargestellt entnehmen.

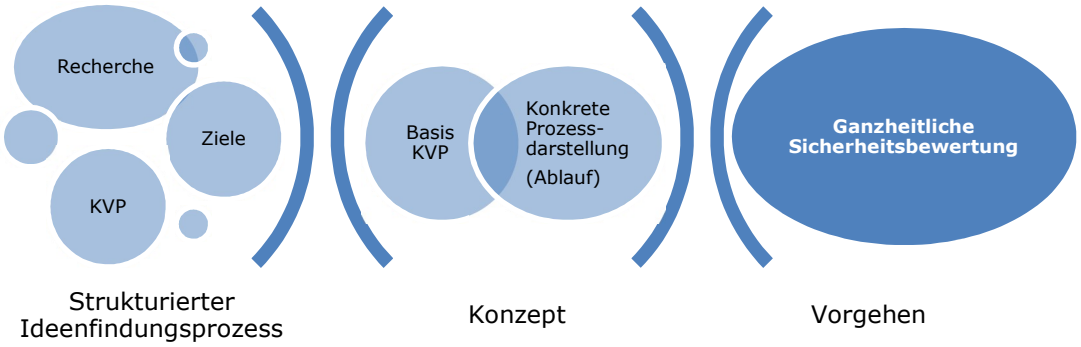


Abbildung 24: Kreationsprozess der ganzheitlichen Sicherheitsbewertung[193]

5.1 Ziele und Ideenfindung

Wichtig bei der Ideenfindung war die Vorgabe konkreter Ziele und Nicht-Ziele. Sie bildeten den Rahmen für die ersten hier dargestellten Überlegungen. Da sich das Themenfeld der Sicherheitsbewertung für Mobile Access-Systeme aus stark differierenden Schwerpunkten wie z. B. Mechanik und Elektronik, Einbruchschutz und IT-Security, traditionelles Geschäft und moderne Geschäftsmodelle etc. zusammensetzt, musste ein möglichst hoher Abstraktionsgrad gewählt werden. Eine umfangreiche Literatur und Marktrecherche sicherten dabei einen professionellen Fokus auf das Wesentliche. Schwachstellen und Auffälligkeiten konnten daher in der Vorbereitung zu diesem Thema als Ausgangsbasis für erste Erkenntnisse dienen.

Wie schon mehrfach angedeutet, dienten die gängigen Normungsverfahren als Ausgangslage für eine neue Bewertungsmethodik. Aufgrund steigender Akzeptanz für Mobile Access-Systeme, die eine Zutrittsgewährung mittels Smartphone ermöglichen, hätte eigentlich mit der Marktreife erster

[193] Eigene Darstellung.

Produkte in diesem Marktsegment auch sofort die Anwendung neuer Normungen bzw. Richtlinien in Kraft treten müssen. Da es hier einen relevanten Nachholbedarf gibt, erscheint die Beschäftigung mit diesem Themenbereich notwendig.

Der Forschungsschwerpunkt dieser Arbeit fokussiert demzufolge auf der Ergänzung bestehender Bewertungsmethoden um Aspekte der IT-Security im Rahmen einer adäquaten Systematik. Diese sollten eine logische Vorgehensweise sicherstellen, die eine Anpassung innerhalb festgesetzter Rahmenkriterien ermöglicht. Herrschende Einsatzbedingungen können es ggf. als sinnvoll erscheinen lassen, dass gewisse Teile der Sicherheitsbewertung skalierbar sind. Dies ist konträr zu den üblichen Normungen, die die Abarbeitung immer gleicher Prüfkriterien fordern. Auch finden sich auf dem Gebiet der Zertifizierungen nach entsprechenden Normen oder Richtlinien ausschließlich dieselben Institutionen. Doch gerade hier müssten auch weiterführende Marktbegleiter zur Zertifizierung einen gewissen Stellenwert haben. Dies ist nicht der Fall. Auch wenn nachweislich die Inhalte der Zertifizierungen nicht als vollständig bezeichnet werden können, so findet sich in den entsprechenden Institutionen keine Bereitschaft, darauf einzugehen. Nicht erst mit der Einbindung des Smartphones in die Zutrittssysteme spielt das Verschlüsseln oder das Verarbeiten sensibler Daten eine wichtige Rolle. Sinnvolle Hinweise sind hierzu aber nicht aufgeführt. Weiterhin fehlen den Ergebnissen von Zertifizierungen auf Basis der Normung Hinweise für adäquate Verbesserungsmaßnahmen. Ansonsten könnte der Kunde im Detail selbst entscheiden, ob die erbrachten Produktleistungen mit seinem Anforderungsprofil übereinstimmen. Zusätzlich ist es nach jetzigem Stand nicht darstellbar, Produkte anhand der Zertifizierungsergebnisse miteinander zu vergleichen. Der Entscheidungsprozess wird somit deutlich erschwert, da sinnvoll zu erzielende Ergebnisse nicht zur Verfügung stehen. Nur einige dieser Ausführungen machen klar, dass sehr wohl ein standardisiertes Verfahren zur Bewertung von Produkten reproduzierbare Ergebnisse liefern kann. Jedoch darf der Standard nicht soweit eingegrenzt sein, dass der Standardisierungsgedanke die Attribute des Verfahrens und die des Produktes so kleinteilig behandelt, dass sinnvolle Erkenntnisse nicht mehr erkennbar sind. Im Resultat muss auf eine ausgewogene Balance zwischen Standardisierung und Flexibilisierung im Sinne der Ergebnisdarstellung geachtet werden. Gerade auch die Ergebnisdarstellung sollte insoweit aussagekräftig sein, dass das Resultat der Überprüfung eindeutig eingeordnet werden kann und mit ähnlichen Produkttypen vergleichbar ist. Falls Zwischenergebnisse für einzelne Themen- oder Funktionsbereiche von Relevanz sind, muss die formale Durchführung auch Zwischenergebnisse zur Verfügung stellen. Zusammenfassend kann an dieser Stelle die Formulierung konkreter Ziele für eine holistische Sicherheitsbewertung im Bereich Mobile Access stattfinden (siehe Tabelle 7):

Ziele	Nicht-Ziele
Integration bewährter Normungen	Stark abstrahierte Ansätze zur Sicherheitsbewertung
IT-Security Aspekte integrieren	Komplizierte und (zum Teil) nicht selbsterklärende Methodik
Anpassbar an technologische Entwicklungen	Auf einzelne Themenschwerpunkte stark konzentrierte Bewertung
Verständliche und detaillierte Ergebnisdarstellung für Hersteller und Kunden	Irreführende Ergebnisse
Anwendbar; praktikables Vorgehen	

Tabelle 7: Ziele und Nicht-Ziele[194]

Diese fünf Punkte (Ziele) kennzeichnen die Eckpunkte des Arbeitsraumes der Bewertungsmethodik, die es zu erfüllen gilt.

[194] Eigene Darstellung.

Selbstverständlich baut die gesamte Überprüfung der Sicherheitsbewertung auch auf einer entsprechenden Expertise des Prüfers auf. Dieser Sachverhält kann nur bedingt durch ein methodisches und verständliches Vorgehen beeinflusst werden. Um optimale Ergebnisse zu erreichen, können Arbeitsgruppen einberufen werden, die sich gegenseitig positiv beeinflussen. Eine Überprüfung findet demnach immer unter der Mitwirkung von zwei Parteien statt: einer externen Arbeitsgruppe, die die Überprüfung durchführen möchte, und einem internen Ansprechpartner, der das zu überprüfende Produkt herstellt oder vertreibt, d. h. einem „Insider" mit Hintergrundwissen zum Produkt. Es soll hier insbesondere auf den Punkt fünf der oben genannten Ziele eingegangen werden. Es muss für eine ausgebildete Fachkraft mit entsprechender Einweisung möglich sein, eine verlässliche Sicherheitsbewertung durchzuführen. Die Gruppendynamik soll dabei punktuell fachliches Nicht-Wissen kompensieren und ein Wechselspiel von Anforderungen seitens der Methodik (externe Arbeitsgruppe) an die Adresse des Herstellers (interner Ansprechpartner) richten.

Orientierung findet die prinzipielle Struktur der Sicherheitsbewertung durch den KVP-Kreislauf. Die Eingangserklärungen enthalten bereits eine grobe thematische Einordnung des Themas; es konnte hier aufgezeigt werden, dass das Prinzip nicht nur in der Produktion angewendet wird. Die besondere Eignung stellt sich u. a. in einer generalistischen Einsatzmöglichkeit dar. So kennzeichnen die vier Phasen Plan-Do-Check-Act unmissverständlich den Status des Vorganges. Da es sich im klassischen Sinne um einen Kreislauf handelt, der bei Nicht-Erreichen der aufgestellten Ziele den erneuten Wiederbeginn fordert, geht das Prinzip von einer stetigen Verbesserung des Anwendungsfeldes aus. Dies ist bei einer einmaligen und abschließenden Sicherheitsbewertung nicht zielführend. Vielmehr wird hier der Kreislauf in ein Wasserfallmodell überführt, um die einzelnen Phasen aufbauend und teilweise parallel final zu bearbeiten. Der Prozess der Sicherheitsbewertung beginnt mit dem „Plan" und schließt mit „Act" ab; er findet dort seine differenzierte Ergebnisdarstellung. Vereinfacht ist dies in Abbildung 25 dargestellt.

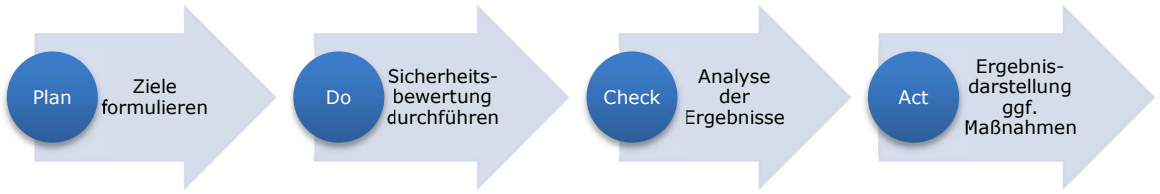


Abbildung 25: Sicherheitsbewertung auf PDCA-Basis[195]

Ein in dieser Arbeit mehrfach angedeuteter Kritikpunkt bei bestehenden Normen im Bereich der mechatronischen Schließsysteme war die nicht betrachtete Einsatzumgebung, in der sich das System befand. Dieser Sachverhalt sollte bei den Mobile-Access-Systemen ergänzt werden, um die Sicherheitsbewertung anforderungsgerecht an die herrschende Einsatzumgebung anzupassen. Aus dieser Anforderung könnten sich detaillierte Fragen in der Analyse ergeben, wie z. B. „Was genau sichert das Mobile Access-System ab? Welche potenzielle Gefahr ist gegeben? Welche Annahmen können in Bezug auf das Mobile Access-System getroffen werden?" Viele weiterführende Fragen schließen sich an und sollten Einfluss auf die Sicherheitsbewertung haben. Nicht zuletzt fördert dies den flexiblen Rahmen der Analyse und erfüllt Teile der aufgestellten Ziele.

Durch die Berücksichtigung von Einsatzbedingungen sollten sich auch Anforderungen an die Sicherheit ableiten lassen. Insbesondere die zu berücksichtigende IT-Security kann in der Umsetzung sehr verschiedene Implementierungsdetails enthalten. So sind bei umfangreichen Sicherheitsanforderungen auch aufwändige Implementierungen notwendig, die auf mechanischer Seite ggf. keinen so großen Entwicklungsaufwand bedeuten. Auch im Hinblick auf zusätzliche Hardware kann die IT-Security nicht immer einfach skalierbar sein. Für diesen Zweck eignet sich die Aufstellung eines Sicherheitsprofils (Soll-Profil) mit Kriterien, die sich an einer konkreten Prüfung orientieren. Im Sinne der praktischen Überprüfung bedeutet das ein gefordertes

[195] Eigene Darstellung.

Mindestmaß an Sicherheitskriterien, die praktisch zu erreichen sind. Aus dem Soll-Profil können sich im Späteren noch weitere Forderungen an die Prüfintensität ergeben; weiterhin lässt sich so die Sicherheitsbewertung zu einer Evaluierung konkretisieren, da es sich jetzt vielmehr um eine relative Prüfung an einer theoretischen Vorgabe, dem Soll-Profil, handelt.

Für die unabhängige Einschätzung der Sicherheitsbewertung sind Vorgaben in Form von konkreten Prüfkriterien am besten geeignet. Ähnlich bestehender Normen oder dem BSI-Grundschutz können dort in einem umfassenden Dokument alle Kriterien zur Prüfung zusammengefasst sein, d. h. einem sogenannten Kriterienkatalog. Dieser sollte sich aus Bedingungen des Soll-Profils ableiten und einheitlich mechanische und elektronische respektive IT-Security-Aspekte berücksichtigen.

Mit dem Ziel einer verständlichen und detaillierteren Ergebnisdarstellung muss eine Bewertungsmetrik gefunden werden, die alle Erkenntnisse der Sicherheitsbewertung einfließen lässt und abschließend die Evaluierung klar präsentiert. Hierbei soll das Ergebnis dem individuellen Anspruch von Hersteller und Kunde gerecht werden. Daher ist hier eine numerische und ggf. ergänzend farbliche Darstellung gewählt worden.

Diese ist in Abbildung 26 weiter detailliert und ausgeführt worden und stellt die Ausgangslage für das konkrete Vorgehen dar.

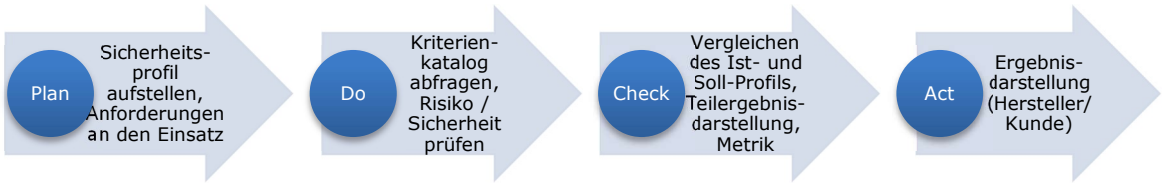


Abbildung 26: Konkretisierte Sicherheitsbewertung auf PDCA-Basis[196]

Wie in Abbildung 26 dargestellt, wird nachfolgend die PDCA-Basis weiter detailliert und mit einer konkreten Prozessdarstellung verbunden.

5.2 Konzept

Mit der Verbindung der ersten Ideen und der KVP-Philosophie konnte eine grobe Struktur erarbeitet werden, die als Ausgangspunkt für die Konkretisierung dient. Zwar befinden sich die PDCA-Schritte in der richtigen Reihenfolge, jedoch ist eine systematische Durchführung zum jetzigen Zeitpunkt noch nicht möglich. Auch fehlen bis dato noch die eigentlichen Inhalte zur Durchführung des Kriterienkatalogs mit einhergehender Bewertung des zugrundeliegenden Risikos.

Zusammengefasst ist bis jetzt die eigentliche Sicherheitsbewertung auf PDCA-Basis isoliert dargestellt und muss noch in einen Prozessablauf integriert werden. Demnach sollte die PDCA-Basis vorgelagerte und nachgelagerte Schritte aufweisen. Für ein besseres Verständnis können die in Abbildung 27 dargestellten Schritte im Sinne eines Prozessablaufes angenommen werden.

[196] Eigene Darstellung.

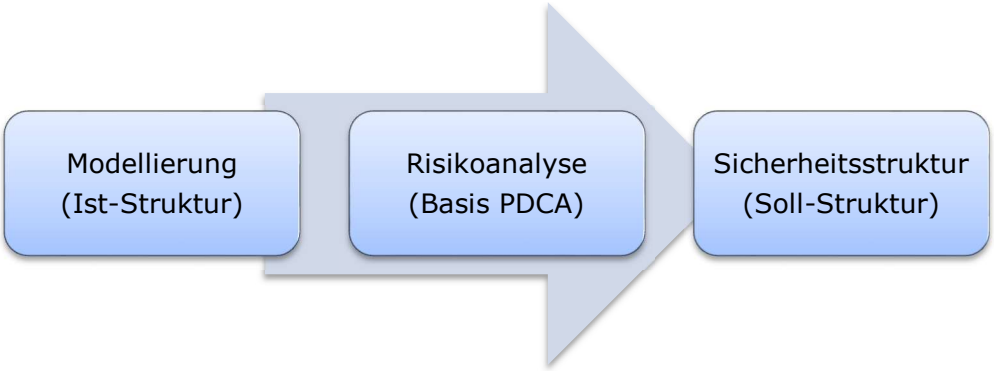


Abbildung 27: Grundkonzept der Prozessdarstellung (Sicherheitsbewertung)[197]

Mit der Eingliederung in eine Prozessdarstellung bezeichnet der vorgelagerte Schritt die Modellierung und der nachgelagerte Schritt die Sicherheitsstruktur. Für die Modellierung ist eine abstrakte Modellbildung angedacht, die es erlaubt, alle wesentlichen Merkmale und Eigenschaften des Mobile Access-Systems schematisch abzubilden. Damit kann sich die weitere Analyse auf wichtige Systemelemente beschränken und hängt im Wesentlichen nicht zu sehr von der speziellen Systemarchitektur ab. Wenn in den ersten Schritten der Analyse schon modellbildende Maßnahmen angestrebt werden, kann auch die eigentliche Risikoanalyse unabhängiger gestaltet und im Umkehrschluss auf eine breitere Systemlandschaft angewendet werden. Zusätzlich sind in der Modellierung Systemgrenzen gesetzt, um alle Elemente auszugrenzen, die nicht Gegenstand der Analyse werden sollen. Dieses Vorgehen unterstützt die Sicherheitsbewertung bei der Fokussierung und zwingt den Prüfer, sich nochmals genau mit dem zu begutachtenden System auseinanderzusetzen. Da dieser im Zweifel nicht genau wissen kann, wo das System zu welchen Bedingungen eingesetzt wird, können getroffene Annahmen dabei helfen, einen bindenden Rahmen zu setzen, der während der gesamten Sicherheitsbewertung Gültigkeit behält. Es bleibt die Überlegung, inwieweit die Bereiche IT-Security und Mechanik geprüft werden. Sind beide Bereiche in der Prüfung miteinander verwoben, dann ist die Konstruktion der Sicherheitsbewertung deutlich enger gefasst und an eine bestimmte Systemauslegung gebunden. Nur durch eine gewisse Trennung können auch artverwandte Mobile Access-Systeme dieser Prüfung unterzogen werden. Vorteile liegen dabei darin, dass die Prüfung nach einem Baukastenprinzip aufgebaut ist, was in der Folge Erweiterungsmöglichkeiten gewährleistet. Generell bietet sich bei der Modellierung die Anwendung einer visuellen Darstellungsform an. Mit abstrakten Symbolen oder kondensierter Schriftform können zentrale Informationen zur Weiterverarbeitung aufbereitet und strukturiert vorbereitet werden.

Zusammenfassend sind nochmal die wichtigsten Merkmale der Modellierung in Tabelle 8 dargestellt.

Merkmal	Ziel / Erklärung
Systembeschreibend	System erklären, Annahmen aufstellen und Verständnis fördern.
Abstrahieren	Fokussieren, Kondensieren und in Teilelemente zerlegen.
Systemgrenzen	Prüfumfang festlegen.
Prüftrennung IT-Security & Mechanik	Generalistisch und Erweiterungsmöglichkeit.

Tabelle 8: Merkmale der Modellierung[198]

Die Sicherheitsstruktur (siehe Abbildung 27) überlappt in größeren Teilen mit den Ergebnissen aus der Risikoanalyse auf PDCA-Basis. Daher bildet sie in Kombination mit der Modellierung, welche die Ist-Struktur abbildet, eine komplementäre Verbindung. Das bedeutet, dass die Soll-Struktur

[197] Eigene Darstellung.
[198] Eigene Darstellung.

(Sicherheitsstruktur) eine abschließende Aussage darüber zulässt, wie das Mobile Access-System bewertet wurde. Dies kann völlig unabhängig im Rahmen der Bewertung geschehen, insgesamt aber muss die Interpretation des Ergebnisses in Verbindung mit der Ist-Struktur fachlich (und vollständig) korrekt eingeordnet werden. Somit stellt die Sicherheitsstruktur einen eher argumentativ-theoretischen Schritt dar, der jedoch für das Verständnis entscheidend ist.

Ein möglicher Kunde oder Interessent des Produktes (Mobile Access) sieht zunächst nur das Ergebnis der Sicherheitsbewertung und könnte durch einen Vergleich mit weiteren Produkten, die gleichermaßen mit der hier dargestellten Sicherheitsbewertung geprüft worden sind, eine bewusste und informierte Kaufentscheidung treffen. Weiterführende und insbesondere für den Hersteller interessante Ergebnisse liefert die Sicherheitsstruktur, was zwingend eine Auseinandersetzung mit der Modellierung (Ist-Struktur) voraussetzt. Demnach führen eigentlich zwei Interpretationen aufgrund unterschiedlicher Detailtiefe zum gleichen Ergebnis.

Abschließend müssen große Teile der Inhalte aus der Risikoanalyse in die Sicherheitsstruktur übertragen werden, damit eine freie, d. h. absolute, Interpretation des Ergebnisses oder eine relative Interpretation im Zusammenhang mit der Modellierung ermöglicht wird. Bei diesem Schritt steht die Sensibilisierung von Ergebnissen im Vordergrund, d. h. es muss nach den entsprechenden Empfängern differenziert werden; wie hier angeführt, nach Kunde (Nutzer) und Hersteller. Beide Gruppen haben unterschiedliche Interessen zur Ergebnisverwertung. Entweder folgt eine reine Kaufentscheidung oder die Einleitung weiterführender Schritte zur Produktverbesserung. Zusammenfassend sind die Merkmale der Sicherheitsstruktur nochmals in Tabelle 9 aufgelistet.

Merkmal	Ziel / Erklärung
Ergebnisdarstellung	„Isoliert-einzelnes" Ergebnis, relatives Ergebnis
Interpretation	Einfach und erweitert
Maßnahmen	Detailliert und mit Bezug zur Modellierung

Tabelle 9: Merkmale der Sicherheitsstruktur[199]

In Anlehnung an Abbildung 27 ist das Grundkonzept zur Prozessdarstellung weiter zu detaillieren, um anwendbare Vorgänge zu bestimmen. Zwar würden die bis hierhin aufgestellten Ansätze für eine rein theoretische Beweisführung der Sicherheitsbewertung auf PDCA-Basis vermutlich annähernd genügen. Da sich die Evaluierung aber an einem methodischen Ansatz orientieren soll, sind in Abbildung 28 erstmals konkrete und aufbauende Arbeitsschritte benannt. Alle bis hierhin beschriebenen Erkenntnisse sind darin enthalten.

[199] Eigene Darstellung.

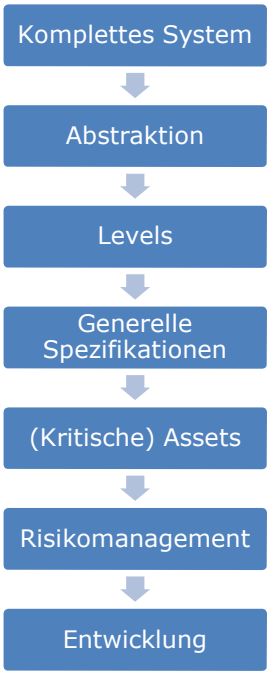


Abbildung 28: Ausdetailliertes Grundkonzept der Prozessdarstellung (Sicherheitsbewertung)[200]

Alle dargestellten Schritte in Abbildung 28 bauen aufeinander auf und benötigen jeweils die Ergebnisse oder Teilergebnisse des vorhergegangenen Schrittes. Damit wird eine konsekutiv aufgebaute Sicherheitsarchitektur gewährleistet. Erst mit dem Absolvieren jeder einzelnen Prozesskomponente wird ein brauchbares Ergebnis erarbeitet. Die Inhalte eines jeden Schrittes stehen für ein Arbeitspaket von einzelnen oder mehreren Aufgabenteilen (Abbildung 29).

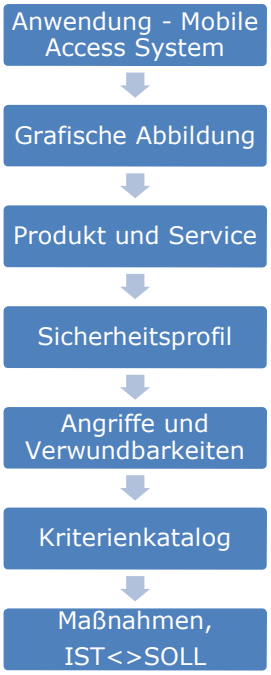


Abbildung 29: Arbeitspakete vom Grundkonzept der Prozessdarstellung (Sicherheitsbewertung)[201]

[200] Eigene Darstellung.
[201] Eigene Darstellung.

Die Erklärung zu den Arbeitspaketen ist wie folgt:

- Anwendung – Mobile Access-System: Um einen ersten Überblick zu erhalten, sollten alle Unterlagen und Dokumente des Systems gesichtet werden. Hier sind alle relevanten Spezifikationen und Leistungsdaten vermerkt. Insbesondere das bevorzugte Einsatzgebiet und die Zielgruppe können bei Vorseriensystemen von großer Bedeutung sein. Somit kann sich der Prüfer bereits über die eingesetzte Technologie informieren und erste Verständnisfragen notieren, die zu einem späteren Zeitpunkt wiederaufgenommen werden können.

- Grafische Abbildung: Zur Vorbereitung der Sicherheitsbewertung sollten die technologischen und anwendungsspezifischen Gegebenheiten in eine abstrakte Form überführt werden. Die Reduzierung auf die wichtigsten Merkmale hilft bei der Fokussierung darauf, was überprüft werden kann und soll. Unterstützend setzen die freiwählbaren Systemgrenzen konkret definierbare Grenzen.

- Produkt und Service: An diesem Punkt sollten die ersten beiden Schritte der Methode den Prüfer insoweit vorbereitet haben, als dass es ihm möglich erscheint, nun eine fachliche Trennung von mechanischer und elektronischer Seite vornehmen zu können, d. h. Systemkenntnisse sind hinlänglich vorhanden.

- Sicherheitsprofil: Wie schon in vorherigen Kapiteln erwähnt, steht hier die Evaluation im Vordergrund, da eine Sicherheitsbewertung mit der Prüfung von absoluter Sicherheit nicht möglich und realitätsfern erscheint. Im Umkehrschluss wird eine Referenz aufgestellt, die einen engen Bezug zu den vorherigen Schritten aufweist.

- Angriffe und Verwundbarkeiten: Bevor die eigentliche Sicherheitsbewertung durchgeführt wird, sollen hier die ganz spezifischen Angriffe und Vulnerabilitäten ermittelt werden, die eventuell nicht mit einem eher generalistischen Fragenkatalog gefunden werden können. Das freie und ungebundene Gedankenspiel soll hier im Vordergrund stehen, also auch Verwundbarkeiten, die nicht direkt erkennbar sind, berücksichtigen.

- Kriterienkatalog: Den Kern der Sicherheitsbewertung stellt der Kriterienkatalog dar, dessen Bestandteile aus unterschiedlichen Fachgebieten entstammen. Aufgrund der Trennung von Mechanik und Elektronik sollen hier beide Themen voneinander abhängig sein, d. h. das Sicherheitsniveau hat einen Bezug zur Mechanik und Elektronik.

- Maßnahmen: Im Ergebnis wird hier die Darstellung der Sicherheitsbewertung zusammengefasst und bei Bedarf sind detaillierte Zwischenergebnisse aus den vorherigen Schritten soweit finalisiert, dass sie einen Anspruch auf Vollständigkeit erheben können.

Alle bis hierhin geltenden Vorarbeiten fließen in die finale Erarbeitung der Sicherheitsbewertung für Mobile Access-Systeme ein.

5.3 Ganzheitliche Sicherheitsbewertung

5.3.1 Einleitung und Schritt „Plan"

Für den zielgerichteten Schritt der Sicherheitsbewertung müssen die Abbildung 27 und Abbildung 29 miteinander verbunden werden. Dies beinhaltet sowohl die zugrundeliegende PDCA-Vorgehensweise als auch die Prozessdarstellung für eine anwendbare Methodik. Da die Arbeitspakete beschrieben und in der Abfolge geregelt sind, müssen die Inhalte klar bestimmt und ausformuliert sein. Alle Detaillierungen dürfen nur im Rahmen der Ziele und Nicht-Ziele durchgeführt werden. Kombiniert mit Hinweisen zur Verständlichkeit stellt somit Abbildung 30 die finale Sicherheitsbewertung dar.

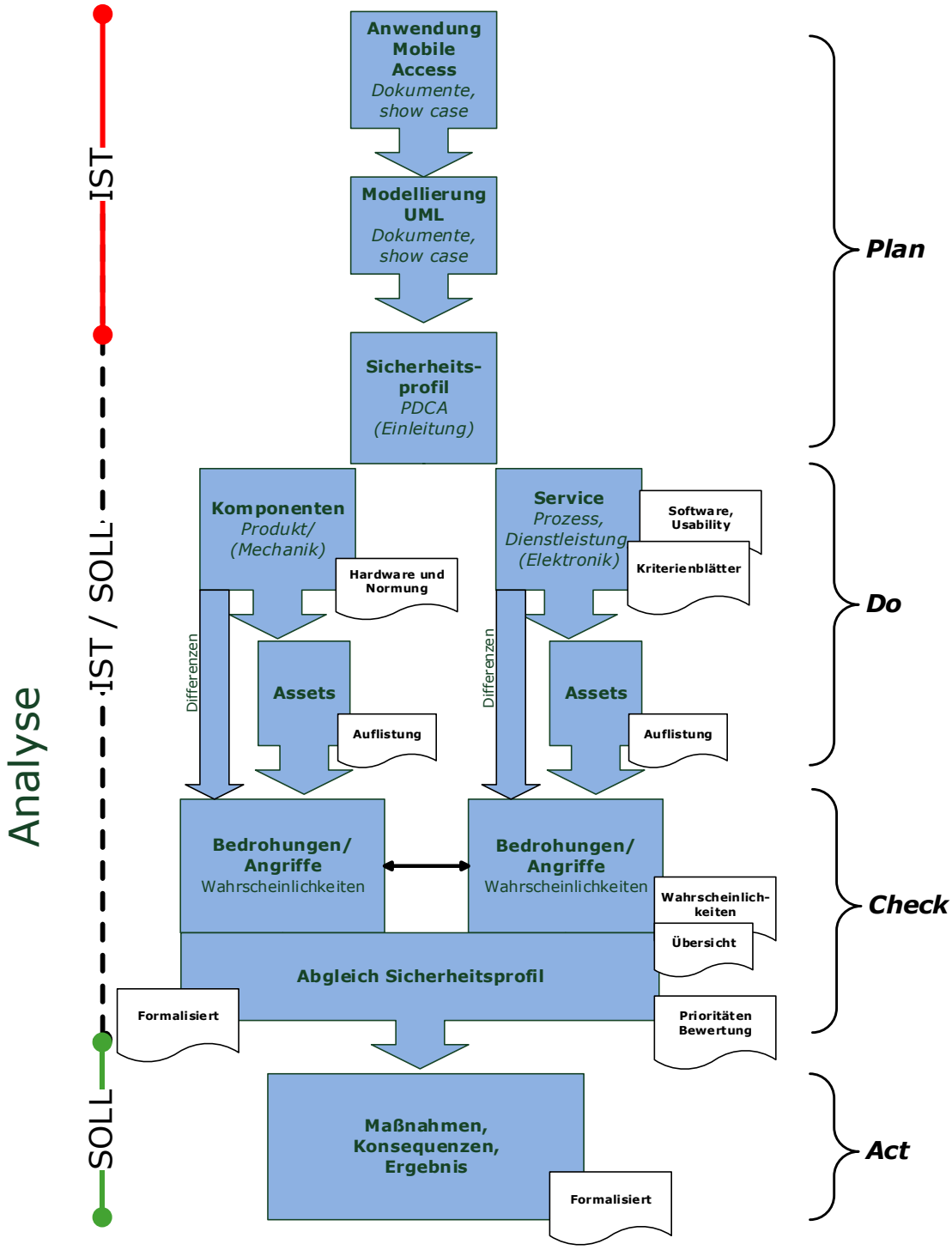


Abbildung 30: Ganzheitliche Sicherheitsbewertung[202]

Die drei einleitenden Schritte: Anwendung Mobile Access, Modellierung UML und Sicherheitsprofil sind schon ausführlich in den vorherigen Kapiteln beschrieben worden. Sie repräsentieren den reinen IST-Zustand und den IST-/SOLL-Zustand, der als Übergang definiert ist, d. h. im Übergangsbereich wird die dezidierte Sicherheitsanalyse durchgeführt. Somit bleiben bei den ersten drei Schritten auch die Arbeitspakete nahezu identisch, wie schon beschrieben. Begonen wird hier mit der vollständigen Zusammenführung aller Systemunterlagen im Schritt „Anwendung Mobile Access". Damit sind auch alle Mehrwertleistungen durch Servicedienste gemeint; vermutlich finden sich hier die größten Unterschiede bei einzelnen Systemen. Von besonderer Bedeutung kann hier das Anwendungsfeld sein, da es dem Prüfer einen Überblick zum eingesetzten Show Case gibt.

[202] Eigene Darstellung.

Diese Informationen werden zunächst stichpunktartig festgehalten. Für den nächsten Schritt Modellierung wird UML kondensiert und bereitgestellt. Sobald das System in die abstrakte Form mithilfe der UML-Notation überführt worden ist, hat der Prüfer an dieser Stelle die Möglichkeit, es kurz zu beschreiben respektive die spezielle UML-Notation sprachlich auszuführen. Empfehlenswert ist hier ein geeignetes Programm mit entsprechender UML-Sprache zur digitalen Umsetzung. Durch ihre verständliche graphische Notation ist die UML-Sprache das hier gewählte Mittel. Dies lässt eine praktikable Lösung im Sinne der Aufgabenstellung zu, d. h. Reduktion auf wesentliche Elemente; Bildung der Systemgrenze sowie Abstraktion der Hard- und Software-Elemente. Der Prüfer entscheidet an dieser Stelle selbst, welche Diagramme für die Umsetzung der UML-Modellierung adäquat sind. Ergänzt wird die Systemgrenze von einem tolerierbaren Rahmen, was die Annahmen bezüglich der drei Themenfelder Technik, Organisation und Personal angeht. Zur Überleitung in den Schritt Sicherheitsprofil auf PDCA-Basis werden beurteilende und für die Sicherheitsbewertung folgenreiche Entscheidungen getroffen. Da dies den Kern der Sicherheitsbewertung darstellt, gibt es dort ein gesondertes Formblatt, das explizit die Auswahlmöglichkeiten des Soll-Sicherheitsprofils beschreibt. Sprachlich äquivalent wäre auch die Möglichkeit, es mit einem eher theoretischen Sicherheitsprofil zu betiteln, d. h. das zu untersuchende Mobile Access-System wird mit bestimmten Attributen der Sicherheit belegt. Sie lassen sich aus den vorherigen Schritten ableiten und sollten Prüfern bzw. ggf. Herstellern eine Beantwortung der Frage „Welche Eigenschaften bezüglich Sicherheit soll mein System mindestens erfüllen?" ermöglichen. Bei Vorgabe des Herstellers, das System mit bestimmten Eigenschaften zu belegen, beeinflusst dieser den nachfolgenden Prüfumfang. Die Eigenschaften des theoretischen Sicherheitsprofils sind in vier Bereiche mit jeweiligen Unterkategorien unterteilt und in Tabelle 10 dargestellt. Für eine entsprechende Auswahl der Qualität der Ausprägung sind im Anhang (ab S. 102) die Unterkategorien weiter ausformuliert und definiert.

Bereiche (wählbares theoretisches Sicherheitsprofil)	**Normenvoraussetzung (ohne mechanischen Zylinder**	**Muss-Fragen**
Angreiferklasse		
Nicht vorhanden	-	0
Anwender	DIN EN 15684 (1) / DIN EN 1303	2
Fachspezialist	DIN EN 15684 (2) / DIN 18252 Klasse 82 (BZ)	3
Professioneller	VdS 2156-2 (1) / VdS 2156-1 B (SKG 3*)	4 (Alle)
Insider	VdS 2156-2 (2) / VdS 2156-1 BZ+ (SKG 3*)	5 (Zusatz)
Kompromittierung von sensiblen Daten		
Nicht vorhanden	-	0
Gefährdend	DIN EN 15684 (1) / DIN EN 1303	2
Möglich	DIN EN 15684 (2) / DIN 18252 Klasse 82 (BZ)	3
Unkritisch	VdS 2156-2 (1) / VdS 2156-1 B (SKG 3*)	4 (Alle)
Usability		
Nicht vorhanden	-	0
Service/Gerät funktionslos	DIN EN 15684 (1) / DIN EN 1303	2

Service oder Gerät funktionslos	DIN EN 15684 (2) / DIN 18252 Klasse 82 (BZ)	3
Eingeschränkt nutzbar	VdS 2156-2 (1) / VdS 2156-1 B (SKG 3*)	4 (Alle)
Nicht spürbar	VdS 2156-2 (2) / VdS 2156-1 BZ+ (SKG 3*)	5 (Zusatz)
Kriterienausprägung		
Nicht vorhanden	-	0
Gering	DIN EN 15684 (1) / DIN EN 1303	2
Basis	DIN EN 15684 (2) / DIN 18252 Klasse 82 (BZ)	3
Mittel	VdS 2156-2 (1) / VdS 2156-1 B (SKG 3*)	4 (Alle)
Stark	VdS 2156-2 (2) / VdS 2156-1 BZ+ (SKG 3*)	5 (Zusatz)

Tabelle 10: Theoretisches Sicherheitsprofil[203]

Für eine leichtere Zuordnung wird daraus ein Nummernschlüssel mit vier Stellen gebildet. Aus diesem Nummernschlüssel lassen sich die weiteren Anforderungen an den Umfang des Kriterienkataloges (Prüftiefe) und die mechanischen Voraussetzungen ableiten. Jeder der vier genannten Bereiche ist beschrieben und gibt die nötigen Anhaltspunkte zu einer validen und belastbaren Systemeinschätzung.

Als Beispiel nachfolgend das theoretische Sicherheitsprofil 2|3|2|4 (Tabelle 11):

Beispiel theoretische Sicherheitsprofil	**Normenvoraussetzung**	**Muss-Fragen**
Angreifer klasse: Anwender	DIN EN 15684 (1) / DIN EN 1303	2
Kompromittierung sensibler Daten: Möglich	DIN EN 15684 (2) / DIN 18252 Klasse 82 (BZ)	3
Usability: Service/Gerät funktionslos	DIN EN 15684 (1) / DIN EN 1303	2
Kriterienausprägung: Mittel	VdS 2156-2 (1) / VdS 2156 B (SKG 3*)	4 (Alle)

Tabelle 11: Beispiel theoretisches Sicherheitsprofil[204]

Der beispielhafte Zahlenschlüssel ist das Ergebnis des aufgestellten theoretischen Sicherheitsprofils und lässt eine Aussage über die Normenvoraussetzung und den Fragenumfang im Kriterienkatalog zu. Bei der Normenvoraussetzung sind sowohl die rein mechatronischen Knaufzylinder berücksichtigt aber auch die angesetzten motorischen Schließzylinder, die ggf. zur Außenseite einen mechanischen Schließzylinder benötigen. Daher muss auch der mechanische Schließzylinder eine entsprechende Normvoraussetzung erfüllen. Entscheidend für die Sicherheitsbewertung ist somit immer die Außenseite, d. h. die kritische Seite, die für mögliche Einbrecher sichtbar ist.

[203] Eigene Darstellung.
[204] Eigene Darstellung.

Unabhängig davon, ob es sich in dem Beispiel nun um einen Knaufzylinder oder auch um eine Kombination von einem mechatronischen mit einem mechanischen Schließzylinder handelt, muss bei der Normenvoraussetzung der entsprechende Normenteil aus dem mechanischen oder mechatronischen Bereich erfüllt werden. Generell gibt der Hersteller darüber Auskunft, welche Normung sein Produkt erfüllt. Da sich mit steigenden Anforderungen auch die Normenvoraussetzungen erhöhen, muss immer die höchste Norm erfüllt werden. In dem Beispiel wäre dies in dem Bereich Kriterienausprägung „Mittel" die VdS 2156-2 (1) / VdS 2156 B (SKG 3*). Hier wird auch gleich ein Sonderfall mit der SKG-Norm ersichtlich. Dabei handelt es sich um eine niederländische Normenvoraussetzung, die hier äquivalent zum VdS aufgestellt wurde. Bei einer weiteren Prüfung von Systemen, die eine ausländische Normung erfüllen und dabei eine Übereinstimmung mit inländischen Normung erkennen lassen, müssen die jeweiligen Anpassungen einmal vorab durchgeführt sein.

Die weiteren Schritte zur Sicherheitsbewertung laufen demnach immer im Vergleich zum theoretischen Sicherheitsprofil ab und gleichen daher einer Evaluierung. So wird ersichtlich, warum es nicht sinnvoll ist, eine absolute Sicherheit abzuprüfen, da herrschende Rahmenbedingungen durchaus Einfluss auf die benötigte Sicherheit haben und komplexe Technologiestrukturen dies verstärken können. Mit Abschluss des dritten Arbeitspaketes, wie in Abbildung 30 dargestellt, ist auch der Schritt „Plan", der die Ziele und Ausgangslage formuliert, erledigt.

5.3.2 Schritt „Do"

In Überleitung zum Schritt „Do" werden, wie in Abbildung 30 angedacht, die Bereiche Mechanik und Elektronik respektive IT-Security getrennt. Zugleich sind die Technologien in ihrer Wertung unterschiedlich betrachtet worden. Aufgrund der verstärkten Einbindung der IT-Security soll dieses Themenfeld primär stärker fokussiert und die Mechanik mit ihrer guten Ausgangsbasis als sekundärer Faktor betrachtet werden. Die Durchführung der eigentlichen Sicherheitsbewertung stellt den Analyseteil von Ist / Soll dar. Da das theoretische Sicherheitsprofil alle weiteren Schritte vorgibt, ist es ratsam, mit dem mechanischen Teil zu beginnen. Das erste Arbeitspaket „Komponenten" stellt sicher, dass der Prüfer sich über die tatsächlich erfüllte Normung ausreichend informiert. Stimmt die ausgewiesene Normung mit der Normenvoraussetzung überein, kann das Ergebnis problemlos dokumentiert werden. Sollte dies nicht der Fall sein, sind eventuelle Abweichungen zu vermerken und die Nichterfüllung im Arbeitspaket „Komponenten" zu protokollieren. Weiterhin besteht noch eine Verbindung zum Arbeitspaket „Assets", wo alle mechanischen Schwachstellen, die eventuell nicht über die Normung abgefangen werden, niedergeschrieben werden sollen. Es handelt sich dabei um eine Art Ideensammlung im Vorgehen der FMEA, die dem Prüfer helfen soll, alle kritischen (mechanischen) Elemente des Systems auszumachen. Hier sind alle möglichen Angriffe oder Schwachstellen aufzulisten. Ferner kann die beschriebene Vorgehensweise zur Überwindung des Systems auf mechanischer Ebene genauer detailliert werden, um auch mögliche Gegenmaßnahmen zu identifizieren, die später in der Analyse auf ihre Wirksamkeit hin bewertet werden. Eine mögliche Darstellungsform ist nachfolgend in Tabelle 12 gegeben.

Assets - kritische Elemente mechanisch - sekundär				
System	Bearbeiter		Datum	
Evaluationssystem 2	*Arne Schwerdtfeger*		*2016*	
Kritisches Element	Status		Verantwortlicher / Leitung	
Mechanische Elemente	*Hauptsächliche Analyse*		*Eigenverantwortliche Leitung*	
Funktion	Anmerkung		Ergebnis	
Konventionelle Schließfunktionalität			*Teilergebnis 1*	
Modus operandi	Beschreibung	Direkte Auswirkung	Asset	Gegenmaßnahme

Tabelle 12: Auflistung der kritischen mechanischen Elemente (Do)[205]

Mit Hilfe der Tabelle lassen sich somit auch Auswirkungen auf das System beschreiben. In einem gewählten Beispiel könnte durch das simple Aufbohren (Modus Operandi) des mechanischen Schließzylinders (Beschreibung) auf der Außenseite der Kern rotatorisch bewegt werden (direkte Auswirkung), was zur Folge hat, dass ein direkter Zugang zur Privatsphäre (Asset) gewährt wird.

[205] Eigene Darstellung.

Die Gegenmaßnahme des Bohrschutzes sollte dann in einem weiteren Schritt der Analyse verifiziert werden.

Da methodisch auf der gegenüberliegenden Seite der Abbildung 30 die Arbeitsschritte für den elektronischen Part respektive der IT-Security ähnlich sind, wird die Beschreibung dort fortgesetzt, d. h. beginnend nach dem Sicherheitsprofil mit dem Arbeitspacket des Services (Prozess, Dienstleistung).

Der Kriterienkatalog stellt für die IT-Security einen umfassenden Fragenkatalog zur Verfügung. Er beschreibt im Ursprung die Expertisen der Common Criteria und des BSI-Grundschutzkataloges. Beginnend mit dem BSI und den Bausteinen des Grundschutzkataloges (Übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze und Anwendungen) sollte ein fiktives Mobile Access-System nachgebildet worden. Dies basierte auf der Frage, welche BSI-Bausteine zur Abbildung eines solchen Systems benötigt werden. Im Anhang (ab S. 106) befinden sich die Seiten mit der entsprechenden Zusammenstellung. Folgend der speziellen Bausteinzusammenstellung sind entsprechend 305 potenzielle Gefährdungen zugewiesen (Anhang, ab S. 107). Es sind 544 weiterführende Maßnahmen hierzu identifiziert worden (Anhang, ab S. 112). Jede Maßnahme ist im BSI-Vorgehen mit einer Qualifizierung belegt, die eine Aussage über die Art der Maßnahme trifft. So steht die Kennung C für eine zwingende Maßnahme, wenn eine Zertifizierung nach dem BSI-Grundschutzkatalog angestrebt wird. Weitere Betrachtungen der Maßnahmen sind hier nicht zielführend, da im Wesentlichen die Gefährdungen von Bedeutung sind. Im Anhang befindet sich die angesprochene Zusammenstellung der Gefährdungen und Maßnahmen, welche aus der Nachbildung der BSI-Bausteine entstanden sind. Hinter jeder einzelnen Gefährdung steht die realistische Annahme, dass diese auch in den meisten Fällen zu einer Sicherheitslücke führen kann respektive das Risiko erhöht, potenziell Opfer eines Angriffes zu werden. Da die Zusammenstellung aus praxisrelevanten Fällen stammt, kann der Anwender sich auf eine repräsentative Datenmenge als Grundlage verlassen. Das BSI hat damit ein Referenz-Standardwerk geschaffen, das im gegebenen Umfang zu allen genannten Bausteinen eine gute Übersicht über mögliche Gefährdungen bietet. Insbesondere trifft ein Großteil der Gefährdungen und Maßnahmen auch auf die Mobile Access-Anwendungen zu. Auch die Common Criteria gibt im Teil 2, der sich mit den funktionalen Sicherheitsanforderungen beschäftigt, eine nötige Auswahl an wichtigen Voraussetzungen an, die für einen sicheren Betrieb gewährleistet sein müssen[206]. Übergeordnet geben die Klassen zu einem Themenfeld bestimmte vordefinierte Anforderungen an, die sich weiter zu Familien und Komponenten detaillieren. Methodisch gesehen ist der BSI-Grundschutz ein Managementansatz, der sich nicht zu sehr auf die technische Ebene herunterbrechen lässt, aber dennoch wertvolle Hinweise gibt. Konträr dazu steht die CC, die im Gegensatz zum BSI-Grundschutzkatalog detaillierter auf technische Belange eingeht, und eher produktspezifisch gesehen werden kann. Diese beiden Varianten lassen sich sehr gut miteinander kombinieren, da sie unterschiedliche Aspekte abdecken. Somit sind Schnittmengen für thematische Ähnlichkeiten in den Gefährdungen und den funktionalen Sicherheitsanforderungen zu suchen. Hierzu ist die genannte Gefährdungszusammenstellung aus dem BSI den Klassen aus Teil 2 der CC gegenübergestellt worden. Eine komplette Übersicht ist im Anhang (Tabelle 29, Tabelle 30, Tabelle 31 und Tabelle 32 ab S. 123) zu finden. Für die Auswertung dienen als Basis die BSI-Bausteine mit den eruierten Gefährdungen und die funktionalen Anforderungen der CC mit dem Abschluss einer begründeten Bewertung (Auszug in Tabelle 13).

[206] Vgl. Common Criteria, Part 2: Security functional components, 2012.

BSI		CC	
Baustein [B Nr.]	Gefährdung [G Nr.]	Security functional components	Verweis
3.101 Allgemeiner Server	4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	FIA_UAU,	
3.101 Allgemeiner Server, 1.4 Datensicherungskonzept, 1.6 Schutz vor Schadprogrammen, 1.9 Hard- und Software-Management, 1.12 Archivierung	4.13 Verlust gespeicherter Daten	FDP_SDI	FDP_ITT, FDP_UCT, FDP_UIT

Tabelle 13: Auszug Schnittmengen BSI & CC[207]

Wie leicht zu erkennen ist, sind einige Gefährdungen in mehreren Bausteinen vorhanden, so dass eine zusätzliche Selektion notwendig wurde. Auch konnten innerhalb der Schnittmengen von BSI und den CC mehrere Übereinstimmungen gefunden werden (siehe die Spalte „Verweis"). Mit diesem Verfahren sind 42 wesentliche Schnittmengen definiert worden. Von den abermals 305 Gefährdungen hat die mehrfach angesprochene Selektion den Bestand sinnhaft dezimiert und einen aussagekräftigen Extrakt aus Themenfeldern geschaffen. Zusätzlich fand für die Aufstellung des endgültigen Leitfragenkataloges eine weitere sinnhafte Dezimierung der Themen statt, da beispielsweise Kommunikationsschnittstellen nicht explizit erwähnt werden müssen, sondern allgemein zusammengefasst werden konnten. Zur Prüfung, ob durch den Selektionsprozess eine gleichmäßige Verteilung aller Themenfelder gewährleistet ist, können die grundlegenden Anforderungen der DIN IEC 62443-3-3[208] angeführt werden. Dabei handelt es sich um den Teil einer Normenreihe für die IT-Sicherheit in industriellen Kommunikationsnetzen. Explizit wird auch in ihr die Beziehung zur ISO/IEC 27002[209] erwähnt (die zur Normenreihe der ISO/IEC 2700x gehört) und damit ihr wichtiger Beitrag zur IT-Sicherheit. Ähnlich den schon vorgestellten Normen oder Richtlinien zeigt auch diese Normenreihe Möglichkeiten zur Handhabung von IT-Sicherheitslücken auf, bei denen insbesondere Anbieter ihre Automatisierungssysteme im Hinblick auf die gestellten IT-Anforderungen prüfen lassen können[210]. Im Resultat sind 34 Bereiche des Leitfragenkataloges mit den thematischen Schwerpunkten der Gefährdungen aus dem BSI-Grundschutzkatalog den Anforderungen der DIN IEC 62443-3-3[211] zugeordnet worden (siehe Abbildung 31).

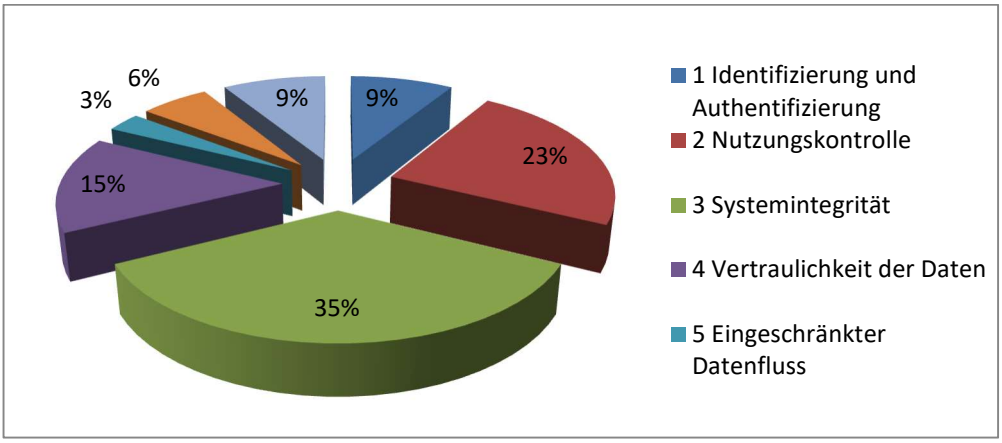


Abbildung 31: Zuordnung der Leitfragen zu den Anforderungen der DIN EN 62443[212]

[207] Eigene Darstellung.
[208] DIN IEC 62443-3-3 (Entwurf), Industrielle Kommunikationsnetze, Systemanforderungen zur IT-Sicherheit und Security-Level, 2015.
[209] ISO/IEC 27002, IT-Sicherheitsverfahren, 2008.
[210] Vgl. DIN IEC 62443-3-3 (Entwurf), Industrielle Kommunikationsnetze, Systemanforderungen zur IT-Sicherheit und Security-Level, 2015, S. 17.
[211] Ebd.
[212] Eigene Darstellung.

Die aufgeführte Verteilung (Abbildung 31) stellt zunächst den Status quo dar und gibt einen Überblick über die gegenwärtige Aufteilung der Leitfragen. Bei genauerem Hinsehen wird ersichtlich, dass die Basiskriterien „Identifizierung und Authentifizierung" sowie die „Nutzungskontrolle" mit 58% einen relativ hohen Anteil an den Leitfragen ausmachen. Da eine starke Einbindung von IT-Security-Themen bei zusätzlichen Serviceleistungen eine wichtige Rolle spielt, stellen die beiden Kriterien auch einen essentiellen Beitrag zum korrekten Betrieb des Systems dar. Alle weiteren fünf Basiskriterien sind auf insgesamt 42% aufgeteilt. Mit drei Prozent stellt der „Eingeschränkte Datenfluss" den geringsten Anteil dar.

Somit setzt sich der Leitfragenkatalog aus den folgenden 34 Bereichen zusammen:

1. Komplexität der Zugangsmöglichkeiten
2. Verlust gespeicherter Daten
3. Software- Schwachstellen oder -Fehler
4. Integritätsverlust schützenswerter Informationen
5. Überlastung von Informationssystemen
6. Schlechte oder fehlende Authentifizierung
7. Kryptographie
8. Gefälschte Zertifikate
9. Undokumentierte Funktionen
10. Nicht getrennte Verbindungen
11. Unzureichende oder fehlende Verbindungs-Sicherheitsmechanismen
12. Nichtzustellung einer Information
13. Mangelnde Verlässlichkeit von Groupware
14. Unterlaufen von Zugriffskontrollen über ODBC
15. Verlust von Daten in einer Datenbank
16. Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services
17. Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen
18. Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services
19. Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung
20. Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen
21. Unerlaubte Ausübung von Rechten
22. Unzureichende Kontrolle der Sicherheitsmaßnahmen
23. Unzureichendes Schlüsselmanagement bei Verschlüsselung
24. Fehlende oder unzureichende Auswertung von Protokolldaten
25. Analyse des Nachrichtenflusses
26. Fehlerhafte Administration von Zugangs- und Zugriffsrechten
27. Unberechtigte IT-Nutzung
28. Manipulation an Informationen oder Software
29. Software mit unerlaubten Zugriff
30. Vertraulichkeitsverlust schützenwerter Informationen
31. Weitergabe von Daten an Dritte
32. Kompromittierung kryptographischer Schlüssel
33. Unberechtigtes Überschreiben oder Löschen von Archivmedien
34. Vertraulichkeitsverlust durch Auslagerungsdateien

Zu jedem einzelnen Bereich gibt es auf einem Vordruck weiterführende Fragen mit einem standardisierten Aufbau. In Summe bilden dann die einzelnen Vordrucke zu den Bereichen den Leitfragenkatalog. Der standardisierte Aufbau ist wie folgt (Abbildung 32):

Nr.7 Kryptographie				
Verweis:	4.35 Unsichere kryptographische Algorithmen (BSI) FCS_COP (CC)			
Beschreibung:	Der Einsatz kryptographischer Algorithmen stellt einen vertraulichen Datenaustausch sicher.			
Implementierung:	Welche kryptographischen Algorithmen werden eingesetzt, inkl. Bitlänge? Werden Signaturen verwendet? Wird ein Zufallsgenerator für Zahlen verwendet? Welche Operationen sind davon betroffen? Kombination weiterer Sicherheitsfunktionen mithilfe von Verschlüsselung? Wie sind die Standards implementiert? Sind alle Übertragungswege und Speicherbereiche abgesichert?			
Schlüsselbegriffe:	Kryptographie, Signatur, Hashwert, Bitlänge, Schlüssellänge, proprietär, AES, 3DES, XOR, Zahlengenerator, Symmetrisch, Asymmetrisch			
Zusatz:	Ist die Aktualität der Verschlüsselung gewährleistet? Werden proprietäre Verfahren eingesetzt?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Abbildung 32: Beispiel-Leitfrage Nr. 7 Kryptographie[213]

In dem hier gewählten Beispiel handelt es sich um die Leitfrage der Kryptographie. Der standardisierte Aufbau der Vorlage ist in Anlehnung an den prinzipiellen Rahmen der DIN IEC 62443-3-3[214]. Dort werden auch in Form von funktionalen Anforderungen und zugehörigen Unterkriterien, wie die Kategorisierung in Abbildung 31 darstellt, sogenannte Security Levels für ein Produkt festgelegt. Insgesamt sind vier Security Levels aufgeführt, die nach ihrer steigenden Sicherheitseinstufung einen möglichen Zugang zu den grundlegenden Anforderungen klassifizieren.

[213] Eigene Darstellung.

Einher geht damit auch die noch tolerierbare Risikoeinschätzung und das im Endergebnis dargestellte Referenzprofil zur IT-Sicherheit.[215,216]

Wie Abbildung 32 zeigt, teilt sich die Vorlage in sieben Abschnitte mit folgender Nennung:

- Verweis
- Beschreibung
- Implementierung
- Schlüsselbegriffe
- Zusatz
- Objekte
- sowie das praktische Sicherheitsprofil (Ausprägung, Angreiferklasse, Usability und Kompromittierung sensibler Daten).

Bei dem Verweis handelt es sich um die ursprünglichen Kennungen aus dem BSI-Grundschutz und den CC. In dem Fall nimmt die Kryptographie Bezug auf die Gefährdung „Unsichere kryptographische Algorithmen" und auf die funktionale Komponente der Klasse FCS_COP (Cryptographic operation). Folgend geht mit der Beschreibung eine spezifische Aussage zum Schwerpunkt der Leitfrage einher: „Der Einsatz kryptographischer Algorithmen stellt einen vertraulichen Datenaustausch sicher." Die Implementierung stellt Fragen zu dem geforderten Schwerpunkt an das Untersuchungsobjekt (Mobile Access-System). Da es sich in dem hier gewählten Beispiel um das theoretische Sicherheitsprofil 2|3|2|4 handelt, gilt die höchste Einstufung zum Umfang der Prüftiefe respektive der Muss-Fragen (Stufe 4 //alle Fragen), d. h. es sind im gesamten Leitfragenkatalog zu allen Themenbereichen alle Implementierungsfragen zu beantworten. Würde zum Verständnis aus dem theoretischen Sicherheitsprofil die Zahl „3" als höchste Einstufung hervorgehen, wären drei Implementierungsfragen zu bearbeiten. Geringere Einstufungen wären entsprechend mit geringerem Prüfumfang zu bewerten. Die höchste Einstufung mit der Zahl „5" hätte zur Folge, dass nicht nur alle Implementierungsfragen zu beantworten wären, sondern auch alle Zusatzfragen. Tabelle 10 stellte die Muss-Fragen anhand des theoretischen Sicherheitsprofils dar. Als Objekt kann bei Bedarf eine spezifische Angabe zum untersuchten Objekt gemacht werden. Wenn alle geforderten Fragen ausreichend beantwortet sind, entscheidet der Prüfer, in welchem Umfang das praktische Sicherheitsprofil zu den bekannten vier Kriterien erfüllt wurde. In dem Fall muss zur Erreichung des theoretischen Sicherheitsprofils 2|3|2|4 auch das praktische Sicherheitsprofil die Kennung 2|3|2|4 erreichen. Das dezidierte Ergebnis ist dann kenntlich zu machen und ggf. zu begründen. Der vollumfängliche Leitfragenkatalog ist im Anhang (ab S. 127) dargestellt.

Als nächster Schritt (siehe Abbildung 30) findet das simultane Arbeitspaket „Assets" statt, welches eine ungezwungene Ideensammlung möglicher IT-Sicherheitslücken auflisten soll (in Anlehnung an die FMEA). Hier können alle Möglichkeiten dokumentiert werden die spezifisch für ein Mobile Access-System sind und nicht im Leitfragenkatalog berücksichtigt wurden. Als Beispiel dient Tabelle 14:

Assets - kritische Elemente elektr. - primär (Check)				
System	Bearbeiter		Datum	
Mobile System	*Max Mustermann*		*2017*	
Kritisches Element	Status		Verantwortlicher / Leitung	
Elektronische Elemente	*Hauptsächliche Analyse*		*Eigenverantwortliche Leitung*	
Funktion	Anmerkung		Ergebnis	
Service-Funktionalität			*Teilergebnis 2*	
Modus operandi	Beschreibung	Direkte Auswirkung	Asset	Gegenmaßnahme

Tabelle 14: Auflistung der kritischen elektronischen Elemente (Do)[217]

[214] DIN IEC 62443-3-3 (Entwurf), Industrielle Kommunikationsnetze, Systemanforderungen zur IT-Sicherheit und Security-Level, 2015.
[215] Vgl. ebd., S. 16 f.
[216] Vgl. ebd., S. 29.
[217] Eigene Darstellung.

5.3.3 Schritt „Check"

In Abschluss zum Schritt „Do" sind alle möglichen Sicherheitslücken, mithilfe des Fragenkataloges, wie auch mit der Ideensammlung für mechanische und elektronische Komponenten zusammengetragen worden. Es muss nun die Abwägung des Risikos (Schritt „Check") erfolgen, ob die zusammengetragenen Informationen auch einen bedrohlichen Zustand herstellen können. Dafür ist jede einzelne Sicherheitslücke auf den potenziellen entstehenden Schaden sowie dessen Eintrittswahrscheinlichkeit hin zu prüfen. Dieses Modell bildet imitierend die in der FMEA-Methode beschriebene Kritizität ab. Es beschreibt den vorletzten Arbeitsschritt „Bedrohungen/Angriffe" sowohl für den Strang der Komponenten (mechanisch) wie auch den Strang Service (elektronisch, IT-Security). Als Orientierung dient wieder eine Formatvorlage, damit alle wichtigen Bewertungen zur Urteilsbildung abgefragt werden. Die Vorlage zur Bestimmung der Wahrscheinlichkeiten ist in Tabelle 15 dargestellt.

Wahrscheinlichkeiten										
Systembaustein		Bearbeiter			Datum					
Außenseite		*Max Mustermann*			*2016*					
Kritisches Element		Status			Verantwortlicher / Leitung					
Mechanische Elemente		*Hauptsächliche Analyse*			*Eigenverantwortliche Leitung*					
Funktion		Anmerkung			Ergebnis					
Konventionelle Schließfunktionalität					*Teilergebnis 3*					
Kriterium	Sicherheitsziel	Soll	Ist	Asset	Wahrscheinlichkeit	Schaden	Risikozahl	Gewichtung	Risikograd	Bemerkung

Tabelle 15: Wahrscheinlichkeiten bestimmen[218]

Das dargestellte Formular führt – beginnend mit dem Kriterium, das in der Benennung aus den vorherigen Analysen übernommen wird – alle Ergebnisse zusammen und stellt eine semi-quantitative Bewertung dar. Das zugehörige Sicherheitsziel wird aus dem theoretischen Sicherheitsprofil übertragen und dient der weiteren Bewertung als Referenz, d. h. der Trennung zwischen den Vorgaben der jeweiligen Norm auf mechanischer Seite und den Vorgaben und Erfüllungsgraden des Kriterienkataloges. Mit dem Soll/Ist-Vergleich werden die tatsächlichen Gegebenheiten geprüft und dokumentiert, d. h. der Arbeitsschritt „Abgleich Sicherheitsprofil", wie in Abbildung 30 beschrieben, ist in die Vorlage der Wahrscheinlichkeitsbestimmung (Tabelle 15) integriert. Explizite Auswirkungen des kritischen Zustandes sind in der Spalte Asset zu vermerken. Die Risikozahl setzt sich aus der Eintrittswahrscheinlichkeit und dem Schadenausmaß zusammen. Zusätzlich beeinflusst die Gewichtung den abschließenden Risikograd, der eine finale Einschätzung des Kriteriums auf das geforderte theoretische Sicherheitsziel gibt In der Bemerkung können spezifische Angaben zum Rahmen des Kriteriums gegeben werden. Die konkrete Durchführung wird beispielhaft auf Seite 74 dargestellt.

Für eine möglichst realistische und semi-quantitative Bewertung sollten im Vorfeld abgestufte Zahlenwerte definiert werden. So können die Grenzen bei der subjektiven Einschätzung besser nachvollzogen und plausibel gesetzt werden. Hier galt jedoch folgendes:

-Wahrscheinlichkeit: 10 (sehr hoch), 6 (eher hoch), 4 (eher gering), 2 (gering), 1 (sehr geringe Wahrscheinlichkeit).

-Schaden: 10 (sehr hoch), 6 (eher hoch), 4 (eher gering), 2 (gering), 1 (sehr geringer Schaden).

-Gewichtung: Individuelle Abweichung pro Kriterium vom theoretischen zum praktischen Sicherheitsprofil.

5.3.4 Schritt „Act"

Gemäß Abbildung 30 sind jetzt alle Ergebnisse in eine Ergebnisdarstellung zu überführen und final für den Hersteller und Kunden auszuwerten. Als erstes folgt eine spezifische Angabe für den Hersteller, inwieweit sein Produkt von den zu erfüllenden Anforderungen des theoretischen Sicherheitsprofils entfernt ist und welcher ungefähre Aufwand noch zu leisten ist, um eine Produktverbesserung zu erreichen. Dazu muss ein eindeutiger Erfüllungsgrad aus der gewählten

[218] Eigene Darstellung.

Methode abgeleitet werden. Dem liegt folgende Berechnung gemäß den Gleichungen (3)–(5) zugrunde:

$$a = 100 - \left(\frac{PG3}{TG3 \times G3} \times 100\right) \qquad (3)$$

$$b = 100 - \left(\frac{PG}{TG \times G4} \times 100\right) \qquad (4)$$

$$S = a|b \qquad (5)$$

Aus den Berechnungen a und b setzt sich der Erfüllungsgrad zusammen. Dazu sind nach getrennter Ermittlung der sekundäre Teilerfüllungsgrad a (mechanisch) und der primäre Teilerfüllungsgrad b (elektronisch) zu bestimmen. Aufgrund der getrennte Stränge (siehe Abbildung 30) sind auch für beide Erfüllungsgrade entsprechend aussagekräftige Ergebnisse in den Wahrscheinlichkeiten ermittelt worden. Somit beschreibt PG die praktische Gesamtpunktzahl der summierten Risikograde aus den Wahrscheinlichkeitsermittlungen. Dividiert wird diese Zahl durch die theoretische Gesamtwahrscheinlichkeit TG und die maximale Einzelgewichtung G. Bei der theoretischen Gesamtwahrscheinlichkeit TG setzt sich der Wert aus den summierten Kriterien in der Wahrscheinlichkeitsbetrachtung und dem maximal möglichen Einzelrisikograd zusammen. Damit Wahrscheinlichkeiten mit einer entsprechend höheren oder niedrigeren Bewertung auch einen repräsentativen Einfluss auf das Gesamtergebnis nehmen können, ist die maximal mögliche Einzelgewichtung G aus den Wahrscheinlichkeitsbetrachtungen zu übernehmen. Wichtig an dieser Stelle ist es zu erwähnen, dass mit der Aufsummierung der einzelnen Risikograde keine Gesamtsicherheit respektive kein Gesamtrisiko des Produktes ermittelt wird. Es sind lediglich die Aufwendungen abschätzbar, die ein Hersteller für die weitere Annäherung an das theoretische Sicherheitsprofil umsetzen muss. Ähnlich einer FMEA können auch dort die RPZ-Werte nicht einfach summiert werden, um ein Gesamtrisiko definieren zu können. Aus diesem Grund dürfen die erzielten Ergebnisse der Teilerfüllungsgrade (a, b) respektive der Erfüllungsgrad (S) nicht an den Kunden weitergegeben werden. Die daraus entstehenden falschen Schlussfolgerungen sind nicht abschätzbar und suggerieren dem Kunden ggf. ein irreführendes Sicherheitsergebnis. Abbildung 33 verdeutlicht nochmals die Problematik der aufsummierten Risiken. Offensichtlich sind diese nicht gleichmäßig verteilt und können lediglich singulär analysiert werden. Dieser Ansatz spielt eine wesentliche Rolle in der weiteren Vorgehensweise für die differenzierte Betrachtung der Sicherheitsbewertung aus Hersteller- und Kundensicht.

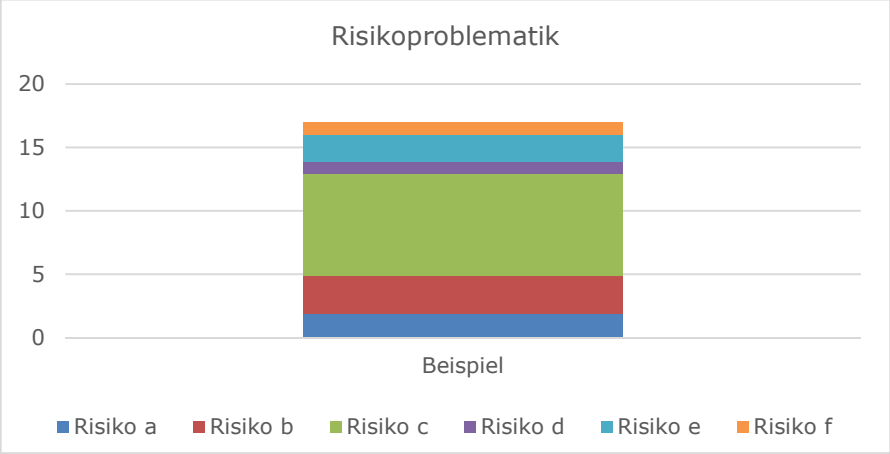


Abbildung 33: Risikoproblematik[219]

Mit dem Erfüllungsgrad S sind beide Teilerfüllungsgrade (primär und sekundär, d. h. elektronisch und mechanisch) in einem Endergebnis zusammengefasst und leicht interpretierbar. Das beste relative Ergebnis wäre demnach S=100|100; das schlechteste relative Ergebnis S=0|0.

[219] Eigene Darstellung.

Die jeweiligen primären oder sekundären Differenzen im Erfüllungsgrad sind in den einzelnen Zwischenschritten dokumentiert und geben Auskunft über den Mangel des einzelnen Teilerfüllungsgrades. Somit lassen sich die Zwischenergebnisse auch als zusammenfassende Maßnahmenliste verstehen, die es dem Hersteller ermöglicht, an seinem System konstruktive Verbesserungen vorzunehmen. Wie bereits schon mehrfach ausgeführt, ist der Schritt „Act" im Kern eine Zusammenfassung aller Ergebnisse und Urteilsbemühungen im Abgleich der Sicherheitsprofile. Ein mangelnder Erfüllungsgrad, also ein Wert, der schlechter als 100|100 ist, soll den Hersteller motivieren, den üblichen und selbstverständlichen Zyklus der Produktverbesserung einzuleiten, um sein Ergebnis und damit das Vertrauen beim Kunden zu optimieren.

Eine schlussendliche Ergebnisdarstellung gegenüber dem Kunden (mit der Kennung Z) steht in enger Abhängigkeit zur ersten Vorgehensweise (Ermittlung des Erfüllungsgrades (S)). Der mechanische und elektronische Bereich wird hier nicht simultan behandelt. Zunächst beschränken sich die folgenden Ausführungen auf den elektronischen Bereich; anschließend findet eine Kommentierung für den mechanischen Bereich statt. Als generelle Grundlage dient jedoch die Wahrscheinlichkeitstabelle (siehe Tabelle 15).

In der Praxis hängt die Sicherheit des Produktes vom kritischen Pfad ab, den ein Angreifer oder Einbrecher nutzen kann, um sich z. B. einen unerlaubten Zugang zu verschaffen. Um diesen Ansatz als Berechnungsgrundlage für die Darstellung der Kundensicht zu nutzen, ist eine Einflussnahme von Risikozahl und Gewichtung des Risikograde zu beurteilen. Die Gewichtung beschreibt eine prinzipielle Abweichung vom theoretischen Sicherheitsprofil; die zunehmende Differenz ist hier ein Indikator für den Grad der Abweichung. Im Zusammenhang mit der Risikozahl, die das Produkt aus Wahrscheinlichkeit und Schaden darstellt, kommt beiden genannten Faktoren eine unterschiedliche Wichtigkeit zu. Demnach ist es für den Kunden von besonderem Interesse, mit welcher Schwere ein möglicher Schaden eintritt, gleichwohl die Eintrittswahrscheinlichkeit eher als gering eingestuft wurde. Auch die nur eher geringe Auswirkung eines Schadens mit einhergehender großer Eintrittswahrscheinlichkeit ist für den Kunden bei Einsatz des Produktes von Bedeutung. Wird nun noch die Gewichtung, dem Abstand des praktischen zum theoretischen Sicherheitsprofil, berücksichtigt, kann demzufolge nur eine gewichtete Risikobewertung aus Kundensicht das Ergebnis der Sicherheitsbewertung adäquat darstellen. Hierfür werden stufenweise Farbkennungen ermittelt und vergeben, die auf dem Ampelprinzip beruhen. Aus den genannten Begründungen werden in einem ersten Schritt die Abstufungen zur Bewertung von Wahrscheinlichkeit und Schaden mit entsprechenden Farben hinterlegt (siehe Tabelle 16). Für eine leichtere Anwendung können die Farben direkt in der Tabelle 15 mit eingetragen werden.

Wahrscheinlichkeit	**Schaden**
1 Sehr geringe Wahrscheinlichkeit	1 Sehr geringer Schaden
2 Geringe Wahrscheinlichkeit	2 Geringer Schaden
4 Eher geringe Wahrscheinlichkeit	4 Eher geringer Schaden
6 Eher hohe Wahrscheinlichkeit	6 Eher hoher Schaden
10 Sehr hohe Wahrscheinlichkeit	10 Sehr hoher Schaden

Tabelle 16: (Farbliche) Beurteilung von Wahrscheinlichkeit und Schaden[220]

Für die farbliche Übertragung der Gewichtung in drei Zustandsfarben (rot, gelb, grün) werden die unten dargestellten Gleichungen (6), (7) und (8) angewendet. Dazu müssen die jeweiligen Gewichtungen aus der Tabelle 15 (Bereich für die IT-Security/Elektronik) gemäß der Berechnungsgrundlage analysiert und dann dort markiert werden. Dabei ist die Variable G_{max} die größte Abweichung vom theoretischen zum praktischen Sicherheitsprofil und bestimmt damit die Grenze respektive die Zustandsfarbe einer jeden einzelnen Gewichtung $G_{1\ldots n}$.

[220] Eigene Darstellung.

$$\text{Zustandsfarbe "Rot"} = G_{1\ldots n} > G_{max} * 0{,}5 \quad (6)$$

$$\text{Zustandsfarbe "Gelb"} = 1 \leq G_{1\ldots n} \geq G_{max} * 0.5 \quad (7)$$

$$\text{Zustandsfarbe "Grün"} = G_{1\ldots n} = 0 \quad (8)$$

Die schlussendliche farbliche Ergebnisdarstellung jedes einzelnen Kriteriums mit den drei Faktoren (Schaden, Wahrscheinlichkeit und Gewichtung) und ihrer farblichen Zuordnung wird zusammenfassend mit der Anforderung der kritischen Sicherheit A_{kS} bewertet. So kann für jedes Kriterium aus der Wahrscheinlichkeitstabelle die Anforderung der kritischen Sicherheit A_{kS} aus Tabelle 17 abgelesen werden.

Schaden				
Wahrscheinlichkeit				
Gewichtung				

Tabelle 17: Anforderung der kritischen Sicherheit (A_{kS})[221]

Mit der Anforderung der kritischen Sicherheit (A_{kS}) ist jedes Kriterium im Bereich der IT-Security/Elektronik auf seine Zustandsfarbe hin zu überprüfen. Die Auswertung über Tabelle 17 ist von den drei Faktoren Schaden, Wahrscheinlichkeit und Gewichtung abhängig. Je nachdem, welche Zustandsfarben miteinander kombiniert sind, ergibt sich eine entsprechende Zustandsfarbe für A_{kS} aus dem entsprechenden Bereich. Schnell wird ersichtlich, dass der Schaden eine stärkere Ergebnisbeeinflussung erlaubt, d. h. wird der Schaden „Rot", die Wahrscheinlichkeit „Grün" oder „Rot" und die Gewichtung „Gelb" oder „Rot", so ergibt sich immer die Zustandsfarbe „Rot". Lediglich bei „grüner" Schadenszuordnung kann das Ergebnis für A_{kS} von „Gelb" bis „Grün" variieren.

Für die schlussendliche Ergebnisdarstellung gegenüber dem Kunden (Mechanik und IT-Security/Elektronik) gilt mit der Kennung Z Tabelle 18. Dazu bildet die farbliche Gesamtheit der A_{kS} pro Kriterium die Grundlage.

Sicherheitsbewertung Teilproduktbereich	Bedingung	Ergebnis
IT-Security/ Elektronik		
Rot	1 oder mehr Kriterien haben die Zustandsfarbe „Rot".	Produktbereich entspricht gar nicht den Anforderungen.
Gelb	Mehr als 20% der Kriterien haben die Zustandsfarbe „Gelb" und kein Kriterium hat die Zustandsfarbe „Rot".	Produktbereich entspricht mit Abweichungen den Anforderungen.
Grün	Mehr als 80% der Kriterien haben die Zustandsfarbe „Grün" und kein Kriterium hat die Zustandsfarbe „Rot".	Produktbereich entspricht in sehr großen Teilen den Anforderungen.
Mechanik		
Rot	1 oder mehr Kriterien haben die Zustandsfarbe „Rot".	Produktbereich entspricht gar nicht den Anforderungen.
Grün	Alle Kriterien haben die Zustandsfarbe „Grün".	Produktbereich entspricht in großen Teilen den Anforderungen.

Tabelle 18: Sicherheitsbewertung Teilproduktbereich IT-Security/Elektronik und Mechanik[222]

Für den mechanischen Bereich gestalten sich die Anforderungen prinzipiell einfacher, da hier aufgrund der gegebenen Normungsvoraussetzungen nur die Zustandsfarben „rot" oder „grün" anzusetzen sind. Demzufolge sollte hier aufgrund der dargestellten Argumentation nur die maximale Gewichtung „1" vergeben werden, was eine große Differenz von vornherein ausschließt.

[221] Eigene Darstellung.
[222] Eigene Darstellung.

Das bedeutet für die einzelnen Kriterien im Bereich der Mechanik der Wahrscheinlichkeitstabelle, dass schon bei einer gewählten Gewichtung mit „1" im gesamten mechanischen Bereich die Sicherheitsbewertung des Teilproduktbereiches auf „rot" gesetzt wird. Im Umkehrschluss erfüllt der Hersteller in einem Produktbereich nicht sofort die Anforderungen und muss zwangsläufig alle Mängel beseitigen respektive die Auswirkungen auf das Produkt abstellen.

Als Beispiel sei folgendes Ergebnis der kundenspezifischen Sicht über die Gesamtheit der Anforderung der kritischen Sicherheit im mechanischen und elektronischen Teilproduktbereich gezeigt: $Z=A_{kS(Mechanik)}|A_{kS(IT\_Security)}$=**grün**|**gelb**. Anhand der Zustandsfarben für die beiden Teilproduktbereiche kann der Kunde eine erste Einschätzung zu den Anforderungen der Sicherheitsbewertung vom Produkt direkt erhalten.

5.3.5 Zusammenfassung / Fazit

Mit dem Bezug zum theoretischen Sicherheitsprofil sind Zustandsfarben vergeben worden, die die Anforderungen zur kritischen Sicherheit A_{kS} abbilden und dadurch gewichtete Risikobeurteilungen zulassen. Zusätzlich wird der Hersteller in die Lage versetzt, über den Erfüllungsgrad eine ungefähre Abschätzung zum Aufwand der Produktverbesserung zu treffen. Alle Einschätzungen und Beurteilungen haben den relativen Bezug zum gleichen theoretischen Sicherheitsprofil und gewährleisten damit die Vergleichbarkeit und Transparenz der ganzheitlichen Sicherheitsbewertung. Insbesondere wirken auch die Einsatzumgebung und der Zweck des Systems auf das erforderliche Sicherheitsniveau ein. Bei einer wachsenden Vielzahl von Mobile-Access-Systemen und unterschiedlichsten Anwendungsfeldern ermöglicht die ganzheitliche Sicherheitsbewertung eine sachliche Einordnung der Bewertung mit Bezug zu individuellen Einsatzbedingungen. Gestellte Grundvoraussetzungen (siehe Tabelle 7) wie Berücksichtigung herrschender Normen sowie Erweiterung und Ausbau der IT-Kriterien konnten in vollem Umfang erfüllt werden. Im Zuge weiterer technologischer Entwicklungen sind die Kriterienkataloge ohne weiteres ausbaufähig. Was im Umkehrschluss auch für die entsprechende Einstufung der Normenvoraussetzung im theoretischen Sicherheitsprofil gilt. Somit kann die Sicherheitsbewertung individuell für sich ändernde Bedürfnisse flexibel angepasst werden. Entscheidend dabei ist das ablauforientierte Vorgehen, das dem Verständnis der praxisnahen Umsetzung folgt. Mit dem Prozessablauf (Abbildung 30) sind die Elemente zur ganzheitlichen Sicherheitsbewertung klar beschrieben und modular veränderbar. Dies ermöglicht es auch dem Prüfer, sukzessive Angleichungen im Prozess vorzunehmen und im Hinblick auf die Anwendbarkeit zu testen. In gleichem Maße wird auch der Anwender in die Lage versetzt, das Ergebnis zu bewerten und nachzuvollziehen. Auf einen Blick stellen somit die Zustandsfarben das Evaluierungsergebnis dar. Bei weiterführendem Verständnis sind die Teilergebnisse innerhalb der Bewertung in der Lage, dezidierte Auskunft über den gegenwärtigen Stand der Beurteilung zu geben. Damit können Kunden den Spielraum für oder gegen eine Produktentscheidung selber variieren; die Hersteller nutzen denselben Spielraum, um Produktverbesserungen nach eigener Interpretation umzusetzen. Die Durchführung der Sicherheitsbewertung ist in Tabelle 19 übersichtlich zusammengefasst:

Prozess- /Arbeitsschritt:	**Inhalt:**	**Hilfsmittel:**	**In methodische Anlehnung an:**
Plan			
Anwendung Mobile Access	Systemauswahl treffen, Überblick verschaffen, Dokumentationen sichten etc.	Dokumente: Hersteller, Dienstleister etc.	
Modellierung UML	System abstrahieren, System modellieren, Funktionalitäten (Systemumfang) beschreiben, Annahmen aufstellen etc.	Software: UML Modellierung, Visio etc. Formatvorlagen: Annahmen (TOP-Themen, Anhang (ab S. 167) etc.	UML-Modellierungssprache
Sicherheitsprofil	Einordnung in den Sicherheitsbedarf, Begründungen etc.	Formatvorlagen: Sicherheitsprofil (Anhang, S. 171)	CC, DIN IEC 62443-3-3
Do			
Komponenten/Service	Normenvoraussetzung/Kriterienkatalog,	Dokumente: Zertifikate des Herstellers, Leitfragen (Leitfragenkatalog, Anhang ab S. 127)	Normenwerke, BSI, CC
Assets	Freie Sicherheitsanalyse	Formatvorlagen: Assets mechanisch(Anhang), Assets elektronisch (Anhang ab S. 174) etc.	FMEA
Check			
Bedrohungen/Angriffe	Zusammenführen der Teilergebnisse, Wahrscheinlichkeitsbetrachtung etc.	Formatvorlagen: Wahrscheinlichkeiten mechanisch / elektronisch (Anhang ab S. 178),	FMEA
Abgleich Sicherheitsprofil	Prioritäten festlegen, Bewerten etc.	Formatvorlagen: Siehe Bedrohungen/Angriffe (Check) etc.	FMEA
Act			
Maßnahmen, Konsequenzen, Ergebnis	Ergebnisdarstellung, Potenzialsammlung, vollständige Sicherheitsbewertung etc.	Formatvorlagen: Ergebnisdarstellung (S. 78), etc.	

Tabelle 19: Zusammengefasste Arbeitsschritte der ganzheitlichen Sicherheitsbewertung[223]

Hinweis: Jedes „etc." kann beispielhaft für eine individuelle Anpassung oder Erweiterung an die entsprechenden Rahmenbedingungen stehen!

[223] Eigene Darstellung.

6 Evaluierung der ganzheitlichen Sicherheitsbewertung

Die Evaluierung der ganzheitlichen Sicherheitsbewertung soll nun den anwendbaren Mehrwert der Methodik unter Beweis stellen. Hierzu sind zwei Mobile Access-Systeme ausgewählt worden, die einen guten Querschnitt angebotener Systeme auf dem Markt bieten. Zur Fokussierung auf die reine Durchführung sind reale Bezüge zu Herstellern nicht zweckdienlich, daher werden die Systeme verklausuliert als Beispielsystem 1 und 2 bezeichnet. Für eine nachvollziehbare Referenz sind beide Beispielsysteme mit einem sehr ähnlichen Funktionsumfang ausgestattet. In den technischen Details konnten aber während der Analyse Divergenzen herausgearbeitet werden, wobei diese für den Anwender nicht offensichtlich waren.

Für den leichteren Einstieg werden zuerst zwei fiktive Beispielsysteme erklärt, um den technologischen Rahmen besser abschätzen zu können. Jedes Mobile Access-System hat einen spezifischen Anwendungszweck, der grundlegend für dessen Entwicklung ist. Somit steht hier der technische Fokus klar im Vordergrund. In den weiteren Kapiteln zielt die Evaluierung auf die Anwendbarkeit der Methodik ab, und es werden im Einzelnen keine tiefgreifenden technologischen Ergebnisse der Beispielsysteme diskutiert. Gewonnene Erkenntnisse beziehen sich hauptsächlich auf die grundsätzliche Durchführbarkeit und Sinnhaftigkeit der Sicherheitsbewertung.

6.1 Beispielsystem 1

Bei den meisten frühen elektronischen Schließsystemen wird zur Speicherung ein Transponder genutzt, der in der Anwendung einem konventionellen Schlüssel sehr nahekommt. So wird bei gewünschtem Zugang der Transponder einfach vor die Leseeinrichtung des Knaufzylinders gehalten. Zur funktionalen Erweiterung sind diese Systeme oftmals um ein Smartphone zur Speicherung der Zugangsdaten ergänzt worden. So kann es üblich sein, dass bestehende elektronische Zugangsanlagen durch die Nutzung eines Smartphones als digitaler Schlüssel erweiterbar sind. Dazu werden die elektronischen Berechtigungen nicht mehr vor Ort über eine Programmierungskarte sondern dezentral mit dem Smartphone über eine Webschnittstelle vom Dienstleister programmiert. So auch im Fall des Beispielsystems 1, das mit der Hardware eines Schließanlagenherstellers per NFC kommunizieren kann. Die gesamte Kommunikation läuft über eine Applikation auf dem Smartphone, welche sich leicht aus dem Download-Center von Google herunterladen lässt. Mit der NFC-Schnittstelle ist per se die vollständige Einbindung eines iPhones ausgeschlossen (nur lesend) und nur für Android-Geräte möglich[224]. Grundsätzlich bietet der Funktionsumfang aber die Ansteuerung einer Bluetooth Low Energy-Schnittstelle an und damit auch die Unterstützung von Apple-Geräten. Mit der Applikation sind alle Funktionalitäten vorhanden, die auch schon mit der Nutzung von Transpondern möglich war. Hier dienen als Beispiel: Blacklist-Funktionen, zeitlich begrenzte Berechtigungen, Log-Daten etc. Hauptsächlicher Vorteil liegt in dem Verteilen der Berechtigungen von Smartphone zu Smartphone über eine entsprechende Administrationshierarchie. Zusätzlich können aber auch Transponder mithilfe der NFC-Schnittstelle des Smartphones beschrieben werden. Dies ist eine zwingende Voraussetzung für Gebiete, in denen kein Datennetz vorhanden ist, da sich die Berechtigungen im Smartphone in zeitlich regelmäßigen Abständen aktualisieren müssen. Bei einem konstruierten Fall könnte sonst der Berechtigungsentzug auf einem Smartphone nicht durchgeführt werden. Bei Zugängen mit zeitlichen Limitierungen kann die Auswerteeinheit am Türzylinder selbst Auswertungen vornehmen. An diesem Beispiel kann aufgezeigt werden, dass hier die gesamte Systemarchitektur von Knaufzylinder, Smartphone und Backend einem sicheren Aufbau folgen muss. Das Beispielsystem 1 folgt in weiten Teilen diesem Grundgedanken und ist daher auch ausgewählt worden, um als Referenzobjekt zu dienen.

Die Bestandteile sind im einfachsten Fall ein Knaufzylinder, ein Smartphone und eine mit dem Backend verbundene Datenverbindung. Im Kern befindet sich die gesamte Intelligenz im Backend beim Dienstleister. Hier sind alle Funktionen und Datenhaltungen vollumfänglich vorhanden. Weitere Dienstleistungen, z. B. die Verwaltung eines Fuhrparks, ist mit der gleichen Systematik darstellbar. Dadurch kann von einer sehr offenen Plattform gesprochen werden, die ein allgemeines

[224] Vgl. Vgl. Apple Inc., Core NFC, Abrufbar im Internet, https://developer.apple.com/documentation/corenfc#overview, 2017.

Berechtigungsmanagement zur Verfügung stellt. Somit könnten über eine Plattform mehrere Dienstleistungen im Bereich des Berechtigungsmanagements angeboten werden, die dem Endkunden Vorteile in der Verwaltung erlauben, ohne dabei verschiedene Systeme in Anspruch nehmen zu müssen.

Die Installation an der Tür kann denkbar einfach vorgenommen werden. Hierzu verläuft der Ein- und Ausbau vergleichbar zu einem mechanischen Schließzylinder, der auch nur über die Stulpschraube einen Halt in der Tür findet. Auffallend ist anschließend in der Betrachtung von innen und außen, dass es sich um einen Knaufzylinder handelt. Auch für Laien ist die nachträgliche Installation sichtbar.

Weitere Details des Beispielsystems 1 finden sich in den folgenden Kapiteln und Verweisen. Auf zusätzliche Erklärungen wird verzichtet, da sie für die Evaluierung der Sicherheitsbewertung unerheblich sind.

6.2 Beispielsystem 2

Das zweite Beispielsystem ist etwas spezieller, da es sich um eine motorisch-angetriebene Einheit handelt, die von innen an den mechanischen Schließzylinder angeflanscht wird. Diese Variante bietet dem Anwender gleich mehrere Vorteile. Zum einen entsperrt das Schloss automatisch, und es muss zum anderen keine manuelle Berührung vor Ort an der Außenseite vorgenommen werden. Der Kommunikationsstandard wird über Bluetooth Low Energy abgewickelt und zeichnet sich durch einen besonders geringen Energieverbrauch aus. Wie auch schon beim Beispielsystem 1 ist die Installation an der Tür denkbar einfach. Hierzu werden im Vorfeld die Abmessungen der Tür bei der Bestellung mit angegeben, so dass der mechanische Zylinder auf die Maße der Tür angepasst werden kann. Bei der Montage kann dann der alte mechanische Zylinder durch den neuen mitgelieferten ausgetauscht werden. Durch eine spezielle Fügestelle an der Innenseite wird die motorische Einheit angeflanscht. Beispielsystem 2 besteht aus den Komponenten der motorischen Einheit, dem mechanischen Schließzylinder und der Applikation auf dem Smartphone.

Für den ordnungsgemäßen Zugang muss die entsprechende Berechtigung in der Applikation hinterlegt sein. Da es sich auch hier um ein Cloud-basiertes System handelt, sind alle Änderungen über eine Web-Schnittstelle konfigurierbar. Es steht hier ein ähnlicher Funktionsumfang zur Verfügung wie bei Beispielsystem 1. So sind Berechtigungen verteilbar oder können auch nur für ein bestimmtes Zeitfenster als Zugang benutzt werden. Auf eine ständige Internetverbindung ist zu achten, um ggf. Modifikationen aktualisieren zu können. Kann dies nicht dauerhaft gewährleistet werden, dann meldet nach einem bestimmten Zeitfenster die interne Aktualisierung einen Fehler und die hinterlegten Berechtigungen in der Applikation sind automatisch deaktiviert. Müssen aber aus zwingenden Gründen einzelne Berechtigungen dauerhaft auch ohne Internetverbindung zur Cloud bestehen, dann ist die Möglichkeit gegeben, eine dafür vorgesehene Fernbedienung einzusetzen. Der Plattformgedanke über die Cloud ermöglicht auch hier die weitere Einbindung von zusätzlichen Komponenten. Diese Betrachtung ist allerdings im Rahmen der Methodenevaluierung nicht weiter von Interesse.

Mit dem Kommunikationsstandard BLE ist es auch für iPhone-Besitzer möglich, das Beispielsystem 2 zu nutzen. Durch den erweiterten Bedienkomfort kann auch auf einer größeren Distanz, im Gegensatz zu NFC, die motorische Einheit angesteuert werden. Allerdings ist für die Funktionsdurchführung ein Antippen des Berechtigungshinweises vonnöten. Somit gleichen sich die Komfortfeatures in gewisser Art und Weise.

Eine sichtbare Veränderung durch den Einsatz des Beispielsystems 2 besteht nicht, da von außen nur ein mechanischer Zylinder sichtbar ist. Möglicherweise können dadurch keine stigmatisierenden Situationen befördert werden. Auch das Interesse von kriminell-motivierten Personen wird hier nicht geweckt.

Weitere Details des Beispielsystems 2 finden sich in den folgenden Kapiteln und Verweisen. Auf zusätzliche Erklärungen wird wiederum verzichtet, da sie für die Evaluierung der Sicherheitsbewertung unerheblich sind.

6.3 Durchführung

Die Durchführung der Evaluierung der ganzheitlichen Sicherheitsbewertung fand teilweise im Austausch mit mehreren Herstellern von Mobile-Access-Systemen statt. Somit war ein guter fachlicher Dialog möglich, der bei Fragen zum Leitfragenkatalog auch zu mancher Zusatzerkenntnis führte. Insbesondere die Anfangsphase wurde intensiv genutzt, um geeignete fiktive Beispielsysteme zu modellieren. Entscheidend ist dabei auch immer die Bereitschaft von Seiten der Hersteller, die eigenen Systeme von einer unabhängigen Stelle analysieren zu lassen. Selbst in Zeiten zunehmender Cyberkriminalität möchten Hersteller nicht in jedem Fall bereitwillig ihre Produkte oder Dienstleistungen für vertrauensbildende Maßnahmen untersuchen lassen. Es überwiegt in den meisten Fällen die Sorge, dass eventuelle Sicherheitslücken zu vorzeitigen Reputationsverlusten führen könnten. Weiterhin müssen die Versprechen von Seiten des Herstellers nicht beweisführend bestätigt sein, da der normale Verbraucher technisch und fachlich nicht in der Lage ist, eventuelle Zusagen zu überprüfen. Bei der Auswahl mehrerer geeigneter Beispielsysteme stand aber eine repräsentative Menge als Querschnitt in der Durchmischung zur Verfügung.

Alle weiteren Schritte (siehe Tabelle 19), die innerhalb der ganzheitlichen Sicherheitsbewertung für die Evaluierung gefordert sind, nehmen Bezug zur selbigen in den folgenden Kapiteln.

Auf eine detaillierte Visualisierung wird hier verzichtet, da sich alle erwähnten Teilergebnisse/-schritte teilweise im Anhang befinden (siehe Verweise im Text). Beschriebene Schlussfolgerungen oder Erkenntnisse sind jedoch verständnishalber im Text erwähnt.

6.3.1 Schritt „Plan"

Im ersten Schritt der „Plan"-Phase wurden für beide Beispielsysteme die Dokumente der Hersteller zusammengetragen. So zeichnete sich schon im Frühstadium der Sicherheitsanalyse ein komplettes Bild über die Funktionsfähigkeit und den Einsatzzweck der Mobile Access-Systeme ab. Auffallend bei den Beispielsystemen war die teilweise nicht ganz vollständige Bereitstellung von dezidierten Unterlagen. Aufgrund der Aktualität der mobilen Dienstleistungen wurden scheinbar alle Kapazitäten in die technologische Entwicklung investiert und alle übrigen Anforderungen, wie beispielsweise Dokumentation oder Produktpräsentation, sind deutlich später entstanden. Mit Hilfe von fest definierten Ansprechpartnern konnten aber die für den Schritt „Plan" nötigen Informationen bereitgestellt werden.

Alle Hersteller haben den Einsatz von IT-Security-Maßnahmen stark befürwortet und verwiesen auf eigene Anstrengungen. Dennoch konnte in den ersten Gesprächen nur bei Beispielsystem 1 eine organisatorische Funktion identifiziert werden, die sich komplett mit dem Thema der IT-Security beschäftigt und dem internen Ausbau dazu forciert. Bei Beispielsystem 2 stammten viele Informationen aus einer Hand; aufgrund der Unternehmensstruktur sind hauptsächliche Informationen vom Entwicklungsleiter selbst weitergegeben worden. Ergänzende Produktpräsentationen konnte das gewonnene Bild klarer aufzeigen. Insbesondere bei Beispielsystem 2 waren zum Zeitpunkt der Analyse keine deutschsprachigen Dokumente verfügbar. Ein erschwertes Verständnis für Teilfunktionalitäten war die Folge. Daher musste hier ein erheblich höherer Zeitaufwand aufgewendet werden als ursprünglich vorgesehen. Leider war es nicht möglich bereits installierte Systeme zu begutachten, weil auch dieser Prozess der Pilotanlagen immer nur zeitlich begrenzt ablief. Es bestand keine Möglichkeit, ein System im realen Einsatz zu sehen. Bei beiden Systemen erhärtete sich der Verdacht, dass viele Prozesse zur Produkteinführung stark bedarfsabhängig gestaltet worden sind oder sich ganz und gar im Aufbau befanden. Dies scheint typisch für kleinere und mittlere Unternehmen zu sein, welche im Zuge von zunehmend benötigten Ressourcen mit wachsenden Anforderungen konfrontiert sind. Im Wesentlichen richtet sich der Fokus auf die Bedürfnisse des Kunden, dabei wird kein allzu großer Wert auf einen stabilen Produkteinführungsprozess gelegt.

Wichtig wäre es aber aus Unternehmersicht, sich einen ausreichenden Überblick über die relevanten Beispielsysteme zu verschaffen; dies schafft die Grundlage für eine

Sicherheitsbewertung. Ein erster Eindruck entsteht zwangsläufig durch erste konkrete Anforderungen an die Hersteller, wie beispielsweise das Zusammentragen der Dokumente.

Nachdem alle zur Verfügung stehenden Unterlagen einen konkreten Überblick der Beispielsysteme ermöglichten, mussten die Informationen auf das Wesentliche reduziert werden. In diesem Schritt lag der Fokus auf den zu untersuchenden Komponenten, die innerhalb der betrachteten Systemgrenze liegen. Da die Beispielsysteme 1 und 2 vernetzte Komponenten beinhalten, erleichterte die bewusste Reduzierung die anschließende Sicherheitsbewertung. Durch einen ähnlichen Leistungsumfang hat sich hier die Aufstellung von Rahmenbedingungen des Mobile Access-Systems als sinnvoll erwiesen. Dazu wurde zu den technischen, organisatorischen und personellen Bezügen (TOP-Themen) Stellung genommen. Bei der Vielfalt der Darstellungsformen, mit denen in UML gearbeitet werden kann, erschien der Typus Anwendungsfall- und Sequenzdiagramm für die Bedarfe geeignet. Das Anwendungsfalldiagramm stellt einzelne Funktionen des Mobile Access-Systems dar und reduziert die Komplexität aus Anwendersicht. Im Sequenzdiagramm sind technologische Abläufe zusätzlich visualisiert, da es im Beispielsystem 1 verschiedene Betriebszustände im Offline- und Online-Modus gibt. Hieraus lassen sich über die Bestimmungen der Systemgrenzen auch die singulären Dienstleistungen ermitteln. Bei den ausführbaren Anwendungen innerhalb der Funktionsspezifika wurde die Gesamtheit „Mobile Access" weiter reduziert. Angefangen bei der Terminologie zur Identifikation der wichtigsten Begrifflichkeiten bis hin zur technischen Visualisierung der internen Abläufe bei NFC und BLE wurden beide Beispielsysteme weiter detailliert (Anhang, Abbildung 37 und Abbildung 38).

Im Ergebnis des ersten Schrittes konnten fachspezifische Begrifflichkeiten identifiziert werden, die es im weiteren Verlauf erleichtern, die Systeme besser zu verstehen. Der Aufbau folgt einer Legende, indem die nicht selbstverständlichen Begrifflichkeiten aufgelistet und erklärt worden sind (Anhang, S. 163 und S. 164). Da sich die Dokumentation bei Beispielsystem 2 noch im Entwurfsstadium befand, war keine deutschsprachige Bedienungsanleitung vorhanden. So können im Nachgang bei der Übergabe der Ergebnisse der Sicherheitsbewertung an den Auftraggeber Missverständnisse entstehen, welche deshalb im Vorfeld zu spezifischen Teilen in einer solchen Übersicht kurz zum eigenen Verständnis erklärt sind. Zusätzlich ergaben sich für die Anwendung bei Evaluationssystem 2 interessante Ansätze für die Erweiterung der Nutzer in Form von Aktivierungskarten. Diese werden einfach über den Web-Account freigeschaltet und anschließend lassen sich weitere Benutzer hinzufügen. Viele weitere Gemeinsamkeiten sind erkennbar und bestätigen das Bild einer sehr ähnlichen Vorgehensweise bei der Benutzung.

An dieser Stelle sollten die Annahmen für die Systeme aufgestellt werden. Die Ergebnisse sind im Anhang für beide Beispielsysteme aufgeführt (Anhang, Tabelle 33 und Tabelle 34). Sie grenzen den Detaillierungsgrad der Sicherheitsbewertung ein und geben die Rahmenbedingungen vor, die für die Analyse maßgeblich sind. Die Vorgaben stellen Bedingungen auf, mit der sich der Prüfer auseinanderzusetzen hat. Voraussetzungen sind dabei die Bezüge zu technischen, organisatorischen und personellen Gesichtspunkten, die abermals direkt oder indirekt beeinflussbar sind. Besonders wichtig werden die Annahmen bei der Definition des Sicherheitsprofils sowohl beim theoretischen wie auch beim praktischen Profil. Das theoretische Sicherheitsprofil soll nur das sinnhafte Security Level fordern, das auch im praktischen Sicherheitsprofil unter Berücksichtigung der Annahmen durchführbar ist. Demnach wurden hier spezifische Bedingungen beachtet. So kann das Beispielsystem 2 nur mit einem SKG-Zylinder eingesetzt werden. Dies ist eine wesentliche Vorgabe vom Produktanbieter, dessen internen Regularien den Einsatz mechanischer Sicherheitszylinder erfordern. In Kombination mit dem Sicherheitsprofil müssen gleichartige Sicherheitslevel auch für ausländische Sicherheitszylinder gefunden werden, wie Tabelle 10 veranschaulicht. Weiterhin nutzen beide Beispielsysteme unterschiedliche Kommunikationstechnologien; beispielsweise bei NFC die Besonderheit der Battery Off-Funktion. Dies bedeutet, dass auch bei ausgeschaltetem Smartphone ein Zugang bei abgespeicherter Berechtigung möglich ist. Ob diese Funktion in Verbindung mit dem Einsatzzweck eine Rolle spielt, wird beim Sicherheitsprofil Beachtung finden. Beide Systeme haben den Zweck, den persönlichen Bereich respektive die Privatsphäre zu sichern. Sie stellen somit höhere Anforderungen an die Mobile Access-Systeme; wie z. B. das Sichern von Stromverteilerkästen in den Städten. Explizit bei Beispielsystem 2 kommt noch hinzu, dass z. B. bei einem Einsatz von Mobile-Access-Systemen im

Bereich der häuslichen Pflege eine Zutrittsgewährung an externes Pflegepersonal erfolgen muss. Hier soll eine aufwändige Schlüsselverwaltung vermieden werden. Unabhängig davon müssen alle Anwender ein technisches Grundverständnis und Zugang zu neuen Technologien haben. Es besteht zudem die Gefahr, dass ein Smartphone verlegt und dadurch ggf. unbefugten Personen ein Zugang ermöglicht wird. Diese aufgezeigten Beispiele unterstreichen die Notwendigkeit, grundlegende Annahmen aufzustellen, die als Vorbereitung der Einzelschritte im theoretischen und praktischen Sicherheitsprofil dienen.

Um das einzelne Leistungsspektrum des jeweiligen Mobile Access-Systems zu durchdringen, stellte die *Modellierung in UML* eine praktikable Methodik dar. So sind in einzelnen Schritten die grundlegenden Leistungsmerkmale evaluiert und im Anwendungsfalldiagramm (Anhang, Abbildung 39 und Abbildung 40) abgebildet worden. Grundlegende Funktionen wie Zugangsfreigabe, Hinzufügen von Zylinder, Freigabe von Personen, Synchronisation etc. sind bei beiden Beispielsystemen erwähnt und beschrieben. Beide Systeme erfordern eine einmalige Initialisierung zur Registrierung ihrer Komponenten und möglicher (mehrerer) Anwender. Der weitere Detaillierungsgrad bestätigt die Vermutung des schon erwähnten gleichartigen Funktionsumfangs. Selbst die Möglichkeit, mithilfe weiterer digitaler Medien als nur das Smartphone Berechtigungen abzuspeichern, sind in beiden Beispielsystemen möglich und beschrieben. In allen Fällen läuft die Initialisierung und Programmierung über die jeweilige Cloud-Plattform. Temporär sind allerdings alle Daten auch zum Zugang auf dem Smartphone gespeichert. Für den Fall, dass die Internetverbindung dauerhaft oder auch temporär abbricht oder Bereiche ohne Internetverbindung (z. B. Tiefgarage) betreten werden, erscheint dies sinnvoll. Unterscheiden lassen sich noch die Prozesse für die allgemeine Verwaltung, die nur vom Besitzer ausgeführt werden können, sowie die der Anwendung, die nur vom Benutzer ausgeführt werden können. Demnach lassen sich hier mindestens zwei unterschiedliche Hierarchieebenen erkennen, mit der sich bestimmte Funktionalitäten nur über den entsprechenden Benutzerkreis ausführen lassen. Bei der technologischen Umsetzung wurde das Sequenzdiagramm eingesetzt (Anhang, Abbildung 41 und Abbildung 42). Es beschreibt in optimal reduzierter Form alle wesentlichen Elemente zur Umsetzung inklusive ablaufender Dienstleistungspakete. Positiv auffallend waren hier bei Beispielsystem 1 das umfangreiche Identitätsmanagement und bei Beispielsystem 2 der Verschlüsselungsalgorithmus AES zwischen der motorisch-angesteuerten Einheit an der Tür und dem Smartphone. Weitere Security-Lösungen, wie eine gesicherte Internetverbindung über HTTPS, sind aus dem Diagramm ersichtlich. Abschließend kann konstatiert werden, dass die Modellierung über die UML-Werkzeuge von der Handhabung mithilfe des Anwendungsfalldiagramms bis zur eigentlichen Technologieumsetzung mithilfe des Sequenzdiagrammes instruktive Erläuterungen gegeben hat. Die UML-Bearbeitung kann mit jedem beliebigen Tool (z. B. Microsoft Visio) erfolgen und dient nur als adäquate Umsetzungshilfe.

Im nächsten und wichtigen Schritt der Bestimmung des Sicherheitsprofils geht es um die sinnhafte Einordnung des Mobile Access-Systems in das theoretische Sicherheitsprofil mit zweckmäßiger Ausrichtung (Anhang, ab S. 171 und ab S. 173). Da es sich um einen ähnlichen Funktionsumfang und Anwendungszweck handelt, sind beide Beispielsysteme identisch eingestuft wurden. In Folge handelt es sich um das theoretische Sicherheitsprofil 2|2|3|3. Für die Qualität des theoretischen Sicherheitsprofils gilt folgendes:

-Angreiferklasse (Anwender, 2): Der Anwender lässt sich exemplarisch durch den Endnutzer des Dienstes beschreiben. Sein physikalischer Zugang zum System ist in der Regel unbegrenzt und er ist im Besitz geringer technischer Fähigkeiten, d.h. seine Möglichkeiten liegen lediglich in der Benutzung des Systems ohne weiterführendes Wissen. Für die Implementierung von Sicherheitsfunktionen ist der finanzielle Einsatz daher gering.

-Kompromittierung sensibler Daten (Gefährdend, 2): Das Gefahrenpotenzial ist für die Kompromittierung von sensiblen Daten stark erhöht. Es kann mit hoher Sicherheit nicht ausgeschlossen werden, dass Daten in die Hände von Dritten gelangen können. Dabei sind die Zugangsmöglichkeiten für Unbefugte mit einem geringen Fertigkeitsaufwand möglich respektive die Daten liegen offensichtlich vor. Besonders betroffen sind hier auch die persönlichen Daten - Datenschutz beeinträchtigt!

-Usability (Service oder Gerät funktionslos, 3): Bei der Kompromittierung des Kriteriums ist entweder der Service oder das Gerät funktionslos. Die resultierende Sicherheitslücke weist dadurch eine Unsicherheit in Bezug auf unbefugte Handlungen/Aktivitäten der funktionslosen Komponente auf.

-Ausprägung (Basis, 3): Die Implementierung des Kriteriums ist in Grundzügen vorhanden. Dabei werden lediglich minimale Standards erreicht, die für dieses Kriterium von Nöten sind. Dabei können mindestens drei Fragen für das Untersuchungsobjekt positiv beantwortet werden.

Für die mechanischen Voraussetzungen gilt für das Beispielsystem 1 folgendes (Tabelle 20):

	DIN 15684:2013-01 (2)
Gebrauchskategorie (1)	1
Dauerhaftigkeit (2)	6
Feuer-/Rauchwiderstand (3)	B
Umweltbeständigkeit (4)	4
Mechanische Verschlusssicherheit (5)	A
Elektronische Verschlusssicherheit (6)	F
Systemmanagement (7)	3
Angriffswiderstand (8)	2

Tabelle 20: Mechanische Voraussetzungen (Beispielsystem 1)[225]

Für die mechanischen Voraussetzungen gilt für das Beispielsystem 2 die Einstufung 18252-82 (BZ)[226].

Da im Außenbereich bei Beispielsystem 1 ein Knaufzylinder angebracht ist und beim Beispielsystem 2 ein mechanischer Schließzylinder, gelten demnach unterschiedliche Normenvoraussetzungen. Zur Vergegenwärtigung siehe nochmals Tabelle 10.

Der Detaillierungsumfang des Leitfragenkatalogs und der zu erfüllenden mechanischen Voraussetzungen sind somit festgelegt. Alle Arbeitsschritte für die Phase „Plan" konnten erfolgreich abgeschlossen werden und leiten die nächste Phase „Do" ein.

6.3.2 Schritt „Do"

Die Phase „Do" beschreibt nun die wesentliche Anwendung der ganzheitlichen Sicherheitsbewertung. Beide Beispielsysteme müssen sich an den inhaltlichen Anforderungen aus den Rahmenwerken der CC und des BSI messen lassen sowie an der Forderung des theoretischen Sicherheitsprofils. In der Prüftiefe des theoretischen Sicherheitsprofils müssen im Leitfragenkatalog zu jedem Themenbereich drei Fragen ausgewählt werden. Ein voller Prüfumfang wäre einschließlich der relevanten Implementierungsfragen erfüllt, bleibt hier mit den Anforderungen aber unberücksichtigt. Aufgrund guter Vorbereitungsarbeiten können beide Systeme bereits fachlich eingeschätzt werden, und die Auswahl fällt somit leichter und konnte besser auf die Bedürfnisse angepasst werden. Der Schritt „Do" umfasst die Bereiche der Komponenten und Service, die simultan zur Anwendung kommen.

Mithilfe der (verschiedenen) Herstellervorgaben konnten die einzelnen Produktzertifizierungen relativ leicht in Erfahrung gebracht werden. Auch wenn es sich noch um Produkte handelt, die einen Vorserienstatus aufweisen, existieren bereits die notwendigen Zertifikate. In der Regel lassen sich diese auch auf den jeweiligen Internetseiten der Hersteller abrufen, auch weiterführende Zertifikatsinhalte oder sonstige Konformitätserklärungen sind hier einsehbar. Im Ergebnis erfüllen beide Beispielsysteme die normativen Anforderungen des theoretischen Sicherheitsprofils. Es konnte sogar eine höhere Konformität bestätigt werden als verlangt. Lediglich Beispielsystem 2 findet seinen Absatz verstärkt in den Niederlanden, daher wurden die normativen Anforderungen auf diese Besonderheit angepasst und finden sich schon ergänzt in Tabelle 10. Das Ergebnis wird in einem weiteren Schritt der Wahrscheinlichkeitsbestimmung respektive Risikobewertung

[225] Vgl. DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013, S. 36 ff.
[226] Vgl. DIN 18252, Profilzylinder für Türschlösser, 2006, S. 11 ff.

dokumentiert. Für den Strang der Komponenten fand die Durchführung des Leitfragenkataloges Anwendung. Wichtig sind hier die Resultate aus den Leitfragen, deren Informationsgehalt eine Abschätzung zum theoretischen Sicherheitsprofil mittels der vier Vorgaben respektive Qualitäten zulässt. Eine sofortige Bewertung im Hinblick auf das Sicherheitsprofil erwies sich als sinnvoll und zugleich zeitsparend. Sicherlich sind Grenzen der Erfüllung oder Nicht-Erfüllung abhängig von der subjektiven Einschätzung des Prüfers, aber durch die genannten Vorarbeiten kann im gewissen Rahmen eine Professionalisierung gefördert werden. Rein objektive Bewertungen hätten den Nachteil, dass ein starrer Rahmen gesetzt würde, der nicht adäquat für die Bewertung technologischer Zukunftsfelder geeignet wäre. Zum besseren Verständnis ist ein fiktiver Beispielbogen aus dem Leitfragenkatalog in Abbildung 34 angeführt.

Nr.1 Komplexität der Zugangsmöglichkeiten

Welche Zugangsmöglichkeiten gibt es prinzipiell?

Der Zugang ist nur über die Management-Secure-Plattform möglich. Über diese wird die gesamte Verwaltung des Systems organisiert. Detailliert, wie folgt:

[…]

Welche Systematik liegt dem Anmeldeprozess zugrunde?

Die Autorisierung wird derzeit mithilfe einem Aktivierungsprozess durchgeführt. Dazu sind folgende Schritte notwendig:

[…]

Sind Aktionen vor dem ordentlichen Zugang möglich?

Für den ordentlichen Zugang wird ein Aktivierungscode und spezielle Sicherheitsfragen eines Schließgerätes benötigt. […]

Abgleich zum Sicherheitsprofil:

Zur Ausprägung des theoretischen Sicherheitsprofils können in allen vier Kriterien keine eklatanten Differenzen festgestellt werden. Alle getroffenen Sicherheitsmaßnahmen entsprechen dem theoretischen Sicherheitsprofil. […]

Abbildung 34: Beantwortung Leitfragenkatalog (Beispiel)[227]

Detaillierte Ergebnisse zu den Beispielsystemen sollten sich jeweils im Abschnitt „Abgleich zum Sicherheitsprofil" befinden. Durchgeführt wurde die Befragung in unterschiedlicher Weise: Es gab zunächst eine Zusammenstellung der Fragen, die dem zuständigen Ansprechpartner bei verschiedenen Herstellern einen Einblick in die Fragen ermöglichten. Gleichermaßen wurden mehrere Abstimmungstelefonate durchgeführt, um die Ergebnisse Schritt für Schritt besprechen und diskutieren zu können. Diese Wechselwirkung zwischen Prüfer und Ansprechpartner beim Hersteller verfestigte ein Vertrauensverhältnis, das sich auch in der Qualität der beantworteten Fragen widerspiegelt. Alle Hersteller waren während der gesamten Analysephase zu einer konstruktiven Kooperation bereit. Aus den einzelnen Ergebnissen wurde die (fiktive) Beantwortung der Beispielsysteme 1 und 2 konstruiert.

Fast nahtlos ging die Zusammenstellung der Assets sowie der bedrohlichen Sicherheitslücken in beide Stränge des Bereichs Komponenten/Service über (Anhang, Tabelle 35, Tabelle 36, Tabelle 37 und Tabelle 38). Er kennzeichnete den freien Teil der Sicherheitsanalyse. Zum Schluss des Analyseteils konnten nochmals alle Erkenntnisse für eine kritische Betrachtung der möglichen Sicherheitslücken zu Rate gezogen werden. Auch im Hinblick eventuell unvollständiger Normen für diese Technologiefelder, ergibt sich der nötige Freiraum zur Ergänzung. Im Abschluss findet die Risikobewertung aller eruierten Informationen statt.

[227] Eigene Darstellung.

Damit gehen die Arbeitsschritte Komponenten/Service und die jeweiligen Assets-Betrachtungen in die Wahrscheinlichkeitsbetrachtung der Bedrohungen und Angriffe über (siehe Abbildung 30).

Alle Arbeitsschritte für die Phase „Do" konnten erfolgreich abgeschlossen werden und leiteten die nächste Phase „Check" ein.

6.3.3 Schritt „Check"

Die Übernahme der Assets-Betrachtung in die Wahrscheinlichkeitsbewertung (Bedrohungen/Angriffe) respektive Risikobewertung beschreibt einen formalen Akt, der in derselben Formatvorlage Anwendung findet. Der Bezugspunkt zum Abgleich des Sicherheitsprofils ebnet den Weg zur vollständigen Risikobetrachtung aufgrund der semi-quantitativen Ausführung. Da sich die Anforderungen auf mechanischer und elektronischer Seite unterscheiden, ist die Zusammenführung der Teilergebnisse in einem mechanischen und elektronischen Teil dargestellt. Beide Teilergebnisse haben als Referenz aber das selbe theoretische Sicherheitsprofil. Eine geordnete Kriterienauswahl stellt nochmals die wichtigsten Punkte zur Bewertung auf. Die strukturellen Vorgaben werden aus Tabelle 15 ersichtlich. Folgende Beispiel anhand der Formatvorlage erläutert die Vorgehensweise der für die Beispielsysteme erarbeiteten Ergebnisse (Anhang: Tabelle 39, Tabelle 40, Tabelle 41, Tabelle 42, Tabelle 43 und Tabelle 44):

1. Durchlaufende Nummer für jede einzelne Position zur späteren Identifizierung der Gesamtpositionen (Beispiel: 1.)

2. Stichpunktartige Darstellung vom Kriterium zur inhaltlichen Zuordnung der freien Ideensammlung (Asset) oder mit Bezug aus dem Fragenkatalog (Leitfragenkatalog)

3. Das theoretische Sicherheitsziel für die jeweils abgeleitete elektronische oder mechanische Vorgabe (Beispiel: 2|2|3|3 oder DIN EN 15684)

4. Beschreibung des Soll-Zustands: Wurde dieser erfüllt oder ist eine Abweichung feststellbar (Beispiel: Erfüllt, nicht erfüllt)? Der Zustand „nicht erfüllt" oder gleichwertige Abweichungen kommen insbesondere dann zum Tragen, wenn aus der freien Ideensammlung (Assets) die mögliche Abstellmaßnahme nicht in der geltenden Norm berücksichtigt wurde und auch keine aus den vorherigen Analyseschritten bekannte Gegenmaßnahme implementiert wurde. Auf elektronischer Seite sind es hier die Abweichungen aus dem Leitfragenkatalog, die bei der Evaluierung entdeckt wurden und eine Differenz zum geforderten Niveau der jeweiligen Leitfrage darstellen (Vergleich zum Sicherheitsprofil).

5. Der Ist-Zustand beschreibt die aktuelle Normung des Beispielsystems oder das bewertete praktische Sicherheitsprofil mit Abwertung der Qualität bezüglich des theoretischen Sicherheitsprofils (Beispiel: 2|2|3|3 als theoretisches Sicherheitsprofil ergibt für das mögliche praktische Sicherheitsprofil die Bewertung 2|2|3|2. Daraus resultiert die einfache Abwertung um eine Stelle in der Qualität „Ausprägung".).

6. Das Asset beschreibt für das Kriterium den bedrohlichen Zustand respektive dessen Auswirkung (Beispiel: direkter Zugang Privatsphäre).

7. Die anschließende Berechnungsgrundlage dient zur semi-quantitativen Bestimmung. Abgeleitet aus den aufgestellten und allgemeinen Definitionen wird die Wahrscheinlichkeit des möglichen Eintritts dieser definierten Sicherheitslücke beschrieben. Der Schaden bewertet das ungefähre Ausmaß im Fall des Eintrittes. Werden beide Zahlenwerte miteinander multipliziert, ergibt sich die Risikozahl, die wiederum mit einer Gewichtung versehen den Risikograd angibt. Damit der Grad der Abweichung berücksichtigt wird, multipliziert man die Gewichtung mit einem entsprechenden Faktor mit der Risikozahl und beeinflusst damit entscheidend die Priorität des Kriteriums. Elektronische Abweichungen, also die Differenz zum theoretischen Sicherheitsprofil, wird überproportional gewichtet, da es in allen vier Qualitäten Abweichungen geben kann. Dies bedeutet beispielsweise eine maximale Abweichung von einem fiktiven theoretischen Sicherheitsprofil mit der Einstufung 2|2|3|3 um den Faktor 6 (0|0|0|0). Auf mechanischer Seite kann die maximale Gewichtung bei 1 liegen, da das Sicherheitsziel hier die mechanische Normung beschreibt, die

entweder den Zustand „erfüllt" oder „nicht erfüllt" einnehmen kann. Welche quantitative Abstufung zur Beurteilung festgelegt wird, ist noch individuell abstimmbar.

8. Die Bemerkungen ergänzen den Bewertungsprozess mit einem individuellen Zusatz.

In Kombination mit den dargestellten Erklärungen lassen sich die Dokumente der Wahrscheinlichkeitsbestimmung für beide Beispielsysteme leichter nachvollziehen. Für die Evaluierung der ganzheitlichen Sicherheitsbewertung konnte eine gute Umsetzbarkeit der in der Theorie aufgestellten Überlegungen festgestellt werden. Alle vorangegangenen Bedingungen und Voraussetzungen ließen sich auf beide Beispielsystemen übertragen. Im Detail sind über die Leitfragenkataloge oder auch die Normenvoraussetzung genau definierbare Sicherheitslücken aufgedeckt worden, welche anschließend semi-quantitativ beurteilt wurden. In Gänze kann keine ausführliche inhaltliche Darstellung stattfinden, da es sich um eine Evaluierung der Sicherheitsmethode handelte. Eine Zusammenfassung der im Anhang beschriebenen Dokumente visualisieren die folgende Tabelle 21 sowie Tabelle 22, die Evaluierungsergebnisse als Folge der Berechnungsgrundlage für die Sicherheitsbewertung zeigen.

Beispielsystem 1						
Kriterium	Sicherheitsziel	Ergebnis	Risikozahl	Gewichtung	Risikograd	A_{kS}
Mechanisch/ Komponente						
Normung erfüllt	DIN EN 15684 (2)	Erfüllt	-	-	-	
Knauf abschlagen/treten	DIN EN 15684 (2)	Erfüllt	10	0	0	
Knauf abschlagen	DIN EN 15684 (2)	Theoretisch möglich	10	0	0	
Zylinder aufbohren	DIN EN 15684 (2)	Erfüllt	8	0	0	
Zylinder fluten	DIN EN 15684 (2)	Erfüllt	8	0	0	
Stigmatisierung	DIN EN 15684 (2)	Nicht erfüllt	60	1	60	
Angriff mit Magnet	DIN EN 15684 (2)	Erfüllt	6	0	0	
Knauf wird in Rotation versetzt	DIN EN 15684 (2)	Erfüllt	8	0	0	
Elektronisch/ Service						
Aufdrehen v. innen	2|2|3|3	Erfüllt	10	0	0	
Smartphone verloren/geklaut	2|2|3|3	0|2|3|0	100	3	300	
Aktualisierung unterbrechen	2|2|3|3	0|2|3|3	60	1	60	
Zugangsschlüssel gehackt	2|2|3|3	Erfüllt	10	0	0	
Internes Sicherheits-management ausnutzen	2|2|3|3	0|0|2|0	60	5	300	
Entleerte Batterien	2|2|3|3	Erfüllt	10	0	0	
Update Funktion	2|2|3|3	0|2|2|0	60	4	240	
Methodische Fehler	2|2|3|3	0|0|2|0	36	5	180	
Security-Lücken	2|2|3|3	Erfüllt	10	0	0	
Karte verloren	2|2|3|3	0|2|3|0	100	3	300	
Smartphone entladen	2|2|3|3	Erfüllt	1	0	0	
Verlust gespeicherter Daten	2|2|3|3	2|2|3|2	24	1	24	

Software-Schwachstellen oder Fehler	2|2|3|3	2|2|3|2	60	1	60	
Gefälschte Zertifikate	2|2|3|3	2|2|3|2	60	1	60	
Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services	2|2|3|3	0|2|2|0	36	4	144	
Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung	2|2|3|3	2|2|3|2	24	1	24	
Unzureichende Kontrolle der Sicherheitsmaßnahmen	2|2|3|3	0|0|2|2	36	4	144	
Fehlerhafte Administration von Zugangs- und Zugriffsrechten	2|2|3|3	2|2|3|0	8	2	16	
Manipulation an Informationen oder Software	2|2|3|3	2|2|2|2	60	2	120	
Vertraulichkeitsverlust schützenswerter Informationen	2|2|3|3	2|0|3|3	60	1	60	
Unberechtigtes Überschreiben oder Löschen von Archivmedien	2|2|3|3	0|0|0|0	12	6	72	
Vertraulichkeitsverlust durch Auslagerungsdateien	2|2|3|3	0|0|0|0	8	6	48	

Tabelle 21: Wahrscheinlichkeitsbestimmung/Risikobewertung Beispielsystem 1[228]

Beispielsystem 2						
Kriterium	Sicherheitsziel	Ergebnis	Risikozahl	Gewichtung	Risikograd	A_{kS}
Mechanisch/ Komponente						
Normung erfüllt	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	-	-	-	
Zylinder an der Trennlinie aufbohren	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Zylinder unterhalb der Trennlinie aufbohren	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Herausziehen des Zylinderkerns	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Herausbrechen des Zylinders mit der Zange	DIN 18252 Klasse 82 (BZ)	Annahmen beachten, korrekter Einbau!	60	0	0	
Handpicking	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Elektropicking	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Schlagtechnik	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	

[228] Eigene Darstellung.

Impressionstechnik	DIN 18252 Klasse 82 (BZ)	Erfüllt (SKG3)	10	0	0	
Elektronisch/ Service						
Aufdrehen v. innen	2|2|3|3	Erfüllt	10	0	0	
Smartphone verloren/gestohlen	2|2|3|3	0|2|3|0	100	3	300	
Aktualisierung unterbrechen	2|2|3|3	Erfüllt	10	0	0	
Zugangsschlüssel gehackt	2|2|3|3	Erfüllt	10	0	0	
Internes Sicherheits-management ausnutzen	2|2|3|3	0|0|2|0	60	5	300	
Entleerte Batterien	2|2|3|3	Erfüllt	10	0	0	
Update Funktion	2|2|3|3	0|2|2|0	60	4	240	
Methodische Fehler	2|2|3|3	0|0|2|0	36	5	180	
Security-Lücken	2|2|3|3	0|2|2|0	60	4	240	
Fernbedienung verloren	2|2|3|3	0|2|3|0	100	3	300	
Smartphone entladen	2|2|3|3	2|2|0|3	36	2	72	
Software-Schwachstellen oder Fehler	2|2|3|3	2|2|2|2	36	2	72	
Unzureichende oder fehlende Verbindungs-sicherheitsmechanismen	2|2|3|3	2|2|2|0	36	3	108	
Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung	2|2|3|3	2|2|3|0	36	2	72	
Fehlende oder Unzureichende Sicherheitsmechanismen in Anwendungen	2|2|3|3	2|2|2|2	36	2	72	
Unerlaubte Ausübung von Rechten	2|2|3|3	2|0|3|3	60	1	60	
Manipulation an Informationen oder Software	2|2|3|3	0|0|0|0	36	6	216	
Software mit unerlaubten Zugriff	2|2|3|3	0|0|0|0	8	6	48	
Kompromittierung kryptographischer Schlüssel	2|2|3|3	2|0|3|2	100	2	200	
Vertraulichkeitsverlust durch Auslagerungsdateien	2|2|3|3	0|0|0|0	8	6	48	

Tabelle 22: Wahrscheinlichkeitsbestimmung/Risikobewertung Beispielsystem 2 [229]

Bei weiterer Betrachtung sind die Ergebnisse von hoher Priorität und hinterlassen schon an dieser Stelle ein umfängliches Bild zum umgesetzten Sicherheitsniveau der beiden Evaluationssysteme.

6.3.4 Schritt „Act"

Im letzten Schritt der Sicherheitsbewertung verdichteten sich alle gesammelten Erkenntnisse zu einem semi-quantitativen Ergebnis. Es wurde ein spezifischer Erfüllungsgrad (S) für die Herstellersicht und die Anforderungen der kritischen Sicherheit über Zustandsfarben für die

[229] Eigene Darstellung.

Kundensicht (Z) erreicht, der sowohl den mechanischen als auch elektronischen Teil berücksichtigte. Wichtigste Grundlage dafür war die semi-quantitative Bewertung unter Berücksichtigung einer gewichteten Risikobeurteilung auf Basis von Tabelle 18. Im Ergebnis sollten idealerweise prägnante und nachvollziehbare Werte ausgewiesen werden, die für Kunden und Hersteller gleichermaßen akzeptabel sind. Wie sich in den nachfolgenden Ergebnissen der Beispielsysteme zeigt, lassen die unterschiedlichen Sichtweisen der Adressaten (Kunde und Hersteller) völlig andere Schlussfolgerungen zu, die nicht miteinander vergleichbar sind: Den vermeintlich positiven Erfüllungsgraden stehen die schlechten Ergebnisse der Zustandsfarben aus Kundensicht gegenüber. Für die Bewertung der Anforderungen der kritischen Sicherheit pro Kriterium sind Tabelle 21 und Tabelle 22 mit den farblichen Kennungen ergänzt worden, die unter Berücksichtig von Tabelle 17 aus der Datengrundlage von Tabelle 39 bis Tabelle 44 gebildet worden sind. Die farbliche Zuordnung von Schaden, Wahrscheinlichkeit und Gewichtung der Tabelle 39 bis Tabelle 44 ist mithilfe der Tabelle 16 und den Gleichungen (6), (7) und (8) ermittelt worden.

Die konkrete Evaluierung hat bei Beispielsystem 1 zu folgendem Ergebnis geführt (Abbildung 35):

Ergebnisdarstellung

Systembaustein	Bearbeiter	Datum
Beispielsystem 1	*Arne Schwerdtfeger*	*2017*
Kritisches Element	Status	Verantwortlicher / Leitung
Mechanisch/Elektronisch	*Ergebnis*	*Eigenverantwortliche Leitung*
Funktion	Anmerkung	Ergebnis
Gesamtfunktionalität		*Gesamtergebnis*

Ergebnis:

Wahrscheinlichkeiten - kritische Elemente mechanisch - sekundär (Check/Teil 3)

Theoretische Gesamtwahrscheinlichkeit [TG3]:	700
Maximale Einzelgewichtung [G3]:	1
Theoretische Gesamtpunktzahl:	700
Praktische Gesamtpunktzahl [PG3]:	60
Sekundärer Teilerfüllungsgrad [a]:	**91**

Wahrscheinlichkeiten - kritischer Elemente elektronisch - primär (Check/Teil 4)

Theoretische Gesamtwahrscheinlichkeit [TG4]:	2200
Maximale Einzelgewichtung [G4]:	6
Theoretische Gesamtpunktzahl:	13200
Praktische Gesamtpunktzahl [PG4]:	2152
Primärer Teilerfüllungsgrad [b]:	**84**

Berechnungsgrundlage

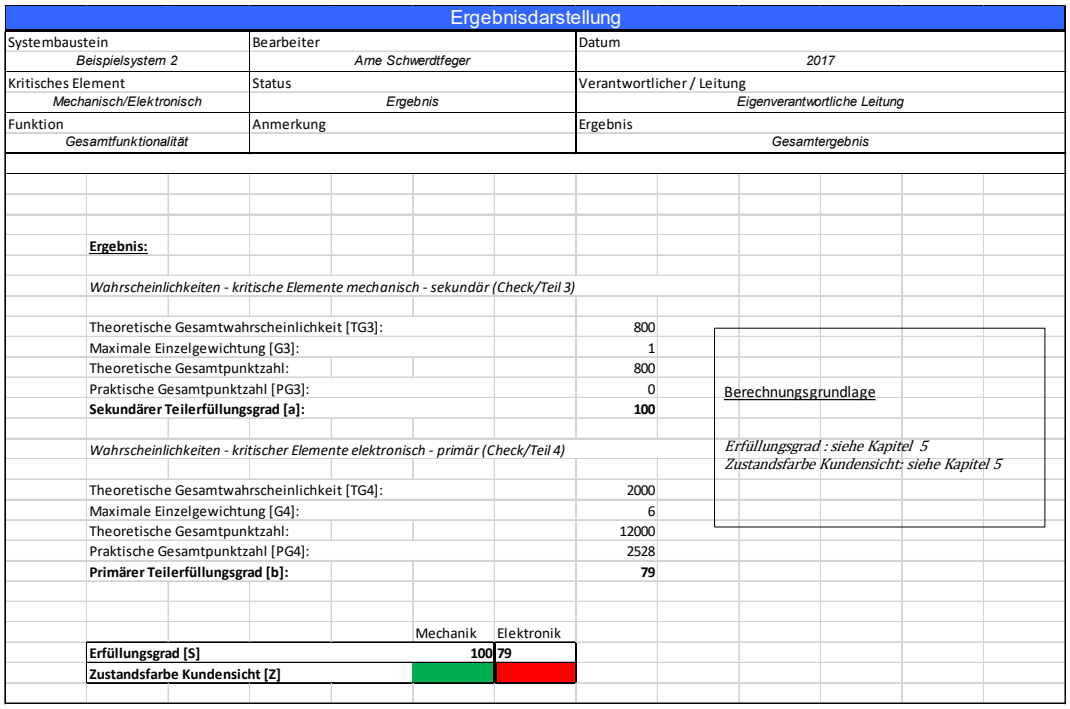
Erfüllungsgrad : siehe Kapitel 5
Zustandsfarbe Kundensicht: siehe Kapitel 5

	Mechanik	Elektronik
Erfüllungsgrad [S]	**91**	**84**
Zustandsfarbe Kundensicht [Z]		

Abbildung 35: Ergebnisdarstellung Beispielsystem 1[230]

Für das Beispielsystem 2 hat sich folgendes Ergebnis gezeigt (Abbildung 36):

[230] Eigene Darstellung.



Ergebnisdarstellung

Systembaustein	Bearbeiter	Datum
Beispielsystem 2	*Arne Schwerdtfeger*	*2017*
Kritisches Element	Status	Verantwortlicher / Leitung
Mechanisch/Elektronisch	*Ergebnis*	*Eigenverantwortliche Leitung*
Funktion	Anmerkung	Ergebnis
Gesamtfunktionalität		*Gesamtergebnis*

Ergebnis:

Wahrscheinlichkeiten - kritische Elemente mechanisch - sekundär (Check/Teil 3)

Theoretische Gesamtwahrscheinlichkeit [TG3]:	800
Maximale Einzelgewichtung [G3]:	1
Theoretische Gesamtpunktzahl:	800
Praktische Gesamtpunktzahl [PG3]:	0
Sekundärer Teilerfüllungsgrad [a]:	**100**

Wahrscheinlichkeiten - kritischer Elemente elektronisch - primär (Check/Teil 4)

Theoretische Gesamtwahrscheinlichkeit [TG4]:	2000
Maximale Einzelgewichtung [G4]:	6
Theoretische Gesamtpunktzahl:	12000
Praktische Gesamtpunktzahl [PG4]:	2528
Primärer Teilerfüllungsgrad [b]:	**79**

Berechnungsgrundlage

Erfüllungsgrad : siehe Kapitel 5
Zustandsfarbe Kundensicht: siehe Kapitel 5

	Mechanik	Elektronik
Erfüllungsgrad [S]	**100**	**79**
Zustandsfarbe Kundensicht [Z]		

Abbildung 36: Ergebnisdarstellung Beispielsystem 2[231]

Trotzdem lassen sich innerhalb einer Sichtweise Ergebnisse referenzierter Basen der Sicherheitsbewertung erzielen. Es konnten somit die jeweiligen Ergebnisse der Hersteller- oder Kundensicht direkt miteinander verglichen werden. Demnach konnte auch innerhalb der Sichtweisen eine präferierte Priorität festgestellt werden. Die Interpretation der Ergebnisse kann somit ganz unterschiedlich ausfallen und auf die Bedürfnisse angepasst werden. Unabhängig von der Ergebnisdarstellung konnte die Evaluierung, wie in den vorherigen Kapiteln bereits dargelegt, vollständig durchgeführt werden, so dass eine Anwendung für hier vorgestellten Mobile Access-Systeme möglich wurde.

Konkrete Ergebnisse in der Sicherheitsbewertung aus Herstellersicht belegen, dass beide Systeme eigentlich gute Ergebnisse im mechanischen Teilerfüllungsgrad mit 91 und 100 zeigen. Lediglich ein geringer Aufwand ist für den Hersteller bei Beispielsystem 1 nötig, um Produktverbesserungen für eine vollständige Teilerfüllung zu erreichen. Die guten Ergebnisse in der Mechanik bei System 2 lassen sich auch dadurch erklären, dass mit einer Kombination aus motorisch angetriebener Einheit und mechanischem Schließzylinder die guten Vorarbeiten aus den bestehenden Normungen Anwendung finden. Für den elektronischen (primären) Part sind die Ergebnisse genau gespiegelt. Hier konnte das System 1 mit einem Erfüllungsgrad von 84 zu 79 besser bewertet werden; respektive zeigten sich geringere Aufwendungen, um die Konformität mit dem theoretischen Sicherheitsprofil zu erreichen.

Die eigentlich guten Herstellerergebnisse täuschen nicht über das schlechte Ergebnis in der Sicherheitsbewertung bei den Zustandsfarben aus Kundensicht hinweg. Die vorangegangenen Überlegungen, die eine differenzierte Sichtweise für unterschiedliche Verwertungen der Ergebnisse forderte, belegen dies. Für den Hersteller sind die Aufwendungen der Produktverbesserungen von Bedeutung, aber der Kunde erachtet für seine persönlichen Anforderungen die gezielte Umsetzung von Sicherheitsmaßnahmen als wichtiger. Demnach stehen die Aufwendungen des Herstellers nur indirekt in Verbindung mit den Anforderungen des Kunden. Begründet liegt dies in den bereits angesprochenen kritischen Pfaden. Beide Beispielsysteme können bezüglich der Anforderungen an die kritische Sicherheit für den elektronischen Bereich nicht überzeugen und erreichen nicht die geforderte Konformität (siehe Tabelle 18). In beiden Fällen liegt mehr als ein Kriterium innerhalb des roten Bereiches. Für ein besseres Resultat müssen also die relevanten kritischen Pfade erheblich nachgebessert werden, damit zumindest eine konforme Wertung in die farbliche Kennung

[231] Eigene Darstellung.

„gelb" übergeht. Gleichzeit sollte gemäß Tabelle 16 der Schaden stärker begrenzt sein, was sich evtl. auch erneut in der Detailierung der Grenzen bei den Wahrscheinlichkeitstabellen wiederspiegeln könnte. Im Detail bedeutet dies die Nacharbeit des Produktes von 17 kritischen Kriterien bei Beispielsystem 1 und 15 Kriterien bei Beispielsystem 2. Hier zeigen die Teilerfüllungsgrade von 84 und 79 einen ungefähren Aufwand für die Hersteller auf. Auf mechanischer Seite kann nur das Beispielsystem 2 überzeugen. Ob die Stigmatisierung bei Beispielsystem 2 nun zu einer gänzlichen Abwertung im mechanischen Bereich führen sollte, hängt auch wesentlich vom Einsatzzweck ab. Kann es zur Anwendung im privaten Pflegebereich kommen, wie im Beispielsystem 2, dann sollten alle Hinweise auf eine ggf. wehrlose Person im Inneren des Hauses vermieden werden. Es zeigt aber die Vielschichtigkeit der Folgen für eine Sicherheitsbewertung auf und erlaubt in diesem Rahmen eine weiterführende Diskussion. In letzter Konsequenz bleibt den Herstellern bei einer Verbesserung der Sicherheitsbewertung nur die explizite Auseinandersetzung mit jedem einzelnen Kriterium. Nach den in der ganzheitlichen Sicherheitsbewertung geltenden Rahmenbedingungen haben die hier gezeigten Beispielsysteme nicht überzeugen können, d. h. eine Konformität zum theoretischen Sicherheitsprofil 2|2|3|3 kann nicht bestätigt werden. Eine erneute Evaluierung nach erfolgten Nachbesserungen am Produkt ist also notwendig. Dafür ist es zwingend erforderlich, dass beide Parteien (Hersteller und Evaluierungsstelle) eng miteinander im Austausch stehen, um eine erneute Bewertung nur auf den benötigten Rahmen der Änderungen zu beschränken. So wird eine Minimierung von Aufwand und Kosten für den Hersteller sichergestellt.

Letztlich wurde die Evaluierung der Sicherheitsbewertung erfolgreich abgeschlossen. Eine genauere Betrachtung und Ergebnisanalyse ist nicht Gegenstand der Forschungsfrage. Laufende Ansätze zur Beurteilung finden sich aber im Verlauf der Arbeit wieder.

6.4 Ergebnis der Methodenevaluierung

Die Methodenevaluierung konnte erfolgreich zum Abschluss gebracht werden. Alle Anforderungen der Ziele und Nicht-Ziele an die Sicherheitsbewertung (Tabelle 7) wurden berücksichtigt und in einer Prüfung bei real existierenden aber fiktiv zusammengestellten Mobile-Access-Systemen angewendet. Insbesondere die stärkere Einbeziehung der IT-Security wurde durch den Leitfragenkatalog erreicht, der auch genügend Freiraum für spezielle Erweiterungen schafft. Ergänzungen sind somit jederzeit umsetzbar, wenn eine geeignete Anforderung besteht. Wichtig zu erwähnen ist hierbei das einfache und systematische Vorgehen bei den angesprochenen Erweiterungen und dessen Anwendbarkeit. Beides ist durch die prozessorientierte Vorgehensweise individuell an die persönliche Struktur und das Verständnis des Prüfers anpassbar. Der modulare Aufbau von einzelnen Arbeitsschritten (Prüfelementen) kann vielfältig auf das Prüfobjekt angepasst werden. Wie im Vorfeld der Evaluierung schon mehrfach aufgezeigt wurde, sind die Bereiche der IT-Security von besonderer Bedeutung und im derzeitigen Modell stärker berücksichtigt worden. Durch den Leitfragenkatalog wurde demnach eine im Detail stärkere Einflussnahme auf das Endergebnis möglich. Der tolerierbare Rahmen in der Beantwortung der Leitfragen konnte somit ein engeres oder aber auch ein etwas breiteres Verständnis des theoretischen Sicherheitsprofils haben. Demnach könnten Beurteilungen und Ergebnisse leicht variieren. Eine Voraussetzung ist hier, dass die Einzelkomponenten des theoretischen Sicherheitsprofils in den vier Kategorien simultan an die Bewertungsveränderungen angepasst werden. Es ist jedem Prüfer freigestellt, diesen Rahmen selbstständig zu nutzen oder sich zwingend an die Vorgaben zu halten. Dies betrifft zum Teil auch eine Normung mit besonders stringenten Kriterien. Für eine reproduzierbare und gesicherte Vorgehensweise müssen die Prüfer einen fachlich ausreichend großen Erfahrungs- und Wissensstand vorweisen. Nur so lassen sich außerhalb von starren Grenzen die Rahmenbedingungen sinnvoll nutzen. Genau dort liegt der Vorteil der ganzheitlichen Sicherheitsbewertung: Es ist dies ein Prozess, die einen ausreichenden Freiheitsgrad in der Schwerpunktsetzung enthält - bei gleichzeitig strenger Vorgabe des Prüfumfangs.

Unter Berücksichtigung der existierenden mechanischen Normungen wird auf bestehende und bewährte Standards aufgesetzt, ohne diese zu verfälschen. Auch wenn in den Normungen der mechatronischen Schließanlagen große Teile der IT-Security fehlen, so setzen sie anerkannte mechanische Bedingungen für einen gesicherten und sicheren Betrieb. Mit dieser kombinierten

Verbindung aus normativen Grundlagen und speziellen Auszügen aus den IT-Werken BSI und CC kann potentiellen Bedrohungen eine adäquate Sicherheitsbewertung für moderne Sicherungssysteme entgegengesetzt werden. Nicht zuletzt spielt auch die Qualität der Kriterien im theoretischen Sicherheitsprofil und die entsprechend wirkungsvolle Beziehung zu den möglichen Einbruchstypen eine Rolle. Weitere wirkungsvolle Kriterien sind die freien Ideensammlungen in der Asset-Betrachtung.

Für die erfolgreiche Durchführung der ganzheitlichen Sicherheitsbewertung ist die selbstständige und aktive Mitarbeit des Herstellers eine wichtige Rahmenbedingung. Gerade in den ersten Arbeitsschritten muss ein gewisses Vertrauensverhältnis wachsen, welches einen ungezwungenen freien Meinungsaustausch zur Folge hat. Der Input zur Bewertung ist zwangsläufig von der Informationsbereitstellung des Herstellers abhängig. Dies beinhaltet die Bereitschaft des Herstellers, aufgrund der erzielten Ergebnisse proaktiv Produktverbesserungen einzuführen. Sicherlich ist es für IT-Experten möglich, durch intensive Analysen ein Mobile Access-System auch ohne Informationen vom Hersteller auf seine Sicherheit zu prüfen. Doch müssen alle Anbieter solcher Systeme sich auf eine einheitliche Vorgehensweise und auf entsprechende Standards einigen. Erst danach sollten individuelle Tests angestrebt werden. Die Evaluierungsergebnisse der Methodik haben gezeigt, dass genau diese Standards möglich und auch sinnvoll bewertbar sind.

Genaueres Augenmerk sollte auf die passende Bewertungsgrundlage für die Kundensicht gelegt werden, da hier mit unterschiedlichen Grenzen von Eintrittswahrscheinlichkeit und Schaden sowie der Gewichtung erheblicher Einfluss auf die Zustandsfarben möglich ist. Eine Anpassung über mehrere Sicherheitsbewertungen respektive Produktvarianten scheint angebracht.

Der finanzielle und zeitliche Aufwand kann hier durchaus in Grenzen gehalten werden. Dies bestätigt der durchgeführte Umfang mit der beschriebenen Prüftiefe, der in einem definierten Zeitrahmen respektable Ergebnisse lieferte. Die Hersteller der Beispielsysteme wären nun mit den definierten Erfüllungsgraden in der Lage, Produktverbesserungen im Sinne der „Sicherheit" anzustoßen, um ihr Produkt beim Kunden mit einer möglichst „grünen" oder zu mindestens „gelben" Zustandsfarbe bestmöglich zu bewerben. Im Umkehrschluss erhalten die Kunden ein plausibles und nachvollziehbares Ergebnis der Sicherheitsbewertung, welches fortan als ein standardisierter Prozess im Sinne der kontinuierlichen Vertrauensbildung einsetzbar wäre.

7 Fazit

Mit dem letzten Kapitel konnte die erfolgreiche Durchführung der ganzheitlichen Sicherheitsbewertung abgeschlossen werden. Es ist ein erster wichtiger Schritt zur Evaluierung moderner Mobile Access-Systeme unter Berücksichtigung eines holistischen Analyseansatzes auf KVP-Basis. Alle betrachteten Normen für mechatronische Schließzylinder konnten allerdings den gewünschten Umfang von IT-Security nicht gewährleisten. Doch gerade die Etablierung neuer Technologien wie die angesprochenen Mobile Access-Systeme, die über das Smartphone gesteuert werden, erfordern einen etablierten Sicherheitsstandard, um einen wirkungsvollen Schutz vor Angreifern zu bieten. Die Schloss- und Beschlagindustrie sollte sich frühzeitig auf die neuen Anforderungen einstellen, damit sie für etwaige Quereinsteiger in der Branche gewappnet ist. Nur wenn frühzeitig Sicherheitsstandards geschaffen werden, kann auch der eigene Markt geschützt werden. Liegen diese Standards bei den neuen Technologien nicht bald vor, ist es nur eine Frage der Zeit, bis bekannte Technologie-Entwickler den überwiegend noch mechanischen Markt erreichen. Bis in die heutige Zeit sind die Erfolge für die etablierten Hersteller konventioneller Schließtechnik noch spürbar. Gehen diese jedoch keine Kooperationen ein, um Technologien zu entwickeln und Sicherheitsstandards aufzubauen, wird der Druck durch neue Wettbewerber immer größer. Merkliche Resonanz auf den Hinweis, dass die bestehenden Normen dringend auf die kommenden Anforderungen angepasst werden müssten, bleibt oftmals aus. Neue Technologien mit entsprechenden Geschäftsmodellen sollten den zukünftigen Markt sichern, allerdings sind viele Unternehmen auf diesen Wandel anscheinend bisher nicht eingestellt. Die ersten Schließsysteme, die mit Hilfe des Smartphones arbeiten, zeigen mittlerweile sehr gute Ansätze zur Optimierung. Beispielsweise lässt sich die Organisation von Pflegediensten so optimieren. Aufwändige und unsichere Schlüsseltransporte entfallen und auch kurzfristige Änderungen können mit dem Smartphone als Schlüssel orchestriert werden. Ein Hindernis liegt in der fehlenden Akzeptanz dieser neuen Technologien; auch Hersteller begegnen ihr zögerlich. Es gibt allerdings eine Reihe von Gründen, um die Vertrauensvorsprünge aus der Mechanik in die Elektronik zu übernehmen. Gerade als unsicher geltende Rahmenbedingungen stellen eine günstige Voraussetzung dar, um solide Versprechen in puncto Vertrauen zu gewährleisten. Nur können mit Normungen ohne eindeutigen Schwerpunkt in der IT-Security keine vertrauensbildenden Maßnahmen folgen. Ungenügende Schwerpunkte und eine nicht adäquate oder fehlende Methodik lieferten in letzter Konsequenz den Forschungsschwerpunkt und die Problemstellung dieser Dissertation.

Den mitunter schwierigsten Bereich innerhalb der Sicherheitsbewertung stellt die geeignete Auswahl an Beispielsystemen dar, da es im Bereich der Unternehmen der Schloss- und Beschlagindustrie nicht üblich zu sein scheint, die eigenen Systeme Dritten, selbst für Forschungszwecke, für eine Sicherheitsbewertung zugänglich zu machen. Dabei lag hier der klare Fokus auf einer Evaluierung der Methodik und nicht auf der detaillierten Analyse eines technischen Systems. Eindrücklich hat sich die Erkenntnis manifestiert, dass die Hersteller solcher Systeme häufig neu in der Branche und auf dem Markt sind. Daher sind Ressourcen das höchste und knappste Gut der Anbieter. Erschwerend müssen sie sich einem sehr fein aufgeteilten Machtverhältnis bei der Marktbearbeitung in der Zugangskontrolle stellen.

Ein stringenter Ablauf auf KVP-Basis konnte die Methode der holistischen Sicherheitsbewertung strukturieren und auf Hersteller- und Kundensicht fokussieren. Dabei ist in der Ausführung die PDCA-Vorgehensweise ein erfolgreicher Problemlösungsansatz. Es wurden ganzheitlich die anfänglich aufgestellten Ziele und Nicht-Ziele für den speziellen Anwendungsfall berücksichtigt. Wesentliche Merkmale waren hierbei die Reduzierung der technischen Komplexität auf ein sinnvolles Maß, Orientierung am theoretischen Sicherheitsprofil, Einbeziehung eines Leitfragenkatalogs, Betrachtung und Evaluierung bestehender Normungen, Durchführung einer Risikobewertung und Ergebnisdarstellung. Ähnlich einem Wasserfallmodell wurden jeweils kaskadenartig aus dem vorherigen Schritt Erkenntnisse zwingend für den Folgeschritt benötigt und dienten dort als eine Art „Eingabe". Im Resultat der Ergebnisdarstellung konnten dann mithilfe der semi-quantitativen Bewertungsgrundlage vergleichende oder absolute Zahlenwerte zur Entscheidung dienen. Für eine Konkretisierung der Ergebnisse sollten zusätzliche Beispielssysteme der Sicherheitsbewertung unterzogen werden. Auch die einzelnen Leitfragen im Strang der IT-Security sind unter weiterer Prüfung noch stärker abzustimmen. Als ein wesentlicher Schritt kann

schlussendlich die Einführung und Berücksichtigung innerhalb eines offiziellen Produktzertifizierungsverfahren gesehen werden. Dabei sollte es nicht um die Abbildung des Verfahrens an sich gehen, sondern auch um eine partielle Extrahierung von Elementen der Sicherheitsbewertung, um einen Impuls für ganzheitliche Bewertungsansätze im Bereich Mobile Access zu geben.

Im Zuge der Erstellung der Dissertation konnte ein sehr guter methodischer und technischer Überblick über die Schließtechnik erworben werden. Weitere Bereiche wie z. B. die Automobilindustrie stellen sich gerade simultan auf, um ihr Angebotsspektrum zu erweitern. Auch dort bestehen ähnliche essentielle Reifungsprozesse zur Finalisierung von mobilen Lösungen. Alle Branchen und Technologieausprägungen haben eine gemeinsame Triebfeder - das visionäre Unternehmertum, das den bewussten Umgang mit Risiken umfasst, die spätere Risikobetrachtungen als sichere Fortführung der gewöhnlichen Geschäftstätigkeit sehen.

8 Literaturverzeichnis

ABI Research, Prognose zum Marktvolumen von Mobil Payment über NFC-Technologie in den Jahren 2012, 2016 und 2017, In Statista: https://de.statista.com/statistik/daten/studie/244800/umfrage/prognose-zum-mobile-payment-umsatz-weltweit/, Abgerufen am 24.08.2017, 2017

Abolhassan, Ferri, Security Einfach Machen, IT-Sicherheit als Sprungbrett für die Digitalisierung, Wiesbaden: Springer Fachmedien, 2017

Anderson S. et al. (Eds.), Safecomp 2002, LNCS 2434, Berlin / Heidelberg: Springer-Verlag, 2002

Apple Inc., Core NFC, Detect NFC tags and read messages that contain NDEF data, Abrufbar im Internet, https://developer.apple.com/documentation/corenfc#overview, Abgerufen am 25.10.2017.

Banse, Gerhard, Techniksicherheit und Sicherheitskulturen, In: Winzer, Petra / Schnieder, Eckehard / Bach, Friedrich-Wilhelm, Sicherheitsforschung, Chancen und Perspektiven, acatech Diskutiert, Berlin / Heidelberg: acatech-Deutsche Akademie der Technikwissenschaften, Springer-Verlag, S. 185-205, 2010

Behnia, Armaghan / Abd Rashid, Rafhana / Chaudhry, Junaid Ahsenali, A Survey of Information Security Risk Analysis Methods, In: Smart Computing Review, Vol. 2, No. 1, S. 79–94, 2012

Beutelspacher, Albrecht / Schwenk, Jörg / Wolfenstetter, Klaus-Dieter, Moderne Verfahren der Kryptographie, Von RSA zu Zero-Knowledge, 8., überarbeitete Auflage, Wiesbaden: Springer Fachmedien, 2015

BHE, Der Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen e.V. Zutrittsregelung und mechanische Sicherungstechnik, Mechatronische Schließsysteme, Brücken: BHE, 2007

Blohm, Hans / Beer, Thomas / Seidenberg, Ulrich / Silber, Herwig, Produktionswirtschaft, 4., vollständig überarbeitete Auflage, Herne: Neue Wirtschafts-Briefe GmbH & Co. KG, 2008

Bowles, John B., An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis, University of South Carolina, In: Proceedings Annual Reliability and Maintainability Symposium, S. 380-386, 2003.

Bretting, Ralf, Lockruf des Geldes, Kommunikation, Sandwichposition, In: business impact, Digitale Wirtschaft, S. 31-34, 01.2017

Bronner, Albert, Handbuch der Rationalisierung, 2., neu bearbeitete Auflage, Renningen: Expert Verlag, 2003

BSI – TL 03405, Bundesamt für Sicherheit in der Informationstechnik, Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme, Anwendungsbereich: Elektronische Systeme mit elektronischer oder manueller Codeeingabe, Version: 1.2, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2011

BSI Magazin, „Das Deutsche Prüfschema genießt weltweit einen exzellenten Ruf", In: BSI-Magazin 2016/02, Mit Sicherheit, Abrufbar im Internet, https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2016_02.pdf?__blob=publicationFile&v=7, S. 18-19, 2016

Bub, Udo / Deleski, Viktor / Wolfenstetter, Klaus-Dieter, Sicherheit im Wandel von Technologien und Märkten, Tagungsband zur vierten EIT ICT Labs-Konferenz zur IT-Sicherheit, Wiesbaden: Springer Fachmedien, 2015

Bundesamt für Sicherheit in der Informationstechnik (BSI), Workshop Common Criteria 3.1, Protection Profile (PP), Security Target (ST), Einführung in die Evaluierung, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2015

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 14. Ergänzungslieferung-2014, Bonn: BSI, 2014

Bundesministerium des Innern, Polizeiliche Kriminalstatistik 2015, Berlin: Bundesministerium des Innern, 2016

C.Ed. Schulte GmbH Zylinderschlossfabrik, Marketing, Bildersammlung (diverse), 2017

C.Ed. Schulte GmbH Zylinderschlossfabrik, Mechanische Konstruktion, Bildersammlung (diverse), 2017

Campbell, Philip L., / Stamp, Jason E., Sandia Report, A Classification Scheme for Risk Assessment Methods, New Mexico / California: Sandia national Laboratories, 2004

Common Criteria for Information Technology Security Evaluation, Abrufbar im Internet: http://www.commoncriteriaportal.org/cc/, Part 2: Security functional components, Version 3.1, Revision 4, September 2012

comScore MobiLens, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2016, In Statista: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/, Abgerufen am 01.12.2016, 2017

Cottin, Claudia / Döhler, Sebastian, Risikoanalyse, Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen, Studienbücher Wirtschaftsmathematik, 2., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2013

Czuchra, Waldemar, UML in logistischen Prozessen, Graphische Sprache zur Modellierung der Systeme, Wiesbaden: Springer Fachmedien, 2010

Deutsche Gesellschaft für Qualität, KVP-Der kontinuierliche Verbesserungsprozess, Praxisleitfaden für kleine und mittlere Organisationen, DGQ-Band 12-92, München: Carl Hanser Verlag, 2014

Dietz, Ulrich, Die Zukunft des Bezahlens, Abrufbar im Internet: https://www.bitkom.org/noindex/Publikationen/2015/Sonstiges/PK-Zukunft-des-Bezahlens/BITKOM-PK-Zukunft-des-Bezahlens-Praesentation-10-06-2015-final.pdf, Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2015

DIN 18252, Deutsches Institut für Normung e.V., Profilzylinder für Türschlösser-Begriffe, Maße, Anforderungen, Kennzeichnung, Berlin: Beuth Verlag GmbH, 2006

DIN 820-12, Deutsches Institut für Normung e.V., Normungsarbeit – Teil12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:2014), Berlin: Beuth Verlag GmbH, 2014

DIN EN 1303, Deutsches Institut für Normung e.V., Baubeschläge - Schließzylinder für Schlösser-Anforderungen und Prüfverfahren; Deutsche Fassung EN 1303:2005, Berlin: Beuth Verlag GmbH, 2005

DIN EN 60812, Deutsches Institut für Normung e.V., Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlerzustandsart- und –auswirkungsanalyse (FMEA) (IEC 60812:2006), Deutsche Fassung EN 60812:2006, Berlin: Beuth Verlag GmbH, 2006

DIN EN 15684, Deutsches Institut für Normung e.V., Schlösser und Baubeschläge-Mechatronische Schließzylinder-Anforderungen und Prüfverfahren; Deutsche Fassung EN 15684:2012, Berlin: Beuth Verlag GmbH, 2013

DIN EN ISO 12100, Deutsches Institut für Normung e.V., Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010, Berlin: Beuth Verlag GmbH, 2011

DIN IEC 62443-3-3 (Entwurf) (VDE 0802-3-3), Deutsches Institut für Normung e.V., Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + Cor..:2014), Berlin: Beuth Verlag GmbH, 2015

DIN ISO/IEC 27001, Deutsches Institut für Normung e.V., Informationstechnik – IT-Sicherungsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, ISO/IEC 27001:2013 + Cor. 1:2014, Berlin: Beuth Verlag GmbH, 2015

DIN ISO/IEC 27002, Deutsches Institut für Normung e.V., Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-management (ISO/IEC 27002:2005), Berlin: Beuth Verlag GmbH, 2008

Dominique Brulé, Gemalto, What`s behind the acceleration of NFC mobile payments?, Abrufbar im Internet, https://blog.gemalto.com/blog/2014/09/30/whats-behind-the-acceleration-of-nfc-mobile-payments/, Abgerufen am 30.08.2017, 2014

Dunker, Hilmar, Lockruf des Geldes, Automobilindustrie, Aufholjagd, In: business impact, Digitale Wirtschaft, S. 31-34, 01.2017

Ebert, Christof, Risikomanagement kompakt, Risiken und Unsicherheiten bewerten und beherrschen, IT kompakt, 2., überarbeitete und erweiterte Auflage, Berlin / Heidelberg: Springer-Verlag, 2013

Eckert, Claudia, IT-Sicherheit, Konzepte-Verfahren-Protokolle, 7., überarbeitete und erweiterte Auflage, München: Oldenbourg Wissenschaftsverlag GmbH, 2012

Edler, Frank / Soden, Michael / Hankammer, René, Fehlerbaumanalyse in Theorie und Praxis, Grundlagen und Anwendung der Methode, Berlin / Heidelberg: Springer Verlag, 2015

EHI Retail Institute, Was halten Sie für die aussichtsreichste mobile Bezahltechnik?, In Statista: https://de.statista.com/statistik/daten/studie/371903/umfrage/umfrage-zu-mobilen-bezahltechniken-im-einzelhandel-in-deutschland/, Abgerufen am 24.08.2017, 2017

Eickemeyer, Danny, Bluetooth-Marketing, Handlungsempfehlungen für die erfolgreiche Planung und Umsetzung einer mobilen Kampagne, Hamburg: Diplomica® Verlag GmbH, 2010

eMarketer, Prognose zur Wachstumsrate der Anzahl an Smartphone-Nutzern in Deutschland von 2015 bis 2019, In Statista: https://de.statista.com/statistik/daten/studie/378125/umfrage/prognose-zur-wachstumsrate-der-smartphone-nutzer-in-deutschland/, Abgerufen am 24.08.2017, 2017

euromicron AG, Anteil von deutschen Unternehmen, die sich für folgende ITK-Trendthemen interessieren, In Statista: https://de.statista.com/statistik/daten/studie/557867/umfrage/interesse-an-itk-trendthemen-in-deutschen-unternehmen/, Abgerufen am 29.08.2017, 2017

euromicron AG, Im Bereich welcher ITK-Trendthemen planen Sie im Jahr 2016 Investitionen zu tätigen?, In Statista: https://de.statista.com/statistik/daten/studie/557850/umfrage/geplante-investitionen-in-itk-trendthemen-in-deutschen-unternehmen/, Abgerufen am 29.08.2017, 2017

Federrath, Hannes, IT-Sicherheitsmanagement nach ISO 17799 und nach BSI-Grundschutzhandbuch – Eine vergleichende Betrachtung, Uni-Regensburg, Abrufbar im Internet: https://epub.uni-regensburg.de/7472/1/2004-06-23IT-Security-Messe.pdf, 2004

Finkenzeller, Klaus, RFID Handbuch, Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC, 7., aktualisierte und erweiterte Auflage, München: Carl Hanser Verlag, 2015

Fox, Dirk, Schutzprofile – Protection Profiles, In: Datenschutz und Datensicherheit, Abrufbar im Internet: https://www.secorvo.de/publikationen/schutzprofile-protection-profiles-fox-2011.pdf8/2011, S. 570-570, 2011

Fredriksen, Rune / Kristiansen, Monica / Gran, Bjørn Axel / Stølen, Ketil / Opperud, Tom Arthur / Dimitrakos, Theo, The CORAS Framework for a Model-Based Risk Management Process, In: Anderson S. et al. (Eds.), Safecomp 2002, LNCS 2434, S. 94 – 105, Berlin / Heidelberg: Springer-Verlag, 2002

Frevel, Bernhard, Sicherheit, Ein (un)stillbares Grundbedürfnis, 2., überarbeitete Auflage, Wiesbaden: Springer Fachmedien, 2016

Gadatsch, Andreas / Mangiapane, Markus, IT-Sicherheit, Digitalisierung der Geschäftsprozesse und Informationssicherheit, Wiesbaden: Springer Fachmedien, 2017

Gartner's Hype cycle places NFC at 'Peak of Inflated Expectations', Abrufbar im Internet: https://www.nfcworld.com/2011/08/11/39008/gartner-hype-cycle-places-nfc-at-peak-of-inflated-expectations/, Abgerufen am 30.08.2017, 2011

Gastl, René, Kontinuierliche Verbesserung von Umweltmanagementsystem und Umweltleistung, Die KVP-Forderung der ISO 14001 in Theorie und Unternehmenspraxis, Dissertation, Zürich: Universität St. Gallen, 2005

Gessler, Ralf / Krause, Thomas, Wireless-Netzwerke für den Nahbereich, Eingebettete Funksysteme: Vergleich von standardisierten und proprietären Verfahren, 2., aktualisierte und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2015

Hasso Plattner Institut, Studie zur Messbarkeit von Sicherheiten in SOA, beauftragt durch das BSI, durchgeführt durch das Hasso-Plattner-Institut im Zeitraum 2010/2011, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2010

Health and Safety Executive, Reducing risks, protecting people, HSE's decision-making process, HSE Books, 2001

Herrmann, Debra S., Using the common criteria for IT Security Evaluation, CRC Press LLC, Auerbach, 2003

HID Global Corporation/ASSA ABLOY AB, Was Sie über Mobile Access wissen sollten (Teil 1), https://www.hidglobal.de/sites/default/files/resource_files/hid-global-mobile-access-enterprise-part-1-eb-de.pdf, Abgerufen am 24.08.2017, 2017

Hruschka, Peter, Requirements Engineering, In: Tiemeyer, Handbuch, IT-Projekt-Management, Vorgehensmodelle, Managementinstrumente, Good Practices, 2., überarbeitete und erweiterte Auflage, München: Carl Hanser Verlag, S. 421-452, 2014

Huhn, Philipp, SMART HOME, In: Statista Digital Market Outlook, Umsatzveränderung im Markt für Smart Home, https://de.statista.com/outlook/279/100/smart-home/weltweit#marketStudy, Abgerufen am 01.12.2016, 2017

IfD Allensbach (ACTA 2015), Handy- bzw. Smartphonenutzer in Deutschland nach genutzten Funktionen des Geräts im Jahr 2015, In Statista:https://de.statista.com/statistik/daten/studie/170596/umfrage/genutzte-zusatzfunktionen-bei-handy-smartphone/, Abgerufen am 01.12.2016, 2017

Jeschke, Hartwig, Elektronische Schließanlagen: Realisierung kundenspezifischer Zutrittskonzepte, In: Sicherheitsmarkt, Nr. 2, S. 5-7, Februar 2003

Kantar Worldpanel, Marktanteile der mobilen Betriebssysteme am Absatz von Smartphones in Deutschland von März bis Mai in den Jahren 2016 und 2017, In Statista: https://de.statista.com/statistik/daten/studie/198435/umfrage/marktanteile-der-smartphone-betriebssysteme-am-absatz-in-deutschland/, Abgerufen am 24.08.2017, 2017

Karabacak, Bilge / Sogukpinar, Ibrahim, ISRAM: information security risk analysis method, In: Computers & Security 2004, Elsevier, S. 1-13, 2004

Kardel, Danilo, IT-Sicherheitsmanagement in KMU, Abrufbar im Internet: https://link.springer.com/content/pdf/10.1007%2FBF03340623.pdf, In: HMD 281, S. 44-51, 2011

Kaymaz, Feyyat, User-Anonymität in Mobile Payment Systemen, Ein Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Systemen, Dissertation, Universität Kassel, Kassel: kassel university press GmbH, 2011

Kersten, Heinrich / Klett, Gerhard / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach der neuen ISO 27001, ISMS, Risiken, Kennziffern, Controls, Wiesbaden: Springer Fachmedien, 2016

Kersten, Heinrich / Klett, Gerhard, Der IT Security Manager, Expertenwissen für jeden IT Security Manager, 2., aktualisierte und erweiterte Auflage, Wiesbaden: GWV Fachverlage GmbH (Vieweg+Teubner), 2008

Kersten, Heinrich / Reuter, Jürgen / Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Der Weg zur Zertifizierung, 4., aktualisierte und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2013

Kleuker, Stephan, Grundkurs Software-Engineering mit UML, Der pragmatische Weg zu erfolgreichen Softwareprojekten, 3., korrigierte und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2013

Klipper, Sebastian, Information Security Risk Management, Risikomanagement mit ISO/IEC 27001, 27005 und 31010, 2., überarbeitete Auflage, Wiesbaden: Springer Fachmedien, 2015

Koch, Susanne, Einführung in das Management von Geschäftsprozessen, Six Sigma, Kaizen und TQM, 2., Auflage, Berlin / Heidelberg: Springer-Verlag, 2015

Langer, Josef / Roland, Michael, Anwendungen und Technik von Near Field Communication (NFC), Berlin / Heidelberg: Springer-Verlag, 2010

Lee, Ming-Chang, Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method, In: International Journal of Computer Science & Information Technology (IJCSIT), Vol. 6, No. 1, S. 29-45, 2014

Lesegeräte für Zutrittskontrolle, Marktübersicht Zutrittskontrolle, In: Protector&WIK, S. 30-31, 03.2017

Lichte, Daniel, Ein analytischer Ansatz zur szenarioübergreifenden Modellierung der Verwundbarkeit von Infrastrukturen, Dissertation, Universität Wuppertal, Wuppertal, 2015

Maier, Joern, Zeit für Erneuerung, Überarbeitung des IT-Grundschutz nach BSI, In: kes, S. 5-8, 08/2015

Mast, Clemens, Neuerfindung einer Industrie, Evolution von Organisationen und Märkte durch die Innovation des Geschäftsmodells, Wiesbaden: Springer Fachmedien, 2017

Matulevičius, Raimundas / Dumas, Marlon, A Comparison of SecureUML and UMLsec for Role-based Access Control, Abrufbar im Internet: http://courses.cs.ut.ee/2010/is/uploads/Main/RBAC-for-UML.pdf, 2010

Morgenroth, Ulrich, Sternstunden der Schlossgeschichte, Tüftler, Forscher und Entdecker – eine Zeitreise durch die Sicherheitstechnik, Duisburg: Gert Wohlfarth GmbH, 2008

Morgenroth, Ulrich, Vierhundert Jahre und mehr…, Schloss und Beschlag in Velbert, Velbert: Scheidsteger Druck GmbH, 2002

Mössner, Thomas, Risikobeurteilung im Maschinenbau, Abschlussbericht zum Projekt „Risikobeurteilung von Produkten – Empfehlungen zur Vorgehensweise, Beurteilungskriterien und Beispiele", Projekt F 2216, Dortmund / Berlin / Dresden: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2012

Mouheb, Djedjiga / Debbabi, Mourad / Pourzandi, Makan / Wang, Lingyu / Nouh, Mariam / Ziarati, Raha / Alhadidi, Dima / Talhi, Chamseddine / Lima, Vitor, Aspect-Oriented Security Hardening of UML Design Models, Switzerland: Springer International, 2015

Müller, Klaus-Rainer, IT-Sicherheit mit System, Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices, 5., neu bearbeitete und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2014

Paar, Christof / Pelzl, Jan, Kryptografie verständlich, Ein Lehrbuch für Studierende und Anwender, Berlin / Heidelberg: Springer-Verlag, 2016

Peltier, Thomas R., Facilitated Risk Analysis Process (FRAP), Data Security Management, Auerbach Publications, CRC Press LLC, 2000

Pelzl, Jan, Aus dem smarten Leben gegriffen, In: Bub, Udo / Deleski, Viktor / Wolfenstetter, Klaus-Dieter, Sicherheit im Wandel von Technologien und Märkten, Tagungsband zur vierten EIT ICT Labs-Konferenz zur IT-Sicherheit, Wiesbaden: Springer Fachmedien, S. 27-32, 2015

Pelzl, Jan, Motivationsvortrag: Das Internet der Dinge, Aber bitte mit Sicherheit!, Hochschule Hamm-Lippstadt, Vorlesung Master an der Universität Wuppertal, 2017

Polizei-Initiative, Einbruchschutz und Brandschutz – es geht um Ihre Sicherheit!, In: Netzwerk „Zuhause sicher", Abrufbar im Internet: http://www.zuhause-sicher.de/einbruchschutz-und-brandschutz/, Abgerufen am 24.08.2017

Preiss, Reinhard, Methoden der Risikoanalyse in der Technik, Systematische Analyse komplexer Systeme, Wien: TÜV Austria, 2009

Pudar, Srdjan/ Manimaram, Govindarasu / Liu, Chen-Ching, PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, In: Computers & Security 28, S. 754-771, Elsevier, 2009

Pyka, Marek / Januszkiewicz, Paulina, The Octave methology as a risk analysis tool for business resources, In: Proceedings of the International Multiconference on Computer Science and Technology, S. 485-497, PIPS, 2006

Rumpe, Bernhard, Modellierung mit UML, Sprache, Konzepte und Methodik, 2., Auflage, Berlin / Heidelberg: Springer-Verlag, 2011

Sauter, Martin, Grundkurs Mobile Kommunikationssysteme, UMTS, HSPA und LTE, GSM, GPRS, Wireless LAN und Bluetooth, 5., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Fachmedien, 2013

Schließmann, Christoph, Das Konzept Interdepency, Chancen und Risiken systemischer Komplexität erkennen und steuern, 2., Auflage, Berlin / Heidelberg: Springer Verlag, 2014

Schutzrecht, 398 35 630, Urkunde über die Eintragung der Marke, C. Ed. Schulte GmbH Zylinderschloßfabrik, Velbert, 03.09.1998

Schutzrecht, Caterino, Mark, Anthony / Einberg, Fredrik, Carl Stefan / Hoyer, Philip / Berg, Daniel, WO 2016/185283 A1, use of mobile device to configure a lock, Assa Abloy AB, 24.11.2016

Schutzrecht, DE 20 2015 003 163 U1, Elektronische Schließeinrichtung und Schließsystem mit einer solchen Schließeinrichtung, BKS GmbH, 08.09.2016

Schutzrecht, Einberg, Fredrik / Philip, Hoyer / Berg, Daniel, WO 2016/177667 A1, one-key vault, Assa Abloy AB, 10.11.2016

Schutzrecht, EP 3 121 795 A1, Aufbau einer Kommunikationsverbindung mit einer Benutzervorrichtung über eine Zugangskontrollvorrichtung, Deutsche Post AG, Pr.: 20.07.2015 DE 102015111711, 25.01.2017

Schutzrecht, Hermann, Stefan, DE 10 2016 204 807 A1, Schlüsselloses Zugangssystem, insbesondere für ein Kraftfahrzeug, Continental Automotive GmbH, 09.03.2017

Schutzrecht, Papagelidis, Mario, DE 10 2015 111 914 A1, Schlüssel für einen Schließzylinder und Schließvorrichtung, DOM-Sicherheitstechnik GmbH & Co. KG, 28.07.2016

Schutzrecht, Reine, Michael / Wallberg, Thomas, DE 10 2010 017 166 B4, Verfahren zum Profilieren eines Flachschlüssels sowie nach dem Verfahren gefertigter Flachschlüssel, C.Ed. Schulte Gesellschaft mit beschränkter Haftung Zylinderschlossfabrik, 07.03.2013

SevenOne Media, Wie viele Smartphones besitzen Sie?, In Statista: https://de.statista.com/statistik/daten/studie/316238/umfrage/anzahl-der-smartphones-pro-besitzer-in-deutschland/, Abgerufen am 24.08.2017, 2017

Stumpf, Michael, Toolunterstützte Zertifizierung auf Basis der Common Criteria, Diplomarbeit, Fachhochschule Würzburg-Schweinfurt, Abrufbar im Internet: http://www.petrastumpf.de/michael/Wissen/CommonCriteria.pdf, 2005

Swoboda, Joachim / Spitz, Stephan / Pramateftakis, Michael, Kryptographie und IT-Sicherheit, Grundlagen und Anwendungen, Wiesbaden: Vieweg+Teubner Verlag, GWV Fachverlage GmbH, 2008

Thies, Karlheinz H. W., Management operationaler IT- und Prozess-Risiken, Methoden für eine Risikobewältigungsstrategie, 2008

Tiemeyer, Ernst, Handbuch, IT-Projekt-Management, Vorgehensmodelle, Managementinstrumente, Good Practices, 2., überarbeitete und erweiterte Auflage, München: Carl Hanser Verlag, 2014

VdS 2156-1, VdS Schadenverhütung GmbH, VdS-Richtlinie für mechanische Sicherungssysteme, Schließzylinder mit Einzelsperrschließung, Anforderungen und Prüfmethoden, Köln: VdS Schadenverhütung GmbH, 2012

VdS 2156-2, VdS Schadenverhütung GmbH, VdS-Richtlinie für mechanische Sicherungssysteme, Schließzylinder mit Einzelsperrschließung, Anforderungen und Prüfmethoden, Teil 2: Elektronische Schließzylinder, Köln: VdS Schadenverhütung GmbH, 2013

VdS 2215, VdS Schadenverhütung GmbH, VdS-Richtlinie für mechanische Sicherungssysteme, Schließsysteme, Anforderungen und Prüfmethoden, Köln: VdS Schadenverhütung GmbH, 2005

VdS 2386, VdS Schadenverhütung GmbH, VdS-Richtlinie für mechanische Sicherungssysteme, Schließanlagen, Anforderungen und Prüfmethoden, Köln: VdS Schadenverhütung GmbH, 2012

Vorster, Anita / Labuschagne, Les, A Framework for Comparing Different Information Security Risk Analysis, University of Johannesburg, In: Proceedings of SAICSIT 2005, S. 95–103, 2005

Walburg, Christian, Migration und Kriminalität, aktuelle kriminalstatistische Befunde, Institut für Kriminalwissenschaften, Universität Münster, Mediendienst Integration, 2016

Winzer, Petra / Schnieder, Eckehard / Bach, Friedrich-Wilhelm, Sicherheitsforschung, Chancen und Perspektiven, acatech Diskutiert, Berlin / Heidelberg: acatech-Deutsche Akademie der Technikwissenschaften, Springer-Verlag, 2010

Wittpahl, Volker, Digitalisierung, iit-Themenband, Bildung | Technik | Innovation, Berlin: Institut für Innovation und Technik in der VDI/VDE Innovation + Technik GmbH, 2017

Wolf, Marko, Security Engineering for Vehicular IT Systems, Improving the Trustworthiness and Dependability of Automotive IT Applications, Wiesbaden: GWV Fachverlage GmbH (Vieweg+Teubner), 2009

9 Anhang

9.1 Anhang: DIN EN 1303[232]

Schließzylinder für Schlösser - Anforderungen und Prüfverfahren		
	Anforderungen / Kategorien	**Mechanisch**
1.	**Anforderungen**	
2.	Schlüsselfestigkeit	x
3.	Dauerhaftigkeit	x
4.	Korrosionsbeständigkeit	x
5.	**Verschlusssicherheit**	
6.	Mindestanzahl der effektiven Verschiedenheiten	x
7.	Mindestanzahl der beweglichen Zuhaltungen	x
8.	Höchstanzahl gleich tiefer Stufen	x
9.	Nachschließsicherheit	x
10.	Torsionsfestigkeit des Schließzylinders/-kerns, bezogen auf Verschlusssicherheit	x
11.	**Angriffswiderstand**	
12.	Widerstandsfähigkeit gegen Angriff durch Aufbohren	x
13.	Widerstandsfähigkeit gegen Angriff eines Meißels	x
14.	Widerstandsfähigkeit gegen Angriff durch Abdrehen	x
15.	Widerstandsfähigkeit gegen Angriff durch Herausziehen des Schließzylinders/Zylinderkerns	x
16.	Torsionsfestigkeit des Schließzylinders/Zylinderkerns, bezogen auf Angriffswiderstand	x
17.	**Prüfverfahren**	
18.	Schlüsselfestigkeit	x
19.	Prüfung der Dauerhaftigkeit	x
20.	Korrosionsbeständigkeit (Prüfung der Funktion bei extremen Temp.)	x
21.	**Klassifikationen**	
22.	Allgemeines	x

[232] DIN EN 1303, Baubeschläge - Schließzylinder für Schlösser, 2005.

23.	Gebrauchsklasse	x
24.	Dauerhaftigkeit	x
25.	Feuerwiderstand	x
26.	Korrosionsbeständigkeit	x
27.	Verschlusssicherheit	x
28.	Angriffswiderstand	x

Tabelle 23: DIN EN 1303 (Zusammenfassung)[233]

[233] Vgl. DIN EN 1303, Baubeschläge - Schließzylinder für Schlösser, 2005, S. 1 ff.

9.2 Anhang: DIN 18252[234]

Profilzylinder für Türschlösser - Begriffe, Maße, Anforderungen, Kennzeichnung		
	Anforderungen / Kategorien	**Mechanisch**
1.	**Anforderungen**	
2.	Allgemeine Anforderungen an Profilzylinder	x
3.	Anforderungen an Profilzylinder für Schließanlagen	x
4.	Anforderungen an Profilzylinder für Türen mit Sicherheitsanforderungen	x
5.	Anforderungen an Profilzylinder für Rauchschutz-/Feuerschutztüren	x
6.	**Prüfung**	
7.	Allgemeines	
8.	Prüfung der Maße	x
9.	Prüfung von Profilzylinder	x
10.	Prüfung der Besonderheiten von Profilzylindern für Schließanlagen	x
11.	Prüfung der Besonderheiten von Profilzylindern für Rauchschutz-/Feuerschutztüren	x

Tabelle 24: DIN 18252 (Zusammenfassung)[235]

[234] DIN 18252, Profilzylinder für Türschlösser, 2006.
[235] Vgl. DIN 18252, Profilzylinder für Türschlösser, 2006, S. 1 ff.

9.3 Anhang: VdS 2156-1[236]

Schließzylinder mit Einzelsperrschließung - Anforderungen und Prüfmethoden		
	Anforderungen / Kategorien	Mechanisch
1.	**Anforderungen**	
2.	Allgemeine Anforderungen	x
3.	Schließzylinder für Schalteinrichtung von Einbruchmeldeanlagen	x
4.	**Prüfung**	
5.	Eingangsprüfung	x
6.	Allgemeine Prüfung	x
7.	Schließzylinder für Schalteinrichtung von Einbruchmeldeanlagen	x

Tabelle 25: VdS 2156-1 (Zusammenfassung)[237]

[236] VdS 2156-1, Schließzylinder mit Sperrschließung, 2012.
[237] Vgl. VdS 2156-1, Schließzylinder mit Sperrschließung, 2012, S. 1 ff.

9.4 Anhang: DIN EN 15684[238]

Leistungsfähigkeit mechatronischer Zylinder			
		Abfrage	
	Anforderungen / Kategorien	Elektronisch	Mechanisch
1.	**Gebrauchskategorie**		
2.	Schlüsselfestigkeit		x
3.	Stabilität des elektronischen Schlüssels		x
4.	Falscher elektronischer Code		x
5.	Dauerschockanforderungen		x
6.	Schwingungsanforderungen		x
7.	Anforderungen hinsichtlich der elektrostatischen Entladung	x	
8.	Mindestübertragungsmoment des Knaufs		x
9.	Anforderungen an die Dauerfunktionstüchtigkeit		x
10.	Feuer-/Rauchwiderstand		x
11.	**Umweltbeständigkeit**		
12.	Anforderungen an die Korrosionsbeständigkeit		x
13.	Wasserbeständigkeit des MC		x
14.	Trockene Wärme		x
15.	Kälte		x
16.	Zyklisch feuchte Wärme		x
17.	Wasserbeständigkeit des elektronischen Schlüssels		x
18.	**Verschlusssicherheit**		
19.	Mindestanzahl der effektiven Varianten des mechanischen Codes		x
20.	Mindestanzahl beweglicher Zuhaltungen		x
21.	Höchstanzahl gleicher Stufen		x
22.	Direkte Schließungsbezeichnung der Schlüssel		x
23.	Torsionsfestigkeit des Schließzylinders/Zylinderkerns, bezogen auf Verschlusssicherheit		x
24.	Mindestanzahl der Varianten des elektronischen Codes	x	
25.	**Systemmanagement**	x	
26.	Anforderungen hinsichtlich des Angriffswiderstands		x

[238] DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013.

27.	Widerstandsfähigkeit gegen Aufbohren		x
28.	Widerstandsfähigkeit gegen Angriff eines Meißels		x
29.	Widerstandsfähigkeit gegen Angriff durch Abdrehen		x
30.	Widerstandsfähigkeit gegen Angriff durch Herausziehen des Schließzylinders/Zylinderkerns		x
31.	Torsionsfestigkeit des Schließzylinders/Zylinderkerns, bezogen auf den Angriffswiderstand		x
32.	Angriff durch Schläge		x
33.	Angriff durch Schwingungen		x
34.	Angriff mit erhöhter Spannung	x	
35.	Angriff durch elektrostatische Entladung	x	
36.	Angriff mit dem Magnetfeld	x	
37.	Anforderungen an die Produktinformation	x	x

Tabelle 26: DIN EN 15684 (Zusammenfassung)[239]

[239] Vgl. DIN EN 15684, Schlösser und Baubeschläge - Mechatronische Schließzylinder, 2013, S. 1 ff.

9.5 Anhang: VdS 2156-2[240]

Schließzylinder mit Einzelsperrschließung (Elektronische Schließzylinder)			
		Abfrage	
	Anforderungen / Kategorien	Elektronisch	Mechanisch
1.	**Konstruktive Anforderungen**		
2.	Codeträger für materielle Codes		x
3.	Kontaktlose Übertragung von Codes	x	
4.	Überlagerte Codes	x	
5.	Codeumstellung	x	
6.	Anforderungen elektronische Codes	x	
7.	Hintergrundspeicher	x	
8.	Sperrzustände	x	
9.	Energieversorgung	x	
10.	**Elektromagnetische Einflüsse**		
11.	Ausfall der Energieversorgung	x	
12.	Widerstand gegen statische Entladungen	x	
13.	Widerstand gegen leitungsgebundene Störungen-Burst	x	
14.	Widerstand gegen leitungsgebundene Störungen-Surge	x	
15.	Widerstand gegen eingestrahlte hochfrequente elektromagnetische Felder	x	
16	Widerstand gegen induzierte hochfrequente elektromagnetische Felder	x	
17.	**Physikalische Einflüsse**		
18.	Klimate	x	x
19.	Korrosionsschutz	x	x
20.	Schlag	x	x
21.	Schock	x	x
22.	Vibration	x	x

[240] VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013.

23.	**Zuverlässigkeit**		
24.	Dauerfunktionstüchtigkeit		x
25.	**Aufsperrsicherheit**		
26.	Widerstand gegen Aufsperrversuche	x	
27.	Manuelle Aufsperrversuche		x
28.	**Widerstand gegen gewaltsame Angriffe**		
29.	Widerstand gegen Aufbohren		x
30.	Widerstand gegen Angriffe mit Ziehwerkzeug		x
31.	**Optionen**		

Tabelle 27: VdS 2156-2 (Zusammenfassung)[241]

[241] Vgl. VdS 2156-2, Schließzylinder mit Einzelsperrschließung, 2013, S. 1 ff.

9.6 Anhang: BSI – TL 03405[242]

Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme			
		Abfrage	
	Anforderungen / Kategorien	Elektronisch	Mechanisch
1.	**Allgemeine Anforderungen**		
2.	Montage- und Bedienungsanleitung		x
3.	Widerstand gegen elektrische Einflüsse	x	
4.	Mechanische Festigkeit		x
5.	Widerstand gegen Manipulation	x	
6.	Verschlusssicherheit	x	
7.	Stromversorgung	x	
8.	**Zusätzliche Anforderungen an Schließzylinder/Schließsysteme mit Codeträger**		
9.	Einmalige, unveränderbare Seriennummer auf jedem Codeträger.	x	
10.	Daten auf dem Codeträger dürfen nicht auslessbar und Rückschlüsse auf gespeicherte Daten geben.	x	
11.	Codeträger müssen gegen Replay-attacken abgesichert sein.	x	
12.	Typische Reichweite von 10 cm darf nicht überschritten werden.	x	
13.	Verlorene Codeträger müssen gesperrt werden können.	x	
14.	Codeträger gleicher Anwendergruppen dürfen sich nicht gegenseitig berechtigen.	x	
15.	Datenaustausch zwischen Codeträger und Eingabeeinheit muss mit einem Authentifizierungsverfahren (Challenge-Response-Verfahren) gemäß ISO/IEC 9798-2 arbeiten.	x	
16.	Datenaustausch muss verschlüsselt erfolgen (Hardwareimplementierung	x	

[242] BSI – TL 03405, Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme, 2010.

	Codeträger).		
17.	Informationsübertragung und die Authentifikation soll bei hohem Schutzbedarf mit 3-DES, bei neuen Anlagen mit AES erfolgen. Common-Criteria zertifizierte Produkte sind mit EAL-3 oder höher einzusetzen.	x	
18.	Forderung aus der BSI Technischen Richtlinie TR-03126(-5) " Technical Guidelines for Secure Use of RFID" nutzen.	x	
19.	**Zusätzliche Anforderungen an Schließsysteme mit memorischem Code**		
20.	Das Schließsystem muss über (mindestens) 10^6 nutzbare Codes verfügen.		x
21.	Maximal 20 Falscheingaben pro Stunde möglich.		x

Tabelle 28: BSI - TL03405 (Zusammenfassung)[243]

[243] Vgl. BSI – TL 03405, Anforderungen und Prüfbedingungen für elektronische Schließzylinder und Schließsysteme, 2010, S. 1 ff.

9.7 Anhang: Qualität der Kriterienausprägung

Die **Angreiferklassen** stehen für unterschiedliche Gefährdungsprofile die über entsprechende Gefährdungskriterien abgebildet sind. Hier sollte bei der Bewertung ein Profil ausgewählt werden, dass dem Maß des Kriteriums aus dem Sicherheitsprofil im Mindesten standhält. Dabei sind die einzelnen Gefährdungskriterien mit Augenmaß an das entsprechende Gefährdungsprofil auszuwählen.

Im Folgenden sind die "Angreiferklassen" dargestellt:

Anwender: Der Anwender lässt sich exemplarisch durch den Endnutzer des Dienstes beschreiben. Sein physikalischer Zugang zum System ist in der Regel unbegrenzt und er ist im Besitz geringer technischer Fähigkeiten, d.h. seine Möglichkeiten liegen lediglich in der Benutzung des Systems ohne weiterführendes Wissen. Für die Implementierung von Sicherheitsfunktionen ist der finanzielle Einsatz daher gering.

Fachspezialist: Der Fachspezialist lässt sich als Anwender mit erweitertem Fachwissen beschreiben. Sein physikalischer Zugang zum System ist in der Regel unbegrenzt und er ist im Besitz mittlerer technischer Fähigkeiten, d.h. seine Möglichkeiten liegen in der Benutzung des Systems mit weiterführendem Wissen. Für die Implementierung von Sicherheitsfunktionen ist der finanzielle Einsatz erhöht.

Professioneller: Der Professionelle lässt sich als Spezialist mit umfangreichem Fachwissen beschreiben. Sein physikalischer Zugang zum System ist unbegrenzt und er ist im Besitz hoher technischer Fähigkeiten, d.h. seine Möglichkeiten liegen in der Analyse des Systems mit hohem Wissen. Für die Implementierung von Sicherheitsfunktionen ist der finanzielle Einsatz hoch.

Insider: Der Insider lässt sich als internen Mitarbeiter mit umfangreichstem Fachwissen beschreiben. Sein physikalischer und virtueller Zugang zum System ist unbegrenzt und der ist im Besitz hoher technischer Fähigkeiten, d.h. seine Möglichkeiten liegen in der Kenntnis genauer entwicklungstechnischem Wissen. Für die Implementierung von Sicherheitsfunktionen ist der finanzielle Einsatz sehr hoch und kann nur durch diversifiziertes Entwicklungswissen erreicht werden.

Das **Kompromittieren von sensiblen Daten** kann Auswirkungen auf verschiedene Aktionen haben, die u.a. in den Kriterienblättern vermerkt sind. Dabei kann nicht sichergestellt sein, dass ein ordentlicher Betrieb gewährleistet ist. Mit dem Verfälschen, Löschen oder einer anderen Art der Änderung von sensiblen Daten kann ein Abfließen von Daten an Dritte nicht ausgeschlossen werden. Dies hat zur Folge, dass dritte Personen möglicherweise in den Besitz von Daten gelangen die für eine missbräuchliche Verwendung bestimmt sind.

Im Folgenden sind die einzelnen Profile der "Kompromittierung sensibler Daten" dargestellt:

Gefährdend: Das Gefahrenpotenzial ist für die Kompromittierung von sensiblen Daten stark erhöht. Es kann mit hoher Sicherheit nicht ausgeschlossen werden, dass Daten in die Hände von Dritten gelangen kann. Dabei sind die Zugangsmöglichkeiten für Unbefugte mit einem geringen Fertigkeitsaufwand möglich respektive die Daten liegen offensichtlich vor. Besonders betroffen sind hier auch die persönlichen Daten - Datenschutz beeinträchtigt!

Möglich: Das Gefahrenpotenzial ist für die Kompromittierung von sensiblen Daten leicht erhöht. Es kann mit Sicherheit nicht ausgeschlossen werden, dass Daten in die Hände von Dritten gelangen kann. Dabei sind die Zugangsmöglichkeiten für Unbefugte mit einem erhöhten Fertigkeitsaufwand möglich respektive die Daten liegen nicht direkt vor.

Unkritisch: Das Gefahrenpotenzial ist für die Kompromittierung von sensiblen Daten eher unkritisch. Es kann davon ausgegangen werden, dass keine Daten in die Hände von Dritten gelangen kann. Dabei sind die Zugangsmöglichkeiten für Unbefugte stark beschränkt und daher nur mit stark erhöhtem Fertigkeitsaufwand beeinflussbar.

Die **Usability** beschreibt die möglichen Auswirkungen bei Kompromittierung des jeweiligen Kriteriums. Dabei können die Auswirkungen verschiedene Formen annehmen, was den Ausfall einer Komponete bedeuten kann aber auch die unbemerkte Weiterführung eines gehackten Dienstes (Services). Hier ist abzuwägen, ob das betroffene Kriterium entscheidende Auswirkung auf die Weiterführung eines ordentlichen Dienstes und die IT-Security hat.

Im Folgenden sind die "Usability" Profile dargestellt:

Service/Gerät funktionslos: Bei der Kompromittierung des Kriteriums ist sowohl der Service, wie auch das Gerät anschließend funktionslos. Die resultierende Sicherheitslücke weißt dadurch eine große Unsicherheit in Bezug auf unbefugte Handlungen/Aktivitäten.

Service oder Gerät funktionslos: Bei der Kompromittierung des Kriteriums ist entweder der Service oder das Gerät funktionslos. Die resultierende Sicherheitslücke weißt dadurch eine Unsicherheit in Bezug auf unbefugte Handlungen/Aktivitäten der funktionslosen Komponente auf.

Eingeschränkt nutzbar: Bei der Kompromittierung des Kriteriums sind die Komponenten des Systems eingeschränkt funktionsfähig. Eine resultierende Sicherheitslücke kann nicht nennenswert festgestellt werden, dadurch besteht keine Unsicherheit in Bezug auf unbefugte Handlungen/Aktivitäten.

Nicht spürbar: Bei der Komnpromittierung des Kriteriums sind die Komponenten des Systems nur für den Benutzer oberflächlich voll funktionsfähig. Die resultierende Sicherheitslücke weißt dadurch eine sehr große Unsicherheit in Bezug auf unbefugte Handlungen/Aktivitäten auf.

Die einzelnen Kriterien des Untersuchungsobjektes müssen bezüglich ihrer **Ausprägung** beschrieben und bewertet werden. Als Grundlage hierzu dienen die Fragestellungen der einzelnen Kriterienblätter, die einen Pflichtanteil und einen Anteil für erhöhten Sicherheitsbedarf enthalten. Für die richtige Einschätzung des jeweiligen Kriteriums sollten die technischen Spezifikationen und mindestens ein Befragter mit internen Erkenntnissen über die Entwicklung zur Verfügung stehen.

Das Merkmal "Ausprägung" wird im Folgenden detailliert:

Gering: Die Merkmalsausprägung findet keine relevante Implementierung. Weder Hardware noch Software haben eine nennenswerte Implementierung des Kriteriums, somit ist es im Untersuchungsobjekt kaum existent respektive gering berücksichtigt.

Basis: Die Implementierung des Kriteriums ist in Grundzügen vorhanden. Dabei werden die minimalsten Standards erreicht, die für dieses Kriterium von Nöten sind. Dabei können mindestens drei Fragen für das Untersuchungsobjekt positiv beantwortet werden.

Mittel: Eine Implementierung in mittlerer Ausprägung bestätigt die positive Beantwortung von allen Fragen für das Untersuchungsobjekt. Damit kann für das Kriterium sichergestellt werden, dass die Umsetzung einen Mindestdurchschnitt erreicht hat.

Stark: Bei einer starken Ausprägung des Kriteriums werden die grundsätzlichen Implementierungsfragen um den Zusatz ergänzt. Somit kann eine hinausgehende Kriterienausprägung gewährleistet werden. Im Resultat sind alle Implementierungsfragen und deren Zusätze positiv zu beantworten.

9.8 Anhang: BSI-Bausteine (Zusammenstellung)[244]

B1 - Übergreifende Aspekte
B 1.0 Sicherheitsmanagement
B 1.1 Organisation
B 1.2 Personal
B 1.3 Notfallmanagement
B 1.4 Datensicherungskonzept
B 1.5 Datenschutz
B 1.6 Schutz vor Schadprogrammen
B 1.7 Kryptokonzept
B 1.8 Behandlung von Sicherheitsvorfällen
B 1.9 Hard- und Software-Management
B 1.14 Patch- und Änderungsmanagement
B 1.15 Löschen und Vernichten von Daten
B 1.17 Cloud-Nutzung
B2 - Infrastruktur
B 2.2 Elektrotechnische Verkabelung
B 2.4 Serverraum
B3 - IT-Systeme
B 3.101 Allgemeiner Server
B 3.201 Allgemeiner Client
B 3.404 Mobiltelefon
B 3.405 Smartphones, Tablets und PDAs
B4 – Netze
B 4.2 Netz- und Systemmanagement
B 4.6 WLAN
B 4.8 Bluetooth
B5 – Anwendungen
B 5.4 Webserver
B 5.7 Datenbanken
B 5.14 Mobile Datenträger
B 5.19 Internet-Nutzung
B 5.21 Webanwendungen
B 5.22 Protokollierung
B 5.23 Cloud Management
B 5.24 Web-Services
B 5.25 Allgemeine Anwendungen

[244] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014.

9.9 Anhang: BSI-Gefährdungen (Zusammenstellung)[245]

11 Personalausfall
12 Ausfall von IT-Systemen
14 Feuer
15 Wasser
16 Kabelbrand
17 Unzulässige Temperatur und Luftfeuchte
18 Staub, Verschmutzung
19 Datenverlust durch starke Magnetfelder
21 Fehlende oder unzureichende Regelungen
22 Unzureichende Kenntnis über Regelungen
23 Fehlende, ungeeignete, inkompatible Betriebsmittel
24 Unzureichende Kontrolle der Sicherheitsmaßnahmen
25 Fehlende oder unzureichende Wartung
26 Unbefugter Zutritt zu schutzbedürftigen Räumen
27 Unerlaubte Ausübung von Rechten
28 Unkontrollierter Einsatz von Betriebsmitteln
29 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
31 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
32 Fahrlässige Zerstörung von Gerät oder Daten
33 Nichtbeachtung von Sicherheitsmaßnahmen
35 Unbeabsichtigte Leitungsbeschädigung
36 Gefährdung durch Reinigungs- oder Fremdpersonal
38 Fehlerhafte Nutzung von IT-Systemen
39 Fehlerhafte Administration von IT-Systemen
41 Ausfall der Stromversorgung
42 Ausfall interner Versorgungsnetze
46 Spannungsschwankungen/Überspannung/Unterspannung
47 Defekte Datenträger
51 Manipulation oder Zerstörung von Geräten oder Zubehör
52 Manipulation an Informationen oder Software
53 Unbefugtes Eindringen in ein Gebäude
54 Diebstahl
55 Vandalismus
56 Anschlag
57 Abhören von Leitungen
58 Manipulation von Leitungen
59 Unberechtigte IT-Nutzung
110 Ausfall eines Weitverkehrsnetzes
115 Beeinträchtigung durch wechselnde Einsatzumgebung
116 Ausfall von Patchfeldern durch Brand
117 Ausfall oder Störung eines Funknetzes
118 Ausfall eines Gebäudes
119 Ausfall eines Dienstleisters oder Zulieferers
210 Nicht fristgerecht verfügbare Datenträger
211 Unzureichende Trassendimensionierung
212 Unzureichende Dokumentation der Verkabelung
213 Unzureichend geschützte Verteiler
215 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
217 Mangelhafte Kennzeichnung der Datenträger
219 Unzureichendes Schlüsselmanagement bei Verschlüsselung
221 Mangelhafte Organisation des Wechsels zwischen den Benutzern
222 Fehlende oder unzureichende Auswertung von Protokolldaten
224 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
226 Fehlendes oder unzureichendes Test- und Freigabeverfahren
227 Fehlende oder unzureichende Dokumentation
228 Verstöße gegen das Urheberrecht
232 Unzureichende Leitungskapazitäten
236 Ungeeignete Einschränkung der Benutzerumgebung
237 Unkontrollierter Aufbau von Kommunikationsverbindungen
238 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

[245] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014.

239 Mangelhafte Konzeption eines DBMS
240 Mangelhafte Konzeption des Datenbankzugriffs
241 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
248 Ungeeignete Entsorgung der Datenträger und Dokumente
254 Vertraulichkeitsverlust durch Restinformationen
257 Nicht ausreichende Speichermedien für den Notfall
259 Betreiben von nicht angemeldeten Komponenten
260 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
261 Unberechtigte Sammlung personenbezogener Daten
262 Ungeeigneter Umgang mit Sicherheitsvorfällen
266 Unzureichendes Sicherheitsmanagement
267 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
284 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
285 Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens
286 Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister
287 Verwendung unsicherer Protokolle in öffentlichen Netzen
293 Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung
296 Veraltete oder falsche Informationen in einem Webangebot
311 Fehlerhafte Konfiguration von sendmail
313 Weitergabe falscher oder interner Informationen
316 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
317 Kein ordnungsgemäßer PC-Benutzerwechsel
323 Fehlerhafte Administration eines DBMS
324 Unbeabsichtigte Datenmanipulation
328 Ungeeignete Konfiguration der aktiven Netzkomponenten
331 Unstrukturierte Datenhaltung
332 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
333 Fehlbedienung von Kryptomodulen
334 Ungeeignete Konfiguration des Managementsystems
335 Server im laufenden Betrieb ausschalten
336 Fehlinterpretation von Ereignissen
337 Unproduktive Suchzeiten
338 Konfigurations- und Bedienungsfehler
343 Ungeeigneter Umgang mit Passwörtern
344 Sorglosigkeit im Umgang mit Informationen
345 Unzureichende Identifikationsprüfung von Kommunikationspartnern
376 Fehler bei der Synchronisation mobiler Endgeräte
377 Mangelhafte Akzeptanz von Informationssicherheit
380 Fehler bei der Synchronisation von Datenbanken
384 Fehlerhafte Konfiguration der WLAN-Infrastruktur
385 Verletzung von Brandschottungen
392 Fehleinschätzung der Relevanz von Patches und Änderungen
393 Falscher Umgang mit defekten Datenträgern
410 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
413 Verlust gespeicherter Daten
420 Überlastung von Informationssystemen
422 Software-Schwachstellen oder -Fehler
423 Automatische Erkennung von Wechseldatenträgern
426 Ausfall einer Datenbank
427 Unterlaufen von Zugriffskontrollen über ODBC
428 Verlust von Daten einer Datenbank
430 Verlust der Datenbankintegrität/-konsistenz
431 Ausfall oder Störung von Netzkomponenten
432 Nichtzustellung einer Nachricht
433 Schlechte oder fehlende Authentikation
434 Ausfall eines Kryptomoduls
435 Unsichere kryptographische Algorithmen
436 Fehler in verschlüsselten Daten
438 Ausfall von Komponenten eines Netz- und Systemmanagementsystems
439 Software-Konzeptionsfehler
441 Nicht-Verfügbarkeit des Mobilfunknetzes
442 Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs
443 Undokumentierte Funktionen
451 Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs

452 Datenverlust bei mobilem Einsatz
460 Unkontrollierte Ausbreitung der Funkwellen
461 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen
462 Verwendung unzureichender Steckdosenleisten
463 Verstaubte Lüfter
471 Probleme bei der automatisierten Verteilung von Patches und Änderungen
479 Schwachstellen in der Bluetooth-Implementierung
480 Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen
484 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services
485 Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services
486 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen
487 Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services
489 Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung
490 Ungewollte Preisgabe von Informationen durch Cloud Cartography
491 Unberechtigtes Wiedereinspielen von Snapshots
492 Inkompatibilität zwischen der Cloud-Administration und der Administration der Cloud-Elemente
493 Ausfall von Verwaltungsservern und Verwaltungssoftware
494 Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services
497 Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister
498 Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung
499 Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen
510 Missbrauch von Fernwartungszugängen
516 Gefährdung bei Wartungs-/Administrierungsarbeiten
518 Systematisches Ausprobieren von Passwörtern
519 Missbrauch von Benutzerrechten
520 Missbrauch von Administratorrechten
521 Trojanische Pferde
522 Diebstahl bei mobiler Nutzung des IT-Systems
523 Schadprogramme
526 Analyse des Nachrichtenflusses
527 Nichtanerkennung einer Nachricht
528 Verhinderung von Diensten
540 Abhören von Räumen mittels Rechner mit Mikrofon und Kamera
542 Social Engineering
548 IP-Spoofing
564 Manipulation an Daten oder Software bei Datenbanksystemen
565 Verhinderung der Dienste eines Datenbanksystems
566 Unberechtigter Anschluss von IT-Systemen an ein Netz
567 Unberechtigte Ausführung von Netzmanagement-Funktionen
568 Unberechtigter Zugang zu den aktiven Netzkomponenten
571 Vertraulichkeitsverlust schützenswerter Informationen
575 Überlastung durch eingehende E-Mails
578 DNS-Spoofing
580 Hoax
581 Unautorisierte Benutzung eines Kryptomoduls
582 Manipulation eines Kryptomoduls
583 Kompromittierung kryptographischer Schlüssel
584 Gefälschte Zertifikate
585 Integritätsverlust schützenswerter Informationen
586 Manipulation von Managementparametern
587 Web-Spoofing
588 Missbrauch aktiver Inhalte
594 Missbrauch von SIM-Karten
595 Abhören von Raumgesprächen über Mobiltelefone
596 Manipulation von Mobiltelefonen
597 Unberechtigte Datenweitergabe über Mobiltelefone
598 Abhören von Mobiltelefonaten
599 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
2100 Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen
2102 Unzureichende Sensibilisierung für Informationssicherheit
2103 Unzureichende Schulung der Mitarbeiter
2105 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
2106 Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen
2107 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

2110 Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken
2117 Fehlende oder unzureichende Planung des WLAN-Einsatzes
2118 Unzureichende Regelungen zum WLAN-Einsatz
2119 Ungeeignete Auswahl von WLAN-Authentikationsverfahren
2120 Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen
2121 Unzureichende Kontrolle von WLANs
2132 Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement
2133 Mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement
2134 Unzureichende Ressourcen beim Patch- und Änderungsmanagement
2135 Mangelhafte Kommunikation beim Patch- und Änderungsmanagement
2136 Fehlende Übersicht über den Informationsverbund
2137 Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen
2138 Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement
2139 Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement
2140 Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement
2141 Nicht erkannte Sicherheitsvorfälle
2142 Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen
2147 Fehlende Zentralisierung durch Peer-to-Peer
2151 Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen
2154 Ungeeignete Anwendungen für den Einsatz auf Terminalservern
2157 Mangelhafte Auswahl oder Konzeption von Webanwendungen
2158 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services
2159 Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services
2160 Fehlende oder unzureichende Protokollierung
2161 Vertraulichkeits- und Integritätsverlust von Protokolldaten
2162 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten
2163 Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten
2164 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
2165 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
2166 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten
2167 Fehlende oder nicht ausreichende Vorabkontrolle
2168 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten
2169 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten
2170 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen
2171 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten
2172 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland
2173 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten
2174 Fehlende oder unzureichende Datenschutzkontrolle
2175 Unzureichende Isolation und Trennung von Cloud-Ressourcen
2176 Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender
2177 Fehlplanung von Cloud-Diensteprofilen
2178 Unzureichendes Notfallmanagement beim Cloud-Diensteanbieter
2179 Fehlende Herstellerunterstützung bei der Bereitstellung von Cloud-Diensten
2180 Fehlerhafte Provisionierung und De-Provisionierung von Cloud-Diensten
2181 Mangelhafte Planung und Konzeption des Einsatzes von Web-Services
2188 Unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung
2189 Fehlende oder unzureichende Strategie für die Cloud-Nutzung
2190 Unzureichendes Administrationsmodell für die Cloud-Nutzung
2191 Unzureichendes Rollen- und Berechtigungskonzept
2192 Unzureichende Verfügbarkeit der erforderlichen personellen Ressourcen mit ausreichender Qualifikation
2193 Fehlende Anpassung der Institution an die Nutzung von Cloud Services
2194 Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung
2195 Mangelnde Überwachung der Service-Erbringung
2196 Fehlende Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus
2197 Unzureichende Einbindung von Cloud Services in die eigene IT
2198 Mangelnde Planung der Migration zu Cloud Services
2199 Unzureichende Auswahl des Cloud-Diensteanbieters
2200 Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs
3105 Ungenehmigte Nutzung von externen Dienstleistungen
3106 Ungeeignetes Verhalten bei der Internet-Nutzung
3107 Rufschädigung

3114 Fehlerhafte Administration bei der Protokollierung
3115 Fehlerhafte Auswahl von relevanten Protokolldaten
3116 Fehlende Zeitsynchronisation bei der Protokolldatenauswertung
3117 Fehlerhafte Automatisierung beim Cloud Management
3118 Ungeeignete Konfiguration von Cloud-Diensten und Cloud-Verwaltungssystemen
3119 Fehlerhafte Anwendung von Standards
3120 Fehler bei der Orchestrierung
3121 Konfigurations- und Administrationsfehler bei Web-Services
3122 Fehlerhafte Nutzung eines Cloud Services
3123 Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs
5102 Sabotage
5104 Ausspähen von Informationen
5114 Missbrauch von Spanning Tree
5123 Abhören von Raumgesprächen über mobile Endgeräte
5124 Missbrauch der Informationen von mobilen Endgeräten
5125 Datendiebstahl mithilfe mobiler Endgeräte
5126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
5131 SQL-Injection
5137 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation
5138 Angriffe auf WLAN-Komponenten
5139 Abhören der WLAN-Kommunikation
5141 Datendiebstahl über mobile Datenträger
5142 Verbreitung von Schadprogrammen über mobile Datenträger
5143 Man-in-the-Middle-Angriff
5145 Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement
5146 Vertraulichkeitsverlust durch Auslagerungsdateien
5156 Bot-Netze
5157 Phishing und Pharming
5158 Missbrauch sozialer Netzwerke
5159 Erstellung von Bewegungsprofilen unter Bluetooth
5160 Missbrauch der Bluetooth-Profile
5165 Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services
5166 Missbrauch einer Webanwendung durch automatisierte Nutzung
5167 Fehler in der Logik von Webanwendungen und Web-Services
5168 Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services
5169 Unzureichendes Session-Management von Webanwendungen und Web-Services
5170 Cross-Site Scripting (XSS)
5171 Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
5172 Umgehung der Autorisierung bei Webanwendungen und Web-Services
5173 Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services
5174 Injection-Angriffe
5175 Clickjacking
5176 Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung
5177 Missbrauch von Kurz-URLs oder QR-Codes
5178 Missbrauch von Administratorrechten im Cloud-Management
5179 Angriffe auf Protokolle
5180 Angriffe auf Registries und Repositories
5181 Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services
5182 Manipulation von Routen (Routing Detours)
5183 Angriffe auf XML
5184 Informationsgewinnung über Web-Services
5190 Missbrauch von Services
5191 Manipulation der Abrechnungsinformationen
5192 Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender
5193 Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs
5194 Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion

9.10 Anhang: BSI-Maßnahmen (Zusammenstellung)[246]

13 (A) Angepasste Aufteilung der Stromkreise
15 (W) Galvanische Trennung von Außenleitungen
17 (A) Handfeuerlöscher
19 (A) Brandabschottung von Trassen
21 (A) Festlegung von Verantwortlichkeiten und Regelungen
22 (C) Betriebsmittelverwaltung
23 (B) Datenträgerverwaltung
24 (B) Regelungen für Wartungs- und Reparaturarbeiten
25 (A) Aufgabenverteilung und Funktionstrennung
26 (A) Vergabe von Zutrittsberechtigungen
27 (A) Vergabe von Zugangsberechtigungen
28 (A) Vergabe von Zugriffsrechten
29 (A) Nutzungsverbot nicht freigegebener Hard- und Software
31 (A) Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
33 (A) Vertretungsregelungen
34 (A) Schulung vor Programmnutzung
35 (A) Schulung zu Sicherheitsmaßnahmen
36 (A) Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
37 (Z) Anlaufstelle bei persönlichen Problemen
38 (Z) Vermeidung von Störungen des Betriebsklimas
41 (A) Passwortschutz für IT-Systeme
42 (A) Bildschirmsperre
43 (A) Einsatz von Viren-Schutzprogrammen
44 (C) Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
47 (A) Änderung voreingestellter Passwörter
51 (A) Entfernen oder Deaktivieren nicht benötigter Leitungen
54 (A) Dokumentation und Kennzeichnung der Verkabelung
55 (A) Schadensmindernde Kabelführung
58 (B) Regelmäßiger Sicherheitscheck des Netzes
59 (B) Protokollierung am Server
110 (Z) Sichere Türen und Fenster
115 (A) Geschlossene Fenster und Türen
118 (Z) Gefahrenmeldeanlage
120 (A) Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
121 (A) Ausreichende Trassendimensionierung
122 (Z) Materielle Sicherung von Leitungen und Verteilern
123 (A) Abgeschlossene Türen
124 (C) Vermeidung von wasserführenden Leitungen
125 (B) Überspannungsschutz
126 (W) Not-Aus-Schalter
127 (B) Klimatisierung der Technik / in Technikräumen
128 (B) Lokale unterbrechungsfreie Stromversorgung
129 (Z) Geeignete Aufstellung eines IT-Systems
131 (Z) Fernanzeige von Störungen
132 (B) Geeignete Aufstellung von Druckern und Kopierern
133 (A) Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
146 (Z) Einsatz von Diebstahl-Sicherungen
152 (Z) Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur
158 (A) Technische und organisatorische Vorgaben für Serverräume
162 (C) Brandschutz von Patchfeldern
163 (B) Geeignete Aufstellung von Access Points
164 (A) Vermeidung elektrischer Zündquellen

[246] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014.

210 (C) Überprüfung des Hard- und Software-Bestandes
211 (A) Regelung des Passwortgebrauchs
212 (C) Betreuung und Beratung von IT-Benutzern
213 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
216 (B) Beaufsichtigung oder Begleitung von Fremdpersonen
217 (A) Zutrittsregelung und -kontrolle
218 (Z) Kontrollgänge
219 (B) Neutrale Dokumentation in den Verteilern
221 (A) Rauchverbot
222 (Z) Hinterlegen des Passwortes
223 (Z) Herausgabe einer PC-Richtlinie
224 (Z) Einführung eines IT-Passes
225 (A) Dokumentation der Systemkonfiguration
226 (A) Ernennung eines Administrators und eines Vertreters
230 (A) Regelung für die Einrichtung von Benutzern / Benutzergruppen
231 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile
232 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
234 (A) Dokumentation der Veränderungen an einem bestehenden System
235 (B) Informationsbeschaffung über Sicherheitslücken des Systems
237 (C) Der aufgeräumte Arbeitsplatz
238 (B) Aufteilung der Administrationstätigkeiten
239 (B) Reaktion auf Verletzungen der Sicherheitsvorgaben
240 (A) Rechtzeitige Beteiligung des Personal-/Betriebsrates
241 (A) Verpflichtung der Mitarbeiter zur Datensicherung
242 (A) Festlegung der möglichen Kommunikationspartner
246 (A) Geeignetes Schlüsselmanagement
262 (B) Software-Abnahme- und Freigabe-Verfahren
263 (A) Einrichten der Zugriffsrechte
264 (A) Kontrolle der Protokolldateien
265 (C) Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
269 (B) Einrichtung von Standardarbeitsplätzen
280 (A) Erstellung eines Anforderungskatalogs für Standardsoftware
289 (C) Deinstallation von Standardsoftware
310 (A) Auswahl eines vertrauenswürdigen Administrators und Vertreters
311 (A) Schulung des Wartungs- und Administrationspersonals
318 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
323 (W) Einführung in kryptographische Grundbegriffe
333 (Z) Sicherheitsüberprüfung von Mitarbeitern
350 (Z) Auswahl von Personal
351 (Z) Geeignetes Konzept für Personaleinsatz und -qualifizierung
355 (C) Vertraulichkeitsvereinbarungen
358 (W) Einführung in WLAN-Grundbegriffe
359 (C) Schulung zum sicheren WLAN-Einsatz
360 (C) Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten
366 (W) Grundbegriffe des Patch- und Änderungsmanagements
367 (C) Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten
369 (W) Einführung in die Bedrohung durch Schadprogramme
377 (A) Sensibilisierung zur sicheren Internet-Nutzung
378 (W) Korrektes Auftreten im Internet
379 (W) Einführung in Grundbegriffe und Funktionsweisen von Bluetooth
380 (A) Sensibilisierung für die Nutzung von Bluetooth
383 (Z) Analyse sicherheitsrelevanter personeller Faktoren
389 (A) Schulung zur Administration der Protokollierung
390 (W) Allgemeine Grundlagen für die zentrale Protokollierung

391 (B) Schulung der Administratoren von Cloud-Infrastrukturen
415 (A) Gesichertes Login
416 (C) Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals
417 (A) Sperren und Löschen nicht benötigter Accounts und Terminals
424 (A) Sicherstellung einer konsistenten Systemverwaltung
431 (A) Sicherstellung der Energieversorgung im mobilen Einsatz
432 (B) Physikalisches Löschen der Datenträger vor und nach Verwendung
433 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
434 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
440 (C) Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras
441 (Z) Einsatz angemessener Sicherheitsprodukte für IT-Systeme
464 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
465 (C) Test neuer Hard- und Software
467 (B) Sperren und Löschen nicht benötigter Datenbank-Accounts
468 (A) Sicherstellung einer konsistenten Datenbankverwaltung
469 (B) Regelmäßiger Sicherheitscheck der Datenbank
470 (C) Durchführung einer Datenbanküberwachung
471 (C) Restriktive Handhabung von Datenbank-Links
472 (Z) Datenbank-Verschlüsselung
473 (C) Festlegung von Obergrenzen für selektierbare Datensätze
478 (A) Sorgfältige Durchführung von Konfigurationsänderungen
484 (A) Nutzung der BIOS-Sicherheitsmechanismen
485 (Z) Geeignetes Schnittstellendesign bei Kryptomodulen
486 (A) Sichere Rollenteilung und Konfiguration der Kryptomodule
487 (Z) Physikalische Sicherheit von Kryptomodulen
488 (A) Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
489 (Z) Abstrahlsicherheit
490 (W) Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells
491 (A) Sichere Installation eines Systemmanagementsystems
492 (A) Sicherer Betrieb eines Systemmanagementsystems
493 (Z) Regelmäßige Integritätsprüfung
494 (A) Schutz der Webserver-Dateien
495 (A) Minimales Betriebssystem
496 (Z) Abschaltung von DNS
497 (Z) Ein Dienst pro Server
498 (A) Kommunikation durch Paketfilter auf Minimum beschränken
510 (A) Restriktive Rechtevergabe
533 (B) Absicherung von Fernwartung
545 (B) Sichere Nutzung von Browsern
558 (B) Auswahl und Installation von Datenbankschnittstellen-Treibern
559 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen
563 (Z) Einsatz von GnuPG oder PGP
564 (Z) Secure Shell
566 (B) Clientseitige Verwendung von SSL/TLS
567 (Z) Verwendung eines Zeitstempel-Dienstes
568 (Z) Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
569 (A) Schutz vor aktiven Inhalten
571 (Z) Intrusion Detection und Intrusion Response Systeme
577 (Z) Bildung von Teilnetzen
578 (Z) Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung
579 (Z) Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung
580 (Z) Schutz vor Abhören der Raumgespräche über Mobiltelefone
581 (B) Sichere Datenübertragung über Mobiltelefone

587	(C)	Vereinbarung über die Anbindung an Netze Dritter
588	(C)	Vereinbarung über Datenaustausch mit Dritten
616	(Z)	Abschließen von Versicherungen
618	(Z)	Redundante Leitungsführung
620	(A)	Geeignete Aufbewahrung der Backup-Datenträger
621	(C)	Sicherungskopie der eingesetzten Software
622	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
623	(A)	Verhaltensregeln bei Auftreten von Schadprogrammen
624	(A)	Erstellen eines Notfall-Bootmediums
627	(C)	Sicheres Update des BIOS
632	(A)	Regelmäßige Datensicherung
633	(B)	Entwicklung eines Datensicherungskonzepts
634	(B)	Erhebung der Einflussfaktoren der Datensicherung
635	(B)	Festlegung der Verfahrensweise für die Datensicherung
636	(A)	Festlegung des Minimaldatensicherungskonzeptes
637	(A)	Dokumentation der Datensicherung
638	(A)	Sicherungskopie der übermittelten Daten
641	(A)	Übungen zur Datenrekonstruktion
648	(A)	Verhaltensregeln nach Verlust der Datenbankintegrität
649	(A)	Datensicherung einer Datenbank
650	(Z)	Archivierung von Datenbeständen
651	(B)	Wiederherstellung einer Datenbank
656	(A)	Datensicherung bei Einsatz kryptographischer Verfahren
657	(C)	Erstellen eines Notfallplans für den Ausfall des Managementsystems
658	(A)	Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
659	(A)	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
660	(A)	Festlegung von Meldewegen für Sicherheitsvorfälle
661	(C)	Eskalationsstrategie für Sicherheitsvorfälle
662	(Z)	Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
664	(A)	Behebung von Sicherheitsvorfällen
665	(A)	Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
666	(B)	Nachbereitung von Sicherheitsvorfällen
667	(Z)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
668	(C)	Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen
672	(C)	Ausfallvorsorge bei Mobiltelefonen
675	(Z)	Redundante Kommunikationsverbindungen
688	(B)	Erstellen eines Notfallplans für den Webserver
695	(C)	Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs
696	(A)	Notfallvorsorge für einen Server
2110	(A)	Datenschutzaspekte bei der Protokollierung
2111	(A)	Bereithalten von Handbüchern
2124	(B)	Geeignete Auswahl einer Datenbank-Software
2125	(A)	Installation und Konfiguration einer Datenbank
2126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
2127	(B)	Inferenzprävention
2128	(A)	Zugangskontrolle einer Datenbank
2129	(A)	Zugriffskontrolle einer Datenbank
2130	(A)	Gewährleistung der Datenbankintegrität
2131	(C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
2132	(A)	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
2133	(A)	Kontrolle der Protokolldateien eines Datenbanksystems
2134	(B)	Richtlinien für Datenbank-Anfragen
2135	(C)	Gesicherte Datenübernahme in eine Datenbank
2137	(C)	Beschaffung eines geeigneten Datensicherungssystems
2138	(B)	Strukturierte Datenhaltung
2143	(A)	Entwicklung eines Netzmanagementkonzeptes

2144 (A) Geeignete Auswahl eines Netzmanagement-Protokolls
2145 (B) Anforderungen an ein Netzmanagement-Tool
2146 (A) Sicherer Betrieb eines Netzmanagementsystems
2154 (A) Erstellung eines Sicherheitskonzeptes gegen Schadprogramme
2157 (A) Auswahl eines geeigneten Viren-Schutzprogramms
2158 (A) Meldung von Schadprogramm-Infektionen
2159 (A) Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
2160 (A) Regelungen zum Schutz vor Schadprogrammen
2161 (A) Entwicklung eines Kryptokonzepts
2162 (A) Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
2163 (A) Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
2164 (A) Auswahl eines geeigneten kryptographischen Verfahrens
2165 (A) Auswahl eines geeigneten kryptographischen Produktes
2166 (A) Regelung des Einsatzes von Kryptomodulen
2167 (B) Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
2168 (A) IT-System-Analyse vor Einführung eines Systemmanagementsystems
2169 (A) Entwickeln einer Systemmanagementstrategie
2170 (A) Anforderungen an ein Systemmanagementsystem
2171 (A) Geeignete Auswahl eines Systemmanagement-Produktes
2172 (A) Entwicklung eines Konzeptes für Webangebote
2173 (A) Festlegung einer Webserver-Sicherheitsstrategie
2174 (A) Sicherer Betrieb eines Webservers
2175 (A) Aufbau eines Webservers
2176 (Z) Geeignete Auswahl eines Internet Service Providers
2177 (Z) Sicherheit bei Umzügen
2188 (A) Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
2189 (A) Sperrung des Mobiltelefons bei Verlust
2190 (Z) Einrichtung eines Mobiltelefon-Pools
2192 (A) Erstellung einer Leitlinie zur Informationssicherheit
2193 (A) Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
2195 (A) Erstellung eines Sicherheitskonzepts
2197 (A) Integration der Mitarbeiter in den Sicherheitsprozess
2199 (A) Aufrechterhaltung der Informationssicherheit
2200 (C) Management-Berichte zur Informationssicherheit
2201 (C) Dokumentation des Sicherheitsprozesses
2204 (A) Verhinderung ungesicherter Netzzugänge
2214 (A) Konzeption des IT-Betriebs
2215 (B) Fehlerbehandlung
2216 (C) Genehmigungsverfahren für IT-Komponenten
2217 (B) Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
2218 (C) Regelung der Mitnahme von Datenträgern und IT-Komponenten
2219 (A) Kontinuierliche Dokumentation der Informationsverarbeitung
2220 (A) Richtlinien für die Zugriffs- bzw. Zugangskontrolle
2221 (A) Änderungsmanagement
2223 (B) Sicherheitsvorgaben für die Nutzung von Standardsoftware
2224 (A) Vorbeugung gegen Schadprogramme
2225 (B) Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
2226 (A) Regelungen für den Einsatz von Fremdpersonal
2272 (Z) Einrichtung eines Internet-Redaktionsteams
2273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
2298 (B) Verwaltung von Internet-Domainnamen
2303 (A) Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs
2304 (A) Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs

2305 (B) Geeignete Auswahl von Smartphones, Tablets oder PDAs
2306 (A) Verlustmeldung
2307 (A) Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses
2313 (A) Sichere Anmeldung bei Internet-Diensten
2314 (Z) Verwendung von hochverfügbaren Architekturen für Server
2315 (A) Planung des Servereinsatzes
2316 (A) Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
2317 (C) Beschaffungskriterien für einen Server
2318 (A) Sichere Installation eines IT-Systems
2319 (C) Migration eines Servers
2320 (A) Geregelte Außerbetriebnahme eines Servers
2321 (A) Planung des Einsatzes von Client-Server-Netzen
2322 (A) Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
2323 (A) Geregelte Außerbetriebnahme eines Clients
2335 (A) Festlegung der Sicherheitsziele und -strategie
2336 (A) Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
2337 (A) Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
2338 (Z) Erstellung von zielgruppengerechten Sicherheitsrichtlinien
2339 (Z) Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
2363 (B) Schutz gegen SQL-Injection
2381 (A) Festlegung einer Strategie für die WLAN-Nutzung
2382 (A) Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung
2383 (A) Auswahl eines geeigneten WLAN-Standards
2384 (A) Auswahl geeigneter Kryptoverfahren für WLAN
2385 (B) Geeignete Auswahl von WLAN-Komponenten
2386 (Z) Sorgfältige Planung notwendiger WLAN-Migrationsschritte
2387 (Z) Installation, Konfiguration und Betreuung eines WLANs durch Dritte
2388 (B) Geeignetes WLAN-Schlüsselmanagement
2389 (Z) Sichere Nutzung von Hotspots
2390 (C) Außerbetriebnahme von WLAN-Komponenten
2391 (B) Frühzeitige Information des Brandschutzbeauftragten
2393 (A) Regelung des Informationsaustausches
2394 (B) Prüfung elektrischer Anlagen
2401 (C) Umgang mit mobilen Datenträgern und Geräten
2402 (Z) Zurücksetzen von Passwörtern
2421 (B) Planung des Patch- und Änderungsmanagementprozesses
2422 (B) Umgang mit Änderungsanforderungen
2423 (A) Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement
2424 (A) Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen
2425 (C) Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement
2426 (C) Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse
2427 (C) Abstimmung von Änderungsanforderungen
2428 (Z) Skalierbarkeit beim Patch- und Änderungsmanagement
2429 (Z) Erfolgsmessung von Änderungsanforderungen
2431 (A) Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen
2432 (Z) Richtlinie für die Löschung und Vernichtung von Informationen
2433 (W) Überblick über Methoden zur Löschung und Vernichtung von Daten
2434 (Z) Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten
2435 (Z) Auswahl geeigneter Aktenvernichter
2436 (Z) Vernichtung von Datenträgern durch externe Dienstleister
2457 (A) Konzeption für die sichere Internet-Nutzung
2458 (A) Richtlinie für die Internet-Nutzung
2459 (W) Überblick über Internet-Dienste

2460 (C) Geregelte Nutzung von externen Dienstleistungen
2461 (A) Planung des sicheren Bluetooth-Einsatzes
2462 (Z) Auswahlkriterien für die Beschaffung von Bluetooth-Geräten
2463 (Z) Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten
2475 (A) Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten
2486 (A) Dokumentation der Architektur von Webanwendungen und Web-Services
2487 (B) Entwicklung und Erweiterung von Anwendungen
2488 (W) Web-Tracking
2496 (A) Geregelte Außerbetriebnahme eines Protokollierungsservers
2497 (A) Erstellung eines Sicherheitskonzepts für die Protokollierung
2498 (C) Behandlung von Warn- und Fehlermeldungen
2499 (A) Planung der Protokollierung
2500 (A) Protokollierung von IT-Systemen
2501 (C) Datenschutzmanagement
2502 (B) Regelung der Verantwortlichkeiten im Bereich Datenschutz
2503 (A) Aspekte eines Datenschutzkonzeptes
2504 (A) Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten
2505 (A) Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten
2506 (A) Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
2507 (A) Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
2508 (A) Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten
2509 (C) Datenschutzrechtliche Freigabe
2510 (A) Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten
2511 (A) Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten
2512 (A) Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten
2513 (Z) Dokumentation der datenschutzrechtlichen Zulässigkeit
2514 (A) Aufrechterhaltung des Datenschutzes im laufenden Betrieb
2515 (A) Datenschutzgerechte Löschung/Vernichtung
2516 (Z) Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender
2517 (A) Vertragsgestaltung mit Dritt-Dienstleistern
2518 (C) Einsatz einer hochverfügbaren Firewall-Lösung
2519 (A) Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing
2520 (C) Sicheres und vollständiges Löschen von Cloud-Anwenderdaten
2521 (A) Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten
2522 (B) Berichtswesen und Kommunikation zu den Cloud-Anwendern
2523 (C) Sichere Automatisierung der Cloud-Regelprozesse
2524 (W) Modellierung von Cloud Management
2530 (B) Planung und Vorbereitung von Migrationen
2531 (A) Erarbeitung einer Sicherheitsrichtlinie für Web-Services
2532 (B) Anbieten von Web-Services für Dritte
2533 (C) Vertragliche Aspekte bei der Bereitstellung von Web-Services
2534 (A) Erstellung einer Cloud-Nutzungs-Strategie
2535 (A) Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
2536 (A) Service-Definition für Cloud-Dienste durch den Anwender
2537 (A) Planung der sicheren Migration zu einem Cloud Service
2538 (A) Planung der sicheren Einbindung von Cloud Services
2539 (A) Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung
2540 (A) Sorgfältige Auswahl eines Cloud-Diensteanbieters

2541 (A) Vertragsgestaltung mit dem Cloud-Diensteanbieter
2542 (A) Sichere Migration zu einem Cloud Service
2543 (A) Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb
2544 (C) Auditierung bei Cloud-Nutzung
2545 (W) Modellierung der Cloud-Nutzung
2546 (A) Analyse der Anforderungen an neue Anwendungen
2547 (A) Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen
2548 (A) Erstellung eines Lastenheftes
2549 (C) Erstellung eines Mandantenkonzeptes
2550 (C) Geeignete Steuerung der Anwendungsentwicklung
2551 (Z) Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens
2552 (A) Erstellung eines Pflichtenheftes
2553 (C) Entwicklung eines Pflegekonzeptes für Anwendungen
2554 (Z) Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen
2555 (A) Entwicklung eines Authentisierungskonzeptes für Anwendungen
2556 (A) Planung und Umsetzung von Test und Freigabe von Anwendungen
2558 (A) Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs
4107 (B) Nutzung von Hersteller- und Entwickler-Ressourcen
4109 (Z) Software-Reinstallation bei Arbeitsplatzrechnern
4114 (A) Nutzung der Sicherheitsmechanismen von Mobiltelefonen
4115 (B) Sicherstellung der Energieversorgung von Mobiltelefonen
4133 (Z) Geeignete Auswahl von Authentikationsmechanismen
4134 (Z) Wahl geeigneter Datenformate
4135 (A) Restriktive Vergabe von Zugriffsrechten auf Systemdateien
4176 (B) Auswahl einer Authentisierungsmethode für Webangebote
4177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen
4200 (Z) Umgang mit USB-Speichermedien
4225 (Z) Einsatz eines Protokollierungsservers in einem Sicherheitsgateway
4227 (C) Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
4228 (A) Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs
4229 (C) Sicherer Betrieb von Smartphones, Tablets und PDAs
4230 (Z) Zentrale Administration von Smartphones, Tablets und PDAs
4231 (Z) Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs
4232 (Z) Sichere Nutzung von Zusatzspeicherkarten
4234 (B) Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
4237 (A) Sichere Grundkonfiguration eines IT-Systems
4238 (A) Einsatz eines lokalen Paketfilters
4239 (A) Sicherer Betrieb eines Servers
4240 (Z) Einrichten einer Testumgebung für einen Server
4241 (A) Sicherer Betrieb von Clients
4242 (Z) Einrichten einer Referenzinstallation für Clients
4250 (Z) Auswahl eines zentralen, netzbasierten Authentisierungsdienstes
4254 (Z) Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
4255 (A) Nutzung von IrDA-Schnittstellen
4293 (Z) Sicherer Betrieb von Hotspots
4294 (A) Sichere Konfiguration der Access Points
4295 (A) Sichere Konfiguration der WLAN-Clients
4296 (C) Einsatz einer geeigneten WLAN-Management-Lösung
4297 (A) Sicherer Betrieb der WLAN-Komponenten
4298 (B) Regelmäßige Audits der WLAN-Komponenten
4305 (B) Einsatz von Speicherbeschränkungen (Quotas)
4306 (Z) Umgang mit Passwort-Speicher-Tools
4323 (Z) Synchronisierung innerhalb des Patch- und Änderungsmanagements

4324 (C) Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement
4325 (Z) Löschen von Auslagerungsdateien
4345 (Z) Schutz vor unerwünschten Informationsabflüssen
4359 (W) Überblick über Komponenten eines Webservers
4360 (B) Sichere Konfiguration eines Webservers
4362 (A) Sichere Konfiguration von Bluetooth
4363 (A) Sicherer Betrieb von Bluetooth-Geräten
4364 (A) Regelungen für die Aussonderung von Bluetooth-Geräten
4392 (A) Authentisierung bei Webanwendungen
4393 (B) Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services
4394 (A) Session-Management bei Webanwendungen und Web-Services
4395 (B) Fehlerbehandlung durch Webanwendungen und Web-Services
4396 (B) Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
4397 (C) Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services
4398 (B) Sichere Konfiguration von Webanwendungen
4399 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen
4400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services
4401 (B) Schutz vertraulicher Daten bei Webanwendungen
4402 (A) Zugriffskontrolle bei Webanwendungen
4403 (C) Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
4404 (A) Sicherer Entwurf der Logik von Webanwendungen
4405 (C) Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services
4406 (Z) Verhinderung von Clickjacking
4430 (A) Analyse von Protokolldaten
4431 (A) Auswahl und Verarbeitung relevanter Informationen für die Protokollierung
4432 (A) Sichere Konfiguration von Serverdiensten
4433 (Z) Einsatz von Datenträgerverschlüsselung
4434 (C) Sicherer Einsatz von Appliances
4435 (Z) Selbstverschlüsselnde Festplatten
4436 (A) Planung der Ressourcen für Cloud-Dienste
4437 (A) Planung von Cloud-Diensteprofilen
4438 (A) Auswahl von Cloud-Komponenten
4439 (Z) Virtuelle Sicherheitsgateways (Firewalls) in Clouds
4440 (Z) Verschlüsselte Speicherung von Cloud-Anwenderdaten
4441 (Z) Multifaktor-Authentisierung für den Cloud-Benutzerzugriff
4442 (C) Zentraler Schutz vor Schadprogrammen in der Cloud-Infrastruktur
4443 (B) Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur
4444 (A) Patchmanagement für Cloud-Komponenten
4445 (A) Durchgängige Mandantentrennung von Cloud-Diensten
4446 (W) Einführung in das Cloud Management
4450 (A) Absicherung der Kommunikation bei Web-Services
4451 (W) Aktuelle Web-Service Standards
4452 (A) Überwachung eines Web-Service
4453 (Z) Einsatz eines Security Token Service (STS)
4454 (A) Schutz vor unerlaubter Nutzung von Web-Services
4455 (A) Autorisierung bei Web-Services
4456 (A) Authentisierung bei Web-Services
4457 (B) Sichere Mandantentrennung bei Webanwendungen und Web-Services
4458 (A) Planung des Einsatzes von Web-Services
4459 (Z) Einsatz von Verschlüsselung bei Cloud-Nutzung
4460 (Z) Einsatz von Federation Services
4461 (Z) Portabilität von Cloud Services

4462 (W) Einführung in die Cloud-Nutzung
4463 (A) Sichere Installation einer Anwendung
4464 (B) Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb
4465 (A) Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs
4466 (C) Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs
4467 (B) Auswahl von Applikationen für Smartphones, Tablets und PDAs
4468 (B) Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs
4469 (A) Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion
5110 (Z) Absicherung von E-Mail mit SPHINX (S/MIME)
5117 (Z) Integration eines Datenbank-Servers in ein Sicherheitsgateway
5121 (B) Sichere Kommunikation von unterwegs
5138 (Z) Einsatz von RADIUS-Servern
5139 (A) Sichere Anbindung eines WLANs an ein LAN
5140 (C) Aufbau eines Distribution Systems
5141 (B) Regelmäßige Sicherheitschecks in WLANs
5150 (Z) Durchführung von Penetrationstests
5152 (C) Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste
5155 (Z) Datenschutz-Aspekte bei der Internet-Nutzung
5156 (Z) Sichere Nutzung von Twitter
5157 (Z) Sichere Nutzung von sozialen Netzwerken
5158 (Z) Nutzung von Web-Speicherplatz
5159 (W) Übersicht über Protokolle und Kommunikationsstandards für Webserver
5160 (W) Authentisierung gegenüber Webservern
5161 (W) Erstellung von dynamischen Web-Angeboten
5168 (A) Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services
5169 (A) Systemarchitektur einer Webanwendung
5171 (A) Sichere Kommunikation zu einem zentralen Protokollierungsserver
5172 (A) Sichere Zeitsynchronisation bei der zentralen Protokollierung
5173 (Z) Nutzung von Kurz-URLs und QR-Codes
5174 (A) Absicherung der Kommunikation zum Cloud-Zugriff
5175 (Z) Einsatz eines XML-Gateways
5176 (B) Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution
5177 (B) Serverseitige Verwendung von SSL/TLS
6102 (A) Verhaltensregeln bei WLAN-Sicherheitsvorfällen
6110 (C) Festlegung des Geltungsbereichs und der Notfallmanagementstrategie
6111 (A) Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene
6112 (A) Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement
6113 (C) Bereitstellung angemessener Ressourcen für das Notfallmanagement
6114 (A) Erstellung eines Notfallkonzepts
6115 (C) Integration der Mitarbeiter in den Notfallmanagement-Prozess
6116 (C) Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse
6117 (B) Tests und Notfallübungen
6118 (A) Überprüfung und Aufrechterhaltung der Notfallmaßnahmen
6119 (C) Dokumentation im Notfallmanagement-Prozess
6120 (C) Überprüfung und Steuerung des Notfallmanagement-Systems
6121 (A) Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
6122 (C) Definition eines Sicherheitsvorfalls
6123 (Z) Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen
6124 (C) Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung
6125 (A) Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen
6126 (W) Einführung in die Computer-Forensik
6127 (Z) Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen

6128	(Z)	Schulung an Beweismittelsicherungswerkzeugen
6129	(C)	Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen
6130	(A)	Erkennen und Erfassen von Sicherheitsvorfällen
6131	(A)	Qualifizieren und Bewerten von Sicherheitsvorfällen
6132	(A)	Eindämmen der Auswirkung von Sicherheitsvorfällen
6133	(A)	Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen
6134	(B)	Dokumentation von Sicherheitsvorfällen
6137	(Z)	Treuhänderische Hinterlegung (Escrow)
6141	(C)	Festlegung von Ausweichverfahren bei der Internet-Nutzung
6151	(A)	Alarmierungskonzept für die Protokollierung
6152	(A)	Notfallvorsorge und regelmäßige Datensicherung im Cloud Computing
6153	(C)	Einsatz von redundanten Cloud-Management-Komponenten
6154	(B)	Notfallmanagement für Web-Services
6155	(A)	Erstellung eines Notfallkonzeptes für einen Cloud Service
6156	(Z)	Durchführung eigener Datensicherungen
6157	(Z)	Entwicklung eines Redundanzkonzeptes für Anwendungen
6158	(B)	Notfallvorsorge für Anwendungen
6159	(C)	Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs

9.11 Anhang: Querverweise von BSI[247] zu CC[248]

BSI		CC		BSI --> CC --> ggf. Begründung
Baustein [B Nr.]	Gefährdung [G Nr.]	SFC	Verweis	Bemerkungen
3.101 Allgemeiner Server	4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	FIA_UAU,		Die Zugriffswege und Funktionen sind für den Anwender häufig nicht transparent und bergen die Gefahr, unentdeckte Schwachstellen zu enthalten. --> This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based. --> gewählt durch gleiche Zielstellung.
3.101 Allgemeiner Server, 1.4 Datensicherungskonzept, 1.6 Schutz vor Schadprogrammen, 1.9 Hard- und Software-Management, 1.12 Archivierung	4.13 Verlust gespeicherter Daten	FDP_SDI	FDP_ITT, FDP_UCT, FDP_UIT	Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. --> This family provides requirements that address protection of user data while it is stored within containers controlled by the TSF. --> gewählt durch gleiche Zielstellung.
1.6 Schutz vor Schadprogrammen, 1.7 Kryptokonzept, 1.9 Hard- und Software-Management, 1.10 Standardsoftware	4.22 Software- Schwachstellen oder -Fehler	FPT_FLS		Bei weitverbreiteter Standardsoftware können Software-Schwachstellen schnell dazu führen, dass weitweit schwerwiegende Sicherheitsprobleme für alle Arten von Institutionen entstehen können. --> The requirements of this family ensure that the TOE will always enforce its SFRs in the event of certain types of failures in the TSF. --> gewählt durch gleiche Zielstellung.
1.6 Schutz vor Schadprogrammen	5.85 Integritätsverlust schützenswerter Informationen	FIA_UID		Integrität ist die Anforderung, dass eine Information unverfälscht sein muss. --> This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification. --> gewählt durch gleiche Zielstellung.
1.12 Archivierung	4.20 Überlastung von Informationssystemen	FTA_MCS		Auslöser für die Überlastung von Informationssystemen können sein, dass zahlreiche Anfragen zur gleichen Zeit ein System überbeanspruchen und dadurch die Prozessoren überlastet werden. --> This family defines requirements to place limits on the number of concurrent sessions that belong to the same user. --> Somit wird eine Überlastung durch zuviele Zugriffe verhindert. --> gewählt durch gleiche Zielstellung.
1.7 Kryptokonzept, 1.11 Outsourcing	4.33 Schlechte oder fehlende Authentikation	FIA_UAU	FCS_CKM	Wenn Authentikationsmechanismen fehlen oder zu schlecht sind, besteht die Gefahr, dass... --> This family defines the types of user authentication mechanisms supported by the TSF. This family defines the required attributes on which the user authentication mechanisms must be based. -> gewählt durch gleiche Zielstellung.
1.7 Kryptokonzept, 1.9 Hard- und Software-Management	4.35 Unsichere kryptographische Algorithmen	FCS_COP		Der Sicherheitszugewinn durch Einsatz kryptographischer Verfahren ist grundsätzlich von zwei Parametern abhängig: es müssen sichere kryptographische Algorithmen eingesetzt werden und die geheimen Schlüssel müssen vertraulich gehandhabt werden. --> This family should be included whenever there are requirements for cryptographic operations to be performed. -> gewählt durch gleiche Zielstellung.
1.7 Kryptokonzept	5.84 gefälschte Zertifikate	FDP_DAU	FMT_SAE	Diese Bindung des Schlüssels an den Namen der Person wird wiederum kryptographisch mittels einer digitalen Signatur einer vertrauenswürdigen dritten Stelle abgesichert. --> Data authentication permits an entity to accept responsibility for the authenticity of information (e.g., by digitally signing it). -> gewählt durch gleiche Zielstellung.
1.9 Hard- und Software-Management	4.43 Undokumentierte Funktionen	FPT_TEE		Dies ist insbesondere dann problematisch, wenn die undokumentierten Funktionen Sicherheitsmechanismen des Produktes betreffen, beispielsweise den Zugriffsschutz. --> This family defines requirements for the testing of one or more external entities by the TSF. These external entities are not human users, and they can include combinations of software and/or hardware interacting with the TOE. --> Die CC kann testen auf welche Systemfunktionen eine gewisse Anwendung zugreift und ebenfalls ob diese ordnungsgemäß konfiguriert ist.

Tabelle 29: Querverweise BSI zu CC (1)[249]

[247] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge, 2014.
[248] Vgl. Common Criteria, Part 2: Security functional components, 2012.
[249] Eigene Darstellung.

4.5 LAN-Anbindung eines IT-Systems über ISDN	4.25 Nicht getrennte Verbindungen	FTA_SSL		Bsp. Ein Netzadministrator hat vor seinem 14-tägigen Urlaub eine ISDN-Datenverbindung zu seinem Internet-Provider aufgebaut. Bei Beendigung der Sitzung wurde die ISDN-Verbindung nicht korrekt ausgelöst. Nach Beendigung des Urlaubs wunderte sich der Administrator über die recht hohe Rechnung für Verbindungsentgelte von Seiten des ISDN-Carriers. --> This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions. --> Die CC könnte bei einer interaktiven Verbindung (z.B. 5min inaktiv) die Verbindung automatisch trennen.
4.6 WLAN	4.61 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen	FCS_CKM	FCS_COP, FMT_SMF	Diese Art des Schlüsselmanagements führt in der Praxis oft dazu, dass die kryptographischen Schlüssel sehr selten oder überhaupt nicht gewechselt werden. Wenn dann ein WLAN-Schlüssel offengelegt wird, wird das gesamte WLAN kompromittiert. --> This family should be included whenever there are functional requirements for the management of cryptographic keys. -> gewählt durch gleiche Zielstellung.
4.8 Bluetooth	4.80 Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen	FCS_CKM	FCS_COP, FMT_SMF	Neben Länge und Komplexität der bei der Authentisierung (bei Bluetooth ohne SSP) verwendeten PIN spielt auch die Länge der für die Verschlüsselung der übertragenen Daten verwendeten Schlüssel eine Rolle für die Sicherheit. --> This family should be included whenever there are functional requirements for the management of cryptographic keys. -> gewählt durch gleiche Zielstellung.
5.3 Groupware	4.32 Nichtzustellung einer Nachricht	FCO_NRR	FCO_NRO	Dabei ist das größte Problem, dass die Benutzer häufig nicht informiert werden, wenn eine E-Mail nicht zugestellt werden konnte. Es kann also nicht darauf vertraut werden, dass eine Nachricht den Empfänger erreicht hat, sofern keine Probleme angezeigt werden. --> Non-repudiation of receipt defines requirements to provide evidence to other users/subjects that the information was received by the recipient. -> gewählt durch gleiche Zielstellung.
5.3 Groupware	4.37 Mangelnde Verlässlichkeit von Groupware	FDP_UCT	FDP_UIT	Der Datenaustausch über Groupware-Dienste wie E-Mail ist schnell und komfortabel, aber nicht immer sehr zuverlässig. --> This family defines the requirements for ensuring the confidentiality of user data when it is transferred using an external channel between the TOE and another trusted IT product. -> gewählt durch gleiche Zielstellung.
5.7 Datenbanken	4.27 Unterlaufen von Zugriffskontrollen über ODBC	FCO_NRO		Bestandteil der Kommunikation über die Schnittstelle zwischen Anwendungsprogramm und Datenbank ist die Identifizierung der Anwendung als registrierter Datenbanknutzer. --> ...about the identity of the originator of some information. --> Die CC könnte kontrollieren wer Zugang besitzt.
5.7 Datenbanken	4.28 Verlust von Daten einer Datenbank	FRU_RSA		... erhöhter Speicherbedarf der Benutzer --> Resource allocation rules allow the creation of quotas or other means of defining limits on the amount of resource space or time that may be allocated on behalf of a specific user or subjects. --> Im CC kann dem User eine gewisse Speichermenge zugesichert werden, somit kommt es nicht zur Überbelastung des physikalischen Speichers.
5.21 Webanwendungen	4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services	FAU_SAA		... Eingabedaten können aber auch hier oft modifiziert werden, beispielsweise durch den Einsatz eines Proxys oder durch Manipulation der Clients. --> This family defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations.
5.21 Webanwendungen	4.86 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen	FAU_STG		Werden sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert. --> This family defines the requirements for the TSF to be able to create and maintain a secure audit trail.
5.21 Webanwendungen	4.87 Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services	FPR_ANO		Wenn demzufolge Informationen unnötig offengelegt werden, kann dies einen erfolgreichen Angriff erleichtern. --> The requirements for Anonymity provide protection of the user identity. -> gewählt durch gleiche Zielstellung.
5.22 Protokollierung	4.89 Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung	FAU_SAA	FAU_ARP	Produkte, die Protokoll- und Monitoringdaten speichern und auswerten, können häufig als optionale Komponenten in einIT-Frühwarnsystem eingebunden werden. --> This family defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to a potential security violation. -> gewählt durch gleiche Zielstellung.
5.25 Allgemeine Anwendungen	4.99 Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen	FMT_MSA		Nach der Erst-Installation sind außerdem häufig die Anwendungen so vorkonfiguriert, dass keine oder nur einige Sicherheitsmechanismen aktiviert sind. --> This family allows authorised users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes. -> gewählt durch gleiche Zielstellung.

Tabelle 30: Querverweise BSI zu CC (2)[250]

[250] Eigene Darstellung.

1.0 Sicherheitsmanagement	2.66 Unzureichendes Sicherheitsmanagement	FMT_MSA		Ein organisiertes Vorgehen bei der Planung, Durchführung und Kontrolle des Sicherheitsprozesses ist daher zwingend erforderlich. --> Examples of security attributes are the groups to which a user belongs, the roles he/she might assume, the priority of a process (subject), and the rights belonging to a role or a user. -> gewählt durch gleiche Zielstellung.
1.0 Sicherheitsmanagement	2.107 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement	FMT_SMR	FRU_PRS	Aus diesem Grund ist es essenziell, beim Sicherheitsmanagement die richtigen Prioritäten zu setzen. --> The capabilities of these roles with respect to security management are described in the other families in this class. -> gewählt durch gleiche Zielstellung.
1.1 Organisation	2.7 Unerlaubte Ausübung von Rechten	FMT_SMR		Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. --> This family is intended to control the assignment of different roles to users -> gewählt durch gleiche Zielstellung.
1.6 Schutz vor Schadprogrammen	2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen	FPT_TST		Werden bereits eingeführte Sicherheitsmaßnahmen (z. B.Klassifizierung von Informationen, Datensicherung, Zutrittskontrolle, Vorgaben für Verhalten bei Notfällen) nicht konsequent umgesetzt und regelmäßig kontrolliert, kann es sein, dass sie nicht wirksam sind oder missachtet werden. --> The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. -> gewählt durch gleiche Zielstellung.
1.7 Kryptokonzept	2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung	FCS_CKM	FCS_COP	Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden. -> Cryptographic keys must be managed throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, entry, storage, access (e.g. backup, escrow, archive, recovery) and destruction. -> gewählt durch gleiche Zielstellung.
1.9 Hard- und Software-Management	2.22 Fehlende oder unzureichende Auswertung von Protokolldaten	FPT_SSP		Dadurch werden in einem Informationsverbund oft große Mengen an Protokolldaten erzeugt, die sich nur schwer und mit einem hohen Zeitaufwand auswerten lassen. Allerdings ist eine sinnvolle Auswertung dieser Protokolldaten notwendig, um beispielsweise Fehleranalysen durchführen und erfolgte Angriffe identifizieren zu können. --> State synchrony protocol (FPT_SSP) establishes the requirement for certain critical functions of the TSF to use a trusted protocol. State synchrony protocol (FPT_SSP) ensures that two distributed parts of the TOE (e.g. hosts) have synchronised their states after a security-relevant action. -> gewählt durch gleiche Zielstellung.
1.9 Hard- und Software-Management	5.26 Analyse des Nachrichtenflusses	FDP_IFC		Über eine Verkehrsflussanalyse versucht ein Angreifer Auskunft darüber zu erhalten, wer wann welche Datenmengen an wen gesendet hat und wie oft. --> This family covers the identification of information flow control SFPs; and, for each, specifies the scope of control of the SFP. -> gewählt durch gleiche Zielstellung.
1.10 Standardsoftware	3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten	FMT_SMR		Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. --> This family reduces the likelihood of damage resulting from users abusing their authority by taking actions outside their assigned functional responsibilities. -> gewählt durch gleiche Zielstellung.
1.10 Standardsoftware	5.9 Unberechtigte IT-Nutzung	FIA_UAU	FIA_UID	Die Identifikation und Authentisierung von Benutzern soll verhindern, dass Informationstechnik unberechtigt benutzt wird. Aber auch bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Passwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn die Zugangsdaten ausgespäht werden. --> This family defines the types of user authentication mechanisms supported by the TSF. This family defines the required attributes on which the user authentication mechanisms must be based. --> Mit Hilfe der CC kann ein Angriff z.B. verhindert werden, indem z.B. bei 2 falschen Einlogversuchen ein neues Passwort erstellt wird und dem Benutzer an seine E-Mail gesendet wird.
1.10 Standardsoftware	5.2 Manipulation an Informationen oder Software	FMT_SMR		Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse vonIT-Systemen besitztbzw.je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. --> Some management actions can be performed by users, others only by designated people within the organisation. This family allows the definition of different roles, such as owner, auditor, administrator, daily-management. --> Die CC verteilt die Userrechte, sodass schwerwiegende Veränderungen nicht von irgendwem durchgeführt werden können.
1.11 Outsourcing	3.105 Ungenehmigte Nutzung von externen Dienstleistungen	FCO_NRO		Es kommt wieder vor, dass Mitarbeiter externe Dienstleistungen in Anspruch zu nehmen, ohne dass dies innerhalb ihrer Institution abgestimmt ist. --> The recipient or a third party can verify the evidence of origin. This evidence should not be forgeable. --> Ohne den Dienst zu kennen wird dieser durch das CC blockiert, da dieser dort verifiziert sein muss. Somit werden unbekannte externe Dienstleistungen blockiert.

Tabelle 31: Querverweise BSI zu CC (3)[251]

[251] Eigene Darstellung.

1.11 Outsourcing	5.71 Vertraulichkeitsverlust schützenswerter Informationen	FPR_ANO		Vertraulichkeit ist die Anforderung, dass eine Information nur den zur Kenntnisnahme berechtigten Personen zugänglich gemacht werden darf. --> Anonymity ensures that a subject may use a resource or service without disclosing its user identity. -> gewählt durch gleiche Zielstellung.
1.11 Outsourcing	5.85 Integritätsverlust schützenswerter Informationen	FDP_DAU		Integrität ist die Anforderung, dass eine Information unverfälscht sein muss. --> Data authentication permits an entity to accept responsibility for the authenticity of information (e.g., by digitally signing it). This family provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified. -> gewählt durch gleiche Zielstellung.
1.11 Outsourcing	5.107 Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister	FPR_PSE	FÜR_ANO	Werden im Rahmen des Outsourcing-Vorhabens personenbezogene Daten beim Dienstleister verarbeitet oder gespeichert, so müssen auch zusätzliche Datenschutzgesichtspunkte beachtet werden. --> This family ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use. -> gewählt durch gleiche Zielstellung.
1.12 Archivierung	5.83 Kompromittierung kryptographischer Schlüssel	FCS_CKM		Beim Einsatz kryptographischer Verfahren hängt der Sicherheitszugewinn entscheidend davon ab, wie vertraulich die verwendeten geheimen kryptographischen Schlüssel bleiben. --> Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. -> gewählt durch gleiche Zielstellung.
1.12 Archivierung	5.106 Unberechtigtes Überschreiben oder Löschen von Archivmedien	FDP_ACF		Auf Archivmedien sollen wichtige Daten langfristig und unverändert gespeichert werden. Daher dürfen diese nicht unberechtigt überschrieben, gelöscht oder anderweitig verändert werden. --> This family describes the rules for the specific functions that can implement an access control policy named in Access control policy (FDP_ACC) which also specifies the scope of control of the policy. An example of such an object is "Message of the Day", which is readable by all, and changeable only by the authorised administrator. -> gewählt durch gleiche Zielstellung.
1.15 Löschen und Vernichten von Daten	5.146 Vertraulichkeitsverlust durch Auslagerungsdateien	FDP_RIP		Meldet sich ein Benutzer vom System ab bzw. wird das System ausgeschaltet, werden die Auslagerungsdateien nicht automatisch gelöscht. Daher finden sich in der Auslagerungsdatei Teile der Informationen wieder, die die Benutzer während ihrer Arbeit mit dem IT-System verwendet haben. --> As an example to satisfy the FDP_RIP requirement for files as objects requires that all sectors that make up the file need to be prepared for re-use. (mehr Informationen wenn man im CC Katalog als Suchbegriff Swap eingibt) -> gewählt durch gleiche Zielstellung.

Tabelle 32: Querverweise BSI zu CC (4)[252]

[252] Eigene Darstellung.

9.12 Anhang: Leitfragenkatalog[253]

Nr.1 Komplexität der Zugangsmöglichkeiten				
Verweis:	4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen (BSI) FIA_UAU (CC)			
Beschreibung:	In komplexen IT-Systemen sind häufig verschiedene Zugangsmöglichkeiten gegeben, um auf das System zugreifen zu können.			
Implementierung:	Welche Zugangsmöglichkeiten gibt es prinzipiell?			
	Welche Systematik liegt dem Anmeldeprozess zugrunde?			
	Wer darf sich alles Zugang verschaffen?			
	Sind Aktionen vor dem ordentlichen Zugang möglich?			
	Gibt es ein Feedback bei fehlerhaftem Anmeldeprozess?			
	Werden weitere Dienste für Zugangsmöglichkeiten genutzt?			
Schlüsselbegriffe:	Authentifizierung, Anmeldung, Passwort, Passwortlänge, gesperrt, Benutzername, Bestätigung, Aufzeichnung			
Zusatz:	Sind die Zugangsmöglichkeiten kontrollierbar?			
	Gibt es eine Sicherheitseinrichtung bei Sabotageversuchen?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

[253] Eigene Darstellung.

Nr.2 Verlust gespeicherter Daten				
Verweis:	4.13 Verlust gespeicherter Daten (BSI)			
	FDP_SDI (CC)			
Beschreibung:	Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben.			
Implementierung:	Existieren Backups von verlorenen Daten?			
	Wie können die Daten verloren gehen?			
	Welche Auswirkungen haben verlorene Daten?			
	Werden direkte oder indirekte Schäden angerichtet?			
	Sind die Daten verfälscht?			
Schlüsselbegriffe:	Daten, Sicherungen, Verlust, Datensicherung, Verwaltung, Verfälschung, Zugriff, Wiederherstellung, Rettung			
Zusatz:	Sind die Daten für immer verloren?			
	Welche Maßnahmen sind zur Vermeidung getroffen worden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.3 Software- Schwachstellen oder -Fehler				
Verweis:	4.22 Software- Schwachstellen oder -Fehler (BSI)			
	FPT_FLS (CC)			
Beschreibung:	Für jede Art von Software gilt: je komplexer das IT-System, umso mehr Schwachstellen oder Fehler können auftreten.			
Implementierung:	Was sind Schwachstellen?			
	Sind die Schwachstellen immer ein Sicherheitsrisiko?			
	Was sind die Gründe für Schwachstellen oder Fehler?			
	Was sind mögliche Risiken?			
	Welche Systeme sind betroffen?			
Schlüsselbegriffe:	IT-System, Sicherheit, Schwachstellen, Fehler, Software, Kommunikation, Verschlüsselung, Warnmeldungen, Zugriff			
Zusatz:	Kann sichergestellt werden, dass die Hauptanwendungen immer laufen?			
	Können Fehler durchgehend unentdeckt bleiben?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.4 Integritätsverlust schützenswerter Informationen				
Verweis:	5.85 Integritätsverlust schützenswerter Informationen (BSI)			
	FIA_UID (CC)			
Beschreibung:	Integrität ist die Anforderung, dass eine Information unverfälscht sein muss.			
Implementierung:	Wie kann die Integrität sichergestellt werden?			
	Was kann durch Integritätsverlust passieren?			
	Wer kann die Integritäten bearbeiten?			
	Kann eine Integrität verfälscht sein?			
	Wann ist die Integrität wichtig?			
Schlüsselbegriffe:	Integrität, unverfälscht, Information, Sicherheit, Kontrolle, Schutz, Kontrolle, Verschlüsselung, Fehler, Daten, Programme			
Zusatz:	Wodurch kann Integritätsverlust entstehen?			
	Welche Informationen brauchen Integrität?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.5 Überlastung von Informationssystemen				
Verweis:	4.20 Überlastung von Informationssystemen (BSI)			
	FTA_MCS (CC)			
Beschreibung:	Wenn Systeme nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, wo sie den Anforderungen der Benutzer nicht mehr gerecht werden.			
Implementierung:	Was sind die Auslöser für eine Überbelastung?			
	Wann ist eine Überbelastung erreicht?			
	Welche Dienste sind von diesem Problem betroffen?			
	Was sind die Folgen der Überlastung?			
	Welche Arten und Möglichkeiten der Informationslimitierung gibt es?			
Schlüsselbegriffe:	Information, Überbelastung, Limitierung, Dimensionierung, System, Kommunikation, Netze, Daten, Archivierung, Protokollierung			
Zusatz:	Können auch Gruppenlimitierungen eingerichtet werden?			
	Werden Fehlermeldungen archiviert?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.6 Schlechte oder fehlende Authentifizierung				
Verweis:	4.33 Schlechte oder fehlende Authentikation (BSI)			
	FIA_UAU (CC)			
Beschreibung:	Authentikationsmechanismen können zur Authentifizierung von Benutzern oder Komponenten oder zur Bestimmung des Datenursprungs eingesetzt werden.			
Implementierung:	Worauf beruht die Authentifikation?			
	Welche Authentifikationsmechanismen gibt es?			
	Was sind die Folgen von keiner oder schlechter Authentifikation?			
	Wie wird eine sichere Authentifikation sichergestellt?			
	Auf welchen Benutzerattributen muss die Authentifikation beruhen?			
Schlüsselbegriffe:	Authentikation, Datenursprung, Sicherheit, Benutzer, Informationen, Daten, Passwort, Zugriff, Quelle, Komponente			
Zusatz:	Woher kommt die Ursprungsdatei?			
	Müssen Benutzer Ihre Daten z.B. Passwörter regelmässig wechseln?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.7 Kryptographie				
Verweis:	4.35 Unsichere kryptographische Algorithmen (BSI)			
	FCS_COP (CC)			
Beschreibung:	Der Einsatz kryptographischer Algorithmen stellt einen vertraulichen Datenaustausch sicher.			
Implementierung:	Welche kryptographischen Algorithmen werden eingesetzt, inkl. Bitlänge?			
	Werden Signaturen verwendet?			
	Wird ein Zufallsgenerator für Zahlen verwendet?			
	Welche Operationen sind davon betroffen?			
	Kombination weiterer Sicherheitsfunktionen mithilfe von Verschlüsselung?			
	Wie sind die Standards implementiert?			
	Sind alle Übertragungswege und Speicherbereiche abgesichert?			
Schlüsselbegriffe:	Kryptographie, Signatur, Hashwert, Bitlänge, Schlüssellänge, proprietär, AES, 3DES, XOR, Zahlengenerator, Symmetrisch, Asymmetrisch			
Zusatz:	Ist die Aktualität der Verschlüsselung gewährleistet?			
	Werden proprietäre Verfahren eingesetzt?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.8 Gefälschte Zertifikate				
Verweis:	5.84 gefälschte Zertifikate (BSI)			
	FDP_DAU (CC)			
Beschreibung:	Zertifikate versichern den Benutzern, dass ein kryptographischer Schlüssel an eine Person gebunden ist, sodass die Quelle einer Informationen oder Datei vertrauenswürdig ist.			
Implementierung:	Welche Zertifikate werden verwendet?			
	Wie werden Zertifikate erstellt?			
	Wie werden gefälschte Zertifkate erkannt?			
	Was kann man mit einem gefälschten Zertifikat anstellen?			
	Wie werden Zertifikate verschlüsselt?			
Schlüsselbegriffe:	Zertifikat, Sicherheit, Kryptographie, Signatur, Benutzer, Daten, Prüfung, Schlüssel, Angaben, Fälschung, Kommunikation			
Zusatz:	Braucht man bei jedem Kommunikationsaustausch ein Zertifikat?			
	Lässt sich die zertifizierte Quelle des Zertifikates wiederfinden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.9 Undokumentierte Funktionen				
Verweis:	4.43 undokumentierte Funktionen (BSI)			
	FPT_TEE (CC)			
Beschreibung:	Viele Programme enthalten undokumentierte Funktionen, die meistens als Hilfefunktionen basieren, jedoch solange diese nicht offengelegt sind, kann nicht sichergestellt werden, dass mit ihnen auch nicht viel Schaden angerichtet werden kann.			
Implementierung:	Wo sind die Funktionen dokumentiert?			
	Welche Funktionen können Schaden anrichten?			
	Was können undokumentierte Funktionen anstellen?			
	Kann ich unerwünschte Funktionen deaktivieren?			
	Können undokumentierte Funktionen als "Hintertür" fungieren?			
Schlüsselbegriffe:	Hintertür, Sicherheit, Funktionen, Programme, Systeme, Entwickler, Anwendungen, Rechte, Backdoor, Software			
Zusatz:	Besitzt jedes Program undokumentierte Funktionen?			
	Werden undokumentierte Funktionen nach einiger Zeit erfasst?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.10 Nicht getrennte Verbindungen				
Verweis:	4.25 nicht getrennte Verbindungen (BSI) FTA_SSL (CC)			
Beschreibung:	Werden Verbindungen nicht automatisch getrennt, können für den Benutzer hohe Risiken entstehen.			
Implementierung:	Welche Verbindungen müssen getrennt werden? Wie trenne ich die Verbindung? Kann ich eine automatische Trennung einstellen? Welche Risiken bestehen bei einer aktiven Verbindung? Welche Attribute können für die automatische Trennung gewählt werden?			
Schlüsselbegriffe:	Verbindungen, Trennen, Benutzer, Daten, Kommunikation, Kosten, Protokoll, Sitzung, Software			
Zusatz:	Gibt es Verbindungen, die immer aufrechterhalten werden müssen? Sind gewisse Verbindungszeiten pflicht?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.11 Unzureichende oder fehlende Verbindungs-Sicherheitsmechanismen				
Verweis:	4.61 unzureichende oder fehlende WLAN-Sicherheitsmechanismen (BSI)			
	4.80 unzureichende oder fehlende Bluetooth-Sicherheitsme			
	FCS_CKM (CC)			
Beschreibung:	Um eine sichere Verbindung zu erstellen, müssen einige Sicherheitsmechanismen nachträglich aktiviert werden.			
Implementierung:	Welche Sicherheitsmechanismen sind eingesetzt?			
	Welcher Verbindungsmechanismus wird benutzt?			
	Was kann passieren, wenn ich die Vorkonfiguration beibehalte?			
	Ergeben sich Gefahren für alle gekoopelten Geräte?			
	Welche Einstellungen sollten nachträglich bearbeitet werden?			
Schlüsselbegriffe:	Verbindungen, Sicherheit, Benutzer, Daten, Kommunikation, Kryptographie, Verschlüsselung, WEP, SSID, Broadcast, Schlüssel, Access Point, Bluetooth			
Zusatz:	Welche Verschlüsselungsmethode ist für mein System geeignet?			
	Welche Schlüssellängen sollten benutzt werden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.12 Nichtzustellung einer Information				
Verweis:	4.32 Nichtzustellung einer Nachricht (BSI)			
	FCO_NRR (CC)			
Beschreibung:	Der Datenaustausch z.B. einer Datei/Nachricht ist meistens schnell und komfortabel, aber nicht immer zuverlässig und sicher.			
Implementierung:	Welche Übertragungsmöglichkeiten gibt es?			
	Welche Gründe existieren, dass z.B. eine Nachricht nicht ankommt?			
	Welche Hardware- oder Softwarefehler führen dazu?			
	Welche Folgen kann ein Nichtzustellen der Daten haben?			
	Was sagt die Meldung „Zustellung bestätigt" wirklich aus?			
Schlüsselbegriffe:	Verbindungen, Sicherheit, Benutzer, Daten, Kommunikation, EMail, SMS, Server, Dienst, Empfänger, Sender			
Zusatz:	Muss der Daten-Server immer online sein, um eine Datei zu erhalten?			
	Können Informationen im Hintergrund weitergeleitet werden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.13 Mangelnde Verlässigkeit von Groupware				
Verweis:	4.37 mangelnde Verlässigkeit von Groupware (BSI) FDP_UCT (CC)			
Beschreibung:	Groupware, wie z.B. Email-Programme, ersetzen immer mehr alltägliche Verfahrenweisen, die jedoch ohne die richtigen Sicherheitsmaßnahmen nicht ausreichend verlässlich sind.			
Implementierung:	Welche Groupware-Dienste werden eingesetzt?			
	Wie werden Daten zwischen Benutzern übertragen?			
	Welche Sicherheitsmaßnahmen sind voreingestellt?			
	Sind die Daten kryptographisch gesichert?			
	Wodurch wird die Authentizität gewährleistet?			
Schlüsselbegriffe:	Verbindungen, Sicherheit, Benutzer, Daten, Groupware, Nachrichten, Systeme, Vertraulichkeit, Authentizität, Software, Informationen			
Zusatz:	Was können Groupware-Dienste mit meinen Daten anstellen?			
	Kann es zu Ausfällen von Groupware-Diensten kommen?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.14 Unterlaufen von Zugriffskontrollen über ODBC				
Verweis:	4.27 Unterlaufen von Zugriffskontrollen über ODBC (BSI) FCO_NRO (CC)			
Beschreibung:	Es muss sichergestellt werden, dass nur Benutzer/Dienste, die die benötigten Rechte besitzen, die Datenbankschnittstellen zur Übertragung der Anweisungen des Anwendungsprogramms zur Datenbank und zurück, benutzen.			
Implementierung:	Welche Datenbankschnittstellen existieren? Welche Personen/Dienste können auf die Schnittstellen zugreifen? Wie sehen die Zugriffskontrollen aus? Kann eine Verknüpfung zu mehreren Datenbanken erstellt werden? Wie sind die Datenbankschnittstellen verschlüsselt?			
Schlüsselbegriffe:	Verbindungen, Sicherheit, Benutzer, Daten, Systeme, Software, Datenbank, ODBC, IDAPI, JDBC, Quelle, API, Programme, Kommunikation, Zugriff, Treiber			
Zusatz:	Wie wird kryptographisch zwischen D.bank und Anwendung kommuniziert? Was kann an den Daten manipuliert werden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.15 Verlust von Daten in einer Datenbank				
Verweis:	4.28 Verlust von Daten in einer Datenbank (BSI)			
	FRU_RSA (CC)			
Beschreibung:	Durch Datenmanipulation oder Zusammenbruch eines Systems, können Verluste von Daten entstehen, die verhindert werden müssen.			
Implementierung:	Wie kann es zum Verlust von Daten kommen?			
	Welche Speichermedien können als Datenbank benutzt werden?			
	Kann Anwendungen individueller Speicher zugesichert werden?			
	Was können die Konsequenzen vom Verlust der Daten sein?			
	Werden die Daten in Deutschland oder in der EU gehostet?			
Schlüsselbegriffe:	Benutzer, Daten, Systeme, Software, Datenbank, Programme, Anwendungen, Zusammenbruch, Speicher, Medien, Kapazität, Sicherheit			
Zusatz:	Kann erkannt werden, wodurch die Daten verloren gingen?			
	Kann eine Datenbanksicherung parallel auf mehreren Medien funktionieren?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.16 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services				
Verweis:	4.84 unzureichende Val. von Ein- und Aus.daten bei W.Anw. und W.Ser. (BSI)			
	FAU_SAA (CC)			
Beschreibung:	Eingabedaten die z.B. in Webanwendungen durchgeführt werden, laufen im allg. über Clients, sodass gegen die Manipulation und Modifikation des Clients entgegengewirkt werden muss.			
Implementierung:	Welche Clients werden eingesetzt?			
	Wie werden sichere Clients erkannt?			
	Wird ein Proxy eingesetzt?			
	Was können Angreifer mit den Daten anstellen?			
	Welche Angriffsmethoden werden von Angreifern öfters verwendet?			
Schlüsselbegriffe:	Benutzer, Daten,Programme, Anwendungen, Sicherheit, Validierung, Web, Service, Browser, SQL-Injection, Remote File Inclusion, Clickjacking, Angriff, Sanitizing,			
Zusatz:	Ist jeder Browser angreifbar?			
	Wie werden Eingabe- oder Ausgabeinformationen validiert?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.17 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen				
Verweis:	4.86 unzureichende Nachv. von sicherheitsrelevanten Ereig. Bei W.Anw. (BSI) FAU_STG (CC)			
Beschreibung:	Werden sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert, können diese zu einem späteren Zeitpunkt nicht nachvollzogen und die Ursache nicht mehr ermittelt werden.			
Implementierung:	Wie werden Ereignisse protokolliert?			
	Werden Angriffe/Fehler direkt bemerkt?			
	Kann die Integrität der Protokollierung gewährleistet werden?			
	Wann ist eine schlechte Protokollierung zu erwarten?			
	Werden alle Aktivitäten protokolliert?			
Schlüsselbegriffe:	Benutzer, Daten,Programme, Anwendungen, Sicherheit, Validierung, Web, Service, Browser, SQL-Injection, Remote File Inclusion, Clickjacking, Angriff, Sanitizing,			
Zusatz:	Können auch bei schlechter Protokollierung Vorfälle nachvollzogen werden?			
	Was wird alles in einem Protokoll protokolliert?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.18 Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services					
Verweis:	4.87 Off. vertr. Informationen bei Webanw. und Web-Services (BSI) FPR_ANO (CC)				
Beschreibung:	Unnötig offengelegte Informationen, die durch Webseiten und Web-Services verteilt werden, könnten Angreifern Hinweise geben, wie Angriffe auf ein System funktioneren.				
Implementierung:	Was sind vertrauliche Informationen?				
	Welche Informationen müssen/dürfen offengelegt werden?				
	Mit welchen Informationen können Angreifer am meisten anfangen?				
	Wie kann die Integrität der Dokumente sichergestellt werden?				
	Sind alle Schnittstellen mögliche Angriffspunkte?				
Schlüsselbegriffe:	Benutzer, Daten,Programme, Anwendungen, Sicherheit, Web, Service, Browser, Angriff, PIN, HTML, WSDL, UDDI, HTTP, Informationen				
Zusatz:	Wer prüft die Daten, die offengelegt werden müssen?				
	Was können die Konsequenzen durch einen solchen Angriff sein?				
Objekte:					
Ausprägung:	Gering	Basis	Mittel	Stark	
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)	
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos		
	Eingeschränkt nutzbar		Nicht spürbar		
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch		

Nr.19 Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung				
Verweis:	4.89 Fehl. od. unzureich. Alarmierungskonzept bei der Prot. (BSI) FAU_SAA (CC)			
Beschreibung:	IT-Frühwarnsysteme werden eingesetzt, um bereits während eines Sicherheitsvorfalls zu warnen, noch bevor mögliche Auswirkungen spürbar sind.			
Implementierung:	Wird ein Frühwarnsystem bereits verwendet?			
	Welche Auswirkungen können frühzeitig verhindert werden?			
	Welche Alarmierungskomponenete wird verwendet?			
	Welche Grenzwerte werden benutzt?			
	Wird eine White-, Blacklist verwendet?			
Schlüsselbegriffe:	Benutzer, Daten, Anwendungen, Sicherheit, Angriff, Whitelist, False-Positives, False-Negatives, Monitoring, System, Gefährdung, Alarm			
Zusatz:	Welche Reaktionen werden auf Sicherheitsvorfälle durchgeführt?			
	Was kann durch einen Angriff mit Hilfe der Whitelist passieren?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.20 Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen				
Verweis:	4.99 Fehl. od. unzureich. Sicherheitsmechanismen in Anwendungen (BSI)			
	FMT_MSA (CC)			
Beschreibung:	Es kann vorkommen, dass Sicherheitsmechanismen in Anwendungen schlecht konzepiert, implementiert oder unzuverlässig sind, sodass häufig nach der Erst-Installation nachkonfiguriert werden muss.			
Implementierung:	Welche Anwendungen werden benutzt?			
	Ist jede Anwendung eine Gefahr?			
	Welche Sicherheitsfunktionalitäten werden gebraucht?			
	Werden die Daten verschlüsselt?			
	Wird eine Benutzertrennung vorgenommen?			
Schlüsselbegriffe:	Benutzer, Daten, Anwendungen, Sicherheit, Angriff, System, Gefährdung, Datenbank, Protokoll, Benutzertrennung, Authentikation, Kryptographie,			
Zusatz:	Gibt es Protokollierungsmöglichkeiten?			
	Existiert eine Datenbankanbindung?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.21 Unerlaubte Ausübung von Rechten				
Verweis:	2.7 unerlaubte Ausübung von Rechten (BSI)			
	FMT_SMR (CC)			
Beschreibung:	Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahme eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen.			
Implementierung:	Wer besitzt Zuritts-, Zugangs- und Zugriffsrechte?			
	Wird die Integrität der Rechte geschützt?			
	Wie werden Rechte verteilt?			
	Werden Authentikationsmöglichkeiten (z.B. Passwort) regel. aktualisiert?			
	Auf welchem Datenträger werden die Rechte gesichert?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Management, Prozess, Informationen, Verantwortung, Schutz, Administration, Kryptographie, Daten, Berechtigung, Rechte			
Zusatz:	Wird der Datenträger verschlüsselt?			
	Kann der Datenträger manipuliert oder entwendet werden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.22 Unzureichende Kontrolle der Sicherheitsmaßnahmen				
Verweis:	2.4 unzureichende Kontrolle der Sicherheitsmaßnahmen (BSI)			
	FPT_TST (CC)			
Beschreibung:	Werden Sicherheitsmaßnahmen nicht konsequent umgesetzt und regelmäßig kontrolliert, kann es sein, dass sie nicht mehr wirksam sind oder missachtet werden.			
Implementierung:	Welche Sicherheitsmaßnahmen werden eingesetzt?			
	Werden die Sicherheitsmaßnahmen regelmäßig aktualisiert?			
	Werden Aktualisierungen oder Verstöße protokolliert?			
	Welche Protokollierungsfunktionen sind im Betrieb?			
	Kontrolliert jeder Verantwortlicher seinen Teil selber?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Management, Prozess, Informationen, Verantwortung, Schutz, Berechtigung, Protokoll, Zugriff			
Zusatz:	Werden die Sicherheitsrichtlinien regelmäßig aktualisiert?			
	Kommt es zu einer externen Kommunikation?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.23 Unzureichendes Schlüsselmanagement bei Verschlüsselung				
Verweis:	2.19 unzureichendes Schlüsselmanagement bei Verschlüsselung (BSI) FCS_CKM (CC)			
Beschreibung:	Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden.			
Implementierung:	Wo werden die kryptographischen Schlüssel aufbewahrt? Wie werden die Schlüssel erzeugt? Wie kommt der Schlüssel zum Kommunikationspartner? Wie wird der Schlüssel verschlüsselt? Werden die Schlüssel regelmäßig aktualisiert?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, Kryptographie, Verschlüsselung, Entschlüsselung, DES, AES, Schlüssel, Key, Management, Daten			
Zusatz:	Welche Schlüssellängen werden verwendet? Wie wird mit verlorenen/vergessenen Schlüssel umgegangen?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.24 Fehlende oder unzureichende Auswertung von Protokolldaten				
Verweis:	2.22 fehl. oder unzu. Auswertung von Protokolldaten (BSI)			
	FPT_SSP (CC)			
Beschreibung:	Eine Auswertung aller Protokolldaten ist notwendig, um beispielsweise Fehleranalysen durchführen und erfolgte Angriffe indentifizieren zu können.			
Implementierung:	Welche Ereignisse werden protokolliert?			
	Wieviele Protokolle werden benutzt?			
	Wofür werden die Protokolle verwendet (Schutz oder Performance)?			
	Werden die Protokolle regelmäßig ausgewertet?			
	Findet eine zentrale Protokollierung statt?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, Management, Daten, Protokoll, System, Datenbank, Ereignis, Konzept			
Zusatz:	Auf welchem Datenträger werden die Protokolle gesichert?			
	Werden Filtereinstellungen genutzt?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.25 Analyse des Nachrichtenflusses				
Verweis:	5.26 Analyse des Nachrichtenflusses (BSI) FDP_IFC (CC)			
Beschreibung:	Über eine Verkehrsflussanalyse versucht ein Angreifer Auskunft darüber zu erhalten, wer wann welche Datenmengen an wen gesendet hat und wie oft.			
Implementierung:	Wie oft werden Datenmengen versendet?			
	Kann auf Uhrzeit und Datum rückgeschlossen werden?			
	Wird die Integrität der Quelle (z.B. Email-Adresse) geschützt?			
	Welche Kommunikationsverbindung wird benutzt?			
	Wie werden die Informationen verarbeitet?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, Management, Daten, Protokoll, System, Datenbank, Ereignis, Konzept			
Zusatz:	Werden regelmäßig Sicherheitschecks durchgeführt?			
	Wer könnte an den Informationen Interesse besitzen?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.26 Fehlerhafte Administration von Zugangs- und Zugriffsrechten				
Verweis:	3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten (BSI) FMT_SMR (CC)			
Beschreibung:	Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind.			
Implementierung:	Wer besitzt welche Rechte?			
	Wie werden die Rechte vergeben?			
	Ist die Integrität der Rechte gewährleistet?			
	Wo befinden sich die Rechtezuweisungen?			
	Ist die Datenbank kryptographisch gesichert?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, Management, Daten, Protokoll, System, Datenbank, Kryptographie, Rechte, Anwendungen			
Zusatz:	Wer kann auf die Protokolldaten zugreifen?			
	Kann die Rechtevergabe nachvollzogen werden (Quelle) ?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.27 Unberechtigte IT-Nutzung				
Verweis:	5.9 unberechtigte IT-Nutzung (BSI)			
	FIA_UAU (CC)			
Beschreibung:	Die Identifikation und Authentifikation von Benutzern soll verhindern, dass Informationstechnik unberechtigt benutzt wird.			
Implementierung:	Wie werden Benutzer identifiziert?			
	Wie werden Benutzer authentifiziert?			
	Wie werden die Daten gesichert?			
	Auf welchen Datenträger befinden sich die Daten?			
	Ist bei der Identifizierung die Integrität des Benutzers gesichert?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, System, Kryptographie, Anwendungen, Authentisierung, Identifikation			
Zusatz:	Wie oft werden die Sicherheitsmaßnahmen aktualisiert?			
	Welche Sicherheitsanwendungen besitzt das System?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.28 Manipulation an Informationen oder Software				
Verweis:	5.2 Manipulation an Informationen oder Software (BSI)			
	FMT_SMR (CC)			
Beschreibung:	Durch die Manipulation von Informationen oder Software kann der reibungslose Ablauf von Geschäftsprozessen nicht mehr gewährleistet werden.			
Implementierung:	Welche Software wird benutzt?			
	Welche Informationen können manipuliert werden?			
	Was sind die möglichen Folgen der Manipulation?			
	Wer hat Zugriffsrechte auf die Daten?			
	Wo bestehen Zugriffsmöglichkeiten?			
Schlüsselbegriffe:	Benutzer, Sicherheit, Schutz, System, Anwendungen, Software, Informationen, Manipulation, Zugriff, Rechte, Daten			
Zusatz:	Welche Informationen sollten besonders geschützt werden?			
	Wie werden die Daten erfasst?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.29 Software mit unerlaubten Zugriff				
Verweis:	3.105 ungenehmigte Nutzung von externen Dienstleistungen (BSI) FCO_NRO (CC)			
Beschreibung:	Bei einer dienstlichen Nutzung, kann es zu Problemen kommen, da häufig andere Rahmenbedingungen als bei privater gelten.			
Implementierung:	Welche Dienstleistungen werden ausgeführt?			
	Sind die Genehmigungsverfahren bekannt?			
	Sind die Dienstleistungen vertraglich geregelt?			
	Werden die Sicherheitsvorgaben eingehalten?			
	Wer hat das Recht Dienstleistungen in Anspruch zu nehmen?			
Schlüsselbegriffe:	Benutzer, Schutz, System, Informationen, Zugriff, Daten, Dienstleistung, Extern, Management, Sicherheit, Dritte			
Zusatz:	Werden die Dienstleistungen regelmäßig überprüft?			
	Welche Risiken bestehen durch den unerlaubten Zugriff?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.30 Vertraulichkeitsverlust schützenwerter Informationen				
Verweis:	5.71 Vertraulichkeitsverlust schützenswerter Informationen (BSI)			
	FPR_ANO (CC)			
Beschreibung:	Für Informationen, die einen Schutzbedarf bezüglich ihrer Vertraulichkeit besitzen, besteht die Gefahr, dass die Vertraulichkeit durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlung beeinträchtigt wird.			
Implementierung:	Wie werden die Daten gesichert?			
	Wo werden die Daten gesichert?			
	Werden die Daten weitergegeben?			
	Wie werden die Daten übertragen?			
	Wie werden die Informationen ausgelesen?			
Schlüsselbegriffe:	Benutzer, Schutz, Informationen, Zugriff, Daten, Sicherheit, Vertraulichkeit, Integrität, Rechte			
Zusatz:	Wann kann ein Angreifer die Informationen abfangen?			
	Welche Informationen benötigen einen Schutzbedarf?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.31 Weitergabe von Daten an Dritte				
Verweis:	5.107 Weitergabe von Daten an D. durch den Outsourcing-Dienstl. (BSI FPR_PSE (CC)			
Beschreibung:	Die Weitergabe von Informationen oder Daten wird meistens durch Dritte veranlasst, die sich um die Integrität und Sicherung der Daten kümmern müssen.			
Implementierung:	Welche Outsourcing-Partner werden eingesetzt?			
	Welche Informationen/Daten werden übermittelt?			
	Wie werden die Daten beim Outsourcing-Partner gespeichert?			
	Wird die Integrität gewährleistet?			
	Wie lange werden die Daten beim Outsourcing-Partner gespeichert?			
Schlüsselbegriffe:	Benutzer, Schutz, Informationen, Zugriff, Daten, Sicherheit, Vertraulichkeit, Integrität, Dritte, Anbieter, Outsourcing, Dienstleister, Verantwortung			
Zusatz:	Wann kann ein Angreifer die Informationen abfangen?			
	Welche Informationen benötigen einen Schutzbedarf?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.32 Kompromittierung kryptographischer Schlüssel				
Verweis:	5.83 Kompromittierung kryptographischer Schlüssel (BSI)			
	FCS_CKM (CC)			
Beschreibung:	Beim Einsatz kryptographischer Verfahren hängt der Sicherheitszugewinn entscheidend davon ab, wie vertraulich die verwendeten geheimen kryptographischen Schlüssel bleiben.			
Implementierung:	Welches kryptographische Verfahren wird angewandt?			
	Wie wird der Schlüssel erzeugt?			
	Werden die Kryptomodule auch geschützt?			
	Ist ein Brute-Force-Angriff möglich?			
	Wie groß ist die Schlüssellänge?			
Schlüsselbegriffe:	Benutzer, Schutz, Informationen, Sicherheit, Schlüssel, Key, Generator, Kryptographie, DES, AES, Brute-Force, Module			
Zusatz:	Ist das Gesamtsystem direkt in Gefahr?			
	Wie oft wird der Schlüssel aktualisiert?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.33 Unberechtigtes Überschreiben oder Löschen von Archivmedien				
Verweis:	5.106 unberechtigtes Überschreiben oder Löschen von Archivmedien (BSI)			
	FDP_ACF (CC)			
Beschreibung:	Auf Archivmedien werden Daten langfristig und unverändert gespeichert, daher soll unberechtigtes Löschen oder Überschreiben verhindert werden.			
Implementierung:	Auf welchem Medium befinden sich die Daten?			
	Welche Benutzer haben das Recht die Daten zu bearbeiten?			
	Werden wiederbeschreibbare Medien benutzt?			
	In welchem Abständen werden die Archive gelöscht?			
	Kann ein Backup der Archive erstellt werden?			
Schlüsselbegriffe:	Benutzer, Schutz, Informationen, Sicherheit, Schlüssel, Key, Daten, WORM, Medien, Archiv, Rechte, Backup			
Zusatz:	Was kann ein Angreifer mit den Archiven anfangen?			
	Kann das Bearbeiten der D. mit einem Schlüssel geschützt werden?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

Nr.34 Vertraulichkeitsverlust durch Auslagerungsdateien				
Verweis:	5.146 Vertraulichkeitsverlust durch Auslagerungsdateien (BSI)			
	FDP_RIP (CC)			
Beschreibung:	Nach dem Abmelden des Benutzers vom System bleiben die Auslagerungsdateien mit den Informationen, die der Benutzer während seiner Arbeit verrichtet hat, erhalten, sodass der Schutz dort gewährleistet werden muss.			
Implementierung:	Welche Prozesse werden von Benutzern benutzt?			
	Welche Auslagerungsdateien werden von Benutzerprozessen erstellt?			
	Wo finde ich die Auslagerungsdateien?			
	Kann ich die Auslagerungsdateien löschen?			
	Welche Informationen befinden sich in der Auslagerungsdatei?			
Schlüsselbegriffe:	Benutzer, Informationen, Daten, Medien, Prozesse, Datei, Auslagerungsdateien, Vertraulichkeit, Swap, Speicher, Schutz, Festplatte, Anwendungen			
Zusatz:	Ist das automatische Löschen der Auslagerungsdateien aktiviert?			
	Kann ich den Speicher für Auslagerungsdateien begrenzen?			
Objekte:				
Ausprägung:	Gering	Basis	Mittel	Stark
Angreiferklasse:	Anwender	Fachspezialist	Professioneller	Insider (intern)
Usability:	Service/Gerät funktionslos		Service oder Gerät funktionslos	
	Eingeschränkt nutzbar		Nicht spürbar	
Kompromittierung sensibler Daten:	Gefährdend	Möglich	Unkritisch	

9.13 Anhang: Beispielsystem 1 (NFC Funktion)

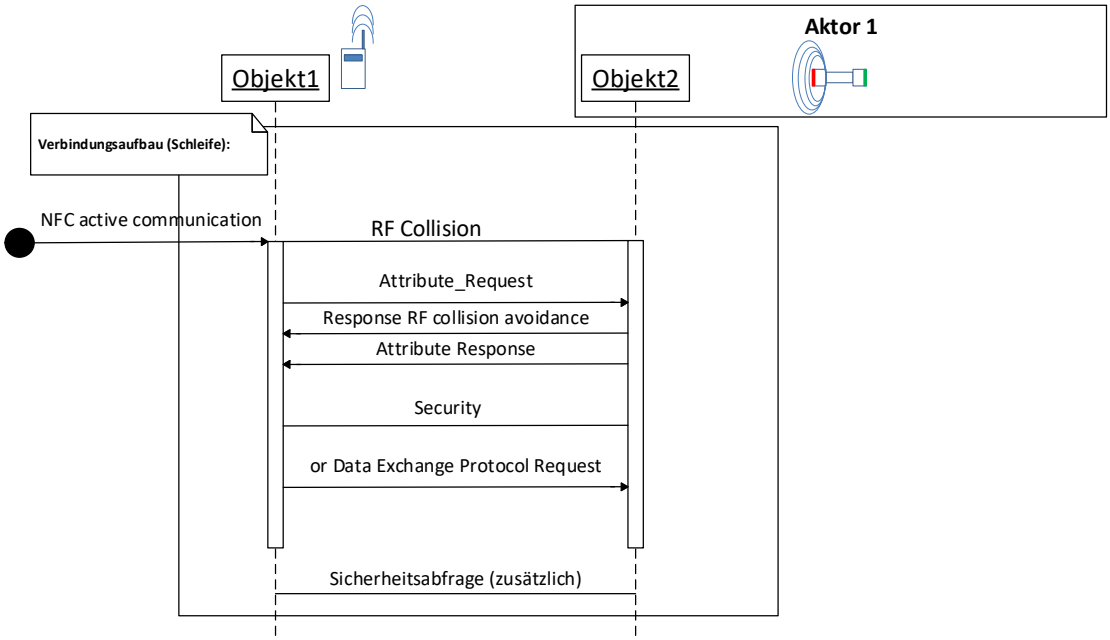


Abbildung 37: Evaluationssystem 1 (NFC)[254]

[254] Eigene Darstellung.

9.14 Anhang: Beispielsystem 2 (BLE)

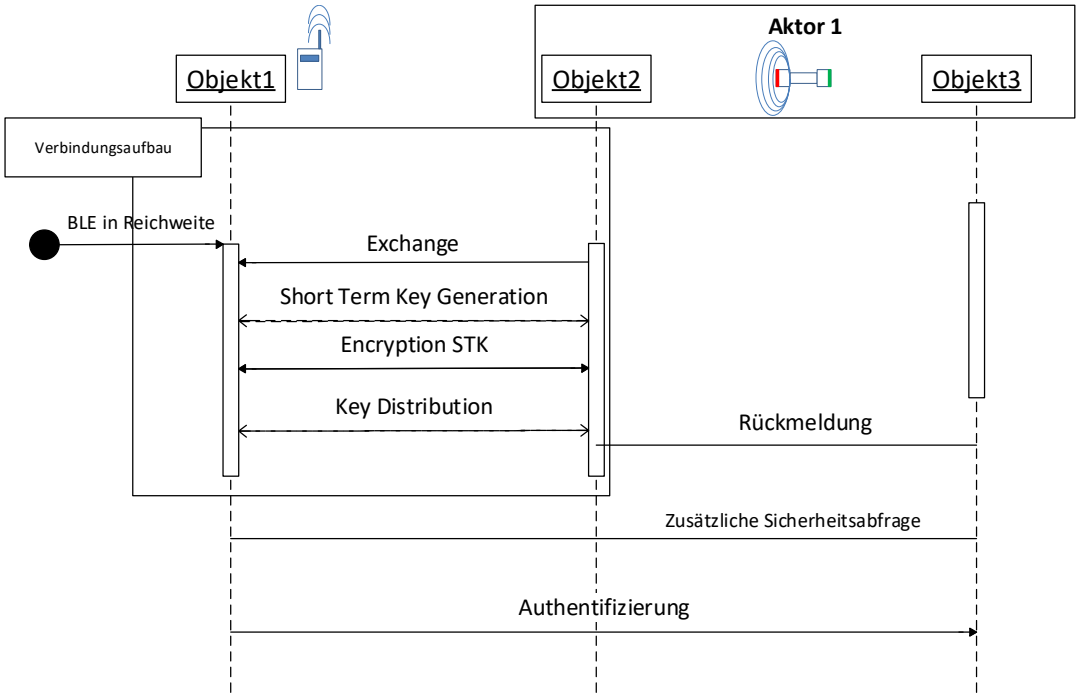


Abbildung 38: Evaluationssystem 2 (BLE)[255]

[255] Eigene Darstellung.

9.15 Anhang: Terminologie Beispielsystem 1

mobile App: App auf dem Smartphone

Trust Service: Data Center / Backend

Lock: Schließzylinder mit NFC-Funktionalität

Owner: Person mit administrativen Rechte

User: Person nur mit ausführenden Rechten

Unlock: Berechtigung zum Verschließen der Tür

Lock: Berechtigung zum Öffnen der Tür

Log in: Anmelden per Digital ID an jedem Smartphone

Manage Locks: Verwaltung / Administration der Berechtigungen / Personen

New access (person): Hinzufügen und Entziehen von Berechtigungen

Revoke access (person): Hinzufügen und Entziehen von Berechtigungen

Check & sync lock-specific information: Aufzeichnen und Abrufen von Aktionen (mit Zeitsignatur)

Key refresh: Updaten der Berechtigungen im Hintergrund

Limited validity (key): Limitierte Zugangsberechtigung

Keyfobs: Mobile NFC Transponder

Reading/edit cards: Verwalten von RFID Karten

9.16 Anhang: Terminologie Beispielsystem 2

Acces App: App auf dem Smartphone

Cloud: Cloud Dienst für den Betrieb und Verwaltung

Mechatronikzylinder: Motorisiertes Türschloss mit BLE-Funktionalität

Besitzer: Person mit administrativen Rechten

Benutzer: Person nur mit ausführenden Rechte

Tür verschließen: Berechtigung zum Verschließen der Tür

Tür öffnen: Berechtigung zum Öffnen der Tür

Registrierung: Erstmalige Registrierung zum Anmelden eines Administrators (Simplex Plattform, übliches Benutzerkonto)

Initialisierung: Schlüsselvergabe bzw. Berechtigung muss vom Besitzer kommen

Schlüssel-/Schlossverwaltung: Verwalten der Berechtigungen und Administrieren der Schlüssel-/Schlösser

Schlüsselvergabe: Hinzufügen und Entziehen von Berechtigungen

Protokollierung: Aufzeichnen und Abrufen der Schlossbetätigungen (mit Zeitsignatur)

Synchronisieren: Updaten der Daten/Änderungen im Hintergrund

Aktivierungs-Code: Hinzufügen weiterer (kostenpflichtiger) Schließberechtigungen

Fernbedienung: Handsender mit drei freiwählbaren Tastenfunktionen: Öffnen und Schließen. Zusätzlich zwei Sonderfunktionen: Privatsphäre und Blockieren.

Öffnen/Privatshäre: Öffnen der Tür mit evtl. Zeitfenster

Schließen/Blockieren: Schließen der Tür mit evtl. Blockierungsfunktion

Schlüssel hinzufügen: Schlüssel werden per Code „händisch" hinzugefügt

Meine Schlüssel: Übersicht gegenwärtiger Berechtigungen

9.17 Anhang: Annahmen Beispielsystem 1

Bezug	Technisch	Organisatorisch	Personell
Direkt	Anbringung vor Ort an der Tür, Gesamtsystem muss mitbetrachtet werden	Sach- & funktionsgerechte Tür	Schulung der Benutzer
	Gelegentliche Internetverbindung des Smartphones gewährleisten	Sicherer Umgang mit der Technologie (wer hat welche Berechtigung und Zugang?)	Unterwiesene Installateure / Errichter
	Gewährleistung einer ordentlichen Spannungsquelle (Batterien)	Regelmäßige Überprüfung der Technik (Smartphone & Zylinder)	Nötige Akzeptanz
	Bekannte Technologie NFC	Errichter übergibt die Anlage	Ansprechpartner vor Ort
	Aktuelles Betriebssystem	Im Notfall Zutritt über herkömmlichen Schlüsseldienst	
	Gegenwärtige Zertifizierung des mechatronischen Zylinders beachten		
	Updates nicht blockieren		
	Battery-off Funktion nur bei NFC		
Indirekt	Sichert persönlichsten Bereich ab	Branchenüblicher Anbieter, seriöser Partner (Updates, etc.)	Technisches Grundverständnis aller Beteiligten
	Neues Produkt, bekannter Produktbereich	Unterwiesene Partner bzw. Benutzer	Schlüssel & Smartphone achtsam benutzen
		Vertrauensvoller Umgang (u.a. Keyfobs)	Gefahrenpotenzial aufgrund der Viktimisierungsängste

Tabelle 33: Annahmen Beispielsystem 1[256]

[256] Eigene Darstellung.

9.18 Anhang: Annahmen Beispielsystem 2

Bezug	Technisch	Organisatorisch	Personell
Direkt	Anbringung vor Ort an der Tür, Gesamtsystem muss mitbetrachtet werden	Sach- & funktionsgerechte Tür	Ggf. Schulung der Pflegeperson
	Internetverbindung des Smartphones gewährleisten	Demontage des Schlüsseltresors (Schlüssel aus dem Verkehr nehmen)	Unterwiesene Installateure / Pflegekräfte
	Ordentliche, sachgerechte Stromversorgung des Zylinders	Regelmäßige Überprüfung der Technik (Smartphone & Zylinder)	Angehörige unterweisen / schulen
	Bekannte Technologie (BLE)	Errichter übergibt die Anlage	Ansprechpartner vor Ort
	Aktuelles Betriebssystem	Im Notfall Zutritt über herkömmlichen Schlüsseldienst	
	Liste der SKG eingesetzten Varianten beachten (bei hohem Sicherheitsbedürfnis)		
	Updates nicht blockieren		
	Smartphone als Gateway		
Indirekt	Sichert persönlichsten Bereich ab	Branchenüblicher Anbieter, seriöser Partner (Updates, etc.)	Technisches Grundverständnis aller Beteiligten
	Pflegeeinsatz (ältere Leute), Heimbereich, begrenzt professioneller Umfang	Unterwiesene Partner bzw. Pflegedienste	Schlüssel & Smartphone achtsam benutzen
	Neues Produkt, bekannter Produktbereich	Vertrauensvoller Pflegedienst	Gefahrenpotenzial aufgrund der Viktimisierungsängste

Tabelle 34: Annahmen Beispielsystem 2[257]

[257] Eigene Darstellung.

9.19 Anhang: Anwendungsfalldiagramme Beispielsystem 1

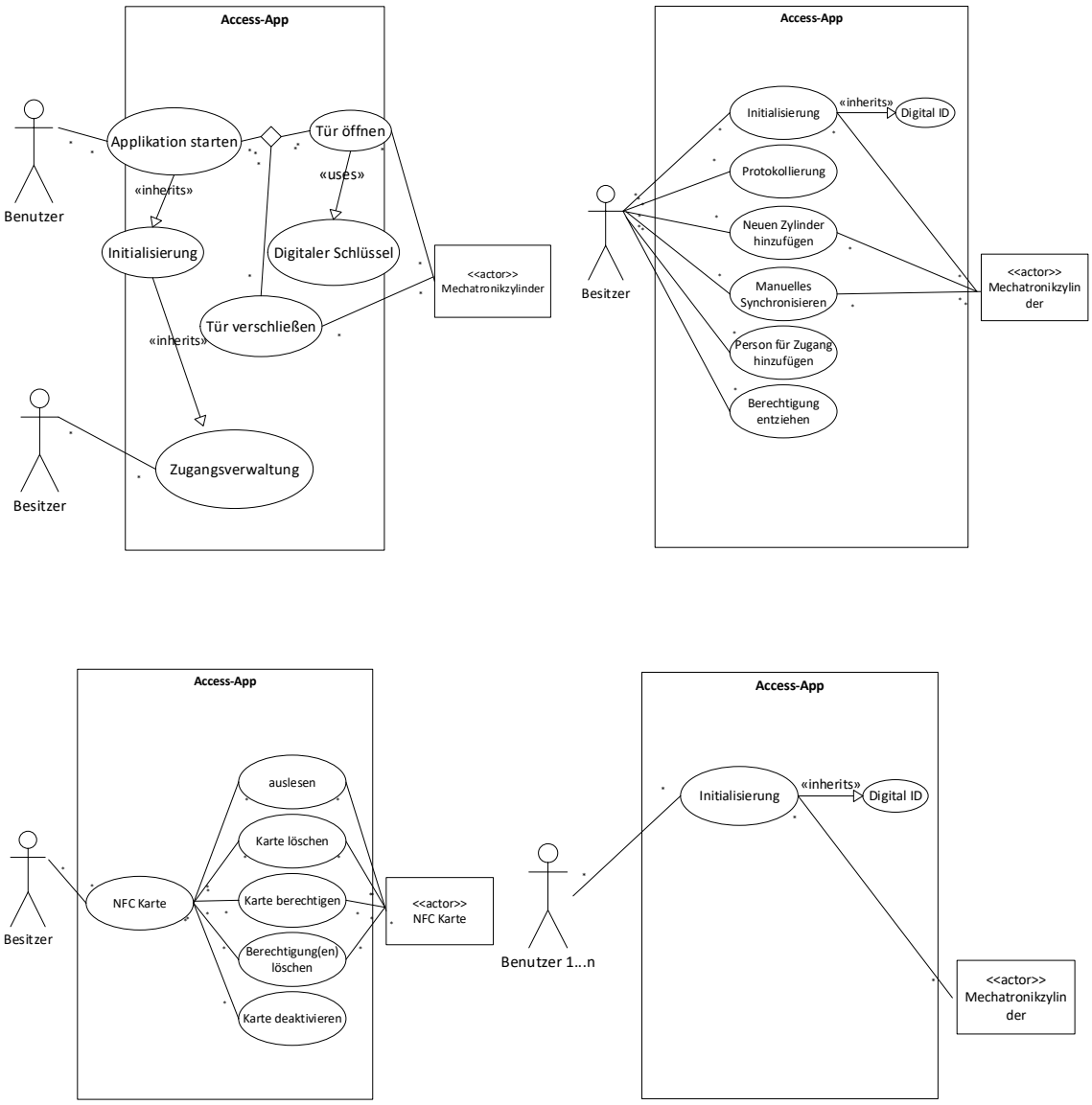


Abbildung 39: Anwendungsfalldiagramme Beispielsystem 1[258]

[258] Eigene Darstellung.

9.20 Anhang: Anwendungsfalldiagramme Beispielsystem 2

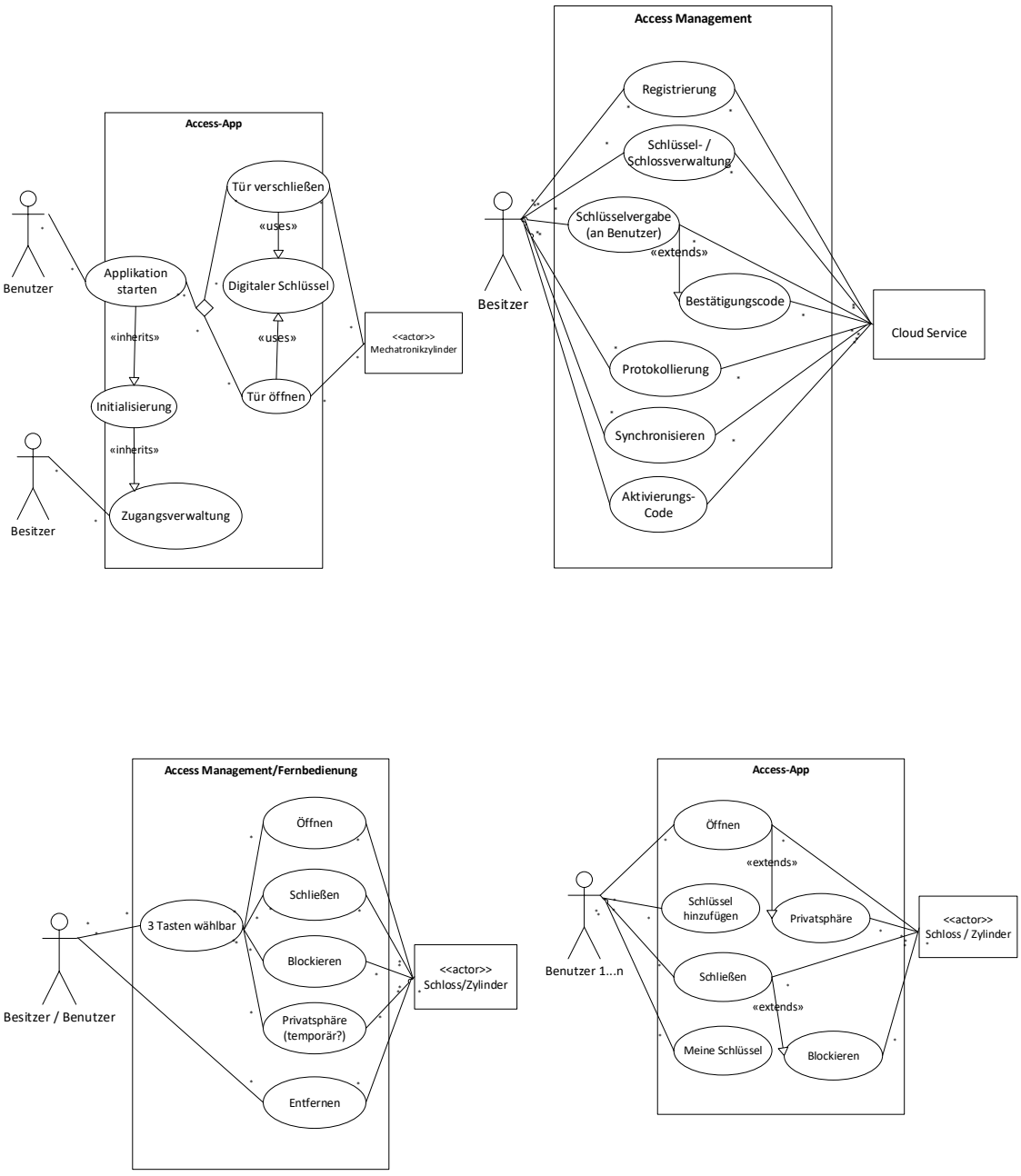


Abbildung 40: Anwendungsfalldiagramme Beispielsystem 2[259]

[259] Eigene Darstellung.

9.21 Anhang: Sequenzdiagramm Beispielsystem 1

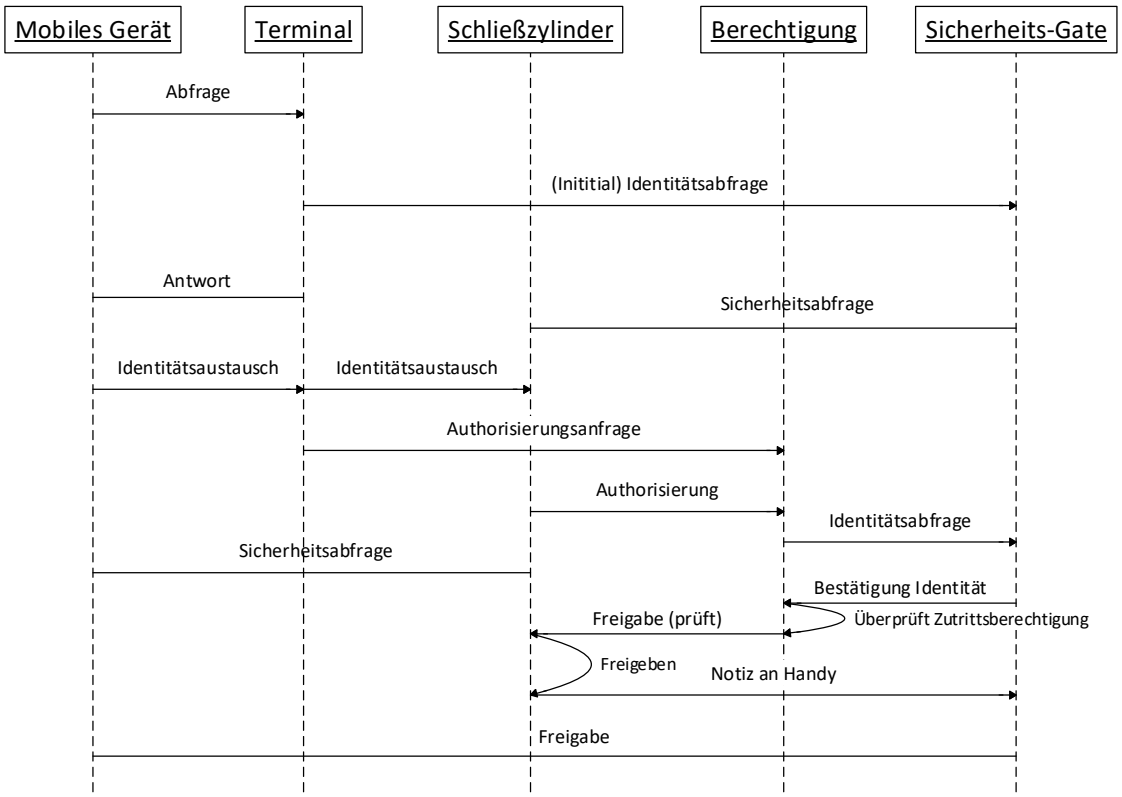


Abbildung 41: Sequenzdiagramm Beispielsystem 1[260]

[260] Eigene Darstellung.

9.22 Anhang: Sequenzdiagramm Beispielsystem 2

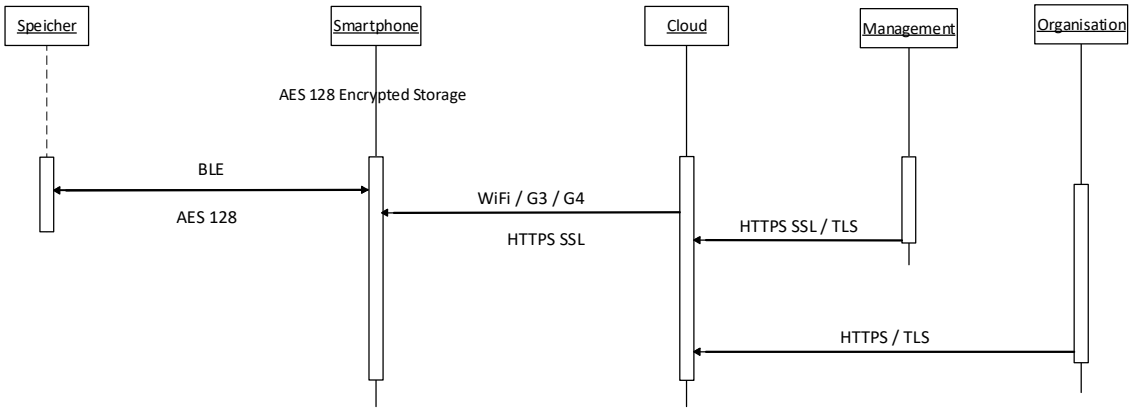


Abbildung 42: Sequenzdiagramm Beispielsystem 2[261]

[261] Eigene Darstellung.

9.23 Anhang: Sicherheitsprofil Beispielsystem 1

Die Aufstellung des Sicherheitsprofils stellt eine grundlegende Referenz der produktspezifischen Merkmale dar, d.h. alle artverwandten Systeme mit gleicher Ausprägung fallen in dieses Profil. Die Maßgabe der einzelnen Kriterien innerhalb des Sicherheitsprofils sind durch die Beschreibung und Darstellung etablierter und öffentlicher Standards zu belegen. Eine sinnvolle Eingruppierung innerhalb der Kriterien sollte einen objektiven Rahmen, der im Umfeld auftretenden Annahmen, berücksichtigen.

Als Orientierung für die durchzuführenden Sicherheitsbewertung sind die Kriterien: Ausprägung, Angreiferklassen, Usability und Kompromittierung sensibler Daten aufgestellt worden.

Begründung des Sicherheitsprofils:"

"Die Zusammenstellung des theoretischen Sicherheitsprofils ist in erheblichen Masse von den Annahmen abhängig und stellt damit den Rahmen für ein sinnvolles Sicherheitsziel. Durch den jeweiligen direkten oder indirekten Bezug von technischen, organisatorischen und personellen Annahmen lassen sich konkrete Kriterien des Sicherheitsprofils bestimmen.

Eine abschließende Bewertung findet immer unter Beachtung der aufgestellten Referenz vom theoretischen Sicherheitsprofil statt. Dies bedeutet, dass auch im besten Fall, eines deckungsgleichen Ergebnisses vom theoretischen und praktischen Sicherheitsprofils, nicht von einer absoluten Sicherheit ausgegangen werden kann. Es wird lediglich die Referenzierung zum theoretischen Sicherheitsprofil bestätigt.

Die Ausprägung des theoretischen (zu erreichenden) Sicherheitsprofils ist, wie folgt angegeben:"

Angreiferklasse:	Anwender (2)
Kompromittierung sensibler Daten:	Gefährdend (2)
Usability:	Service oder Gerät funktionslos (3)
Ausprägung:	Basis (3)

Mechanische Voraussetzung:

DIN 15684:2013-01 (2)

Gebrauchskategorie (1)	1
Dauerhaftigkeit (2)	6
Feuer-/Rauchwiderstand (3)	B
Umweltbeständigkeit (4)	4
Mechanische Verschlusssicherheit (5)	A
Elektronische Verschlusssicherheit (6)	F
Systemmanagement (7)	3
Angriffswiderstand (8)	2

Für weitere Erklärungen sind die Kriterienausprägungen heranzuziehen!

Zusatz:

Bei abweichenden mechanischen Voraussetzungen im Ausland sind hier die angegebenen Deutschen Normen als Referenz zu sehen.

9.24 Anhang: Sicherheitsprofil Beispielsystem 2

"Die Aufstellung des Sicherheitsprofils stellt eine grundlegende Referenz der produktspezifischen Merkmale dar, d.h. alle artverwandten Systeme mit gleicher Ausprägung fallen in dieses Profil. Die Maßgabe der einzelnen Kriterien innerhalb des Sicherheitsprofils sind durch die Beschreibung und Darstellung etablierter und öffentlicher Standards zu belegen. Eine sinnvolle Eingruppierung innerhalb der Kriterien sollte einen objektiven Rahmen, der im Umfeld auftretenden Annahmen, berücksichtigen.

Als Orientierung für die durchzuführenden Sicherheitsbewertung sind die Kriterien: Ausprägung, Angreiferklassen, Usability und Kompromittierung sensibler Daten aufgestellt worden.

Begründung des Sicherheitsprofils:"

"Die Zusammenstellung des theoretischen Sicherheitsprofils ist in erheblichen Masse von den Annahmen abhängig und stellt damit den Rahmen für ein sinnvolles Sicherheitsziel. Durch den jeweiligen direkten oder indirekten Bezug von technischen, organisatorischen und personellen Annahmen lassen sich konkrete Kriterien des Sicherheitsprofils bestimmen.

Eine abschließende Bewertung findet immer unter Beachtung der aufgestellten Referenz vom theoretischen Sicherheitsprofil statt. Dies bedeutet, dass auch im besten Fall, eines deckungsgleichen Ergebnisses vom theoretischen und praktischen Sicherheitsprofils, nicht von einer absoluten Sicherheit ausgegangen werden kann. Es wird lediglich die Referenzierung zum theoretischen Sicherheitsprofil bestätigt.

Die Ausprägung des theoretischen (zu erreichenden) Sicherheitsprofils ist, wie folgt angegeben:"

Angreiferklasse:	Anwender (2)
Kompromittierung sensibler Daten:	Gefährdend (2)
Usability:	Service oder Gerät funktionslos (3)
Ausprägung:	Basis (3)

Mechanische Voraussetzung:

DIN 18252 Klasse 82 (BZ)

Für weitere Erklärungen sind die Kriterienausprägungen heranzuziehen!

Zusatz:

Bei abweichenden mechanischen Voraussetzungen im Ausland sind hier die angegebenen Deutschen Normen als Referenz zu sehen.

9.25 Anhang: Assets Beispielsystem 1

Assets - kritische Elemente mechanisch - sekundär			
System	Bearbeiter	Datum	
Beispielsystem 1	*Arne Schwerdtfeger*	*2017*	
Kritisches Element	Status	Verantwortlicher / Leitung	
Außenknauf	*Hauptsächliche Analyse*	*Eigenverantwortliche Leitung*	
Funktion	Anmerkung	Ergebnis	
Leseeinheit / Außenbereich		*Teilergebnis 1*	

	Modus operandi	Beschreibung	Direkte Auswirkung	Asset	Gegenmaßnahme
Nr.					
Zerstörend					
01	Knauf abschlagen/treten	Knauf wird im Außenbereich abgeschlagen oder abgetreten, so dass die Sperreinheit frei liegt.	Zylinder kann von außen geöffnet werden, indem Gegenstände eingeführt werden.	Direkter Zugang Privatsphäre.	Sperreinheit liegt nicht frei und ist abgeschirmt.
02	Knauf abschlagen	Knauf wird im Außenbreich abgeschlagen oder abgetreten, so dass die Kontakte frei liegen.	Zylinder kann von außen bestromt werden.	Direkter Zugang Privatsphäre.	Bestromung ergebnislos.
03	Zylinder aufbohren	Zylinder wird auf der Außenseite aufgebohrt.	Sperreinheit liegt frei.	Direkter Zugang Privatsphäre.	Bohrschutz
04	Zylinder fluten	Zylinder mit einer Flüssigkeit fluten und anschließend Spannung anlegen oder runterkühlen.	Sperreinheit zum Öffnen bewegen oder die diffuse Spannung nutzen.	Direkter Zugang Privatsphäre.	Abdichten
Zerstörfrei					
05	Stigmatisierung	Andersartiger Türzylinder.	Weckt interesse an einem Einbruch	Einbruchgefahr / Eingriff Privatshäre.	Konstruktionsänderung.
06	Angriff mit Magnet	Runder Magnet wird auf den Knauf gesetzt und in Rotation versetzt. Das magnetische Feld betätigt die interne Kupplung.	Interne Kupplung/Verriegelungsmechanismus stellt Formschluss her. Zylinder lässt sich betätigen und die Tür kann geöffnet werden.	Direkter Zugang Privatsphäre.	Magnetisch unempfindlich.
07	Knauf wird in Rotation versetzt	An den Knauf wird z.B. eine Bohrmaschine angebracht, die den Knauf in sehr schnelle Rotation versetzt.	Interne Kupplung/Verriegelungsmechanismus stellt Formschluss durch die Fliehkraft dar.	Direkter Zugang Privatsphäre.	Knauf sperrt ab einer bestimmten Drehzahl.

Tabelle 35: Assets Beispielsystem 1 (mechanisch)[262]

[262] Eigene Darstellung.

Assets - kritische Elemente elektr. - primär					
System	Bearbeiter		Datum		
Beispielsystem 1	*Arne Schwerdtfeger*		*2017*		
Kritisches Element	Status		Verantwortlicher / Leitung		
Elektronische Elemente	*Hauptsächliche Analyse*		*Eigenverantwortliche Leitung*		
Funktion	Anmerkung		Ergebnis		
Service-Funktionalität			*Teilergebnis 2*		
Modus operandi	Beschreibung	Direkte Auswirkung	Asset	Gegenmaßnahme	
Nr.					
Zerstörend					
01 Aufdrehen v. innen (Zugriff außen).	Es kann von aussen auf den innenliegenden Motorzyl. zugegriffen werden, z.B. eingschl. Scheibe.	Zylinder öffnet und gewährt Zutritt.	Direkter Zugang Privatsphäre.	Annahmen beachten/Blockieren	
Zerstörfrei					
02 Smartphone verloren/geklaut	Smartphone ist nicht gegen die ungewollte Benutzung gesichert (Automatische Ausführung).	(Unrechtmäßiger) Benutzer kann Berechtigungen ausführen	Direkter Zugang Privatsphäre.	Annahmen beachten / Manuelle Ausführung .	
03 Aktualisierung unterbrechen.	Änderungen am Server werden nicht an das Smartphone ohne Internetverbindung weitergeleitet. (u.a. Zeitstempel ohne Internetverbindung zu lang-7 Tage.)	Alte und nicht gewollte Berechtigungen können noch Zutritt gewähren.	Direkter Zugang Privatsphäre.	Annahmen beachten / Weitere berechtigte Smartphones aktualisieren das Schloss.	
04 Zugangsschlüssel gehackt.	Ein digitaler Zugangsschlüssel wird gehackt.	Alle Berechtigungen könnten über einen dig. Schlüssel organisiert sein.	Zugang zu allen Berechtigungen im System.	Diversifiziertes Schlüsselmanagement.	
05 Internes Sicherheits-management ausnutzen.	Personal des Dienstanbieters verschafft sich unberechtigten Zugriff auf das System.	System kann unberechtigt geändert werden oder z.B. auch Berechtigungen vervielfältigt werden.	Gesamtes System ist gefährdet bzw. zugänglich.	Security-Dokumentation, wie z.B. Schutzniveaus, geschützter Personenkreis, etc.	
06 Entleerte Batterien (Grundstellung).	Bei entleerten oder schwachen Batterien wird der "geschlossene Zustand" nicht mehr erreicht.	Tür ist nicht gesichert bzw. verschlossen.	Direkter Zugang Privatsphäre.	Frühzeitige Batteriewarnung, "gesperrter Zutritt".	
07 Update-Funktion.	Aktualisierungen werden nicht durchgeführt.	Es gibt keine Rückmeldung über den Status und es könnten alte Berechtigungen weiter gültig sein.	Direkter Zugang Privatsphäre.	Rückmeldung vom System bei Aktualisierungen.	
08 Methodische Fehler.	System würde im Vorfeld nicht auf den use-case (Einsatz-/umgebung) konkret abgestimmt.	Schutzniveaus sind z.B. nicht richtig ausgelegt. Generell fehlendes Security-Konzept.	Grobe (unendeckte) Sicherheitslücken.	Aufstellung Security-Sicherheitskonzept.	
09 Security-Lücken.	Konsequentes Ausnutzen von fehlerhafter Security-Implementierung.	Sicherheitslücken schwächen das System.	Direkter Zugang Privatsphäre	Externe Überprüfung der Security-Implementierung.	
10 Karten verloren	Programmierte Karte kann ohne zusätzliche Authentifizierung benutz werden. Reaktionszeit wird benötigt um sie zu deaktivieren.	(Unrechtmäßiger) Benutzer kann Berechtigungen ausführen.	Direkter Zugang Privatsphäre	Nur im Notfall benutzen, Annahmen beachten.	
11 Smartphone entladen	Smartphone wurde nicht ordentlich aufgeladen und kann jetzt nicht mehr eingeschaltet werden	Berechtigter Zutritt kann nicht gewährt werden.	Kein Zugang!	Battery-off Funktion (NFC)	

Tabelle 36: Assets Beispielsystem 1 (elektronisch)[263]

[263] Eigene Darstellung.

9.26 Anhang: Assets Beispielsystem 2

Assets - kritische Elemente mechanisch - sekundär			
System	Bearbeiter	Datum	
Beispielsystem 2	*Arne Schwerdfeger*	*2016*	
Kritisches Element	Status	Verantwortlicher / Leitung	
Mechanische Elemente	*Hauptsächliche Analyse*	*Eigenverantwortliche Leitung*	
Funktion	Anmerkung	Ergebnis	
Konventionelle Schließfunktionalität		*Teilergebnis 1*	

	Modus operandi	Beschreibung	Direkte Auswirkung	Asset	Gegenmaßnahme
Nr.					
Zerstörend					
01	Zylinder an der Trennlinie aufbohren	Kürzen der Kern- und Gehäusestifte durch Schaffung künstlicher Trennebene.	Kern rotatorisch bewegbar.	Zugang zur Privatsphäre.	Bohrschutz
02	Zylinder unterhalb der Trennlinie aufbohren	Aufbohren aller Federn im Gehäuse, dadurch fallen Kern und Gehäusestifte heraus.	Kern rotatorisch bewegbar.	Zugang zur Privatsphäre.	Bohrschutz
03	Herausziehen des Zylinderkerns (Kernziehen)	Einführen einer speziellen Schraube in den Kern mit anschließendem herausziehen des Kernes (Hilfsmittel).	Freier Zugang zur Schließnase.	Zugang zur Privatsphäre.	Ziehschutz
04	Herausbrechen des Zylinders mit der Zange	Bei >= 3 mm Überstand des Schließzylinders an der Beschlagsvorderseite ergibt sich eine Ansatzfläche zum Herausbrechenrechen.	Freier Zugang zum Schloss.	Zugang zur Privatsphäre.	Einbau beachten / Annahmen beachten.
Zerstörfrei					
05	Handpicking	Verklemmen der Stiftreihen an der Trennebene.	Kern rotatorisch bewegbar.	Zugang zur Privatsphäre.	Fertigungsverfahren, Diabolos
06	Elektropicking	Stifte in Schwingung versetzen.	Kern rotatorisch bewegbar.	Zugang zur Privatsphäre.	Fertigungsverfahren, Diabolos
07	Schlagtechnik	Spezieller Schlagschlüssel zum Entsperren.	Kern rotatorisch bewegbar.	Zugang zur Privatsphäre.	Gekürzter Stift.
08	Impressionstechnik	Nachbilden des Schlüssels.	Kern rotatorisch bewegbar.	Schließgeheimnis.	Organisatorisch

Tabelle 37: Assets Beispielsystem 2 (mechanisch)[264]

[264] Eigene Darstellung.

Assets - kritische Elemente elektr. - primär						
System	Bearbeiter		Datum			
Beispielsystem 2	*Arne Schwerdtfeger*		*2016*			
Kritisches Element	Status		Verantwortlicher / Leitung			
Elektronische Elemente	*Hauptsächliche Analyse*		*Eigenverantwortliche Leitung*			
Funktion	Anmerkung		Ergebnis			
Service-Funktionalität			*Teilergebnis 2*			
Modus operandi	Beschreibung		Direkte Auswirkung	Asset		Gegenmaßnahme
Nr.						
Zerstörend						
01	Aufdrehen v. innen (Zugriff außen).	Es kann von aussen auf den innenliegenden Motorzyl. zugegriffen werden, z.B. eingschl. Scheibe.	Zylinder öffnet und gewährt Zutritt.	Direkter Zugang Privatsphäre.		Annahmen beachten/Blockieren
Zerstörfrei						
02	Smartphone verloren/geklaut	Smartphone ist nicht gegen die ungewollte Benutzung gesichert (passwortgeschützer Sperrbildschirm).	(Unrechtmäßiger) Benutzer hat direkten Zugriff auf alle Berechtigungen.	Direkter Zugang Privatsphäre.		Annahmen beachten / Sperrbildschirm schützen.
03	Aktualisierung unterbrechen.	Änderungen an der Management-Plattform werden nicht an das Smartphone ohne Internetverbindung weitergeleitet.	Alte und nicht gewollte Berechtigungen können noch Zutritt gewähren.	Direkter Zugang Privatsphäre.		Annahmen beachten / Weitere berechtigte Smartphones aktualisieren das Schloss.
04	Zugangsschlüssel gehackt.	Ein digitaler Zugangsschlüssel wird gehackt.	Alle Berechtigungen könnten über einen dig. Schlüssel organisiert sein.	Zugang zu allen Berechtigungen im System.		Diversifiziertes Schlüsselmanagement.
05	Internes Sicherheits-management ausnutzen.	Personal des Dienstanbieters verschafft sich unberechtigten Zugriff auf das System.	System kann unberechtigt geändert werden oder z.B. auch Berechtigungen vervielfältigt werden.	Gesamtes System ist gefährdet bzw. zugänglich.		Security-Dokumentation, wie z.B. Schutzniveaus, geschützter Personenkreis, etc.
06	Entleerte Batterien (Grundstellung).	Bei entleerten oder schwachen Batterien wird der "geschlossene Zustand" nicht mehr erreicht.	Tür ist nicht gesichert bzw. verschlossen.	Direkter Zugang Privatsphäre.		Frühzeitige Batteriewarnung, "gesperrter Zutritt".
07	Update-Funktion.	Aktualisierungen werden nicht durchgeführt.	Es gibt keine Rückmeldung über den Status und es könnten alte Berechtigungen weiter gültig sein.	Direkter Zugang Privatsphäre.		Rückmeldung vom System bei Aktualisierungen.
08	Methodische Fehler.	System würde im Vorfeld nicht auf den use-case (Einsatz-/umgebung) konkret abgestimmt.	Schutzniveaus sind z.B. nicht richtig ausgelegt. Generell fehlendes Security-Konzept.	Grobe (unendeckte) Sicherheitslücken.		Aufstellung Security-Sicherheitskonzept.
09	Security-Lücken.	Konsequentes Ausnutzen von fehlerhafter Security-Implementierung.	Sicherheitslücken schwächen das System.	Direkter Zugang Privatsphäre		Externe Überprüfung der Security-Implementierung.
10	Fernbedienung verloren	Die programmierte Fernbedienung kann verloren werden und ist ohne zusätzliche Authentifizierung benutzbar. Reaktionszeit wird benötigt um sie zu deaktivieren	Zylinder öffnet und gewährt Zutritt.	Direkter Zugang Privatsphäre		Annahmen beachten, nur im Notfall benutzen
11	Smartphone entladen	Smartphone wurde nicht ordentlich aufgeladen und kann jetzt nicht mehr eingeschaltet werden	Berechtigter Zutritt kann nicht gewährt werden.	Kein Zugang!		Battery-off Funktion (NFC)

Tabelle 38: Assets Beispielsystem 2 (elektronisch)[265]

[265] Eigene Darstellung.

9.27 Anhang: Wahrscheinlichkeitsbetrachtung Beispielsystem 1

Wahrscheinlichkeiten - kritische Elemente mechanisch - sekundär (Check)

Systembaustein		Bearbeiter				Datum							
Beispielsystem 1 (eingebauter Zustand)		*Arne Schwerdtfeger*				*2017*							
Kritisches Element		Status				Verantwortlicher / Leitung							
Außenknauf		*Hauptsächliche Analyse*				*Eigenverantwortliche Leitung*							
Funktion		Anmerkung				Ergebnis							
Leseeinheit / Außenbereich						*Teilergebnis 3*							
	Kriterium	Sicherheitsziel	Soll	Ist	Asset	Wahrscheinlichkeit	Schaden	Risikozahl	Gewichtung	Risikograd	Bemerkung		
Nr.													
01	Normung erfüllt	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Keines						Erfüllt!		
02	Knauf abschlagen/kreten	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Direkter Zugang Privatsphäre	10	1	10	0	0	Nur Schaden am Zylinder.		
03	Knauf abschlagen	DIN EN 15684 (2)	Theoretisch möglich.	DIN EN 15684	Direkter Zugang Privatsphäre	10	1	10	0	0	Kontakte geschützt.		
04	Zylinder aufbohren	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Direkter Zugang Privatsphäre	8	1	8	0	0	Bohrschutz		
05	Zylinder fluten	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Direkter Zugang Privatsphäre	8	1	8	0	0	Unempfindlich		
06	Stigmatisierung	DIN EN 15684 (2)	Nicht erfüllt	DIN EN 15684	Einbruchgefahr / Eingriff Privatsphäre	6	10	60	1	60	Generelles Problem.		
07	Angriff mit Magnet	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Direkter Zugang Privatsphäre	6	1	6	0	0	Unempfindlich		
08	Knauf wird in Rotation versetzt	DIN EN 15684 (2)	Erfüllt	DIN EN 15684	Direkter Zugang Privatsphäre	8	1	8	0	0	Sperreineinrichtung		
Legende:		Legende:											
Wahrscheinlichkeit		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringe Wahrscheinlichkeit)							
Schaden		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringer Schaden)							
Aufgrund der geringeren Komplexität der mechanischen Komponente kann die maximale Gewichtung mit 1 angegeben!													

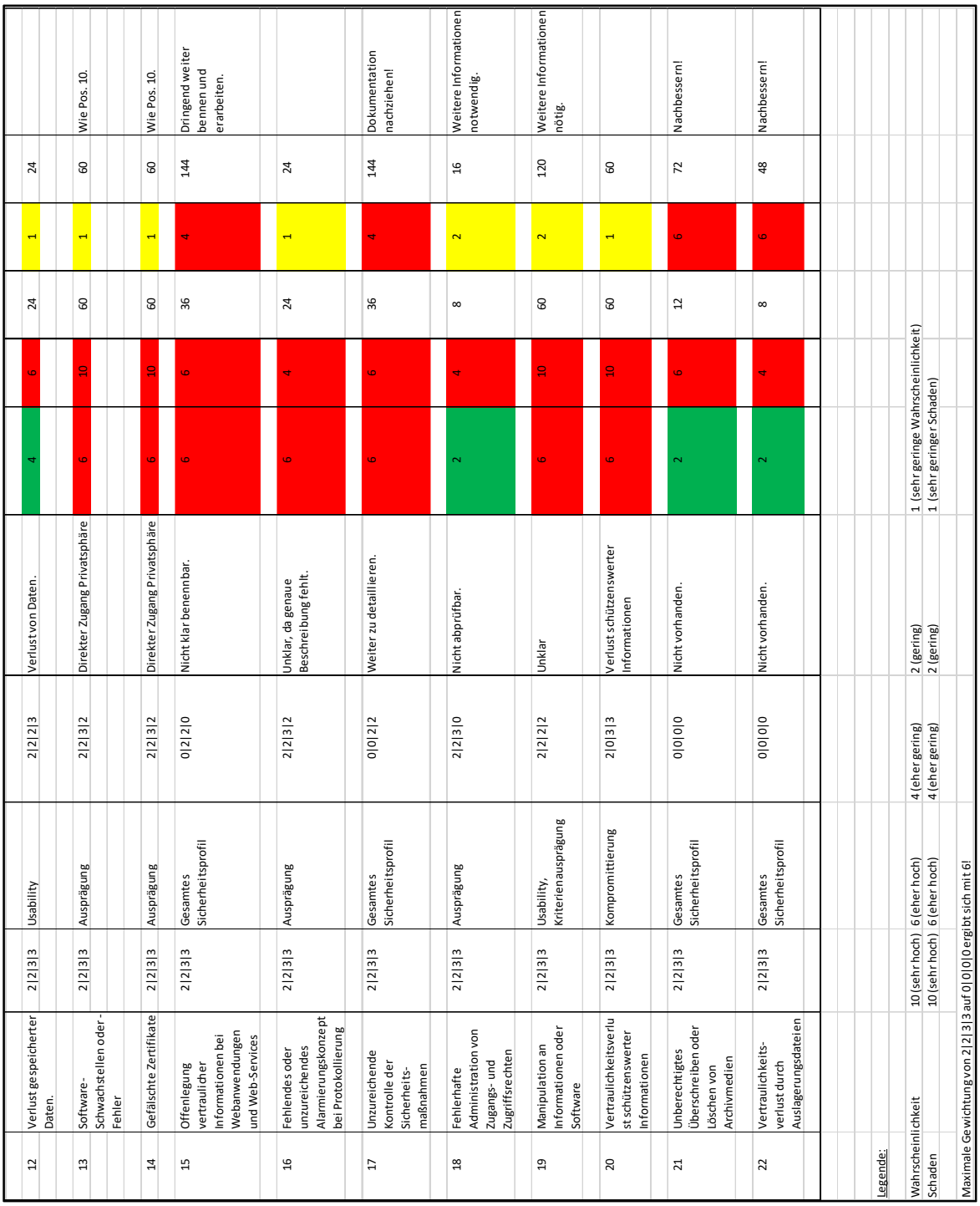
Tabelle 39: Wahrscheinlichkeitsbetrachtung Beispielsystem 1 (mechanisch)[266]

[266] Eigene Darstellung.

Wahrscheinlichkeiten - kritische Elemente elektronisch - primär (Check)												
Systembaustein		Bearbeiter			Datum							
Beispielsystem 1 (eingebauter Zustand)		*Arne Schwerdtfeger*			*2017*							
Kritisches Element		Status			Verantwortlicher / Leitung							
Elektronische Elemente		*Hauptsächliche Analyse*			*Eigenverantwortliche Leitung*							
Funktion		Anmerkung			Ergebnis							
Service-Funktionalität					*Teilergebnis 4*							
	Kriterium	Sicherheitsziel	Soll	Ist	Asset	Wahrscheinlichkeit	Schaden	Risikozahl	Gewichtung	Risikograd	Bemerkung
Nr.											
01	Aufdrehen v. innen (Zugriff außen).	2|2|3|3	Blockieren	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	
02	Smartphone verloren/geklaut	2|2|3|3	Manuelle Ausführung	0|2|3|0	Direkter Zugang Privatsphäre	10	10	100	3	300	Individuell
03	Aktualisierung unterbrechen.	2|2|3|3	Zeitstempel verkürzen	0|2|3|3	Direkter Zugang Privatsphäre	6	10	60	1	60	
04	Zugangsschlüssel gehackt.	2|2|3|3	Diversifiziertes Schlüsselmanagement.	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	
05	Internes Sicherheits-management ausnutzen.	2|2|3|3	Security-Dokumentation, z.B. Schutzniveaus, etc.	0|0|2|0	Gesamtes System ist gefährdet bzw. zugänglich.	6	10	60	5	300	
06	Entleerte Batterien (Grundstellung).	2|2|3|3	Frühzeitige Batteriewarnung.	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	
07	Update-Funktion.	2|2|3|3	Rückmeldung vom System.	0|2|2|0	Direkter Zugang Privatsphäre	6	10	60	4	240	
08	Methodische Fehler.	2|2|3|3	Aufstellung Security-Sicherheitskonzept.	0|0|2|0	Grobe (unendeckte) Sicherheitslücken.	6	6	36	5	180	
09	Security-Lücken.	2|2|3|3	Externe Überprüfung.	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	Auswirkungen noch genau zu bennen.
10	Karten verloren	2|2|3|3	Annahmen beachten, nur im Notfall	0|2|3|0	Direkter Zugang Privatsphäre	10	10	100	3	300	
11	Smartphone entladen	2|2|3|3	Battery-off Funktion	Erfüllt	Kein Zugang!	1	1	1	0	0	

Tabelle 40: Wahrscheinlichkeitsbetrachtung Beispielsystem 1 (elektronisch) (1)[267]

[267] Eigene Darstellung.



12	Verlust gespeicherter Daten.	2|2|3|3	Usability	2|2|2|3	Verlust von Daten.	4	6	24	1	24			
13	Software-Schwachstellen oder -Fehler	2|2|3|3	Ausprägung	2|2|3|2	Direkter Zugang Privatsphäre	6	10	60	1	60	Wie Pos. 10.		
14	Gefälschte Zertifikate	2|2|3|3	Ausprägung	2|2|3|2	Direkter Zugang Privatsphäre	6	10	60	1	60	Wie Pos. 10.		
15	Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services	2|2|3|3	Gesamtes Sicherheitsprofil	0|2|2|0	Nicht klar benennbar.	6	6	36	4	144	Dringend weiter benennen und erarbeiten.		
16	Fehlendes oder unzureichendes Alarmierungskonzept bei Protokollierung	2|2|3|3	Ausprägung	2|2|3|2	Unklar, da genaue Beschreibung fehlt.	6	4	24	1	24			
17	Unzureichende Kontrolle der Sicherheits-maßnahmen	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|2|2	Weiter zu detaillieren.	6	6	36	4	144	Dokumentation nachziehen!		
18	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	2|2|3|3	Ausprägung	2|2|3|0	Nicht abprüfbar.	2	4	8	2	16	Weitere Informationen notwendig.		
19	Manipulation an Informationen oder Software	2|2|3|3	Usability, Kriterienausprägung	2|2|2|2	Unklar	6	10	60	2	120	Weitere Informationen nötig.		
20	Vertraulichkeitsverlust schützenswerter Informationen	2|2|3|3	Kompromittierung	2|0|3|3	Verlust schützenswerter Informationen	6	10	60	1	60			
21	Unberechtigtes Überschreiben oder Löschen von Archivmedien	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|0|0	Nicht vorhanden.	2	6	12	6	72	Nachbessern!		
22	Vertraulichkeits-verlust durch Auslagerungsdateien	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|0|0	Nicht vorhanden.	2	4	8	6	48	Nachbessern!		
Legende:													
Wahrscheinlichkeit		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)		2 (gering)		1 (sehr geringe Wahrscheinlichkeit)					
Schaden		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)		2 (gering)		1 (sehr geringer Schaden)					
Maximale Gewichtung von 2|2|3|3 auf 0|0|0|0 ergibt sich mit 6!													

Tabelle 41: Wahrscheinlichkeitsbetrachtung Beispielsystem 1 (elektronisch) (2)[268]

[268] Eigene Darstellung.

9.28 Anhang: Wahrscheinlichkeitsbetrachtung Beispielsystem 2

Wahrscheinlichkeiten - kritische Elemente mechanisch - sekundär (Check)

Systembaustein	*Beispielsystem 2*	Bearbeiter	*Arne Schwerdtfeger*			Datum	*2016*							
Kritisches Element	*Mechanische Elemente*	Status	*Hauptsächliche Analyse*			Verantwortlicher / Leitung	*Eigenverantwortliche Leitung*							
Funktion	*Konventionelle Schließfunktionalität*	Anmerkung				Ergebnis	*Teilergebnis 3*							
	Kriterium	Sicherheitsziel	Soll	Ist	Asset	Wahrscheinlichkeit	Schaden	Risikozahl	Gewichtung	Risikograd	Bemerkung			
Nr.														
01	Normung erfüllt	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Keines						Erfüllt!			
02	Zylinder an der Trennlinie aufbohren	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Bohr- und Ziehschutz vorhanden.			
03	Zylinder unterhalb der Trennlinie aufbohren	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Bohr- und Ziehschutz vorhanden.			
04	Herausziehen des Zylinderkerns (Kernziehen)	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Bohr- und Ziehschutz vorhanden.			
05	Herausbrechen des Zylinders mit der Zange	DIN 18252 Klasse 82 (BZ)	Annahmen beachten, korrekter Einbau muss gewährleistet sein!	SKG 3	Zugang zur Privatsphäre	6	10	60	0	0	Gewährleistet der Errichter vor Ort.			
06	Handpicking	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Gegenmaßnahme inkludiert.			
07	Elektropicking	DIN 18252 Klasse 82 (BZ)	Erfüllt		Zugang zur Privatsphäre	1	10	10	0	0	Gegenmaßnahme inkludiert.			
08	Schlagtechnik	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Gegenmaßnahme inkludiert.			
09	Impressionstechnik	DIN 18252 Klasse 82 (BZ)	Erfüllt	SKG 3	Zugang zur Privatsphäre	1	10	10	0	0	Profil mit Hinterschnitt.			

Hinweis: Normung bezieht sich nur auf die Außenseite!

Legende:

Legende:				
Wahrscheinlichkeit	10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringe Wahrscheinlichkeit)
Schaden	10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringer Schaden)

Aufgrund der geringeren Komplexität der mechanischen Komponente kann die maximale Gewichtung mit 1 angegeben!

Tabelle 42: Wahrscheinlichkeitsbetrachtung Beispielsystem 2 (mechanisch)[269]

[269] Eigene Darstellung.

Wahrscheinlichkeiten - kritische Elemente elektronisch - primär (Check)													
Systembaustein	*Beispielsystem 2*	Bearbeiter	*Arne Schwerdtfeger*		Datum	*2016*							
Kritisches Element	*Elektronische Elemente*	Status	*Hauptsächliche Analyse*		Verantwortlicher / Leitung		*Eigenverantwortliche Leitung*						
Funktion	*Service-Funktionalität*	Anmerkung			Ergebnis		*Teilergebnis 4*						
Nr.	Kriterium	Sicherheitsziel	Soll	Ist	Asset	Wahrscheinlichkeit	Schaden	Risikozahl	Gewichtung	Risikograd	Bemerkung		
01	Aufdrehen v. innen (Zugriff außen)	2|2|3|3	Blockieren	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	Gegenmaßnahme inkludiert.		
02	Smartphone verloren/geklaut	2|2|3|3	Sperrbildschirm	0|2|3|0	Direkter Zugang Privatsphäre	10	10	100	3	300	Individuell beachten.		
03	Aktualisierung unterbrechen	2|2|3|3	Weitere Smartphones aktualisieren das Schloss.	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0	(24 Std. dann Internetverbindung nötig!)		
04	Zugangsschlüssel gehackt	2|2|3|3	Diversifiziertes Schlüsselmanagement	Erfüllt	Zugang zu allen Berechtigungen im System.	1	10	10	0	0			
05	Internes Sicherheits-management ausnutzen	2|2|3|3	Security-Dokumentation, z.B. Schutzniveaus, etc.	0|0|2|0	Gesamtes System ist gefährdet bzw. zugänglich.	6	10	60	5	300			
06	Entleerte Batterien (Grundstellung)	2|2|3|3	Frühzeitige Batteriewarnung	Erfüllt	Direkter Zugang Privatsphäre	1	10	10	0	0			
07	Update-Funktion	2|2|3|3	Rückmeldung vom System.	0|2|2|0	Direkter Zugang Privatsphäre	6	10	60	4	240			
08	Methodische Fehler	2|2|3|3	Aufstellung Security-Sicherheitskonzept.	0|0|2|0	Grobe (unendeckte) Sicherheitslücken.	6	6	36	5	180			
09	Security-Lücken	2|2|3|3	Externe Überprüfung.	0|2|2|0	Direkter Zugang Privatsphäre	10	6	60	4	240			
10	Fernbedienung verloren	2|2|3|3	Annahmen beachten, nur im Notfall	0|2|3|0	Direkter Zugang Privatsphäre	10	10	100	3	300			

Tabelle 43: Wahrscheinlichkeitsbetrachtung Beispielsystem 2 (elektronisch) (1)[270]

[270] Eigene Darstellung.

11	Smartphone entladen	2|2|3|3	Battery-off Funktion	2|2|0|3	Kein Zugang!	6	6	36	2	72		
12	Software-Schwachstellen oder -Fehler	2|2|3|3	Usability, Ausprägung	2|2|2|2	Service und Gerät funktionslos.	6	6	36	2	72	Schon in Position 9 erwähnt!	
13	Unzureichende oder fehlende Verbindungs-Sicherheits-mechanismen	2|2|3|3	Usability, Ausprägung	2|2|2|0	Service/Gerät funktionslos, nicht vorhanden	6	6	36	3	108		
14	Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung	2|2|3|3	Ausprägung	2|2|3|0	Nicht vorhanden	6	6	36	2	72		
15	Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen	2|2|3|3	Usability, Ausprägung	2|2|2|2	Geringe Ausprägung, Service/Gerät funktionslos	6	6	36	2	72	Teiweise mit Bezug zu Pos. 11!	
16	Unerlaubte Ausübung von Rechten	2|2|3|3	Kompromittierung sensibler Daten	2|0|3|3	Nicht vorhanden	6	10	60	1	60		
17	Manipulation an Informationen oder Software	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|0|0	Nicht vorhanden	6	6	36	6	216	Fand keine Anwendung!	
18	Software mit unerlaubten Zugriff	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|0|0	Nicht vorhanden	2	4	8	6	48	Fand keine Anwendung!	
19	Kompromittierung kryptographischer Schlüssel	2|2|3|3	Kompromittierung, Ausprägung	2|0|3|2	Nicht vorhanden, geringe Ausprägung	10	10	100	2	200	Genauere Informationen fehlten!	
20	Vertraulichkeits-verlust durch Auslagerungsdateien	2|2|3|3	Gesamtes Sicherheitsprofil	0|0|0|0	Nicht vorhanden	4	2	8	6	48	Fand keine Anwendung!	
Legende:												
Wahrscheinlichkeit		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringe Wahrscheinlichkeit)						
Schaden		10 (sehr hoch)	6 (eher hoch)	4 (eher gering)	2 (gering)	1 (sehr geringer Schaden)						
Maximale Gewichtung von 2|2|3|3 auf 0|0|0|0 ergibt sich mit 6!												

Tabelle 44: Wahrscheinlichkeitsbetrachtung Beispielsystem 2 (elektronisch) (2)[271]

[271] Eigene Darstellung.

Wissenschaftlicher Werdegang (CV)

Der Lebenslauf ist in der Online-Version aus Gründen des Datenschutzes nicht enthalten.