Entwicklung eines Modells zur Überprüfung des Niveaus der betrieblichen Informationssicherheit

Vom Fachbereich Bauingenieurwesen, Maschinenbau, Sicherheitstechnik

Abteilung Sicherheitstechnik

der Bergischen Universität Wuppertal

zur Erlangung des akademischen Grades

Doktor der Sicherheitswissenschaft

genehmigte **Dissertation**

von

Dipl.-Psych. Manfred R. Tietze

aus Kaufbeuren

Gutachter:

Prof. Dr. Bernd Hans Müller

Prof. Dr. Hartmut Häcker

Tag der mündlichen Prüfung:

23. Februar 2007

Zusammenfassung

Informationen und die für die Informationsverarbeitung und Kommunikation benutzten Anwendungen und Einrichtungen sind wertvolles und schützenswertes Unternehmensgut. Aus diesem Grund wird die Frage nach dem „betrieblichen Niveau der Informationssicherheit“ auf Mitarbeiterebene und Möglichkeiten dem Aspekt der „Human Firewall“ effektiv entgegenzutreten in Konzernen, Behörden und Betrieben immer stärker.

Das Ziel dieser Arbeit richtet sich in erster Linie auf die Entwicklung eines Modells zur Überprüfung des betrieblichen Niveaus der Informationssicherheit. Zur Realisierung dieser Aufgabe wird in einem ersten Schritt der Status quo der Informationssicherheit auf der Ebene der Mitarbeiter hinsichtlich relevanter Faktoren ermittelt. Hierzu wird ein Fragebogeninstrument entwickelt, das zum einen eine Einschätzung des Führungsverhaltens und der organisatorischen Gegebenheiten aus Sicht der Mitarbeiter verlangt. Zum anderen wird von den Mitarbeitern eine Selbsteinschätzung bzgl. der betrieblichen Informationssicherheit in Anlehnung an die Theorie des geplanten Verhaltens von AJZEN & MADDEN (1986) und an die wahrgenommene „Soziale Unterstützung“ durch Kollegen und Vorgesetzte gefordert. In zweiter Linie werden neben dem entwickelten Fragebogen weitere bereits standardisierte Fragebögen zur Analyse der „Belastung am Bildschirmarbeitsplatz“ und „Softwareergonomie“ eingesetzt.

Die aus den Fragebögen gewonnenen Ergebnisse werden sowohl zwischen „IT-Anwender“ und „IT-Experten“, als auch mit innerhalb der Gruppen ermittelten Typen-profilen in Beziehung gesetzt, ausführlich diskutiert und Umsetzungsmaßnahmen empfohlen.

Abstract

Information as well as the applications and devices used for information processing and communication are a company’s own capital that is precious and worth to be protected. Therefore, the issues regarding the “internal level of information security” on employee-level as well as the possibilities of handling the aspect of the “human firewall” in enterprises, authorities and business are getting more and more important.

The prime target of this work is the development a model that enables to review the internal level of information security. For realisation of this target, the status quo of information security on employee-level in view of the relevant factors will be determined as a first step. For this purpose, a questionnaire will be designed that demands an assessment of managerial behaviour and organisational structures from the employees’ point of view on the one hand. On the other hand, the employees are asked to do a self-assessment regarding the internal information security following the theories of AJZEN & MADDEN (1986) as well as the percieved “social support” by colleagues and superiors. Secondly, standardised questionnaires for analysis of “strain by on-screen work” as well as “software ergonomics” will be used besides the designed questionnaire mentioned above.

The results of the questionnaires will be set in relation between “IT-users” and “IT-experts” as well as between the types of characters determined within a single group. Afterwards, the results will be discussed and measures for realisation will be recommended.

Resumé

Les informations ainsi que les applications et les installations utilisées pour le traitement de l’information et la communication sont un bien précieux et digne de protection de l’entreprise. C’est pourquoi la question « du niveau de la sécurité de l’information au sein de l’entreprise » devient de plus en plus importante à l’échelon des collaborateurs dans les konzerns, les administrations et les entreprises, de même que les possibilités pour faire face de manière efficace à l’aspect du « Human Firewall »

L’objectif de ce travail vise en premier lieu la réalisation d’un modèle de contrôle du niveau de la sécurité de l’information au sein de l’entreprise. En vue de réaliser cette tâche, il s’agit dans un premier temps de déterminer le statu quo de la sécurité de l’information à l’échelon des collaborateurs quant aux facteurs significatifs. A cet effet, un instrument contenant un questionnaire doit être élaboré qui demande d’un côté une appréciation du comportement de la direction et de la réalité de l’organisation dans l’optique des collaborateurs. De l’autre côté, l’on demande aux collaborateurs une auto-évaluation relative à la sécurité de l’information au sein de l’entreprise sur le modèle de la théorie du comportement prévu de AJZEN & MADDEN (1986) et de « l’assistance « des collègues et des supérieurs perçue. En second lieu, il s’agit d’utiliser accessoirement au questionnaire réalisé d’autres questionnaires déjà standardisés en vue d’analyser les « contraintes dues au poste de travail sur écran » et l’ergonomie relative au logiciel.

Les résultats obtenus par les questionnaires sont mis en relation non seulement entre les utilisateurs de l’informatique et les informaticiens mais aussi avec des profils type établis à l’intérieur des groupes. Ils sont discutés en détail et des recommandations sur les mesures à prendre pour une mise en pratique sont présentées.

INHALTSVERZEICHNIS

1 Einleitung

Der vor ca. 25 Jahren begonnene Einzug von Informationssystemen in Unternehmen, Behörden und Privathaushalten führte zu einer Veränderung bzw. Wandel der Arbeitsumwelt, den -bedingungen, der Arbeitsorganisationen, den sozialen Strukturen, der Arbeitsaufgabe und letzten Endes der gesamten Gesellschaft.

Wurde anfangs der Einsatz von Informationssystemen in den Betrieben und Behörden als „Werkzeug“ zur Vereinfachung von Arbeitsabläufen betrachtet, so ist heute in nahezu allen Bereichen von Organisationen der nachhaltige Erfolg der jeweiligen Geschäftsprozesse vom Einsatz heterogener und vernetzter Informationssysteme und der damit verbundenen Informationstechnologie abhängig. Dieser Wandel verdeutlicht die Bedeutung von Informationssicherheit, da Informationen und die für die Informationsverarbeitung und Kommunikation benutzten Anwendungen (Software) und Einrichtungen (Hardware) wertvolles und schützenswertes Unternehmensgut geworden sind.

Die Vergangenheit zeigte, dass Hacker, Viren, Trojanische Pferde etc. synonym für Angst stehen, dass Daten beschädigt oder gelöscht bzw. geheime und unternehmensbezogene Informationen abgefangen und zu kriminellen Zwecken genutzt werden. Bei genauerer Betrachtung der Situation lassen sich die schädigenden Personen weniger außerhalb des Unternehmens als in den eigenen Reihen finden. So liegen ca. 70% der „Systemangriffe“ in der Verantwortung der eigenen Mitarbeiter (COLE & MATZER; 1999). Informationssysteme und die darauf installierte Software zum Schutz von Daten (Virenprogramme, Firewall etc.) haben inzwischen ein relativ hohes Sicherheitsniveau erreicht. KÜNZLER (2002) sieht daher in den „Systemangriffen“ weniger die absichtliche Herbeiführung durch den Mitarbeiter als Hauptursache, sondern viel mehr die Kombination von spezifischen Bedingungen und Situationen, die durch unglückliche Verkettungen zu Störungen führen, an deren Ende der Mensch steht. Daher richtet KÜNZLER (2002) seine Forderung weniger an Konzepte, die versuchen, Störungen durch neue Vorschriften und Regelungen zu verhindern, sondern an Konzepte, die Sicherheit proaktiv fördern.

KONRAD (1998) fordert in diesem Sinne eine neue und übergeordnete Betrachtungsweise für die Untersuchung der Sicherheitsproblematik, da die traditionellen Konzepte zur Gestaltung der Informationssicherheit die Sicherheit von Informationssystemen hauptsächlich als Techniksysteme in den Mittelpunkt stellen. Zudem sind die meisten sicherheitsspezifischen Aktivitäten auf dieser Ebene initiiert und koordiniert und nicht auf der Führung- und Mitarbeiterebene.

Um diesem Gedanken der „Human Firewall" Rechnung zu tragen, richtet sich das Ziel der vorliegenden Arbeit in erster Linie auf die Ermittlung eines Status quo zum Thema „IT-Sicherheitsbewusstsein der Mitarbeiter". In zweiter Linie soll auf Grund der gewonnen Erkenntnisse abgeleitet werden, wie Informationssicherheit in Organisationen auf der Führungs- und Mitarbeiterebene gefördert werden kann. Dabei steht die Frage im Vordergrund, welche konkreten Maßnahmen getroffen werden können, um die Mitarbeiter zu einer zielgerichteten Umsetzung sicherheitsbezogener Aspekte zu motivieren und dabei zu unterstützen? Ein betriebliches Sicherheitsmanagement hat demnach mindestens so viel mit Mitarbeiterführung und Kommunikation zu tun, wie mit Hard- und Software.

Zur Realisierung dieser Zielsetzung soll ein Instrument konstruiert und entwickelt werden, um individuelle Leistungen und erfolgskritische Anforderungen bei der betrieblichen Umsetzung von Sicherheitsmaßnahmen am Bildschirmarbeitsplatz (BSAP) ökonomisch, zuverlässig und vergleichbar zu erfassen. Auf der Basis der theoretischen und praktischen Defizite sollen kritische Anforderungen an ein effektives und effizientes methodisches Vorgehen - in Form eines Maßnahmenkatalogs – abgeleitet werden.

Um dieser Aufgabe Rechnung zu tragen, werden einerseits Bestimmungsgrößen in Anlehnung an die Theorie des geplanten Verhaltens von AJZEN & MADDEN (1986) für sicherheitsgerechtes Verhalten herangezogen. Andererseits soll das Führungsverhalten der direkten Vorgesetzten aus der Sicht der Mitarbeiter zum Thema und die unternehmerische Aktivitäten eingeschätzt werden.

Eine weitere Bewertungsgrundlage bildet das Konzept des sozio-technischen Systemansatzes. Mit diesem Ansatz wird das Arbeitssystem ganzheitlich betrachtet und der Faktor „Mensch“ wird nicht nur als Risikofaktor und Hauptverursacher von Systemausfällen verantwortlich gemacht, sondern auch als Sicherheitsfaktor bewertet. Diese Sichtweise soll helfen, spezifisches intrapersonelles Potential zu nutzen und zu fördern und damit die Zuverlässigkeit und die Sicherheit der Systeme zu fördern. Die Schnittstelle hierzu bildet die Arbeitsaufgabe am BSAP. Dort werden zum einen die Kriterien einer sicherheitsfördernden Arbeitsgestaltung umgesetzt, zum anderen werden IT-bezogene Gefahrenpotentiale und –quellen eingeschätzt und kommuniziert.

Die hierzu notwendigen Daten wurden mit Durchführung einer Fragebogenaktion bei IT-Anwendern im Dienstleistungsbereich erhoben und anhand der klassischen teststatistischen Gütekriterien nach LIENERT & RAATZ (1992) ausgewertet. Auf Basis der gewonnenen Daten wurde der Fragebogen analysiert, bewertet und modifiziert. Dies geschieht unter Beachtung der Kriterien: 1) „Ökonomische Durchführbarkeit“ bei der Befragung und 2) „Objektivität“, „Reliabilität“ und „Validität“ bei der Fragebogenkonstruktion.

In einem weiteren Schritt werden die Bestimmungsgrößen sicherheitsgerechten Verhaltens mit relevanten Einflussgrößen am BSAP in Beziehung gesetzt. Diese Leistungsindikatoren auf der Arbeitsplatzebene beziehen sich konkret auf den software-ergonomischen Bereich und den mentalen Belastungsgrößen bei der Gestaltung der Arbeitsaufgabe. Es wird untersucht, ob sich die Wahrnehmung der arbeitsbedingten Belastung und Beanspruchung auf der individuellen Ebene zusätzlich auf persönliche Einstellungen, Überzeugungen und wahrgenommene Kontrollmöglichkeiten bzgl. des IT-Sicherheitsbewusstseins auswirken.

Es werden Zusammenhänge bzgl. der Bestimmungsgrößen zwischen einer Gruppe von „IT-Experten“[1] und einer Gruppe von „IT-Anwendern“[2] untersucht. Damit soll

[1] „IT-Experten“ sind Mitarbeiter mit fundierten Kenntnissen der IT und deren Prozesse. Sie sind für die Erhaltung der Sicherheit der IT-Komponenten in der Organisation verantwortlich.
[2] „IT-Anwender“ sind Mitarbeiter ohne spezielle Kenntnisse der IT und deren Prozesse. Sie benötigen die IT und deren Prozesse zur Durchführung Ihrer Arbeitstätigkeit.

herausgefunden werden, ob die Variablen, welche das Verhalten zur Sicherheitsumsetzung beeinflussen, durch IT-spezifische Kenntnisse determiniert werden.

Die Datenerhebung zur Konstruktion des Fragebogens fand bei einem Konzern der Finanzdienstleistung in NRW statt. Hier wurden in insgesamt 11 Bereichen 470 Mitarbeiter ohne spezielle Vorkenntnisse von IT-bezogenen Themen schriftlich befragt. Zusätzlich wurden die leistungsbezogenen Kriterien an Hand evaluierter Messinstrumente erhoben. Zur Bewertung der kriteriumsorientierten Validität wurden Bestimmungsgrößen nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) herangezogen. Diese Kriterien des BSI-Grundschutzkatalogs wurden mittels Interviews mit Experten erhoben.

Abschließend wird die Bedeutung der Bestimmungsgrößen zur Bewertung des betrieblichen Sicherheitsniveaus zusammenfassend beurteilt. Dabei werden zweck- und zielgerichtete Maßnahmen abgeleitet und deren Dienlichkeit bei der Umsetzung eines Sicherheitsprozess diskutiert.

Als Motivation für die Beschäftigung mit dem Thema betriebliche IT-Sicherheit im Rahmen dieser Arbeit wird darauf hingewiesen, dass der Autor einige Jahre als Diplom-Psychologe und Berater in dem Bereich Sicherheitsberatung von Informationssystemen tätig war. Dabei wurde er immer wieder mit theoretischen und praktischen Fragestellungen wie beispielsweise „Sensibilisierung der Mitarbeiter zum Thema IT-Sicherheit“ konfrontiert. Die vorgefundene Diskrepanz zwischen theoretischem Anspruch und vorgefundener Wirklichkeit kann als wesentlicher Antrieb dafür angesehen werden, sich wissenschaftlich mit der Gestaltung der Informationssicherheit auseinanderzusetzen, sowie der Ableitung von für die Praxis relevanten und hilfreichen Handlungsempfehlungen.

Im Folgenden werden die Inhalte der einzelnen Kapitel dieser Arbeit kurz erläutert:
Im Kapitel 2 wird von der allgemeinen Forderung der Systemsicherheit einer Organisation auf die spezifischen Bereiche, die zum Erhalt von elektronischen Daten und Informationen beitragen, eingegangen. Die Problematik der Systemsicherheit wird dabei als übergeordnetes Organisationsziel betrachtet. Es werden Begriffe, die im Zusammenhang mit der Informationstechnologie (IT) und der IT-Sicherheit stehen erläutert und definiert, als auch die rechtlichen Bestimmungen in der IT umrissen. Ein Hauptaugenmerk richtet sich an die Unternehmensführung als Hauptverantwortlicher zur Umsetzung von IT-Sicherheitsaspekten. Es werden diesbezüglich verschiedene Führungsstile erläutert und diskutiert. Des Weiteren werden die spezifischen Bereiche des personen- und arbeitsplatzbezogenen Risikomanagements betrachtet. Dies beinhaltet sowohl die Diskussion von Erklärungsmodellen zur Beurteilung menschlichen Handelns, als auch Umsetzungskriterien zur sicherheitsgerechten Arbeitsplatz- und Arbeitsaufgabengestaltung. Abschließend werden Belastungs- und Beanspruchungskonzepte und die damit verbundenen Folgen für den Menschen am Bildschirmarbeitsplatz eingehend erörtert.

Im Kapitel 3 werden die Untersuchungsdesigns für die vorliegende Arbeit vorgestellt und erläutert.

Das Kapitel 4 beinhaltet die Methodik und Durchführung der Datenerhebung zur Konstruktion eines Fragebogens, der das Niveau der betrieblichen Informationssicherheit bei den Mitarbeitern messen soll. Abgeschlossen wird dieses Kapitel mit der Darstellung der Kovarianzstrukturen zum IT-Sicherheitsverhalten und der IT-Sicherheitskultur. Dabei wird überprüft, ob die vorliegenden Daten in Verbindung mit den Erklärungsmodellen eine Aussage zum IT-Sicherheitsverhalten zulassen.

Mit dem Kapitel 5 werden Zusammenhänge auf Basis der Fragebogendaten sowohl zwischen der Organisations- und Mitarbeiterebene, als auch innerhalb der einzelnen Ebenen betrachtet.

Die Kapitel 6 und 7 widmen sich dem Zusammenhang zwischen einer Gruppe von „IT-Experten“ und einer Gruppe von „IT-Anwendern“ (Kapitel 6) und dem Einfluss der erhobenen soziodemographischen Daten auf das IT-Sicherheitsverhalten der Mitarbeiter (Kapitel 7).

Im Kapitel 8 werden die vorgefundenen Ergebnisse zusammenfassend dargestellt und an Hand der Kriterien des Bundesamtes für Informationssicherheit diskutiert.

Die Arbeit schließt mit dem Kapitel 9, in dem Empfehlungen für eine IT-sicherheitsgerechte Handhabung der IT-Sicherheitsmaßnahmen stichpunktartig dargestellt werden.

2 Informationssicherheit als Kriterium der Systemgestaltung

Die Einführung der Informations- und Kommunikationstechnologie (IuK) sowie Informationstechnik (IT) in fast allen betrieblichen Bereichen und Unternehmen hat dazu geführt, dass sich unsere Industriegesellschaft zusehends in Richtung Dienstleistungs- und Informationsgesellschaft entwickelt. Aus dem schnellen und sicheren Austausch von Informationen resultiert ein großer Wettbewerbsvorteil. Dabei beziehen sich die Auswirkungen sowohl auf die Organisationsstruktur und deren Prozessabläufe, als auch auf die Arbeitstätigkeit selbst. Auf der einen Seite führt die Zunahme der Systemkomplexität, und damit auch die Störanfälligkeit des sozio-technischen Systems, zu neuen Herausforderungen an die Systemgestaltung. Auf der anderen Seite werden körperliche Arbeiten und motorische Tätigkeiten von kognitiven Anforderungen abgelöst. Dadurch ergeben sich sowohl für die Führungskräfte als auch für die Mitarbeiter neuartige Belastungsfaktoren, sowie damit zusammenhängende Veränderungen und Konsequenzen. Modewörter hierfür sind „Technostress“ oder „informational overload“ (vgl. UDRIS & FRESE, 1988).

Den zentralen Punkt des Kapitels 2 bilden die Vorstellung und die Diskussion vorherrschender aktueller Ansätze für die Gestaltung der Systemsicherheit, insbesondere für das Management der Systemsicherheit.

So wie die Informationssicherheit den übergeordneten Bereich des Sicherheitsmanagements bildet, geht aus dem Sicherheitsmanagement das Risikomanagement hervor. Im Bereich „Informationssicherheit“ werden begriffliche und rechtliche Grundlagen erläutert. Im Bereich „Sicherheitsmanagement“ werden Konzepte zur Umsetzung des betrieblichen Risikomanagements dargestellt. Innerhalb des Risikomanagements erfolgt die Aufteilung in die Bereiche „technikorientiertes“, „personenbezogenes“ und „arbeitsplatzbezogenes“ Risikomanagements.

Der Fokus in diesem Kapitel wird auf die Themen „Sicherheit als Führungsaufgabe“, dem „personenbezogenen“ und dem „arbeitsplatzbezogenen“ Teilbereich des Risikomanagements gelegt und dargestellt.

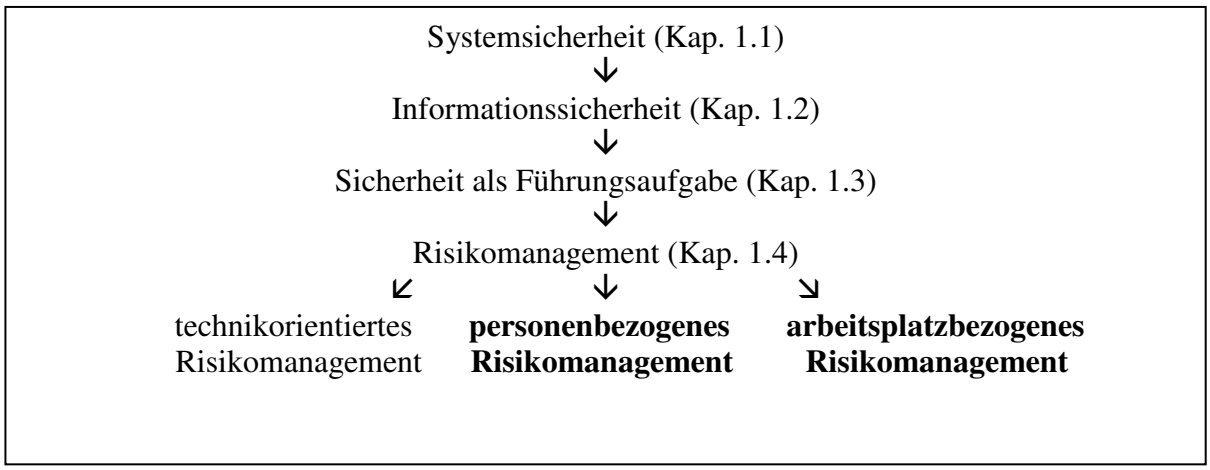


Abbildung 1: Vom Allgemeinen zum Speziellen gehende Struktur von Kapitel 2 (Modifiziert nach STADELMANN, 1996)

Abgeschlossen wird das Kapitel mit einer zusammenfassenden Darstellung und Beurteilung.

2.1 Systemsicherheit als Organisationsziel

Das Bedürfnis nach Sicherheit ist so alt wie der Mensch selbst. Es beinhaltet das Verlangen, die Situation unter Kontrolle zu bekommen. Die Stärke dieses Kontrollbedürfnisses richtet sich sowohl nach dem subjektiven Empfinden einer Bedrohung als auch nach der objektiven Notwendigkeit des Schutzes.

Das Streben nach Sicherheit beinhaltet in erster Linie die Abwesenheit bzw. den Schutz vor tatsächlich drohenden Gefahren. Man versteht darunter auch die „objektive Sicherheit“. Dem gegenüber fühlt sich der Mensch auch dann sicher, wenn er keine Gefahr wahrnimmt oder glaubt, ihr gewachsen zu sein. Dies gilt insbesondere für Menschen, die sich ihrer Fähigkeiten sicher fühlen, d. h. ohne weitere Vorkehrung entschlossen handeln (vgl. HALLER, 1997). Hier wird von der „subjektiven Sicherheit„ gesprochen. Zum einen können in komplexen sozio-technischen Arbeitssystemen mögliche Konsequenzen aus den resultierenden Handlungen übersehen werden (vgl. POY & WEISBACH, 1994), zum anderen erhöht sich mit steigender Systemkomplexität die Anforderung der Systemsicherheit.

DÖRNER (1993) steht „einem Eingriff, der einen Teil des Systems betrifft oder betreffen soll“ kritisch gegenüber, denn dieser würde sich „immer auch auf viele andere Teile des Systems“ auswirken. Diese „Vernetztheit bedeutet, dass die Beeinflussung einer Variablen nicht isoliert bleibt, sondern Neben- und Fernwirkungen hat“ (a. a. O.; S. 60f). Die Auswirkungen sind meist unkalkulierbar. Somit beinhaltet der Begriff „Sicherheit“ im Sinne von „sich sicher fühlen“ aus individuumsbezogener Sicht eine negative Komponente der falschen Gewissheit oder Sorglosigkeit sowie eine positive Komponente der Kompetenzen und Fähigkeiten (vgl. KÜNZLER, 2002, S. 16).

Gerade in der heutigen Zeit, in der die Veränderung sozio-technischer Systeme mit rasantem Tempo voran schreitet, werden „… Gefahren der Unzulänglichkeit des Systems dem unzuverlässigen, sorglosen Menschen zugeschrieben und nicht der mangelnden Funktionstüchtigkeit des gesamten Mensch-Maschine-Systems. Die Betonung, dass v. a. der „menschliche Faktor“ das Versagen verursacht wird notwendig, um nicht Zweifel über die generelle Funktionstüchtigkeit der Systeme aufkommen zu lassen“ (KÜNZEL, 2002, S. 16). Diese Meinung wird häufig von Vorgesetzten vertreten. WENNINGER (1991) nimmt als Erklärungsansatz eine prozentuale Aufteilung von möglichen Gründen vor, welche die Non-Compliance der Mitarbeiter beschreiben soll:

- „70% Nicht-Wollen
- 20% Nicht-Wissen
- 10% Nicht-Können“

(a. a. O.; S. 52)

Bei der Idee der technischen Systemsicherheit greift KAUFMANN (1970) den Gedanken der von „menschlichen Eingriffen unabhängigen Harmlosigkeit und Zuverlässigkeit des Systems“ (a. a. O.; S. 80) auf. Damit wird das Ziel der Sicherheit von (Arbeits-) Systemen zwar von der technischen Betrachtungsweise auf das gesamte Arbeitssystem übertragen, in letzter Konsequenz jedoch durch die Schaffung von Normen, Richtlinien, Vorschriften etc. wieder auf den Beschäftigten verschoben. Diese innerbetrieblichen Verhaltensnormen – auch als Teilaspekte einer Sicherheitskultur

eines Unternehmens zu verstehen – sollen die Menschen dazu veranlassen, sich in der Organisation systemkonform und damit zuverlässig zu verhalten.

Damit nun die Sicherheit eines Arbeitssystems nicht nur eine Sachlage ist, die vielleicht irgendwann einmal erreicht wird, sehen HOYOS & RUPPERT (1993) darin eine Leistung, die durch die „Aktivitäten der Betriebsleitung, der Vorgesetzten und der Beschäftigten fortwährend erbracht werden“ (HOYOS & RUPPERT, 1993, S. 12).

Das Konzept der Systemsicherheit von HOYOS & RUPPERT (1993) basiert im Wesentlichen auf der Planung der Sicherheit und auf der präventiven Kontrolle der Gefahren und Gefährdungen während des Betriebes. Das übergeordnete Ziel besteht in einer Verbesserung der Funktionszuverlässigkeit, so dass niemand durch eine Störung zu Schaden kommt. Primäres Ziel einer präventiven Systemsicherheit ist deshalb die Vermeidung o. g. Ereignisse durch entsprechende Qualifizierung des Managements, Kompetenzbildung der Mitarbeiter und einer entsprechenden Technik- und Arbeitsgestaltung. Zur Unterstützung dieses Organisationsziels bedarf es der Einrichtung und ständigen Anpassung eines Sicherheitsmanagements und der Entwicklung einer positiven Sicherheitskultur (vgl. ZIMOLONG, 1995). Dies kann auch mit der Anforderung verbunden sein, einen geeigneten Maßstab für den Vergleich von Alternativen innerhalb der Systemgestaltung zu finden (vgl. GROTE, 1997).

Die Fragen, die sich in diesem Zusammenhang an jedes Unternehmen hinsichtlich ihrer bestehenden IT stellen lautet: „Wo liegen die Gefahren?“, „Bin ich richtig dagegen geschützt?“ und „Habe ich mich ausreichend abgesichert, falls ich etwas übersehen habe?“ Um über diese Fragen den Antworten näher zu kommen, werden im folgenden Abschnitt die begrifflichen Grundlagen dargestellt.

2.2 Informationssicherheit

Ein großer Wettbewerbsvorteil der IT resultiert aus der hohen strategischen und operativen Bedeutung bei der Erfüllung von Unternehmenszielen. Dies gilt insofern, als nahezu alle Geschäftsprozesse IT-gestützt ablaufen. Wesentliche Entscheidungen hängen von der Richtigkeit, Aktualität, Verfügbarkeit und Vertraulichkeit von Informationen ab, die mittels IT erarbeitet werden. Insbesondere werden durch die IT die Geschwindigkeit, Kapazität, Zuverlässigkeit und Flexibilität der Geschäftsprozesse gewährleistet. Um diesen Wettbewerbsvorteil effektiv nutzen zu können, ist es wichtig, auf dem vernetzten multimedialen Kommunikationsweg den Transfer von sensiblen Daten so sicher als möglich zu gestalten. Dies bedeutet, dass auf der Ebene der Organisation Bedingungen geschaffen werden sollten, die auf der einen Seite technische Standards umsetzen können und auf der anderen Seite die Mitarbeiter hinsichtlich dieser Thematik sensibilisieren und motivieren.

In diesem Kapitel wird der gesellschaftliche Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dargestellt. Es werden die relevanten Begrifflichkeiten per Definition festgelegt und allgemeine Sicherheitsziele dargestellt.

2.2.1 Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Um ein hohes Sicherheitsniveau für IT-Systeme in Organisationen zu erreichen und damit der oben genannten gesellschaftlichen Forderung sicherer IT-Systeme nachzukommen, wurde im Juni 1989 von der Bundesregierung das Zukunftskonzept IT verabschiedet. Darin verpflichtete sich die Bundesregierung, alle Betroffenen und Interessierten über Risiken, Schutzmaßnahmen in der IT und dem Zusammenwirken verschiedener Stellen (Hersteller, Sicherheitsbehörden, Anwender) zu unterrichten.

Dies zog den Entwurf eines „Rahmenkonzeptes zur Gewährung der Sicherheit bei Anwendung der Informationstechnik“, dem „IT-Sicherheitsrahmenkonzept“ nach sich, in dem erstmals konkreter Handlungsbedarf umschrieben wurde:

„Die Sicherheit von IT-Systemen gewinnt für die Funktionsfähigkeit von Wirtschaft und Staat zunehmend an Bedeutung. Maßnahmen zur Schaffung und Erhöhung dieser Sicherheit sind deshalb dringend notwendig. Die Verminderung der potentiellen Gefährdung durch geeignete Maßnahmen ist eine staatliche Aufgabe. Zur Durchführung entsprechender Risikoanalysen und der Entwicklung darauf basierender Sicherheitskonzepte bedarf es einer selbstständigen Bundesoberbehörde. Nur eine staatliche Stelle verfügt über die erforderlichen umfassenden Sicherheitsinformationen und bietet zudem Gewähr für ausreichende Neutralität. Zusätzlich kann eine selbstständige Bundesbehörde für die angestrebte bundesweite Einheitlichkeit von Sicherheitskriterien sorgen und zugleich die internationale Vereinheitlichung (z. B. durch Zusammenarbeit mit entsprechenden Behörden anderer Staaten) fördern. ...." (BGBl,1990; S. 2834 ff).

2.2.2 Aufgaben des BSI

Um ein „vernünftiges“ IT-Sicherheitsmanagement in deutschen Unternehmen einzuführen, hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) dieser Thematik angenommen. Zur Realisierung des Konzepts wurden dem BSI mit § 3 des BSI-Errichtungsgesetzes folgende Aufgaben zugewiesen:

- Untersuchung von Sicherheitsrisiken beim Einsatz von IT und Entwicklung informationssichernder Technik,
- Entwicklung von Prüfkriterien und –methoden zur Sicherheitsbeurteilung von Systemen,
- Sicherheitsbewertung und Erteilung von Zertifikaten,
- Zulassung von Systemen für den Verschlusssachenbereich (VS-Bereich),
- Herstellung von Schlüsselmitteln für im VS-Bereich eingesetzten Chiffriergerät,
- Fachliche Unterstützung des Bundesbeauftragten für den Datenschutz,
- Unterstützung von Strafverfolgungsbehörden,
- Beratung von Herstellern und Anwendern informationssichernder Techniken. (vgl. BSI, 2000)

2.2.3 Abgrenzung und Definition des Begriffs „IT“

Der Begriff „IT“ stammt aus den 80er Jahren und wurde ursprünglich für die rein technisch orientierten Betrachtungsweisen verwendet. Heutzutage wird IT salopp für alles verwendet, was in irgendeinem Zusammenhang mit den physisch-materiellen Bestandteilen von Computern (Hardware) steht (vgl. STADELMANN, 1996).

Generell muss zwischen den Begriffen (Informations-)Technologie und (Informations-)Technik abgegrenzt werden. Nach STADELMANN (1996) ergibt sich die Informationstechnologie aus dem funktionellen Zusammenschluss der Informationstechnik, d. h. Technologie setzt das Vorhandensein einer bestimmten Technik voraus. Damit kann IT als „…die Gesamtheit der anwendbaren und der tatsächlich angewendeten Arbeits-, Entwicklungs-, Produktions- und Implementierungsverfahren der Informationstechnik“ (STADELMANN, 1996; S. 134) betrachtet werden.

Das BSI spezifiziert hier auf folgende Weise:
Die „... Informationstechnik (IT) umfasst [...] alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Unter Verarbeitung von Informationen im allgemeinen Sinn fällt auch:

- die Erhebung,
- die Erfassung,
- die Nutzung,
- die Speicherung,
- die Übermittlung,
- die programmgesteuerte Verarbeitung (im engeren Sinn),
- die interne Darstellung und
- die Ausgabe von Informationen.

Die Informationstechnik beruht heute im Allgemeinen auf der digitalen Darstellung von Informationen im binären Zahlensystem als Folge der Zahlen „0“ und „1“.
(BSI, 2000; S. 297).

Nach dieser Definition beinhaltet der Begriff „IT“ sowohl Software als auch Hardware. Die funktionelle Gesamtheit bezeichnet das BSI als IT-System. Nach dem BSI besteht ein IT-System „...aus einer Kombination von Hardware und Software, die für unterschiedliche Aufgaben der Informationsverarbeitung eingesetzt werden kann. Ein besonderes Kennzeichen von IT-Systemen ist die freie Programmierbarkeit. Zu den IT-Systemen zählen typischerweise "Computer" und "Allzweck-Rechner" ("general purpose computer").

„Beispiele für IT-Systeme sind:

- Großrechner ("mainframe"),
- Abteilungsrechner und Workstation,
- Arbeitsplatzrechner (APC), Personal Computer, Laptop, Notebook oder andere Mikrocomputer,
- Bürosysteme und
- Kommunikationssysteme (Rechnernetz, Telekommunikationsanlage usw.)

einschließlich der für die Einsatzzwecke benötigten Software wie Betriebssystem-Software und Anwendungsprogramme“ (BSI; 2000; Anhang A; S. 298).

In dieser Definition liegt das Hauptaugenmerk deutlich auf der singulären Betrachtungsweise der Technik. Die funktionelle Gesamtheit von IT wird beim BSI nicht deutlich hervorgehoben. Aus diesem Grund schlägt der Autor zur weiteren Verwendung des Begriffs „IT“ die Modifikation der von STADELMANN (1996) verwendete Definition vor:

IT ist „die Gesamtheit der anwendbaren und der tatsächlich angewendeten Arbeits-, Entwicklungs-, Produktions- und Implementierungsverfahren der Informations-technik“ (modifiziert nach STADELMANN, 1996; S. 134).

Diese Definition beinhaltet die Sichtweise der vom BSI verwendeten Begrifflichkeiten „IT“ und „IT-Systeme“, nicht eingesetzte Technik wird dabei ausgeklammert. Darüber hinaus wird der Aspekt der Funktionalität von IT hervorgehoben. Die Funktionalität

resultiert dabei aus dem Austausch und der Übertragung von Daten mittels Kabel, Funkwellen oder Infrarot. Dies ist insofern für die weitere Arbeit wichtig, da sich die Sicherheitsaspekte in der IT größtenteils erst durch den funktionellen Zusammenschluss der Technik ergeben.

2.2.4 Definition und Charakterisierung des Begriffs „Sicherheit“ in der IT

Unterhält man sich mit Vertretern aus Wissenschaft und Praxis über das Thema „IT-Sicherheit“ so stellt man schnell fest, dass das Phänomen „Sicherheit“ im Zusammenhang mit dem Einsatz von elektronischen Rechnersystemen eine unklare Definitionslage beinhaltet. Folgende Begriffe werden häufig synonym verwendet: „Informationssicherheit“, „IT-Sicherheit“, „IV-Sicherheit“, „DV-Sicherheit“, „Informatik-Sicherheit“, „Datensicherheit“, „Informationsschutz“, „Computer-sicherheit“ oder einfach „Sicherheit“ (vgl. Konrad, 1998). Es folgen einige Aufzählungen und Definitionen:

- „Security: the combination of confidentiality, integrity and availability“. (European Communities /ITSEC, 1991; S. 115 in KONRAD, 1998).
- “Informationssicherheit ist (a) die Zielsetzung bzw. das Ergebnis geeigneter und ausreichender Maßnahmen (des Informationsschutzes und der –sicherung), um Informationen und ihre Verarbeitung vor Verlust, Verfälschung und unerlaubtem Zugriff zu bewahren, (b) der Maßstab für das Fehlen von Risiken und Beeinträchtigungen sensitiver Informationen und ihrer Vermeidung“ (LIPPOLD, 1992; S. 913 in KONRAD, 1998).
- „Information security: The protection of information assets from accidental or malicious unauthorized disclosure, modification, or destruction, ort he inability to process that information.“ (DEVARGAS, 1995; S. 67 in KONRAD, 1998).
- “Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).” (NIST, 1995; S.5 in KONRAD, 1998).

- "Computer Security may be defined as (1) control to ensure the continuity of adequate information and (2) protection of computing assets from loss or damage. As natural extension, the avoidance of loss or damage to other assets through information inadequacy or through abuse or mususe of computer facilities is also within the scope of this topic." (HUTT, 1995; S. 1f in KONRAD, 1998).
- "Sicherheit der Informationsverarbeitung bezeichnet eine Sachlage, bei der alle sicherheitswürdigen Belange vor Beeinträchtigungen, die im Zusammenhang mit der Informationsverarbeitung entstehen können, bewahrt sind." (STELZER, 1993; S. 23 in KONRAD, 1998).

Nach dem BSI-Errichtungsgesetz beinhaltet die Sicherheit in der IT „... die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten und bei der Anwendung von informationstechnischen Systemen oder Komponenten" (BSI; 2000; Anhang A; S. 300).

Die Sicherheitsstandards richten sich dabei nach dem Stand der Technik bzw. nach dem technisch Möglichen. Der zentrale Begriff „IT-Sicherheit", wird wie folgt definiert:

„IT-Sicherheit ist der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses IT-Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind." (a. a. O., 2000; Anhang A; S.300).

Bei der genauen Betrachtung der Definitionen wird ersichtlich, dass „Sicherheit in der IT" hauptsächlich mit Techniksystemen in Verbindung gebracht wird. In dieser Arbeit möchte der Autor sich aus dieser Betrachtungsweise lösen und ein sozio-technisches Verständnis unterstreichen.

2.2.5 Sicherheitsziele in der IT

Das Erreichen der oben genannten Informationssicherheit kann als ein holistisches Ziel betrachtet werden. Dabei können mehrer Teilziele untergliedert werden, deren Charakter in erster Linie wieder technikorientiert ist. Das resultierende IT-Sicherheitsziel lautet dabei, dass die eingesetzten Informationstechniken (Hard- und Software, Telekommunikationstechnik) wirtschaftlich effizient durch organisatorische und technische IT-Sicherheitsmaßnahmen gemäß den folgenden Grundsätzen zu schützen sind:

Integrität: Informationen können nur von Befugten in beabsichtigter Weise verändert und modifiziert werden. Außer der Unversehrtheit wird unter Integrität noch die Vollständigkeit, die Widerspruchsfreiheit und die Korrektheit der Daten verstanden.

Vertraulichkeit: Die Information ist nur Befugten zugänglich und verfügbar. Es kann kein unbefugter Informationsgewinn durch nicht zugangsberechtigte Personen stattfinden.

*Verfügbarkeit***:** Damit bezeichnet man den Tatbestand, dass Funktionen eines IT-Systems ständig bzw. innerhalb einer vorgegebenen Zeit zur Verfügung stehen und die Funktionalität des IT-Systems nicht vorübergehend bzw. dauerhaft beeinträchtigt ist.

COLE & MATZER (1999) spezifizieren dieses Spektrum und fügen noch die Begriffe „Unversehrtheit“, „Authentizität“ und „Verbindlichkeit“ hinzu. Dabei möchten sie die Begriffe folgendermaßen verstanden wissen:

Unversehrtheit: „Daten dürfen nur im Rahmen genau definierter Geschäftsprozesse verändert werden. Die Veränderungen müssen autorisiert und nachvollziehbar sein.“ (a. a. O.; 1999; S. 19)

Authentizität: Es geht „...darum: Wie stelle ich fest, dass sich mein Computer wirklich mit dem richtigen Partner unterhält?“ d. h., die Herkunft der Daten ist nachgewiesen (a. a. O.; 1999; S. 19).

Verbindlichkeit: Darunter verstehen die o. g. Autoren, dass auch „eine Übertragung von Daten stattgefunden hat, die von niemandem geleugnet wird“ (a. a. O.; 1999; S. 19).

Das BSI hat sich die Gewährleistung der oben beschriebenen Sicherheitsziele zur Aufgabe gemacht. Die darin formulierten IT-Sicherheitsmaßnahmen schützen die strategischen Planungen eines Unternehmens sowie den laufenden Geschäftsbetrieb und reduzieren die entstehenden Kosten im eventuellen Schadensfall. Sie stellen darüber hinaus die Qualität der Arbeit sicher.

2.2.6 Rechtliche Bestimmungen in der IT

Hinsichtlich der Etablierung und Förderung einer gesamtgesellschaftlichen Sicherheitskultur auf internationaler Ebene ist namentlich die Organisation für Wirtschaft und Entwicklung (OECD; Organisation for Economic Co-operation and Development) zu nennen. Die OECD hat sich zum Ziel gesetzt, die Sensibilisierung von Sicherheitsthemen bei der Entwicklung von Informations- und Netzwerksystemen bis hin zum Endanwender am Bildschirm zu fördern (vgl. OECD; 2001). Die Forderungen in den Sicherheitsrichtlinien zielen darauf ab, dass in einem Umfeld der weltweiten Abhängigkeit von Informationssystemen und Netzwerken die Entwicklung der Online-Kommunikation stabil und produktiv voranschreitet. Es werden darin „alle Anwender der Informationstechnologie, einschließlich Regierungen, Wirtschaft und Individuen“ dazu aufgefordert, „die ... Basisgrundsätze, die sich auf Gebiete wie Sicherheitsbewusstsein und Verantwortlichkeit sowie Respekt vor ethischen und demokratischen Werten beziehen, zu befolgen und umzusetzen“ (OECD-Pressemitteilung; August 2002).

Auf nationaler Ebene steht hier das Gesetz zur Kontrolle und Transparenz (KonTraG). Mit dem Beschluss des KonTraG im Unternehmensbereich hat der Gesetzgeber einen wichtigen Grundstein gelegt, um den Umgang mit Risiken bewusster zu erleben und um eine risikobewusste Unternehmenskultur entstehen zu lassen. Dabei schreibt der

Gesetzgeber nicht vor, wie das Risikofrüherkennungssystem als Baustein eines holistischen Risiko-Management-Systems auszugestalten ist.

Zur Früherkennung und damit Abwehr von Risiken sind im KonTraG folgende Umsetzungsmaßnahmen durch den Gesetzgeber enthalten:

- Etablierung eines Überwachungssystems zum Erkennen von bestandsgefährdenden Entwicklungen im Sinne der Identifikation und Analyse
- Schaffung von angemessenen Kommunikationsstrukturen, die ein frühes Erkennen der Risiken durch die Entscheidungsträger sichern.

Eine klare rechtsverbindliche Aussage von Seiten des Gesetzgebers zur Umsetzung und Einhaltung von Sicherheitsmaßnahmen am BSAP blieben bisher jedoch noch aus. Sie sind indirekt im rechtlichen Umfeld des betrieblichen Arbeits- und Gesundheitsschutzes geregelt, wie z. B. das Arbeitsschutzgesetz (ArbSchG) oder die Bildschirmrichtlinien.

Um sicherheitsgerechte Maßnahmen auf der Ebene der Organisation zu ergreifen und auf das IT-sicherheitsgerechte Verhalten der Mitarbeiter steuernd einwirken zu können, werden zwischen impliziten und expliziten Formen der Verhaltensausrichtung und –koordination in Organisationen unterschieden. In den folgenden Kapiteln wird zum einen auf die Kultur eines Unternehmens und deren Umsetzungsmöglichkeiten, zum anderen auf verhaltenssteuernde Maßnahmen durch die Mitarbeiterführung eingegangen. Damit zusammenhängend werden die Interaktionsmöglichkeiten zwischen dem Vorgesetzten und seinem Mitarbeiter und die Art und Weise, wie Verhaltenssteuerung und –konditionierung gehandhabt werden, näher betrachtet.

2.3 Sicherheit als Führungsaufgabe

Der Erfolg eines Unternehmens kann unter anderem darin liegen, wie dieses an den Wandel und die Veränderungen des Marktes angepasst ist und möglicherweise darüber hinaus den Konkurrenten einen Schritt voraus ist. Aus diesem Grund können sich Maßnahmen wie die zielgerichtete Koordination von Prozessen, Informationstechnologien und den Menschen innerhalb einer Unternehmung als günstig erweisen. Diese Aufgabe obliegt der Führungsetage. Hier werden Budgets verteilt und die Wichtigkeit von Unternehmensinhalten kommuniziert. Dies kann in Form von verbalen und nonverbalen Verhaltensweisen geschehen. Die nonverbale Kommunikation wird unter dem Thema „Unternehmenskultur“ zusammenfassend dargestellt. Die verbale Kommunikation wird hier unter dem Titel „Führungsstrategien“ erläutert.

2.3.1 Die Sicherheitskultur eines Unternehmens

Damit arbeitsaufgabenspezifische Einflussfaktoren greifen können, müssen auf der Ebene der Organisation Faktoren unterschieden werden, die auf das IT-Sicherheitsverhalten des Mitarbeiters einwirken. Die Organisation bildet eine übergreifende Instanz, die durch ihre Rahmen- & Randbedingungen und Richtlinien direkt bzw. indirekt auf den Mitarbeiter einwirkt. In den folgenden Abschnitten wird die Umsetzung der Informationssicherheit im Sinne einer Unternehmenskultur in den Betrieben sowie diverse Ansätze zur Umsetzung durch das Management dargestellt. Deren betriebliche Ausgestaltung und integratives Zusammenwirken können jedoch nur vor dem Hintergrund einer konkreten Organisation detailliert formuliert und konkretisiert werden. Doch zunächst ein paar abgrenzende Definitionen:

Nach GEBERT (1978) kann eine Organisation wie folgt definiert werden:
„Eine Organisation lässt sich als ein ihrer Umwelt gegenüber offenes System verstehen, das langfristig existiert, spezifische Ziele verfolgt, sich aus Individuen bzw. Gruppen zusammensetzt, also ein soziales Gebilde ist und eine bestimmte Struktur

aufweist, die meist durch Arbeitsteilung und eine Hierarchie von Verantwortung gekennzeichnet ist.“ (a. a. O., 1978; S. 23 In H. SCHULER; 1995; S. 48).

Die Organisationsstruktur und deren Wirkung auf das soziale Gebilde, werden unter dem Begriff „Unternehmenskultur“ zusammengefasst. Dies bedeutet, dass die Organisation eigene, unverwechselbare Vorstellungs- und Orientierungsmuster besitzt bzw. über die Jahre entwickelt. Diese prägen das Verhalten der Mitarbeiter und die betrieblichen Funktionsbereiche tief greifend (vgl. ROSENSTIEL & REGNET, 1999). Die Kultur eines Unternehmens spiegelt sich in den Wertevorstellungen, Verhaltensnormen, Denk- und Handlungsweisen, die von den Mitarbeitern der Unternehmung erlernt und akzeptiert wurden, wider (vgl. MACHARZINA, 1995).

Um (Veränderungs-)Prozesse in einem Unternehmen zu initiieren, müssen diese oft historisch gewachsenen Strukturen und Symbole begriffen und interpretiert werden. SCHEIN (1984) beschreibt in seinem Kulturebenenmodell (siehe Abbildung 2) die Beziehungen zwischen den einzelnen Kulturebenen. Diese bieten unterschiedliche Ansatzpunkte bei der Initiierung eines Veränderungsprozesses. Den Kern der Unternehmenskultur bildet nach SCHEIN (1984) die von allen Organisationsmitgliedern geteilten Basisannahmen, die sich teilweise sichtbar in bestimmten Normen und Standards sowie einem entsprechenden Symbolsystem manifestieren.

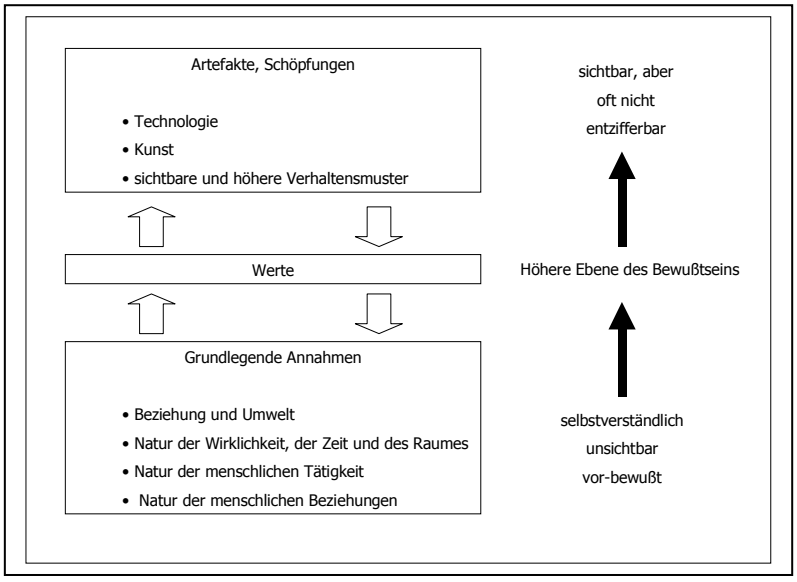


Abbildung 2: Ebenen der Unternehmenskultur nach Schein (In G. COMELLI & L. VON ROSENSTIEL, 2001; S. 275).

Die grundlegenden Annahmen bei den Mitarbeitern sind das Produkt eines jahrelangen Entwicklungsprozesses. Sie werden meist als selbstverständlich angenommen bzw. übernommen. Diese gelebten, aber nicht erlebten Annahmen stehen im wechselseitigen Austausch mit den bewussten bzw. bewusstseinsfähigen Werten, welche sich sowohl durch das nach außen gerichtete Handeln sichtbar machen als auch den Werten, die sie selbst wiederum beeinflussen. Dabei spielt der Ausprägungsgrad der grundlegenden Annahmen eine entscheidende Rolle über Erfolg bzw. Arbeitsaufwand von Veränderungsprozessen. Dies spiegelt sich in der Prägnanz, dem Ausmaß der Akzeptanz und der Tiefe der Verankerung wider (vgl. MACHARZINA 1995).

Eine Kultur ist gewachsener Natur und darf nicht den Mitarbeitern künstlich aufoktroyiert werden. Jede Art von Kultur in einem Unternehmen kann als die Seele des Unternehmens bezeichnet werden und entwickelt sich folglich aus sich selbst. Sie kann nicht gemessen, sondern muss erschlossen und interpretiert werden. Aus diesem Grund müssen die eben beschriebenen Einzelphänomene in ihrer Gesamtbetrachtung gemäß den Umweltumständen interpretiert werden. Um diesen Prozess im Unternehmen zu gestalten bzw. zu unterstützen, bedarf es zum einen einer eingehenden Organisationsdiagnose und zum anderen Führungskräfte, die den Unternehmensgedanken als Multiplikatoren transportieren.

Um die Organisation im Sinne der Unternehmensführung zu gestalten, müssen die Veränderungen auf der Verhaltensebene im Rahmen von Organisationsentwicklungs-maßnahmen organisiert werden. Dies bedarf einer systematischen und ganzheitlichen Organisationsdiagnose, die letztlich in einem kontinuierlichen Qualitätsprozess[3] mündet. Auf Basis der gewonnenen Ergebnisse kann das Unternehmen in die gewünschte Richtung geführt werden. Eine genaue Analyse der beschriebenen Kulturebenen kann hilfreich sein. Im Vordergrund stehen dabei Dokumente, Kommunikations- und Informationsstrukturen, Anweisungen sowie

[3] Für eine ausführliche Darstellung gängiger Qualitätskonzepte wird auf die einschlägige Literatur verwiesen. Z. B. GABLER (1997), LOH (1995) für das Change Management, WOMACK, JONES & ROOS, (1991) für das Lean Management, W. Edwards DEMING, Kaoru ISHIKAWA, Joseph M. JURAN, Philip B. CROSBY FÜR das Total Quality Management (TQM).

Mitarbeiterinformationen. Für die Einführung eines IT-Sicherheits-managementsystems bedeutet dies konkret, alle Mittel und Wege zu analysieren, durch die das Thema IT-Sicherheit transportiert und den Mitarbeitern zugänglich gemacht werden kann.

Der erste Schritt beinhaltet das Erarbeiten einer IT-Sicherheitsleitlinie sowohl mit den Verantwortlichen innerhalb einer Organisation, als auch mit Externen. Dies bietet mehrere Vorteile:

- Unterstützung bei der Reflexion der eigenen Arbeit.
- Einbringung der Erfahrungen externer Berater.
- Nutzung des Kenntnisstandes interner Mitarbeiter über Strukturen und Problemfelder innerhalb des Unternehmens.

Die so erstelle IT-Sicherheitsleitlinie steht den bisherigen Verfahren als Vergleichsmerkmal gegenüber, so dass schließlich eine Bewertung erfolgen kann. Gemeinsam wird nun ein IT-Sicherheitsmanagementsystem gemäß den eigenen Vorstellungen erarbeitet, implementiert und kann, so bleibt zu hoffen, einen Niederschlag auf der Verhaltensebene finden. Um diesen Schritt zu bewerkstelligen, stehen verschiedene Konzepte zur Verfügung, welche in den nachfolgenden Abschnitten beschrieben werden.

2.3.2 Führungsstrategien zur Umsetzung von Sicherheit

Um IT-sicherheitsgerechtes Verhalten im betrieblichen Alltag einzuleiten, zu fördern und stabil zu halten, stellt sich als erstes die Frage nach der Art der Aufgabe, den Aktivitäten, den vorhandenen und benötigten Kompetenzen sowie den vorhandenen bzw. neu zu schaffenden Stellen. Sind die dem sachlichen Unternehmenszweck dienenden Anforderungen erfüllt, steht des Weiteren die direkte Interaktion zwischen dem Mitarbeiter und seiner Führungskraft im Mittelpunkt des Interesses. Der zuletzt genannte Sachverhalt wird unter dem Begriff Personal- oder Mitarbeiterführung, d. h. die Führung von Menschen durch Menschen, zusammengefasst. WUNDERER (1997) versteht darunter die „zielorientierte wechselseitige Beeinflussung zur Erfüllung gemeinsamer Aufgaben in und mit einer strukturierten Arbeitssituation“ (a. a. O.,

1997, S. 3). Für ihn erfüllt die Mitarbeiterführung zwei Aufgaben: Zum einen formt die Führungskraft selbst die Rahmenbedingungen zur Gestaltung der Situation und zum anderen übt sie über die direkte situative und individualisierte Kommunikation Einfluss aus (vgl. WUNDERER, 1997). Den Hauptzweck der Führung sieht er folgendermaßen: „Sie soll dabei vor allem inspirieren, kommunizieren, interpretieren, integrieren, evaluieren, abstimmen, Prioritäten setzten, Entscheide für die Gruppe oder für einzelne treffen [...], Konflikte lösen, anerkennen und belohnen oder konstruktiv kritisieren [...].“ (a. a. O., 1997, S. 4f).

Grundsätzlich können zwei direkte Mitarbeiterführungsstrategien unterschieden werden: die explizite und die implizite Führungsstrategie. Ihnen werden die Führungsinstrumente „Zielsetzung“, „Vorbild“, „Motivation“ und „Partizipation“ zugeordnet.

2.3.2.1 Explizite Steuerungsformen

Explizite Steuerungsformen beinhalten Methoden, die das Verhalten direkt beeinflussen (z. B. wöchentliches Mitarbeitergespräch). Sie übernehmen darüber hinaus auch wesentliche Sachfunktionen wie u. a. Information, Koordination, sachdienliche Hinweise und Ressourcenverteilung. In diesem Kapitel stehen die Führungsstrategien „Vorbild“, „Zielsetzung“ und „Zielkontrolle“ im Vordergrund. Doch zunächst werden die psychologischen Funktionen von Zielsetzung und –kontrolle in Anlehnung an COMELLI & V. ROSTENSTIEL (2001) aufgezeigt. Die Autoren betonen folgende Punkte:

- „Der Mitarbeiter wird informiert. Ihm wird klar, um was es geht, was erreicht werden soll.
- Der Mitarbeiter wird motiviert. Das Ziel wird zur Herausforderung, die es durch aktives Handeln zu bewältigen gilt.
- Das Ziel ermöglicht Erfolgserlebnisse; die Erfahrung, das Ziel zu erreichen, befriedigt und stärkt das Selbstwertgefühl und das Wissen um die eigene Kompetenz, was für das künftige Verhalten von zentraler Bedeutung ist.“ (a. a. O., 2001; S.88)

Diese Komponenten finden sich in den verschiedenen Führungsmodellen wieder, die nun im Einzelnen aufgeführt werden.

2.3.2.1.1 Management by Exception

In diesem Führungsmodell entscheidet und handelt der Mitarbeiter selbständig. Der Führung wird hier die Aufgabe der Rahmengebung und Kontrolle der Leistungen zuteil, d. h. der Ermessensspielraum und die zu erfüllenden Soll-Werte werden definiert. Bei HENTZE, KAMMEL & LINDERT (1997) bezieht sich der Handlungsspielraum auf „sämtliche Routineaufgaben im weitesten Sinn“ (a. a. O., S. 641). Der Vorgesetzte greift erst bei Abweichung der Soll-Werte ein, also nur im Ausnahmefall (vgl. LOCKE & LATHAM, 1990a). Damit übergibt der Vorgesetzte den wesentlichen Teil der Arbeit in die Eigenverantwortung des Mitarbeiters und kann sich selbst auf die wesentlichen und übergeordneten Probleme seiner Arbeit konzentrieren. Allerdings muss „[...] er jederzeit durch Kontrollen über den Arbeitsablauf orientiert sein“ (WUNDERER, 1997; S. 641).

2.3.2.1.2 Management by Delegation (MbD)

Dieses Modell zielt auf eine Hierarchieverflachung und gleichzeitigen Einbindung der Mitarbeiter auf Entscheidungsprozesse ab. MbD bildet den Ansatz zur kooperativen bzw. partizipativen Führung, die den Vorgesetzten entlasten soll. Die Entscheidungsprozesse werden dabei auf untergeordnete Hierarchiestufen delegiert, wobei die Mitarbeiter lernen, Entscheidungen eigenverantwortlich zu treffen und durchzuführen.

2.3.2.1.3 Management by Objektives (MbO)

Hier nehmen die Zielkomponenten – Zielsetzung, -bindung und Feedback über die Zielerreichung – eine zentrale Position ein, wobei die Zielsetzung als „key element“ (vgl. LOCKE & LATHAM, 1984) des MbO zu sehen ist. Der Mitarbeiter wird

partizipativ in den Zielfindungsprozess mit eingebunden, wodurch die Akzeptanz durch den Mitarbeiter gefördert wird. Sinn und Zweck ist es, auf der einen Seite die Führungsspitze zu entlasten, und auf der anderen Seite die Leistungsmotivation, die Eigeninitiative und die Bereitschaft zur Übernahme von Verantwortung zu stärken, insbesondere ihre Selbstregulationsbereitschaft (vgl. MEIER, 1998; S. 212). Dieses Führungsmodell verlangt von der Organisation die Bereitschaft für einen zeitaufwändigen Planungs- und Zielbildungsprozess, wobei darauf zu achten ist, dass die Zielidentifikation auf Seiten des Mitarbeiters stattfindet und inwieweit die Ziele von anderen Abteilungen und deren Ziele abhängig sind bzw. dagegen arbeiten.

2.3.2.1.4 Zielsetzung/High Performance Cycle

In Anlehnung an dieses Führungsmodell wird die direkte Verhaltensbeeinflussung durch das Setzen oder Vereinbaren von Zielen, die Kontrolle über die Zielerreichung sowie eine regelmäßige Rückmeldung über die Ist-Leistung definiert (vgl. LOCKE & LATHAM, 1990B; SCHMIDT & KLEINBECK, 1999). Das Modell des Hight Performance Cycle wurzelt in der Zielsetzungstheorie von LOCKE (1968). LOCKE berücksichtigt in seinem Modell die Faktoren Umweltgegebenheiten, Wahrnehmungen, Kognitionen und Wertentscheidungen. Er postuliert dabei folgende Punkte:

- Das Setzen von Zielen führt dann zu besserer Leistung, je höher und je spezifischer die Ziele sind – unter Voraussetzung der Zielakzeptanz,
- Feedback ist wesentlich für die Zielerreichung (vgl. KLEINBECK, 1996; SCHMIDT, 1987),
- der Handelnde hat die Erwartung, dass eine bestimmte Handlung zu einem bestimmten Ergebnis führt (outcome-expectation) und dass er auch in der Lage ist, diese Handlung erfolgreich auszuführen (efficacy expectation),
- Die Zielsetzung wirkt dann besser, wenn sie mit Informationen über sinnvolle Handlungsstrategien verbunden ist, und
- Zielsetzung und Strategie-Informationen fördern sowohl die Anstrengung als auch das Planungsverhalten.

In Metaanalysen konnten die formulierten Aussagen bestätigt werden. Die Zusammenhänge zeigten sich gleichermaßen bei Einzelpersonen wie in Gruppen, in Feld- und Laborsituationen, bei Zielspannen differierender Zeitlänge sowie bei den unterschiedlichsten Aufgabentypen und Personengruppen der verschiedensten Kulturkreise (vgl. MENTO, STEEL & KARREN, 1987; TUBBS, 1986; LATHAM & LEE, 1986). Der größte Erfolg der Zielsetzung wird in Verbindung mit der Ergebnisrückmeldung gesehen. So nähren die Ergebnisse mehrer Untersuchungen die Annahme, dass der leistungsfördernde Effekt dann eintritt, wenn verbindliche Ziele und darauf bezogene Rückmeldung gemeinsam gegeben werden (vgl. LOCKE & LATHAM, 1990a, TUBBS, 1986; LOCKE, SHAW, SAARI & LATHAM, 1981).

In dieser Modellvorstellung bilden die Ziele und die damit verbundenen Emotionen die eigentlichen motivierenden Faktoren. Sie wirken sowohl steuernd auf das Verhalten bei der Zielausrichtung, regulieren den Energieaufwand, beeinflussen die Aufrechterhaltung des Verhaltens und wirken bei der Strategieentwicklung und –ausrichtung mit (vgl. HECKHAUSEN, 1989). HECKHAUSEN (1989) weist damit auf die verhaltenswirksame Leistung einer Zielsetzung hin. Um Zielsetzung praktikabel im Unternehmen umzusetzen, haben COMELLI & VON ROSENSTIEL (2001) eine Checkliste zur Zielvereinbarung zusammengestellt:

Checkliste zur Zielvereinbarung

- Was ist das beabsichtigte Ziel? Ist es präzise beschrieben? Was ist als Ergebnis, Endprodukt bzw. erwünschte Verhaltensweise definiert worden? (Wege zu diesen Ergebnissen sind keine Ziele!)
- Wie ist das angestrebte Ziel (Ergebnis, Endprodukt, erwünschte Verhaltensweise) zu kontrollieren?
- Wie kann man hinreichend genau feststellen, ob das Ziel erreicht wurde?
- Wie ist es messbar bzw. beobachtbar?
- Lässt sich das Ziel mit den Zielen...
  - des Mitarbeiters,
  - seiner Stellenbeschreibung,
  - seiner Abteilung und
  - seines Unternehmens vereinbaren?

- (Ggf. Zielhierarchie entwickeln: Was hat im Zweifelsfall Vorrang?)
- Wird das Arbeitsgebiet durch Ziele vollständig abgedeckt oder gibt es Lücken?
- Ist das Ziel wirklich wichtig? Was passiert, wenn es nicht erreicht wird?
- Ist das Ziel eine Herausforderung?
- Ist das Ziel positiv formuliert? („Ich soll (darf?) ...“, nicht „Ich darf nicht ...“)
- Wer muss mitwirken, um das Ziel erreichen zu können?

Abbildung 3: Worauf soll man bei der Arbeit mit Zielen achten? (In: COMELLI & VON ROSENSTIEL, 2001; S. 95).

Die o. g. Zusammenhänge konnten LOCKE & LATHAM (1984) in einem Feldexperiment bei Mitgliedsunternehmen der American Pulpwood Association empirisch untermauern und wurden auch in anderen Untersuchungen bestätigt (vgl. LOCKE, SAARI, SHAW & LATHAM, 1981). LOCKE & LATHAM (1984) betrachten das Setzen von Zielen aber auch kritisch und warnen davor, dass durch den falschen Einsatz des Führungsinstruments ein gegenteiliger, kontraproduktiver Effekt eintreten könne. Dabei zählen sie folgende Gefahren auf:

- Excessive risk talking,
- Increasing stress
- Failure, which may undermine self-confidence,
- Treating goals as cleiling rather than as minimums,
- Ignoring nongoal areas,
- Encouraging short-range thinking,
- Dishonesty and cheating. (a. a. O., S. 171f).

Zusammenfassend kann festgehalten werden, dass das Führungspersonal durch adäquaten Einsatz expliziter Führungsstrategien das Verhalten direkt und positiv – d. h. den eigenen bzw. den unternehmerischen Zielen entsprechend – beeinflussen kann. Durch das „richtige“ Herausarbeiten bzw. Vereinbaren von Zielen, entsprechender Kontrolle sowie regelmäßiger und effizienter Rückmeldung über die Arbeitsleistung, ist eine Operationalisierung dieser Führungsstrategien möglich (vgl. STAPP, ELKE & ZIMOLONG, 1999).

2.3.2.2 Implizite Steuerungsformen

Im vorherigen Kapitel wurde auf die direkte Beeinflussung der Mitarbeiter durch das Steuerungsinstrument „Zielsetzung“ eingegangen. Im nächsten Kapitel wird beschrieben, wie der Mitarbeiter indirekt dazu angeleitet werden kann, IT-Sicherheit effektiv umzusetzen. Dabei steht das Ziel im Vordergrund, IT-Sicherheit zur Selbstverständlichkeit bei allen Mitarbeitern werden zu lassen. Es werden die impliziten Steuerungsformen „Vorbild“, „Partizipation“ und „Motivation“ näher dargestellt, da erst durch die Aktivierung und Einbindung der Mitarbeiter das vorbildliche Verhalten der Vorgesetzten und der aus diesen genannten Punkten resultierenden „IT-Sicherheitskultur“ die Bereitschaft und Verantwortung des Mitarbeiters gestärkt und erhöht wird (vgl. DEDOBBELEER & BÉLAND, 1991).

2.3.2.2.1 Der Vorgesetzte als Vorbild

Die Verhaltensweisen der in einer Hierarchie höhergestellten Mitarbeiter, sollten mit den Anweisungen an die hierarchisch niedriger gestellten Mitarbeitern übereinstimmten. Ist dies nicht der Fall, wird der Vorgesetzte unglaubwürdig und seine Autorität wird durch seine Mitarbeiter in Frage gestellt. So konnte MULDER (1977) nachweisen, dass Mitarbeiter ihre in der Hierarchie höher stehenden Kollegen besonders intensiv beobachten. Das Verhalten der Führenden zeigt dem Mitarbeiter an, was wirklich bedeutsam ist und worauf das Unternehmen Wert legt. Aus diesem Grund ist es zu vermeiden, dass Vorgesetzte die zu verwirklichenden Ziele selbst nicht ernst nehmen und sie durch ihr Verhalten den Respekt der Mitarbeiter verlieren.

2.3.2.2.2 Partizipation

Mit Partizipation wird der direkte und individuelle „Einfluss, der durch aktives Teilnehmen an einem Entscheidungsprozeß ausgeübt wird“ (VROOM & JAGO; 1991, S. 15) verstanden. Die Autoren differenzieren zwischen der tatsächlichen und der wahrgenommenen Partizipation, wobei sie Letzterer die eigentliche motivierende Wirkung zuschreiben. LATHAM, EREZ & LOCKE (1988) konnten feststellen, dass

mittels partizipativer Zielfestlegung eine Erhöhung der Arbeitsmotivation stattfindet, was sich in einer verbesserten Leistung ausdrückt.

Nach FRESE & BRODBECK (1989) kann die Partizipation bei der Einführung von neuen Techniken in drei Bereichen stattfinden:

- Bei der Entscheidung, ob eine neue Technik eingeführt wird,
- bei der Entscheidung, welche neue Technik eingeführt wird,
- bei Entscheidungen, wenn die neue Technik gekauft wird, welches Training man dabei besucht, und/oder ob sich jemand zum lokalen Experten ausbilden lässt etc.

FRESE & BRODBECK (1989) sehen den Vorteil der partizipativen Führung darin, dass bei der Einführung neuer Techniken die zu erwartenden Ängste, Befürchtungen und Schwierigkeiten bei den Mitarbeitern minimiert werden. Die resultierenden Folgen bei fehlender Partizipation sehen die Autoren in Passivität, Reaktanz und Oberkonformität nach Einführung der neuen Technik. Werden die Mitarbeiter in allen Entscheidungsschritten mit einbezogen und hinreichend informiert, kann die Einführung neuer Techniken als Herausforderung betrachtet werden, wodurch:

- weniger Widerstand,
- schnellere und häufigere Anwendungen,
- ein kreativerer und aktiverer Umgang mit der Technik,
- höhere Produktivität,
- weniger Absentismus und Fluktuation und
- mehr Innovationsbereitschaft,

auch in der Zukunft zu erwarten sind (vgl. FRESE & BRODBECK, 1989; S. 41). Wie der Mitarbeiter in diesem Prozess mit eingebunden werden kann, erläutern TROY, BAITSCH & KATZ (1986) in den vier Schritten der Partizipation:

1. Schritt: Motivierung der Beteiligten und Ist-Analysen
2. Schritt: Erstellung von Alternativen zur Ist-Situation
3. Schritt: Ermittlung von Qualifikationsdefiziten
4. Schritt: Schulungsmaßnahmen

Wie wichtig partizipative Beteiligung der Mitarbeiter im Arbeitsprozess ist, wird von REGNET (1995) folgendermaßen umschrieben. „Es wird nicht länger nur gehorcht, man will auch wissen warum“ (a. a. O., 1995; S. 47). Somit erhöht der Einsatz von Partizipation sowohl im Zielsetzungsprozess als auch im Planungsprozess der Arbeitsaufgabe die Akzeptanz aller Beteiligten. Der Mitarbeiter hat dabei die Möglichkeit, „das Ergebnis mit Rücksicht auf die eigenen Interessen und Sorgen zu gestalten“ (VROOM & JAGO, 1991).

2.3.2.2.3 Motivation

Erst wenn das IT-Sicherheitsbestreben des Unternehmens von allen Beteiligten akzeptiert wurde, kann IT-Sicherheit auch im betrieblichen Alltag „gelebt“ werden. Um die Mitarbeiter zu diesem Schritt zu motivieren, wird in der Arbeitswissenschaft zwischen den Inhaltskonzepten und den Prozesstheorien unterschieden.

Die Inhaltskonzepte richten sich direkt auf die persönliche Reifung und das menschliche Wachstum in der Arbeitswelt. Sie konzentrieren sich auf die Frage nach den zentralen Motiv-Inhalten, d. h. „Wonach strebt der Mensch?“. Die bekanntesten Vertreter dieser Richtung sind MASLOW (1954) und HERZBERG ET AL. (1959), deren Modelle bzw. Theorien nun näher umschrieben werden:

Maslow´sche Bedürfnispyramide

MASLOW (1954) entwickelte eine Theorie, um die Motivationen des gesunden Menschen zu erklären. Er formulierte dabei ein Modell, bei dem der Mensch in einem Zwiespalt zwischen dem Bestreben nach Sicherheit und Defizitvermeidung auf der einen Seite und Streben nach Wachstum und Selbstverwirklichung auf der anderen Seite steht. Er zählt in seinem hierarchischen Motivationsmodell fünf Motivklassen auf, die hierarchisch bzw. pyramidenförmig übereinander stehen:

5. Bedürfnis nach Selbstverwirklichung
4. Bedürfnisse der Achtung und Wertschätzung
3. Soziale Bedürfnisse
2. Sicherheitsbedürfnisse
1. Physiologische Bedürfnisse

Bei den Bedürfnisklassen 1. – 4. spricht MASLOW (1954) von Mangel-Bedürfnissen bzw. Defizitmotiv. Die Bedürfnisse sind umso dominanter, je weiter unten sie in der Hierarchie stehen und so lange sie nicht befriedigt sind (Präpotenz-Annahme). Erst wenn eine Bedürfnisklasse befriedigt ist, d. h. nicht mehr verhaltenswirksam ist, kann die nächst höherer Stufe aktiviert werden. Die Übergänge sind dabei fließend und individuenabhängig. Sind die ersten vier Klassen befriedigt, kann das Bedürfnis nach Selbstverwirklichung wirksam werden. MASLOW spricht hier von einem Wachstums-Bedürfnis, das niemals erreicht werden kann. Das Bestreben nach Selbstverwirklichung umschreibt MASLOW (1954) wie folgt: „What a man can be, he must be“ (a. a. O., 1954; S. 102). Allerdings ist es auch möglich, dass ein Individuum bei einer Motivklasse stehen bleibt. Ist dies der Fall, erfolgt nur noch eine selektive Situationswahrnehmung und –deutung.

Besonders hervorzuheben an diesem Modell ist, dass MASLOW „den Aspekt der Selbstverwirklichung des Menschen als Zielvorstellung“ (ULICH, 2001; S. 46) formuliert. Des Weiteren wurden aufgrund seiner augenscheinlichen Plausibilität gerade im Bereich Betriebs- und Wirtschaftswissenschaft zahlreiche Diskussionen und Kontroversen ausgelöst, denen weitere Konzepte folgten oder wodurch andere Konzepte beeinflussten wurden – bis heute. Doch so sehr sich dieses Modell großer Beliebtheit erfreut, unterliegt es auch starker Kritik:

- Die Theorie ist nicht sehr präzise formuliert.
- Die Abgrenzung der einzelnen Ebenen fällt schwer.
- Oftmals treten bei der Zuordnung einzelner Motive zu den Motivkategorien Schwierigkeiten auf.
- Die fünf Motivkategorien sind in empirischen Untersuchungen nicht universell auffindbar.

- Ein Bedürfnis kann nach Erlangung der Befriedigung seiner selbst willen erwünscht und weiter verfolgt werden.

Alles in allem ist es MASLOW gelungen, die menschlichen Bedürfnisse zu kategorisieren und je nach Bedeutungsgehalt des Überlebens in eine Rangreihenfolge zu bringen. Die Bedeutung dieser pyramidenförmigen Auflistung ist wahrscheinlich erst unter Bezugnahme kognitiver Ressourcenmodelle zu erkennen. Je weniger Ressourcen man in die Befriedigung der niedrigeren Bedürfnisse stecken muss, desto mehr kognitive, emotionale und motivationale Ressourcen stehen dem Streben höher stehender Bedürfnisse zur Verfügung.

Zwei-Faktoren-Theorie von Herzberg

Eine andere Herangehensweise zeigt HERZBERG ET AL. (1959) auf. Er unterscheidet in seiner „Zwei-Faktoren-Theorie“ nicht wie MASLOW in erster Linie nach den Motivinhalten, sondern klassifiziert nach Anreizbedingungen. Er begründet die Aufteilung in zwei Faktoren mit der Dualität menschlicher Bedürfnisse (HERZBERG ET AL., 1959). So entsteht intrinsische Motivation (Inhalts- bzw. Content-Faktoren) durch die Befriedigung in der Arbeitstätigkeit selbst. Der Mitarbeiter übernimmt Verantwortung und erhält durch seine Leistung Anerkennung. Dies stellt für den Mitarbeiter Wachstumsmöglichkeiten dar. Die Inhalts-Faktoren wirken somit als Motivatoren und führen im positiven Fall zur Zufriedenheit, ihr Fehlen führt nicht zu Unzufriedenheit sondern bleibt neutral. Die Hygiene-Faktoren hingegen bewirken extrinsische Motivation. Sie beziehen sich nicht auf den Inhalt, sondern auf den Kontext der Arbeit (z. B. soziale Beziehungen, äußere Arbeitsbedingungen, Bezahlung etc.). Im positiven Fall tragen die Hygiene-Faktoren dazu bei, Unzufriedenheit abzubauen. Allerdings kann keine bewusst erlebte Zufriedenheit aufgebaut werden.

Die empirische Überprüfung der Theorie konnte diesen Zusammenhang nicht immer bestätigen. So konnte z. B. nicht befriedigend erklärt werden, warum Mitarbeiter angeben, mit ihrer Arbeit zufrieden zu sein, obwohl diese stark partialisiert ist und die Abläufe sehr einförmig sind.

Generell kann gesagt werden, dass in den eben beschriebenen Modellen der Führungskraft konkrete und praktikable Informationen und Anregungen an die Hand gegeben werden. Es wird aufgezeigt, dass das Hauptaugenmerk auf die Arbeitsinhalte gelegt werden sollte, um so den Mitarbeiter zu selbständigen und verantwortungsbewussten Arbeiten zu motivieren. Allerdings werden in den dargestellten Theorien interindividuelle Unterschiede vernachlässigt, die gerade für die Entwicklung von Arbeits- und Organisationsstrukturen von konkreter Bedeutung sind (vgl. ULICH, 1994; S. 45). Dieses Defizit kann durch die Prozesstheorien der Motivation ausgeglichen werden. Diese Modelle beschäftigen sich vor allem mit den Prozessen, die die Ausführung (oder Unterlassung), sowie die Art der Ausführung einer Handlung bestimmen und bauen in ihrer Grundannahme auf den sog. „Erwartungs-mal-Wert-Modellen“ auf. Dies bedeutet, dass menschliches Verhalten bestimmt wird von wahrgenommenen situativen Anreizen und der Wahrscheinlichkeit, mit der die betreffende Person glaubt, diese konkret vorhandenen oder vorstellungsmäßig repräsentierten Anreize erreichen zu können (vgl. LEWIN ET. AL., 1944).

Job-Characteristic-Modell von HACKMANN & OLDHAM

Für die psychologische Arbeitswissenschaft sind hier die Modelle von HACKMAN & OLDHAM (1980) mit dem Job-Characteristics-Modell und das von VROOM (1964) entwickelte VIE-Modell hervorzuheben. Die zwei Grundkonzepte unterscheiden sich lediglich hinsichtlich der Erwartungen. HACKMAN & OLDHAM (1980) verwenden in ihrem Job-Charcteristics-Modell den Faktor „Motivationspotential“. Der Wert gibt an, in welchem Ausmaß eine Tätigkeit eine hohe intrinsische Motivation, Arbeitszufriedenheit und sehr gute Qualität bewirken kann (vgl. HACKMAN & OLDHAM, 1980). Er setzt sich zum einen additiv aus den Kern-Merkmalen „Variabilität der Arbeit“, „Ganzheitlichkeit der Arbeit“ und „Bedeutungsgehalt der Arbeit und für das Leben“ zusammen. Auf Grund dieser Verknüpfung finden kompensatorische Ausgleichsmöglichkeiten statt. Zum anderen multiplizieren sie die o. g. Faktoren mit den Faktoren „Autonomie“ und „Feedback“.

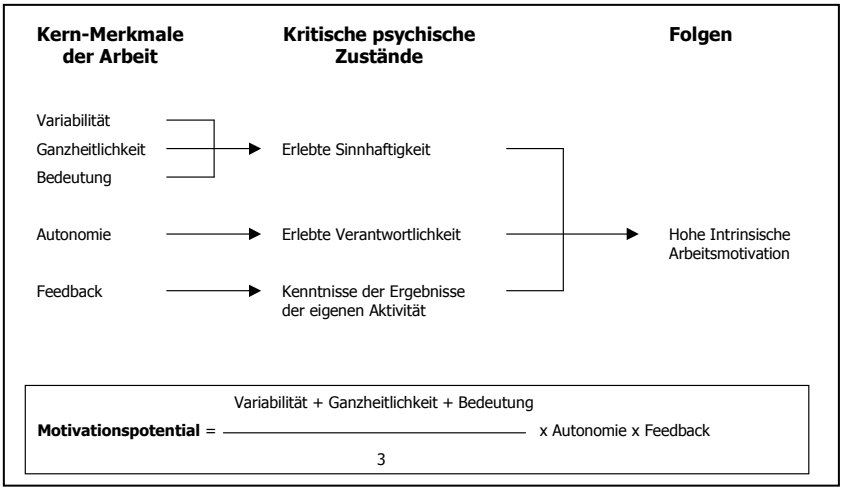


Abbildung 4: Das „Job-Characteristics-Modell" nach HACKMAN & OLDHAM (1980, S. 77F).

Diese genannten Merkmale sehen die Autoren als unabdingbare Voraussetzung für die Entstehung intrinsischer Motivation. Bei der empirischen Untersuchung konnte allerdings wegen den hohen Interkorrelationen zwischen den Kerndimensionen die Unabhängigkeit der Faktoren nicht zufrieden bestätigt werden. Des Weiteren fehlt es an einer Rechtfertigung der additiven Verknüpfung.

Valence-Instrumentality-Expectancy-Modell (VIE) von VROOM

Im „Valence-Instrumentality-Expectancy-Modell (VIE) von VROOM (1964) stehen die drei folgenden Komponenten im Vordergrund:

- Valenz (Wert)
- Instrumentalität
- Erwartung, dass eine Handlung zu einem bestimmten Ergebnis führt.

Das entscheidende Bindeglied ist die Erwartung an eine Handlung, deren Durchführung zu einem bestimmten Wert führt und der Wert auch erreicht wird. Hier siedeln sich Fragen an wie: „Wie wahrscheinlich ist ein bestimmtes Ergebnis?", „Wie wird diese Ergebnis bewertet?" Die Bewertung wird dabei von Qualitäts- und Quantitätsaspekten der Konsequenzen und dem Ergebnis beeinflusst. Situative Aspekte fließen indirekt in die „Wertigkeit" bestimmter Ereignisse mit ein. Die Gesamtmotivation ergibt sich hier aus der Summe aller Produkte von „Erwartung x

Wert“. VROOM (1964) betont jedoch, dass das Einzelergebnis im Moment nicht bedeutsam ist, wohl aber dafür langfristige Ziele.

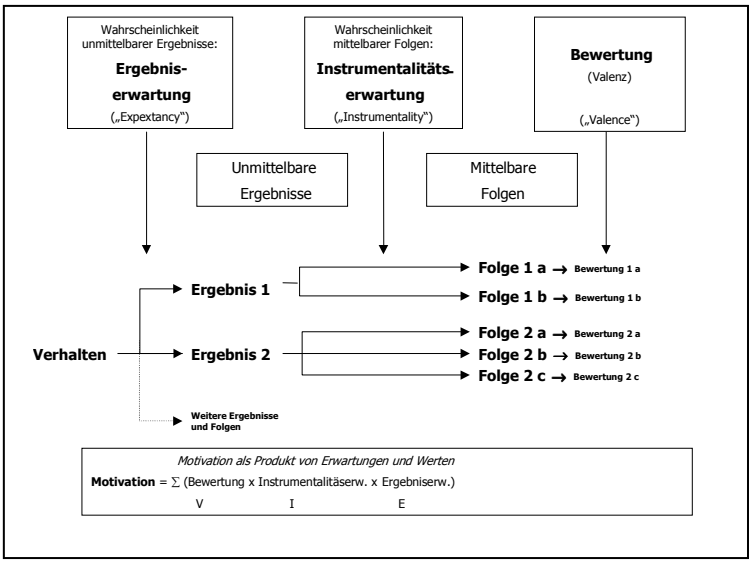


Abbildung 5: Das „VIE-Modell“ nach VROOM (1964; S. 31).

Die Hauptpunkte des VIE-Modells sind:

- Die Vorhersagen des Modells beziehen sich nicht auf die Arbeitsergebnisse (Leistungen), sondern auf motiviertes Verhalten – speziell auf Entscheidungen und auf Anstrengungen.
- Das Modell weist besonders gut auf die Bedeutung multipler Ergebnisse bzw. Folgen hin, deren Wahrscheinlichkeiten und Bewertungen interindividuell unterschiedlich sind.
- Das Modell kann als empirisch gut bestätigt angesehen werden.

So kann durch das VIE-Modell plausibel erklärt werden, warum Geld den wirksamsten einzelnen Motivationsfaktor darstellt – es kann zur Befriedigung anderer Bedürfnisse instrumentalisiert werden.

Generell kann gesagt werden, dass sich die dargestellten Prozesstheorien näher am tatsächlichen Verhalten bewegen als die Inhaltstheorien. Sie berücksichtigen die Verbindungen zwischen den Ergebnissen und deren Bewertung. In den Prozesstheorien wird darüber hinaus nicht unterstellt, dass alle Menschen von denselben Motiven geleitet werden, sondern betonen die individuellen Bedürfnisse des

Menschen. Ein Nachteil der Prozesstheorien ist jedoch, dass sie auf Grund ihrer Komplexität, geringen Handhabbarkeit und Formalisierung nur schwer in praktische Anwendung umzusetzen sind (vgl. WUNDERER, 1997; S. 145).

2.4 Risikomanagement

Mit IT-sicherem Verhalten sind nicht nur Verhaltensweisen zur direkten Gefahrenkontrolle, wie die Einhaltung von Sicherheitsvorschriften oder die korrekte Handhabung von Arbeitsmitteln gemeint, sondern auch vorbeugende Verhaltensweisen, wie sorgfältiges Arbeiten oder Ordnung und Sauberkeit am Arbeitsplatz. Die Entstehung von IT-sicherheitsgerechten Verhaltensweisen kann mit Hilfe ganz unterschiedlicher psychologischer Theorien und Modelle erklärt und beschrieben werden. In diesem Abschnitt werden verschiedene Vorgehensweisen für das Risikomanagement dargestellt. Dabei wird der Fokus auf die Empfehlung nach BSI-Grundschutz gelegt. Dies ist auch Gegenstand dieser Arbeit. Des Weiteren werden hinsichtlich des personenbezogenen, d. h. verhaltensbeeinsflussenden Risikomanagement entscheidungstheoretische und motivationspsychologische Perspektiven exemplarisch skizziert und zwei theoretische Konzepte genauer beschrieben.

Generell können zwei Arten von Strategien bzw. Vorgehensweisen beim Risikomanagement unterschieden werden:

1. Soll-Ist-Vergleich: Dieser geschieht in Form eines Abgleichs von möglichen Maßnahmen. Nach der Erfassung der Systemstrukturen und den relevanten Systembereichen, werden gängige und allgemein anerkannte Verfahren zusammengestellt und damit der IST-Zustand der Organisation erhoben. Aus dem Soll-Ist-Vergleich lassen sich die noch zu realisierenden Sicherheitsmaßnahmen direkt ableiten. Entscheidend für eine erfolgreiche Anwendung von Soll-Ist-Vergleichen sind die vorhandenen eingesetzten Sicherheitsstandards.

2. Individualanalysen: Hier wird die konkrete Ausgangssituation in einer Organisation, die vorhandenen sicherheitsrelevanten Objekte, deren Schwachstellen, die als relevant erkannten Gefahr-Objekt-Kombinationen und Konsequenzen sowie alternative Sicherungsmaßnahmen und deren Potentiale zur Risikoreduzierung analysiert und evaluiert. Dies erlaubt eine systematische und umfassende Betrachtung von Risiken, da das IT-System nicht isoliert betrachtet wird, sondern im Kontext der Organisation und den umgebenden Rahmenbedingungen. Dies hat aber auch einen erhöhten Arbeitsaufwand zur Folge.

Eine konkrete Anwendung, sowohl des Soll-Ist-Vergleichs als auch der Individualanalyse, erfolgt durch folgende Standards bzw. Konzepte:

- „Generally Accepted Principles and Practices for Securing Information Technology Systems (GASPP) vom National Institute of Standards and Technology (USA),
- "Code of practice for Information security management" (Standard 7799) des British Standards Instituion,
- Konzept „IT-Grundschutz" des BSI.

In Deutschland werden sowohl der „Soll-Ist-Vergleich" als auch die Individualanalyse mit dem Konzept „IT-Grundschutz" des BSI wesentlich beeinflusst. Es wird darin ein umfassender und detaillierter Anforderungsbedarf kleiner, mittlerer und großer Unternehmen beschrieben. Mit der Herausgabe des IT-Sicherheithandbuchs im Jahre 1992 und dessen regelmäßiger Überarbeitung wurde weiterhin ein reges Interesse zur Umsetzung von Schutzmaßnahmen in Betrieben und Privatbereichen in Gang gesetzt. Bei der Sicherheits- bzw. Schutzbedarfsermittlung folgt das Konzept einem Baukastenprinzip. So können relevante Untersuchungsbereiche herausgenommen und problemlos dargestellt werden. Die Bausteine enthalten konkrete Maßnahmenempfehlungen. Die Nichterfüllung eines Kriteriums impliziert dabei die erforderliche Maßnahmenentwicklung. Im Folgenden wird das Konzept „IT-Grundschutz" des BSI näher dargestellt.

2.4.1 BSI-Grundschutzkonzept

Dem IT-Grundschutzkonzept liegt die Idee zugrunde, dass für einen Großteil der in Behörden und Unternehmen eingesetzten IT-Systeme nur geringe bis mittlere Sicherheitsanforderungen bestehen. In diesem mittlerweile allgemein anerkannten, modular aufgebauten Kriterienwerk sind Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel formuliert, um den Schutzbedarf von IT-Systemen in Organisationen zu gewährleisten. Ausgangspunkt bildet dabei die Initiierung des Sicherheitsprozesses. Dieser beinhaltet zum einen die Erstellung von Sicherheitsleitlinien und zum anderen die Einrichtung eines Sicherheitsmanagements, dessen Kernaufgabe die Erstellung des Sicherheitskonzepts ist (vgl. BSI, 2000). In der nachfolgenden Abbildung 6 wird die prinzipielle Vorgehensweise des Sicherheitskonzepts grob schematisch dargestellt[4]:

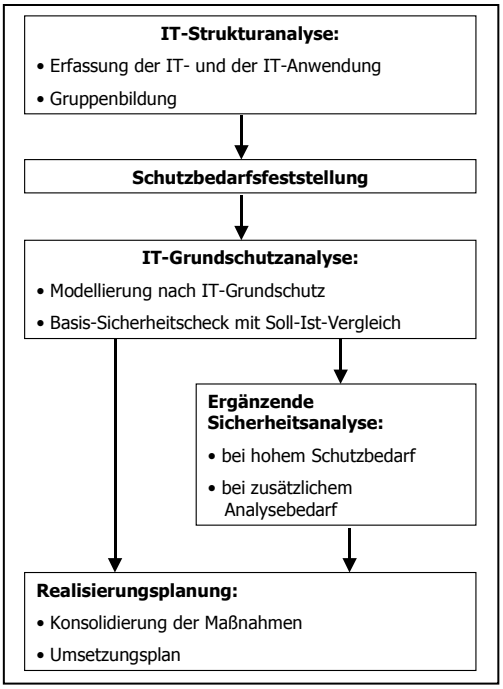


Abbildung 6: Erstellung eines IT-Sicherheitskonzepts (BSI, 2000; Kap. 2, S. 2).

Im Folgenden wird die Vorgehensweise für einen Soll-Ist-Vergleich exemplarisch dargestellt: Den einleitenden Schritt bildet die IT-Strukturanalyse. Sie dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Im Anschluss erfolgt die Schutzbedarfsfeststellung. Hier werden typische Schadensszenarien

[4] Für eine detaillierte Darstellung vgl. IT-Grundschutzhandbuch des BSI (2000).

durchgespielt, wonach sich schließlich die Schutzbedarfskategorie richtet. Dadurch leitet sich der Schutzbedarf der einzelnen IT-Systeme, Übertragungsstrecken und der zur Verfügung stehenden Räume ab. Aufbauend auf diesen Erkenntnissen, wird mit Hilfe des nach dem Baukastenprinzip erstellten IT-Grundschutzhandbuchs der betrachtete IT-Verbund nachgebildet. Die Bausteine spiegeln typische Bereiche des IT-Einsatzes wider. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren. So können mittels Ist-Soll-Vergleich die empfohlenen Standard-Sicherheitsmaßnahmen und die bereits realisierten Maßnahmen aufeinander abgestimmt werden.

Damit schließlich der IT-Sicherheitsprozess flexibel und dynamisch den Veränderungen in der Organisation angepasst werden kann, bedarf es einer kontinuierlichen Rekursion bzw. Abgleichs des erstellten IT-Sicherheitskonzepts. Durch dieses Vorgehen und der laufenden Überarbeitung des IT-Grundschutzhandbuchs durch den BSI ist die Basis für IT-Sicherheit geschaffen.

Die integrierte und pragmatisch zu nennende Vorgehensweise und die vorgeschlagenen Sicherheitsmaßnahmen aus dem IT-Grundschutzhandbuch sind tendenziell angemessen und konkret. Kritisch äußern sich POHL & WECK (1995) zum „IT-Grundschutz“ des BSI. Sie sehen darin folgende Mängel:

- Fehlende Objektivität und Bewertbarkeit durch die Notwendigkeit einer Einordnung aller Schutzbedürfnisse und Risiken in vorgegebene oder auch selbst definierte Maßstabsskalen.
- Unklarheit des verwendeten Bewertungsverfahrens und fehlende Rückkopplungs-prozesse bei der Bewertung
- Wenig Hilfe bei der Maßnahmenauswahl, vor allem für Nicht-Experten.
- Sehr hoher Aufwand des Verfahrens, vor allem bei großer IT-Landschaft.(a. a. O., S. 13).

Die Gewährleistung einer ausreichenden „IT-Sicherheit“ setzt nicht nur die Untersuchung der betrieblich verwendeten Systeme voraus, sondern auch die Bereitschaft und die ernsthafte Bekenntnis zur Umsetzung dieser IT-Sicherheitsmaßnahmen.

Im nächsten Kapitel werden Bewertungsmöglichkeiten des menschlichen Verhaltens dargestellt und diskutiert. Weiterhin wird aufgezeigt, wie IT-sicherheitsgerechtes Verhalten bei den Organisationsmitgliedern aufgebaut werden kann.

2.4.2 Personenbezogenes Risikomanagement

Gerade in risikoreichen Systemen (z. B. Chemiewerken etc.) ist es von großer Bedeutung, die Auftretenshäufigkeit von menschlichen Fehlhandlungen zu kontrollieren und damit einen möglicherweise auftretenden Schaden zu minimieren. Dies kann in Form von Sicherheitsberechnungen der Systemkomponente „Mensch“ geschehen.[5] Hierbei geht es sowohl um die Analyse potentiell fehlerhafter oder Fehler verursachender Handlungen, als auch um externe Einflussgrößen, die Auswirkungen auf die menschliche Zuverlässigkeit haben können (z. B. soziale Unterstützung, Stress, Arbeitsplatzgestaltung etc.).

2.4.3 Erklärungsmodelle menschlichen Handelns

Einer der zentralen Gegenstände in der Arbeits- und Organisationspsychologie ist die Untersuchung, Vorhersage und Veränderung menschlichen Handelns bzw. Verhaltens bei der Arbeit. Ziel dabei ist es, unter Beachtung der Kosten, der Nutzen und der Anforderung das Optimum an Qualität und Effizienz in der Arbeitsleistung zu erbringen. KASTNER & KREISSEL (1999) sprechen in diesem Zusammenhang von „Qualifizienz“ (a. a. O., 1999; S. 65). Dies setzt zunächst voraus, menschliches Verhalten bei der Arbeit zu beobachten. Danach werden die Ergebnisse analysiert und

[5] HOLLNAGEL (1998) gibt dazu eine aktuelle und ausführliche Übersicht und Beurteilung der verschiedenen gebräuchlichen Methoden der menschlichen Zuverlässigkeit.

mittels verhaltenssteuernder Konzepte und Theorien erklärt. Erst dann kann das individuelle Verhalten mittels organisatorischer Maßnahmen beeinflusst werden.

Entscheidungstheoretische Ansätze, wie die subjektive Erwartungsnutzentheorie (SEU-Theorie = Subjective Expected Utility Theory) (vgl. SAVAGE, 1954) oder neuere Varianten des Ansatzes in Form der Prospect-Theorie (KAHNEMANN & TVERSKY, 1979) bzw. der Regret-Theorie (vgl. BELL, 1982), setzen der Handlung eine rationale Entscheidungsfindung voraus. Entscheidungsgrundlage ist die Beziehung zwischen dem Nutzen und den Wahrscheinlichkeiten unterschiedlicher Handlungsalternativen. Ziel ist es hierbei, eine persönliche Nutzenmaximierung herbeizuführen.

Während entscheidungstheoretische Ansätze beschreiben, dass eine bestimmte Handlungsalternative einen Nutzen für eine Person hat, sind es die motivationspsychologischen Theorien, die erklären, warum etwas einen bestimmten Wert besitzt (vgl. HECKHAUSEN, 1989). Die Motivation ist dabei als Interaktionsprozess zwischen dem Aufforderungscharakter einer Situation auf der einen Seite und den Motiven der Person auf der anderen Seite zu verstehen. Dabei bietet der Aufforderungscharakter der Situation einen bestimmten Anreiz zum Handeln und die Motive der Person können als überdauernde Dispositionen verstanden werden, die sich hinsichtlich einer bestimmten Klasse von Handlungszielen unterscheiden lassen. Zentrale Bestimmungsgröße des Handelns ist das Produkt aus Anreiz und Erwartung. Dieses Verhältnis kann über Lernprozesse beeinflusst und verändert werden.

Eine Reihe von sozial kognitiven Theorien betrachtet die Bildung einer Absicht als notwendige Voraussetzung für die Verhaltensausführung. Das „Prozessmodell präventiven Handelns“ von WEINSTEIN (1988) bezieht sich auf konkretes präventives Verhalten zur Vorbeugung bestimmter Gefahren und Erkrankungen. Ähnlich wie das Health Belief-Modell (vgl. WEINSTEIN, 1988) wird das Konstrukt der Vulnerabilität (Verwundbarkeit) fokussiert. Um den Prozesscharakter des Modells zu betonen, wird das Vulnerabilitätskonstrukt in drei zeitliche, aufeinander folgende Phasen unterteilt,

die sich aus dem Wissen über die Gefahr, eine Bewertung der Folgen und die Einschätzung der Effektivität eigenen Vorsorgeverhaltens ergibt.

Phase 1 ist durch das Fehlen von Informationen und Erfahrungen gekennzeichnet. Wird dieser Mangel durch entsprechenden Input kompensiert, kommt es zum Übergang in die zweite Phase. Hier steht die wahrgenommene Verwundbarkeit anderer Menschen im Vordergrund. Der Übergang von der zweiten zur dritten Phase wird durch eine „optimistische Verzerrung" initiiert. Nach SCHWARZER (1996) liegt eine optimistische Verzerrung (optimistic bias) dann vor, „…wenn es darum geht, die persönliche Wahrscheinlichkeit für das Eintreffen einer Gefahr anzugeben, dann unterschätzt man sie leicht, indem man glaubt, man sei weniger verwundbar als andere Leute" (a. a. O.; S. 57). Fühlt man sich durch individualisierte Informationen direkt angesprochen, so befindet man sich in der dritten Phase. WEINSTEIN (1988) überträgt diese dreiphasige Abfolge des Konstruktes „subjektive Verwundbarkeit" auch auf die Konstrukte „eingeschätzter Schweregrad" und „Handlungswirksamkeit".

Den drei Phasen und den drei Konstrukten liegt ein hierarchisches Verständnis zugrunde. Dabei steht der Entwicklungsaspekt von Überzeugungen im Vordergrund. Erst wenn eine bestimmte qualitative Stufe erreicht ist, werden Überzeugungen zu einer Absicht, und erst wenn eine Reihe von Barrieren oder Kosten-Nutzen-Abwägungen beseitigt bzw. vollzogen worden sind, kommt es schließlich zur Handlungsausführung.

2.4.3.1 Die Handlungsregulationstheorie

Die Wurzeln der Theorie gehen auf die Ideen der russischen Tätigkeitspsychologie zurück. Sensu HACKER (1986) ist die allgemeine Handlungstheorie als „Theorie der psychischen Regulation von Arbeitstätigkeiten" zu verstehen. Um die innere Struktur des Handelns abzubilden, entwickelte HACKER (1973) ein Modell der psychischen Regulation des Handelns mit folgenden Grundannahmen:

Die Arbeitstätigkeit ist eine zielgerichtet-volitive Tätigkeit: Die Arbeitstätigkeit bildet eine funktionelle Einheit, bestehend aus motivationalen, willensmäßigen und kognitiven Vorgängen und den damit verbundenen auszuführenden Bewegungen. Damit ist sie dem Akteur bewusst (vgl. VOLPERT, 1987; HACKER, 1986; MARX, 1962). Die Initialisierung findet durch Übernahme eines objektiven Arbeitsauftrags statt. Dabei fließen individuelle Bewertungen aufgrund der mitgebrachten Fähigkeiten, Fertigkeiten, Einstellungen, Bedürfnisse, Wertvorstellungen usw. bei der Redefinition (vgl. HACKMAN & OLDHAM, 1980) der Arbeitsaufgabe mit ein; genauer gesagt, sollte schon vor dem Vollzug der Tätigkeit eine relativ stabile und invariante Vorstellung mit den entsprechenden Handlungsprogrammen „im Kopf" vorhanden sein. Man spricht hier vom „operativen Abbildsystem" (OAS) (vgl. HACKER, 1998).

Die Arbeitstätigkeit ist sequentiell-hierarchisch (bzw. heterarchisch) organisiert: Damit ist zu verstehen, dass die durch menschliche (Arbeits-)Tätigkeit angestrebten Ziele in einem Über-, Neben- und Unterordnungsverhältnis (multi-level-multi-goal-Konzept) stehen. Aus dieser Hierarchie von Zielen werden Handlungen abgeleitet und sequentiell abgearbeitet. Je weiter oben ein Ziel in der Hierarchie steht, desto komplexer und allgemeiner ist es. Da mit den Zielen stets aktivations- und inhaltsbezogene Motivationsprozesse verknüpft sind, „ist die heterarchisch bzw. hierarchisch-sequentielle Organisation der Tätigkeit sowohl kognitiver als auch motivationaler Art" (HACKER, 1998; S. 221). Die subjektive Bedeutung der Arbeitstätigkeit liegt in der Zielannäherung und letzten Endes in der Zielerreichung (siehe Abbildung 7, mit Z_0 als Oberziel).

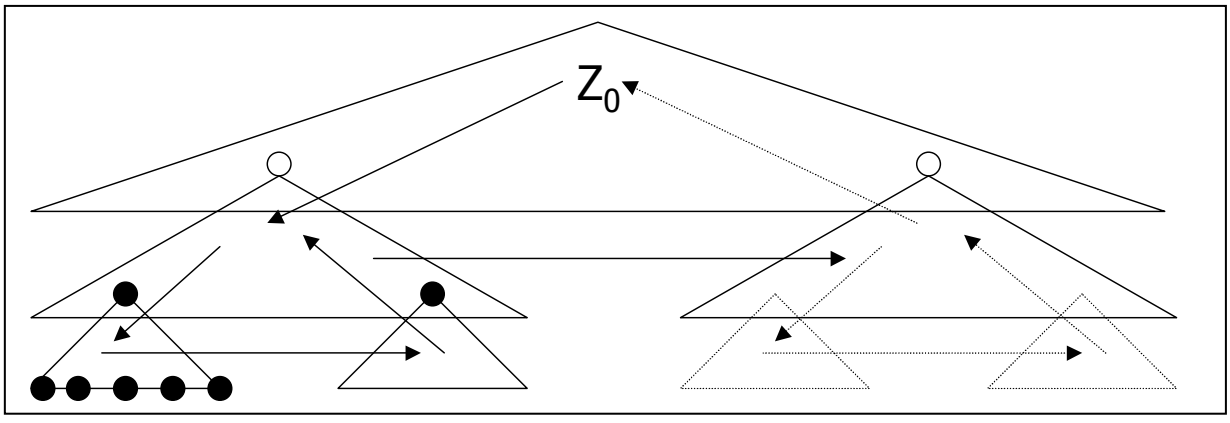


Abbildung 7: Die hierarchisch-sequentielle Organisation (nach VOLPERT, 1982; In K. LEITNER, 1999; S. 9).

Die Rückmeldung der Handlungsergebnisse: Zielgerichtetes Handeln folgt dem Prinzip eines Regelkreises, d. h., nachdem die Handlung ausgeführt ist, werden die erreichten Ist- mit den angestrebten Soll-Zuständen verglichen und ggf. an das gewünschte Arbeitsergebnis angepasst. Die regulativen Funktionseinheiten werden TOTE-Einheiten (Test-Operate-Test-Exit-Einheit) (vgl. MILLER ET. AL, 1973), VVR-Einheiten (Vergleichs-Veränderungs-Rückkoppelungseinheiten) (vgl. HACKER; 1998) oder zyklische Einheiten (vgl. VOLPERT, 1982) genannt. Sie stellen die Basis der Handlungsregulation dar, weil dadurch Korrekturen der Zielprioritäten und der Programme ermöglicht werden können. Die Zielannäherungsprozesse haben „einen erheblichen Einfluss auf die Einstellung, das Befinden und das Selbstwerterleben sowie auf die Leistungen“ (HACKER; 1998; S. 235).

Das Menschliche Handeln ist in gesellschaftliche Zusammenhänge eingebunden: Der Mensch als soziales Wesen zeichnet sich durch die Kommunikation und Kooperation mit anderen aus, wobei die Art und Weise sowie der Inhalt durch gesellschaftlich-geschichtliche Situationen geprägt ist (vgl. VOLPERT; 1982). Auch die entwickelte individuelle Handlungsregulation sieht HACKER (1998) als Ergebnis der Aneignung gesellschaftlich angehäufter Erfahrung. Daher ist eine Analyse gesellschaftlich bestimmter Handlungsmöglichkeiten und –einschränkungen für die Untersuchung der psychischen Struktur des Handelns unabdingbar.

Mit dem Modell der Handlungsregulation ist es möglich, die „übergreifenden Strukturen und Prozesse der kognitiven Handlungsregulation zu erfassen“ (SCHULER, 1995; S. 215). Das Modell der Handlungsregulation steht in einer langen Tradition und findet allgemeine Anerkennung. Allerdings ist sie auch starker Kritik ausgesetzt. GREIF (1994) und VOLPERT (1992) fassen folgende Kritikpunkte zusammen:

- Es fehlt eine übergreifende Darstellung des Modells zur Theorie.
- Es findet eine Fokussierung auf körperliche Arbeit statt.
- Teilweise entsprechen die Formulierungen den Thesen einer Tautologie.
- Motivationale Aspekte der Handlung werden teilweise unzureichend berücksichtigt.
- Der soziale Kontext der Handlung wird unzureichend berücksichtigt.

- Nicht-rationale Handlungen werden unzureichend erklärt.
- Menschliches Handeln orientiert sich nicht permanent an Plänen und Zielen.

Bei diesem Modell der Handlungsregulation hat der Mitarbeiter die Möglichkeit, Entscheidungen und Ziele selbständig zu treffen bzw. zu setzten und er verfügt über die Ergebniskontrolle. Damit übernimmt er die volle Verantwortung für sein Vorgehen und hat hinsichtlich seiner Tätigkeitsausführung freie Wahl, d. h. er muss selbständig, kreativ und schöpferisch sein. Somit liefert die Handlungsregulationstheorie Aussagen über den Grad der Bewusstheit einer Handlung, allerdings werden dahinter liegende Motive weniger berücksichtigt. Dies soll mit einer Theorie erfolgen, deren Nutzen bereits vielfach empirisch belegt worden ist.

2.4.3.2 Die Einstellungs-Verhaltens-Forschung

Die anfangs in diesem Abschnitt beschriebene Aufgabe widmet sich u. a. der Einstellungs- und Verhaltens-Forschung mit ihrer nunmehr über 70-jährigen empirischen Forschungstätigkeit. Im Mittelpunkt ihres Interesses stehen zwei zentrale Grundfragen:

- Wann und durch welche Umstände wird das Verhalten durch Einstellungen gesteuert?
- Wie bzw. durch welche Prozesse wird das Verhalten durch Einstellungen gesteuert?

Zur Beantwortung dieser Fragen kann der Verhaltensprozess aus drei Perspektiven gesehen werden:

1. Die Bildung von Verhaltensabsichten ist ein durch die Einstellung bewusst intendierter Prozess: Hierunter fallen die in dieser Arbeit näher erläuterte Theorie von FISHBEIN & AJZEN (1975) bzw. deren Erweiterung durch AJZEN & MADDEN (1986).

2. Verhalten wird automatisch durch Einstellungen gesteuert: Dieser Betrachtungsweise widmet sich FAZIO (1986) mit seiner „Theorie des automatischen Einstellungs-Verhaltens-Prozesses“. FAZIO (1990) geht in seinem Modell davon aus, dass Einstellungen durch Erfahrung im Gedächtnis bewertet und gespeichert wurden. Je nach Stärke dieser gespeicherten Objekt-Bewertungs-Assoziation wird von Hinweisreizen in der Situation ausgegangen, welche eine Einstellung automatisch aktivieren und somit verhaltensbestimmend wirken. Fazio spricht in diesem Zusammenhang von „Einstellungszugänglichkeit“ („attitude accessibility“). Diese ist maßgeblich für die Stärke der Einstellungs-Verhaltens-Relation. Ursprünglich sah FAZIO (1986) sein Modell unvereinbar mit der „Theorie des geplanten Verhaltens“ von AJZEN & MADDEN (1986), in der die Einstellungs-Verhaltens-Relation ein willentlicher Prozess ist. Diesen Standpunkt gab er später auf und räumt ein, dass der Einstellungs-Verhaltensprozess sowohl bewusst, als auch automatisch ablaufen könne (vgl. BAMBERG ET AL. (1996).

3. Ein bestimmtes Verhalten zeigt sich nur bei Personen mit bestimmten Dispositionen: Siehe dazu die Arbeiten von SHETH (1974) über die Typologie von Wahlmechanismen zur Erklärung repetitiven Wahlverhaltens.

Um das Mitarbeiterverhalten in Bezug auf „IT-sicherheitsgerechtes Verhalten“ sinnvoll und ökonomisch zu erheben, zu erklären und schließlich im Sinne der Unternehmensziele zu verändern, wird auf die „Theorie des geplanten Verhaltens“ von AJZEN & MADDEN (1986) zurückgegriffen. Diese erhebt den Anspruch, eine allgemein gültige Theorie zur Erklärung jeglichen Verhaltens zu sein (VGL. BAMBERG ET AL., 1999). Darüber hinaus stellt sie einen theoretischen Ansatz dar, mit dessen Hilfe die durch die Situation determinierten Verhaltensweisen analysiert werden können und bietet damit einen direkten Ansatzpunkt für die systematische Entwicklung und Evaluation von Interventionsmaßnahmen. In der Vergangenheit wurde die Theorie hauptsächlich in dem Bereich „Gesundheits- und umweltgerechtes Verhalten“ eingesetzt. Die darin postulierten Zusammenhänge konnten größtenteils empirisch belegt werden (vgl. DEVRIES, KIJKSTRA & KUHLMAN, 1988; FREY, STAHLBERG &

GOLLWITZER, 1993; SCHIFTER & AJZEN, 1985; BAMBERG & LÜDEMANN,1996; BAMBERG, 1996; SIX & ECKES, 1996; REINECKE, SCHMIDT & AJZEN, 1997).

Theorie des geplanten Verhaltens

Der in dieser Arbeit entwickelte Fragebogen greift u. a. auf die „Theorie des geplanten Verhaltens“ (Theory of Planned Behavior) von AJZEN & MADDEN (1986) zurück, da deren Nutzen bereits vielfach empirisch belegt worden ist. Die Theorie stellt eine Weiterentwicklung der ursprünglich entwickelten „Theorie des überlegten Handelns“ (Theory of Reasoned Action) von FISHBEIN & AJZEN (1975) dar. Als rationale Handlungstheorie wird darin der Mensch als vernunftgesteuertes Wesen betrachtet, der Informationen aus seiner Umwelt bewusst verarbeitet. Er reflektiert seine Verhaltensweisen und Handlungen über den subjektiv wahrgenommenen Nutzen, d. h., sein Verhalten steht unter der vollständigen willentlichen Kontrolle, wobei jedoch die dafür verwendeten Informationen nicht auf ihren Wahrheitsgehalt und deren Vollständigkeit[6] überprüft werden. Diese Kosten-Nutzen-Rechnung erfolgt in Abhängigkeit der zu erwartenden Konsequenzen und dem sozialen Druck, sich entsprechend den Erwartungen bedeutsamer Bezugspersonen konform zu verhalten.

Die „Theorie des geplanten Verhaltens“ stimmt hinsichtlich ihres Menschenbildes mit der „Theorie des überlegten Handelns“ überein, versucht jedoch, in ihrer Erweiterung die Schwachstellen des „Vorgängers“ ausgleichen. Im Folgenden werden zuerst einzelne Kritikpunkte der Ursprungstheorie von JONAS & DOLL (1996)[7] aufgezählt und es wird darauf eingegangen, wie ihnen begegnet wurde, bevor auf die „Theorie des geplanten Verhaltens“ Bezug genommen wird.

Postulate der „Theorie des überlegten Handelns“, Kritik daran und Einfluss auf die „Theorie des geplanten Verhaltens“:

[6] Aufgrund der Begrenztheit kognitiver Verarbeitungskapazität, berücksichtigt der Mensch in der Regel nur 5-9 für ihn subjektiv bedeutsame Verhaltenskonsequenzen (vgl. BAMBERG & SCHMIDT 1999).
[7] Eine sehr übersichtliche Darstellung der detaillierten Kritikpunkte und die daraufhin erfolgten Erweiterungen findet sich in JONAS & DOLL (1996) S.20f.

1. „Der Geltungsbereich [...] erstreckt sich auf willentlich kontrolliertes Verhalten [...]": (JONAS & DOLL, 1996; S. 19), d. h. es besteht bei der betreffenden Person eine Intention zur Ausführung dieses Verhaltens. Bei dieser Betrachtung werden zum einen keine zusätzlichen Ressourcen (z. B. Zeit, finanzielle Mittel, Fähigkeiten, soziale Unterstützung etc.) zur Verhaltensausführung vorausgesetzt und zum anderen beschränkt sich die Anwendung auf motivationsabhängige Verhaltensweisen wie z. B. Wahlentscheidungen in experimentellen Spielen oder Stimmabgabe bei politischen Wahlen (vgl. LISKA, 1984). Doch wird häufig auf die o. g. Ressourcen zur Ausführung einer Handlung zurückgegriffen (vgl. REINECKE, SCHMIDT & AJZEN, 1997). Um diesem Kritikpunkt entgegenzutreten, wurde das Modell um das Konstrukt „wahrgenommene Verhaltenskontrolle" erweitert. Es spiegelt die Selbsteinschätzung der Person über den Schwierigkeitsgrad einer Verhaltensausführung wieder. Diese Reflexion erfolgt anhand kontrollrelevanter internaler Faktoren (die o. g. Ressourcen) und externen Variablen (z. B. Hindernisse). Somit wird Verhalten nicht mehr ausschließlich durch motivationale Faktoren determiniert. Diese Erweiterung führt zu einer Verbesserung der Vorhersage von Verhalten und Intention (vgl. JONAS & DOLL; 1996). Trotz dieser Erweiterung bleiben noch Lücken zu schließen. So kritisieren BAGOZZI & YI (1989), dass spontanes, nicht intentioniertes Verhalten weiterhin nicht erklärt werden kann. Nach ihren Untersuchungsergebnissen kann Einstellung direkt in Verhalten münden, ohne eine Intention auszubilden. Dies ist vor allem vom affektiven Impuls der Situation abhängig (vgl. BAGOZZI & WARSHAW, 1992). Des Weiteren reicht die erweiterte Theorie nicht aus, habituelles Verhalten zu erklären. Das Hauptaugenmerk der Theorie richtet sich auf „erstmalig bzw. selten durchgeführte Verhaltensweisen, bei denen der Einfluss kontrollierter kognitiver Prozesse maximal ist" (JONAS & DOLL, 1996; S. 22).

2. Intention wird definiert als die subjektive Wahrscheinlichkeit einer Person, mit der sie annimmt, das Verhalten zu einem späteren Zeitpunkt durchzuführen (AJZEN & FISHBEIN, 1980): Diese Begriffsdefinition wird als unbefriedigend betrachtet, da die ihr zugrunde liegende Entschlossenheit zur Durchführung einer bestimmten Handlung nicht zum Ausdruck kommt (vgl. JONAS & DOLL, 1996; GOLLWITZER, 1993; WARSHAW & DAVIS, 1985; HECKHAUSEN, 1989; KUHL, 1985). Diesem Kritikpunkt

wird durch Abwandlung der Intentionsdefinition entsprochen. Intentionen werden nicht mehr als subjektive Wahrscheinlichkeiten betrachtet, sondern als „indicators of how hard people are willing to try, of how much of an effort they are planning to exert“ (AJZEN, 1991; S. 181), d. h., es wird die bewusste Absicht verstanden, eine Verhaltensweise unter Aufwendung aller zu Verfügung stehenden physischen und psychischen Energien und Ressourcen auszuführen.

3. Mangelnde Suffizienz der „Theorie des überlegten Handelns“: Da FISHBEIN & AJZEN (1980) nur die hinreichenden Determinanten von Intention bzw. Verhalten spezifizieren, schließen sie eine andere verhaltensbeeinflussende Variable aus. Es wurden aber in empirischen Untersuchungen darüber hinaus verhaltensbestimmende Variablen wie „Selbstdefinition“ (SPARKS & SHEPAHERD; 1992), „Rollenidentität“ (CHARNG ET AL.; 1988), „Moralvorstellung“ (BECK & AJZEN, 1991) und „antizipiertes Bedauern“ (MANSTEAD & PARKER; 1995). gefunden. Des Weiteren reicht das Modell nicht aus, Verhalten mit mehreren Verhaltensalternativen ausreichend vorherzusagen. Dieser Punkt wurde auch im erweiterten Modell nicht mit berücksichtigt. SIX & ECKES (1996) konnten in einer Metaanalyse in der Einstellungs-Verhaltens-Forschung höhere Einstellungs-Verhaltens-, Einstellungs-Intentions- und Intentions-Verhaltens-Korrelationen für Verhaltensweisen mit dichotomer Wahlmöglichkeit gegenüber polytomen Alternativen aufzeigen. Aus diesem Grund plädiert AJZEN (1991) für eine Aufgabe des Suffizienzprinzips, um so der Einstellungs-Verhaltens-Forschung den Weg für Erweiterungen zu ebnen.

Um die Kritikpunkte der „Theorie des überlegten Handelns“ und deren Modifikation besser zu verstehen, soll nun auf die „Theorie des geplanten Verhaltens“ auf der Modellebene näher eingegangen werden:

Damit eine nicht unter vollständiger willentlicher Kontrolle stehende Handlung ausgeführt wird, muss nach AJZEN & MADDEN (1986) zuerst die Intention (Absicht) zur Ausführung dieser Verhaltensweise gegeben sein. Diese Absicht wird von den Faktoren „positive Einstellung zu dieser Verhaltensweise“, „subjektive Normenvorstellung“ und „Verhaltenskontrolle“ determiniert. Diese drei

Determinanten sind konzeptionell unabhängig und werden wiederum von kognitiven Antezedentien (vgl. SCHWARZER, 1996) bestimmt:

Die *Einstellung* als global-affektive Bewertung der Verhaltensweise setzt sich multiplikativ zusammen aus der Ergebnisbewertung – d. h. subjektive Bewertung der Konsequenz bei der Ausführung einer Verhaltensweise von dem Handelnden – und der Überzeugungsstärke – d. h. ähnlich wie in den Erwartung-mal-Wert-Modellen, geht es hier um die Einschätzung der Wahrscheinlichkeit, dass ein bestimmtes Verhalten zu einem bestimmten Ergebnis führt.

Die Bestimmungsgröße *Subjektive Norm* wird determiniert durch die Faktoren normative Überzeugung – d. h., die subjektive Wahrnehmung des eigenen Verhaltens wird bestimmt durch die Erwartungen relevanter Personen- bzw. Vergleichsgruppen und der Einwilligungsbereitschaft zur Konformität mit dieser Gruppe.

Die letzte Komponente *Verhaltenskontrolle* beinhaltet als Persönlichkeitsdisposition die Überzeugung einer Person, dass eine Handlung erfolgreich ausgeführt werden kann. Diese Überzeugung basiert auf der subjektiven Einschätzung eigener Fähigkeiten und Gelegenheiten. Sie bilden eine unabdingbare Voraussetzung, um eine Verhaltensausführung zu veranlassen. Die Verhaltenskontrolle von AJZEN & MADDEN (1986) zeigt starke Gemeinsamkeiten mit dem Konzept der „Selbstwirksamkeit“ von BANDURA (1977). Darin bezieht BANDURA (1977) die Kontrolle auf die subjektive Verfügbarkeit einer wirksamen Handlung. Allerdings werden in der Theorie des geplanten Verhaltens interne und externe Faktoren gleichermaßen berücksichtigt, dabei wird nicht eindeutig zwischen wahrgenommener und tatsächlicher Kontrolle unterschieden.

Die folgende Abbildung 8 soll die beschriebenen Zusammenhänge veranschaulichen:

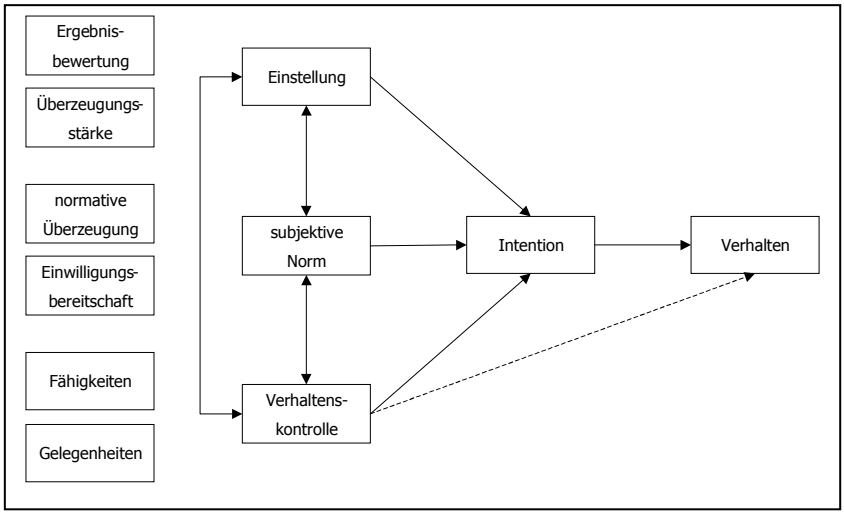


Abbildung 8: Theorie des geplanten Verhaltens nach AJZEN & MADDEN (1986; S. 458).

Die Einleitung eines bestimmten Verhaltens kann in diesem Modell über die Bestimmungsgrößen Einstellung, subjektive Norm und Verhaltenskontrolle zum einen über den Weg der Intention zum Verhalten erfolgen, wobei keine Intention zur Verhaltensausführung erfolgt, wenn eine Person ein bestimmtes Verhalten aufgrund fehlender Ressourcen oder mangelnder Fähigkeiten nicht ausführen kann. Die Intention selbst erfolgt durch eine Absichtserklärung, ein entsprechendes Verhalten zu zeigen. Zum zweiten kann Verhalten direkt durch die Verhaltenskontrolle initiiert werden. Dabei muss die wahrgenommene Verhaltenskontrolle mit der realen Verhaltenskontrolle übereinstimmen.

Insgesamt kann gesagt werden, dass diejenige Verhaltensweise ausgeführt wird, die mit den meisten positiven Handlungskonsequenzen verbunden ist und deren Ausführung am einfachsten zu bewerkstelligen ist. Um nun Veränderungen beim Verhalten herbeizuführen, müssen die subjektiv wahrgenommenen und auf das eigene Verhalten bezogenen Konsequenzen verändert werden, die nicht den Unternehmenszielen entsprechen. Konkret bedeutet dies, die zugrunde liegenden Interventionsmaßnahmen sind zum einen in der Einstellung zugrunde liegenden behavioralen Überzeugungen zu finden. Zum anderen kann das menschliche Verhalten über die Bereiche der „normativen Überzeugung“ und der „Kontrollüberzeugung“, in die gewünschte Richtung gelenkt werden. BAMBERG & SCHMIDT (1999) stellen

ausführlich die detaillierte Beschreibung dar, wie die „Theorie des geplanten Verhaltens“ bei der Entwicklung von Veränderungsmaßnahmen gehandhabt werden soll:

- „Erhebung der bedeutsamen behavioralen, normativen und Kontrollüberzeugungen mit einer qualitativen Vorstudie in einer für die Zielpopulation repräsentativen Stichprobe.
- Auf der Basis dieser in der Vorstudie ermittelten Überzeugungen wird ein standardisierter Fragebogen zur Messung der „Theorie des geplanten Verhaltens“-Konstruktes entwickelt. Die mit diesem Instrument in der Hauptstudie erhobenen Daten werden dazu benutzt, um die Überzeugungen zu ermitteln, die Personen, die die Ausführung der interessierenden Verhaltensweise beabsichtigen, von Personen zu unterscheiden, die die Ausführung dieses Verhaltens nicht beabsichtigen. Ein zweites Ziel dieser Analyse besteht darin, den jeweiligen Einfluss von Einstellung, Norm und Verhaltenskontrolle auf die Intentionsbildung zu bestimmen.
- Auf der Basis dieser Informationen wird eine entsprechende Interventionsmaßnahme konzipiert. Die Interventionsmaßnahme sollte auf eine Veränderung der bedeutsamen Überzeugungen abzielen, in denen sich Personen, die die Verhaltensausführung beabsichtigen, am stärksten von Personen unterscheiden, die diese Verhaltensausführung nicht beabsichtigen. Neben der Strategie, die Wahrnehmung der bereits von einer Person mit der Verhaltensausführung verbundenen bedeutsamen Konsequenz zu beeinflussen, kann auch versucht werden, bisher von einer Person nicht berücksichtigte Verhaltenskonsequenzen subjektiv bedeutsam zu machen.“ (a. a. O., 1999; S. 28).

Insgesamt ist es schwierig, das „Einstellungs“-Konstrukt befriedigend zu definieren und als alleiniges Konzept zur Erklärung des menschlichen Verhaltens heranzuziehen. Aufgrund der Ergebnisse von Metaanalysen in der Einstellungs-Verhaltens-Forschung (vgl. SIX & ECKES, 1996) bleibt das Konzept der Einstellung zwar ein wichtiger Prädiktor für Verhalten, darüber hinaus müssen aber weitere Einflussgrößen in Betracht gezogen werden.

Ein Ansatzpunkt stellt dabei die „Soziale Unterstützung am Arbeitsplatz“ dar. Der Grad der erwarteten bzw. tatsächlichen Unterstützung kann indirekt dazu beitragen, wie die Meinungen und Ansichten der Kollegen die eigenen Wertvorstellungen zu der Thematik „IT-Sicherheit“ beeinflussen. Werden IT-Sicherheitsumsetzungsmaßnahmen in der eigenen Arbeitsgruppe als überflüssig angesehen, so reduziert sich auch die persönliche Motivation bei deren Umsetzung. Das gleiche gilt auch für den umgekehrten Fall. Aus diesem Grund soll das Konzept der „Sozialen Unterstützung“ in einem eigenen Kapitel ausführlich behandelt werden.

2.4.3.3 Soziale Unterstützung

Das Konstrukt Soziale Unterstützung (SU) stammt aus dem Konzept der „Sozialen Integration“, in dem qualitative Fragen über die strukturellen Aspekte von Sozialbeziehungen untersucht werden, d. h., in wie weit ist ein Individuum in einem sozialen System involviert bzw. nimmt daran teil. Des Weiteren leitet sich SU aus dem Konstrukt „Soziale Netzwerke“ ab, worunter das Ausmaß sozialer Kontakte bzw. deren Austausch erfasst wird. Hier siedeln sich Fragen an, die sich mit der quantitativen Einbindung in ein soziales Netzwerk befassen. Die drei genannten Begriffe stammen aus der Netzwerk- und Unterstützungsforschung und finden aufgrund der Forschungsarbeiten von CAPLAN (1976) und COBB (1976) zunehmend Beachtung.

2.4.3.3.1 Definition des Begriffs „Soziale Unterstützung“

Im Grunde kann alles, was irgendwie mit der Wirkung zwischenmenschlicher Beziehungen zu tun hat, unter diesem Begriff zusammengefasst werden. So kann z. B. die subjektive Wahrnehmung des Empfängers von informeller Hilfe zur Befriedigung grundlegender sozialer Bedürfnisse in den Vordergrund gestellt werden, wobei materielle Hilfen ausgeschlossen werden (vgl. COBB; 1976). Mann kann aber SU auch eher in Verbindung mit gesundheitlichen Aspekten betrachten. Dies beinhaltet die

Mobilisierung individueller Ressourcen, die zur Bewältigung von Problemen und Belastungen eingesetzt werden (vgl. CAPLAN; 1976).

BADURA (1981b) greift den gesundheitsförderlichen Aspekt auf und gibt folgende Definition von SU wider:
SU sind „...Fremdhilfen, die dem einzelnen durch Beziehungen und Kontakte mit seiner sozialen Umwelt zugänglich sind und die dazu beitragen, dass die Gesundheit erhalten bzw. Krankheiten vermieden, psychische oder somatische Belastungen ohne Schaden für die Gesundheit überstanden und die Folgen von Krankheiten überwunden werden“ (BANDURA, 1981b; S. 157).

2.4.3.3.2 Wirkung der „Sozialen Unterstützung“ auf den Menschen

Die Wirkung von sozialer Unterstützung auf die psychische und physische Gesundheit ist in der psychologischen Forschung seit vielen Jahren immer wieder Gegenstand von Untersuchungen.[8]. Querschnittstudien zeigen, dass der Einfluss naher Beziehungen entscheidend für das Ausmaß des Stressempfindens ist, wobei dies hauptsächlich von der Erwartungshaltung des Hilfesuchenden abhängt (vgl. SARASON, SHEARIN, PIERCE & SARASON, 1987). SU wirkt ressourcenschonend, so dass die Auftretenswahrscheinlichkeit von Handlungsfehlern reduziert werden kann (vgl. UDRIS & FRESE, 1988). Es werden zwei mögliche Wirkungsweisen der SU zugeschrieben:

Direkteffekte: Sie beinhalten den direkten Einfluss von SU auf individuelle Befindlichkeiten durch die Befriedigung elementarer, nicht-situationsabhängiger Bedürfnisse. Darunter gehören die Befriedigung von Zugehörigkeits- und Rückzugsbedürfnissen sowie die Ausbildung und Stützung individueller Orientierungs- und Handlungsmuster.

[8] Vgl. NESTMANN, 1988, S. 76; KEUPP, 1987b, S. 153ff; RÖHRLE & STARK, 1985, S. 32; RÖHRLE, 1987, S. 94 f; SCHENK, 1984, S. 178f.

Puffereffekte: Im Gegensatz zu den Direkteffekten wirken sich die Puffereffekt indirekt dadurch aus, „dass sie den Einfluss der Stressoren auf die Stressreaktion verändern, oder aber auch die Einwirkungen der Stressreaktionen auf die individuellen Befindlichkeiten mildern“ (RÖHRLE, 1994, S. 75)[9]. Die Wirkung resultiert aus dem Einfluss auf die Wahrnehmung und Interpretation der Situation und auf die Quantität bzw. Qualität der SU.

Nicht ganz so positiv sehen DUNKEL-SCHETTER & BENNETT (1990) SU. Sie räumen ein, dass die erhaltene SU nur dann Stress reduziert, wenn sie je nach Art der Belastung auch passend geleistet wird (vgl. DUNKEL-SCHETTER & BENNETT, 1990). Gar mit schädigender Wirkung verbunden sieht DIEWALD (1991) SU. SO resultiert nach seiner Ansicht ein Kostenaspekt aus dem Aufbau von Verpflichtungen und Machtungleichgewichte, dem Austragen von Konflikten und der Höhe der Diskrepanz zwischen der Absicht zur Unterstützungsleistung beim „Helfer“ und der Wahrnehmung und Interpretation des Unterstützungsprozesses durch den „Geholfenen“ (vgl. DIEWALD, 1991)[10].

2.4.3.3.3 Soziale Unterstützung am Arbeitsplatz

Gerade wenn es bei der Arbeit „eng und stressig“ wird, ist es von entscheidender Bedeutung, sich auf die Unterstützung durch Kollegen und Vorgesetzte verlassen zu können. Wenn man das Gefühl hat, dass andere in solchen Situationen einem „zur Seite stehen“, reicht die antizipierte SU oft aus, den subjektiv erlebten Arbeitsstress – auf Grund einer übermäßigen erlebten Anspruchshaltung durch die Kollegen oder einem übermäßigen Arbeitsaufkommen – bis zu einem gewissen Maß kompensieren zu können.

Am Arbeitsplatz werden zu den potentiellen „Helfern“ Vorgesetzte und Kollegen der eigenen Institution gezählt. Die Problematik der SU, die sich aus dieser Situation ergibt, umschreibt Gusy (1994) folgendermaßen: „Die Arbeit ist ein Lebensabschnitt,

[9] Vgl. auch FISCHER, 1982, S. 137.
[10] Näheres über negative Effekte SU siehe LAIREITER (1993), WORTMAN & LEHMAN 1985); NESTMANN (1988).

in dem die Wahl der Interaktionspartner weder freiwillig noch durch Sympathien bedingt, erfolgt, sondern das Zusammentreffen in erster Linie auf Grund der Rolle oder Aufgaben beruht, die den Mitarbeitern durch die Institution übertragen wurden“ (a. a. O., 1994, S. 118). Die SU am Arbeitsplatz durch Kollegen/Vorgesetzte resultiert aufgrund der potentiellen Verfügbarkeit, der fachlichen Kompetenz und der notwendigen Kontextinformation, die für adäquate Hilfeleistungen im Arbeitsalltag bedeutsam sind. So können nach Gusy (1994) Vorgesetzte und/oder Kollegen bei fachlichen Problemen aufgesucht, nach ihrer Meinung zu bestimmten Problemsituationen befragt, oder auch instrumentell an der Erledigung von konkreten Arbeitsaufgaben beteiligt werden. Die positive Wirkung der SU in der Arbeit ergibt sich dabei aus einem positiven Sozialklima. Die Hilfe von Kollegen und Vorgesetzten vermittelt das Gefühl der arbeitsbezogenen sozialen Einbettung und beeinflusst nachweislich das Wohlbefinden bzw. verhindert Beeinträchtigungen der allgemeinen Befindlichkeit (vgl. PFAFF, 1989). Damit spielt SU eine wichtige Rolle bei der Bewältigung von Arbeitsproblemen.

SU liefert einen wichtigen Beitrag zum humanen Arbeitsleben. Es handelt sich dabei um eine notwendige Ressource, die hilft „...in komplexen Umwelten die Fähigkeit zu erlangen, flexibel, kompetent und effizient auf verschiedene Anforderungen und Bedrohungen reagieren zu können“ (DIEWALD, 1991; S. 94). Dabei ist es wichtig, in schwierigen Situationen am Arbeitsplatz bzw. bei der Bewältigung der Arbeitsaufgabe auf die Unterstützung des Vorgesetzten bzw. Kollegen zurückgreifen zu können bzw. das Gefühl zu haben, dass diese Hilfe potentiell vorhanden ist. Nur wenn diese Gewissheit vorliegt und effizient genutzt wird, werden neue Anforderungen, die an den Mitarbeiter gestellt werden (z. B. IT-Sicherheitsumsetzungsmaßnahmen) als weniger belastend empfunden und können erfolgreich in den gewohnten Arbeitsprozess mit einfließen. Gerade im Bereich der IT werden oft Kenntnisse vom Anwender abverlangt, die Wissen und Kenntnisse des Anwenders weit übersteigen und der Betroffene schnell eine Überforderung wahrnimmt. Damit liefert SU am Arbeitsplatz auch eine subjektive Ressource zur Vermeidung von psychischen und physischen Belastungen und deren Beanspruchungsfolgen.

2.4.4 Problematik der Bewertung menschlichen Handelns

Lange Zeit war die Vermeidung von Fehlern und Unfällen das primäre Ziel der Sicherheitsförderung. Dabei wurde der Stand der Sicherheit, anhand von Unfallzahlen und anderen outputbezogenen Indikatoren gemessen und beurteilt. Eine solche Betrachtungsweise sieht KÜNZLER (2002) mit einigen Mängeln verbunden:

- „Unfälle und Fehler geben keine direkten Hinweise auf die Sicherheit eines Systems, da sie lediglich auf den Output eines Systems bezogen sind“ (KÜNZLER, 2002; S. 28).
- „Unfälle und Fehler haben eine stochastische Komponente, sie können auch zufällig entstehen und sind erst im Nachhinein verschiedenen Ursachen zuzuordnen“ (KÜNZLER, 2002; S. 28, vgl. PERROW, 1987)
- „Für Tätigkeiten mit einem sehr hohen Schadenspotenzial muss die Wahrscheinlichkeit eines Unfalles sehr tief sein. Das Fehlen von sehr unwahrscheinlichen Ereignissen ist dann aber kein präziser Indikator mehr für ein gutes Sicherheitsmanagement (KÜNZLER, 2002; S. 28).

GROTE (1997) beschreibt in seiner Darstellung ausführlich die Schwierigkeit eines geeigneten Maßstabs, um einen sinnvollen Vergleich zwischen Alternativen einer Systemgestaltung zu ermöglichen. So stellt sich die Problematik vor allem durch den Prozesscharakter von Sicherheit im sozio-technischen System dar. Diese Schwierigkeit wird von Seiten der Wissenschaft wie folgt bewertet:

„Dem Begriff „Gefahr“ und den möglichen Folgen, die eintreten, wenn die potenziell schädigenden Energien wirksam werden, steht das Ziel „Sicherheit“ gegenüber als ein Ausdruck präventiven Bemühens und eine Abkehr von der Tendenz, sich alleine auf die Analyse von Unfallursachen nach dem Eintritt von Schädigungen zu konzentrieren. Wir haben daher versucht, den sicheren Zustand eines Systems hypothetisch durch Leistungen des Managements, der Führungskräfte und der Beschäftigten zu definieren. Die Ergebnisse dieser Leistungen sollen sich in Sicherheitskriterien niederschlagen, die von sicheren Betriebsmitteln bis zum sicherheitsförderlichen Führungsstil reichen. Wir betrachten sie als Bausteine für eine

um Prävention bemühte Sicherheitsarbeit. Unsere Kenntnisse und die sicherheitswissenschaftliche Diskussion reichen indessen noch nicht aus, um eine begründete Liste solcher Kriterien aufzustellen“ (HOYOS & RUPPERT, 1993; S. 113). Trotz dieser Kritik, kommen die Autoren nicht umher, auch ihre Arbeiten an Hand von Unfallzahlen auszurichten.

Zu einer ähnlichen Einschätzung kommt REASON (1993). Auch er stellt fest, dass Fehler und Unfälle kein geeignetes Maß zur Bewertung von Sicherheit sein kann. Er fordert die Auflistung von Indikatoren und Merkmalen zur Beschreibung von Sicherheit eines Systems.

Die Bewertung menschlicher Zuverlässigkeit führt zu methodischen Schwierigkeiten, die ZIMOLONG (1990) in Mängeln bei der Konzeptionalisierung von Fehlern auf der Wissensebene, der unzureichenden Datenbasis für die Schätzung der Fehlerwahrscheinlichkeit durch Experten und Mängel bei den zugrunde liegenden Modellen zuverlässiger Aufgabenerledigung sieht. CACCIABUE (1998) kritisiert darüber hinaus die fehlende Beachtung dynamischer Prozesse in der Mensch-Maschine Interaktion. Dabei zeigt es sich, dass probabilisitische Methoden der Ingenieurwissenschaft mit theoretischen Methoden der Sozialwissenschaft schwierig miteinander in Verbindung gebracht werden können (vgl. KIRWAN, 1994). Dies fordert nicht nur die Untersuchung der einzelnen Teilsysteme „Mensch“ und „Technik“, sondern darüber hinaus deren Interaktion bzw. gegenseitigen Abhängigkeiten. Somit kann die Sicherheit des sozio-technischen Systems anhand definierter Kriterien der sog. Komplementären Aufgabenverteilung beurteilt werden (vgl. GROTE ET AL., 1999).

FRESE & ZAPF (1991) griffen die Handlungsregulationstheorie auf, um sie als Erklärungsansatz bei Handlungsfehlern am BSAP heranzuziehen. Trotz der negativen Konnotation des Begriffs „Fehler“ bilden sie das Fenster, um dahinter liegende Denk- und Handlungsprozesse zu untersuchen. Nur durch die Möglichkeit, Fehler zu begehen kann der Mensch komplexe und unübersichtliche Situationen verstehen und überwinden (vgl. FRESE & ZAPF, 1991; S. 16). Sie leisten einen wichtigen Beitrag zur Kompetenzentwicklung bei. Fehler sind nicht zufällig, sondern beinhalten immer eine

Tendenz zum Richtigen (vgl. WEHNER 1984a). Auf Grund der Intentionalität sind Fehler menschlich (vgl. REASON, 1994), wobei diese Intention von einer absichtlich abweichenden Handlung abgegrenzt werden sollte (vgl. SELLEN, 1990). Darum kann nur dann von einem Fehler gesprochen werden, „wenn die Situation und das eigene Können eine andere Handlungsweise erlaubt hätten“ (WINGERT, 1984; S.4). Zusammengefasst geben FRESE & ZAPF (1991) folgende Begriffsbestimmung von „Fehler“:

- „Fehler treten nur bei zielorientiertem Verhalten auf.
- Ein Fehler beinhaltet das Nichterreichen eines Ziels oder Teilziels.
- Man spricht nur dann von einem Fehler, wenn er potentiell vermeidbar gewesen wäre.“ (a. a. O., 1991; S. 15).

Ausgehend von der Nicht-Passung (Mismatch) auf den Dimensionen der Trias „Aufgabe – Benutzer – Computer“ (vgl. RASMUSSEN, 1985), entwickelten FRESE & ZAPF (1991) eine Taxonomie von Fehlern in der Mensch-Computer-Interaktion. Jede der aufeinander aufbauenden und miteinander verknüpften Regulationsebenen ist durch Angaben zum Ziel und zum Aktionsprogramm, d. h. der vorwegnehmenden Planung für die nachfolgend auszuführenden Aktivitäten, gekennzeichnet. Treten auf den einzelnen Regulationsebenen Fehler auf, dann basieren diese auf fehlenden oder falschen Fakten, Regeln und Modellen (vgl. FRESE & ZAPF, 1991).

Basierend auf den oben beschriebenen Gedanken der Handlungsregulationstheorie, unterscheidet Hacker (1998) verschiedene Ebenen der Handlungsregulation, die aufeinander aufbauen und miteinander verknüpft sind. Jede Ebene ist durch Angaben zum Ziel und zum Aktionsprogramm, d. h. der vorwegnehmenden Planung für die nachfolgend auszuführenden Aktivitäten, gekennzeichnet. Treten auf den einzelnen Regulationsebenen Fehler auf, dann basieren diese auf fehlenden oder falschen Fakten, Regelen und Modellen (vgl. FRESE & ZAPF, 1991).

Im Folgenden werden die einzelnen Regulationsebenen nach HACKER (1998) differenziert und die Ursachen von Handlungsfehlern in dieser Ebene nach FRESE & ZAPF (1991) zugeordnet:

Die sensumotorische Regulationsebene: Sie beinhaltet stereotype Handlungen mit ähnlichem Zeitbedarf und gleich bleibendem Zeitabstand. Die Handlungen laufen unterhalb der Bewusstseinsschwelle ab. Fehlhandlungen entstehen hier aufgrund einer Unangemessenheit der automatisierten Reaktionen gegenüber der Situation (Fehlaktivation).

Die perzeptiv-begriffliche Regulationsebene: Die Handlungen sind in ihrem Zeitbedarf variabel, wiederholen sich unregelmäßig und erfordern regelmäßig komplexere Aktivitätseinheiten. Die Zielangleichung richtet sich nach der Situation, wobei die operativen Abbilder bewusstseinfähig aber nicht –pflichtig sind. FRESE & ZAPF (1991) sehen die Fehlerursache hier im „Similarity matching" und „frequency gambling".

Die intellektuelle Regulationsebene: Hier sind die Handlungen aufgrund ihrer Unregelmäßigkeit nicht vorherzusehen. Die Handlungen sind bewusstseinspflichtig, um Entwürfe für neue Handlungspläne unter Bezugnahme und Bewertung von Alternativhandlungen zu erstellen. Fehlhandlungen werden dabei verursacht durch begrenzte Informationsverarbeitungskapazität.

Je nach Regulationsebene werden die Handlungen unterschiedlich stark kognitiv, emotional und motivational verarbeitet. Die Regulation der Handlung erfolgt über das allgemeine Wissensreservoir, wo Fakten, Regeln und Modelle über die Realität gespeichert sind. FRESE & ZAPF (1991) erweitern die o. g. Regulationsebenen um die Ebene des „*abstrakten Denkens*". Hier entstehen nach ihrer Ansicht Fehler nicht per se, sondern es werden nur Fehlertendenzen innerhalb bestimmter Rahmenbedingungen erkennbar (falsche Handlungsstile, falsche kognitive Stile und fehlende Selbstreflexion). Die Regulation erfolgt auch hier bewusst, wobei man sich allgemeinen Heurisitkas bedient (vgl. FRESE & ZAPF, 1991; S. 20).

Rückgreifend auf die Mismacht-Situation in der Mensch-Computer-Interaktion wird bei der Fehlerentstehung zwischen den Funktionsproblemen und den Nutzungsproblemen unterschieden. Funktionsprobleme entstehen dadurch, dass Arbeitsaufgaben mit dem verwendeten Computersystem nicht in der gewünschten Art

und Weise erledigt werden können. Frese & Zapf (1991) stellen die Phasen des Softwareentwicklungszyklus in den Vordergrund und sehen zwei Fehler als ausschlaggebend an (vgl. a. a. O., 1991; S. 33ff):

Fehler in der Analyse- oder Definitionsphase: „Diese Fehler sind dadurch gekennzeichnet, dass Details der zugrunde liegenden Arbeitsaufgaben zwar berücksichtigt wurden, jedoch nicht in dem Ausmaß, wie es aufgrund arbeitsanalytischer Ergebnisse sinnvoll wäre“ (a. a. O., 1991; S. 33).
Programmierfehler: „Diese Fehler zeichnen sich dadurch aus, dass zwar die richtige Anwendung programmiert worden ist. Diese ist softwaretechnisch jedoch noch nicht ausreichend genug“ (a. a. O., 1991; S. 34).

Die Autoren verzichten auf eine Gliederung der Funktionsprobleme nach der Entstehung im Softwareentwicklungsprozess, sondern akzentuieren deren Auswirkungen auf den Handlungsprozess. Insgesamt lässt sich nach Einschätzung der Autoren ca. jeder 10. Fehler auf ein Funktionsproblem zurückführen (vgl. ZAPF, 1991; S. 45).

Ein Mismatsch zwischen dem Benutzer und dem Computer wird als Nutzungsproblem angesehen. Ihre Taxonomie und anteilige Häufigkeit des Auftretens des Mismatch zwischen dem Benutzer und dem Computer im Handlungsprozess am BSAP wird in der folgenden Tabelle 1 dargestellt:

Regulationsgrundlage:	**Wissensfehler 15%**		
Regulationsebenen	**Ziele/ Planung**	**Gedächtnis/ Monitoring**	**Feedback**
Intellektuelle Regulationsebene	Denkfehler 16 %	Merk-/ Vergessensfehler 7%	Urteilsfehler 3%
Regulationsebene der flexiblen Handlungsmuster	Gewohnheitsfehler 13%	Unterlassensfehler 14%	Erkennensfehler 6%
Sensumotorische Regulationsebene	Bewegungsfehler 26%		

Tabelle 1: Taxonomie von Nutzungsproblemen und Häufigkeiten des Auftretens (In: FRESE & ZAPF, 1991; S. 36).

Fehler in der Mensch-Computer Interaktion sind meist mit hohem Zeit- und Geldaufwand verbunden. BRODBECK (1991) konnte in einer Untersuchung den durchschnittlichen Zeitaufwand zur Fehlerbewältigung auf ca. 10% der Arbeitszeit festsetzen. Er kalkuliert den Kostenaufwand bei einem Unternehmen mit 300 Mitarbeitern durch Fehlerbewältigung am Computer auf jährlich ca. 0,6 Mio. Euro. Darüber hinaus führen lange Fehlerbewältigungszeiten zu einer Erhöhung der Stressauswirkungen (vgl. FRESE & ZAPF, 1991). BRODBECK (1991) zeigte außerdem auf, das Fehler, die nicht in den ersten 10 Minuten bewältigt werden, zu erhöhtem Ärger-, Frustrations- und Anspannungsempfinden führen. Dies hat eine weitere Zunahme von Handlungsfehlern und eine Abnahme der Arbeitsleistung zur Folge. Im sozialen Kontext führen Handlungsfehler zu Schuldzuweisungen seitens der Kollegen bzw. Vorgesetzten und tragen so zu einem schlechten Betriebsklima bei (vgl. FRESE & ZAPF, 1991).

Weitere Auswirkungen von Handlungsfehlern während der Arbeit können nach HACKER (1998) folgender Art sein:

- Qualitätsminderung
- Verstöße gegen Sicherheitsbestimmungen
- Beschädigungen von Arbeitsmitteln

Werden Fehler begangen, ist es wichtig, auf die Unterstützung anderer Personen oder auf Hilfsmittel zurückgreifen zu können. Dies wird umso bedeutender, je höher die Regulationsebene steht, in der der Fehler auftritt. Es zeigt sich, dass bei der erwarteten Hilfestellung der Kollege „hoch im Kurs steht“. Der Vorgesetzte wird im Gegensatz dazu erst in letzter Instanz konsultiert. Weitere Hilfsmittel sind Handbücher oder externe Berater (vgl. BRODBECK, 1991; S. 85ff).

Abschließend kann festgehalten werden, dass bei der Bewertung eines Systems hinsichtlich seiner Sicherheit nicht nur Unfälle und Fehlerzahlen herangezogen werden können, da deren Zusammenhang mit Sicherheit nicht eindeutig nachgewiesen werden kann, sondern auch input- und transformationsprozessbezogene Kriterien mit einfließen sollten. Dabei erweist es sich als günstig, die Leistungen aller Organisationsmitglieder mit zu berücksichtigt.

2.4.5 Arbeitsplatzbezogenes Risikomanagement

In diesem Kapitel wird untersucht, welche Voraussetzungen erfüllt sein müssen, damit der Mitarbeiter die Umsetzungsmaßnahmen zur Einhaltung von Sicherheitskriterien an seinem Arbeitsplatz annimmt und verantwortungsbewusst in seinen Wirkungsbereich einfließen lässt. Als zentraler Gegenstand ist hierbei die Arbeitstätigkeit am BSAP zu nennen, da hier Gefahren auftreten, die vom Mitarbeiter erkannt und als IT-sicherheitsgerechte Handlung umgesetzt werden soll.

2.4.5.1 Die Gestaltungsgrundlage: Das Sozio-technische System an der Schnittstelle „Bildschirmarbeitsplatz“

Im Jahr 2001 saß in der BRD jeder zweite Arbeitnehmer an einem Bildschirmarbeitsplatz (BSAP) (vgl. Statistisches Bundesamt, 2001). Unter einem BSAP versteht man einen „Arbeitsplatz mit einem Bildschirmgerät, der folgende Ausstattungen aufweisen kann:

- Einrichtungen zur Erfassung von Daten,
- Software, die den Beschäftigten bei der Ausführung ihrer Arbeitsaufgaben zur Verfügung steht,
- Zusatzgeräte und Elemente, die zum Betreiben oder Benutzen des Bildschirmgeräts gehören oder
- sonstige Arbeitsmittel sowie Ausstattungen der unmittelbaren Arbeitsumgebung“

(Artikel 3, § 2 BildschArbV; In: EISFELLER et. al, 1999; S. 9).

Beschäftigte im Sinne dieser Verordnung sind Mitarbeiter, „die gewöhnlich bei einem nicht unwesentlichen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.“ (§ 2 Abs. 3 BildschArbV; vgl. ERTEL ET AL., 1997; S. 9).

Die Arbeitsaufgabe am BSAP vereint die Teilsysteme „Organisation“, „Mensch“, und „Technik“. Die Arbeitsaufgabe hat direkten Einfluss auf die genannten Teilsysteme und weist damit der Arbeitsaufgabengestaltung eine zentrale Rolle zu. Die Gestaltung

der Arbeitsaufgabe beeinflusst indirekt die Wirtschaftlichkeit, Effektivität und Effizienz eines Unternehmens und direkt beeinflusst sie die Arbeitsmotivation, Leistung und das Wohlbefinden beim Menschen (vgl. KÜHLMANN, 1993). Der starke Einfluss von IT auf die Arbeitstätigkeit und der unternehmerischen Ausrichtung ist mit umfassenden Veränderungen des Arbeitsinhalts, den –bedingungen, der Qualifikation und den sozialen Interaktionen verbunden (vgl. a. a. O., 1993).

Um negative Auswirkungen am BSAP zu reduzieren und damit Zeit, Kosten und Nerven zu schonen, rückt die Arbeitsaufgabengestaltung in den Fokus des Interesses.

2.4.5.2 Kriterien der Arbeitsgestaltung am BSAP

Ein falscher „Klick" am Computer kann zu einem hohen Arbeitsmehraufwand und den damit verbundenen Kosten führen. HACKER (1998) sieht die Entstehung von Fehlhandlungen als Ursache von unzureichender organisatorischer und technischer Arbeitsgestaltung. Dadurch erhält der Mitarbeiter nur „mangelhafte handlungsregulierende Informationen um einen effektiven Sicherheitsprozess einzuleiten bzw. umzusetzen" (HACKER; 1998; S. 676). Damit wird der humanen Aufgabengestaltung zur Förderung eines IT-sicherheitsgerechten Verhaltens und Bewusstseins eine wesentliche Rolle beigemessen. Die grundlegenden Kriterien der Arbeitsgestaltung in der Arbeitswissenschaft werden in übersichtlicher Weise von LUCZAK & VOLPERT (1987) dargestellt. Sie finden in dieser Form auch einen allgemeinen Konsens[11]:

Schädigungslosigkeit und *Erträglichkeit* der Arbeit, bezogen auf die physiologisch-ökologische Ebene. Dieses Kriterium richtet sich beim BSAP hauptsächlich an ergonomische Gegebenheiten. So können schlecht gestaltetes Arbeitsmobiliar oder unzureichende Umgebungsbedingungen zu Beeinträchtigungen des Bewegungs- und Sehapparates führen. Diese Forderungen werden bereits vom Gesetzgeber durch entsprechende Gesetze und Verordnungen überwacht (z. B.

[11] Vgl. auch HACKER, 1980; BACHMANN, 1978; ROHMERT, 1972; HOYOS & WENNINGER; 1995; ULICH; 2001

Bildschirmarbeitsrichtlinien, Arbeitsstättenverordnung u. a.). Diese Vorschriften werden aber leider immer noch zu selten umgesetzt (vgl. Wieland-Eckelmann et. al, 1996).

Ausführbarkeit der Arbeit, bezogen auf die Ebene der Operationen mit Werkzeugen und an Maschinen, d. h., die Arbeit darf nicht durch unzureichende Arbeitsmittel in ihrem Ablauf gestört sein. Dies beinhaltet darüber hinaus Aspekte der Informationsdarbietung am Bildschirm (vgl. WIELAND & KOLLER; 1999). Gerade bei BSAP wird über diesen Punkt häufig diskutiert, da z. B. durch Systemabstürze, lange Wartezeiten beim Laden von Programmen und unzureichende Hardwareausstattung der Nutzer bei der Ausführung einer Arbeitstätigkeit stark behindert wird.

Zumutbarkeit, *Beeinträchtigungsfreiheit*, *Handlungs- und Tätigkeitsspielraum* der Arbeit, bezogen auf die Gestaltung der Arbeitsaufgaben und Arbeitsumgebungen. Dieser Aspekt ist nicht erfüllt, wenn eine große, anhaltende Diskrepanz zwischen der Aufgabenanforderung und den individuellen Leistungsvoraussetzungen besteht. Das Resultat sind psychische Ermüdung, Monotonieerleben, psychische Sättigung und Stress und die damit verbundenen Leistungs-, Qualifikations- und Motivationsverlust (vgl. FRESE & ZAPF, 1991; KUHMANN, 1994; RICHTER & HACKER, 1997; WIELAND & KOLLER, 1999).

Zufriedenheit der Arbeitenden, *Persönlichkeitsförderlichkeit* der Arbeit, bedeutet, dass die Arbeitsaufgabe den Fähigkeiten und Qualifikationen des Mitarbeiters angepasst ist. Es kann Einfluss auf die Arbeitsbedingungen und –systeme genommen werden, um Kompetenzen und Fähigkeiten auszuweiten. Konkret beschreibt dies die Förderung der Mitarbeiter durch Qualifizierung, Verantwortungsübertragung und selbständiges Setzen von Zielen. Dies kann beim BSAP durch individuell zugeschnittene Nutzerrechte bzw. Software mit Absprache des Anwenders realisiert werden.

Sozialverträglichkeit der Arbeit bedeutet Beteiligung der Arbeitenden an der Arbeitsgestaltung und der –abläufe. Dies bezieht sich auf die kooperative Organisation

der Dienstleistung und beinhaltet u. a. die Möglichkeit der Kommunikation und Kooperation mit den Kollegen.

Die genannten Kriterien sind hierarchisch klassifiziert und voneinander abhängig. Dies bedeutet, die Kriterien einer niedrigeren Ebene müssen erfüllt sein, damit die Kriterien in der nächst höherer Ebene greifen können. Bei den ersten vier Kriterien steht die individuelle Perspektive im Vordergrund. Diese sind nur unter Verwendung eines „anwenderfreundlichen" Systems zu realisieren. Finden diese Punkte z. B. im Arbeits- und Gesundheitsschutz allgemeinen Konsens durch entsprechende rechtliche Fixierungen, so ist man in der IT noch weit davon entfernt, dies reibungslos umzusetzen. Gründe hierfür sind teilweise fehlende Rechtsgrundlagen, mangelhafte Hard-/Software und unzureichendes Engagement des Managements.

In diesem Abschnitt wurden die Bedingungen betrachtet, die zu einer humanen Arbeitsgestaltung beitragen. Es folgt nun eine detaillierte Betrachtung des „Mikrokosmos Arbeit", d. h. welche Forderungen werden an die Arbeitsaufgabe selbst gestellt, damit sie den Anforderungen des Menschen gerecht werden können und somit die Umsetzung von IT-Sicherheitsmaßnahmen fördern.

2.4.5.3 Gestaltungsgrundlage: Das „Sozio-Technische System"

Mit Einführung der IT in die Unternehmen, wurden klassische Arbeitsschritte, wie beispielsweise Verwaltungsarbeiten, rigoros verändert. Unzählige Formulare und Schriftstücke mussten nicht mehr in Ordnern abgeheftet werden. Die Verwaltung findet nun virtuell in elektronisch angelegten Dateien statt. Diese Veränderung lässt sich analog dem Eingriff durch neue Technik im englischen Bergbau in den 50er Jahren vergleichen. Die Untersuchungen im englischen Bergbau zeigten, dass eine Verbesserung der Arbeitsbedingungen durch verbesserte Technik einher ging mit der Erhöhung der Unfallzahlen anstatt (wie erhofft) zu einer Verringerung der Unfallzahlen zu führen. Dies resultierte aus der Verlagerung der Eigenverantwortung der Mitarbeiter auf die Umgebungsbedingungen. Die Ergebnisse der damals

stattgefundenen Untersuchung lassen sich auf heutige „Organisationseingriffe“ durch die IT transformieren. Die Wirkungen und Gestaltungsmaßnahmen werden im Konzept des sozio-technischen Systems beschrieben und zusammengefasst (vgl. TRIST & BAMFORTH, 1951; RICE, 1958; EMERY, 1959; EMERY & TRIST, 1960; SUSMAN ,1976; TRIST & BAMFORTH , 1951; ALIOTH, 1980; TRIST ET AL., 1971). Die hieraus gewonnenen Erkenntnisse bzw. Notwendigkeiten bei einer angestrebten Veränderung eines bestehenden sozio-technischen Systems lassen sich wie folgt beschreiben:

Schaffung von relativ unabhängigen Organisationseinheiten: Dies setzt voraus, dass die Arbeitsaufgabe ganzheitlich durch eine Arbeitsgruppe zu erfüllen ist, und sie muss „eine Herausforderung mit realistischen Anforderungen“ (ALIOTH, 1980; S. 31) darstellen. Dadurch erhält die Arbeitsgruppe die notwendigen Freiräume (Autonomie) und Kontrollmöglichkeiten bei der Aufgabenbewältigung, um auftretende Schwankungen, Störungen oder Abweichungen selbständig zu überprüfen und ggf. zu regulieren. Die Gruppenmitglieder müssen nicht bei auftretender Veränderung reagieren, sondern können durch Kommunikations- und Kooperationsprozesse agieren. Dies steigert die Qualifikation und die soziale Eingebundenheit des Einzelnen in der Gruppe (vgl. ALIOTH, 1980; LEITNER, 1999). VOLPERT (1975) bezeichnet die Beschränkung des Arbeitshandelns als „Partialisierung“. Der Grad der Partialisierung ist entscheidend für das Maß der eigenen Zielsetzung und damit der Handlungsmöglichkeiten (vgl. VOLPERT, 1975; LEITNER, 1999). Je höher der Grad der Partialisierung ist, desto geringer sind die Handlungsfreiheiten.

Schaffung einer gemeinsamen Aufgabenorientierung: EMERY (1959) versteht unter dem Begriff „Aufgabenorientierung“ die persönliche Identifikation mit der zu erfüllenden Arbeitsaufgabe. Die Kernelemente zur Erreichung einer gemeinsamen Aufgabenorientierung bestehen zum einen darin, dass sich die Organisationsmitglieder sowohl mit der Unternehmung, als auch mit dem Produkt identifizieren und zum anderen die inhaltlichen Zusammenhänge bei der Aufgabenerfüllung erkennen, verstehen und akzeptieren. EMERY (1959) spricht in diesem Zusammenhang von der erlebten „Sinnhaftigkeit“ der Arbeitstätigkeit. Dies bedeutet auch, dass die

Arbeitsgruppe nicht eine geschlossene Einheit bilden darf, sondern sie muss im Austausch und Kontakt mit anderen Arbeitsgruppen stehen.

Bei der Erfüllung der Arbeitsaufgabe fließen sowohl technische, organisationsbezogene als auch soziale Komponenten in den Gesamtbetrachtungsgegenstand ein. Auch am BSAP bilden sie den zentralen Gestaltungsansatz und deren Analyseeinheit, „...weil die ausschlaggebenden psychischen Anforderungen der Arbeitstätigkeiten durch die Merkmale der zu erfüllenden Aufgaben bedingt sind“ (HACKER, 1995; S. 23; vgl. VOLPERT ET AL.; 1987). Dieser Forderung wird durch die o. g. Schnittstellenbetrachtung des BSAP Rechnung getragen.

Um aber eine Arbeitsaufgabe am BSAP so zu gestalten, damit sie über dem Anspruch der Aufgabenorientierung hinaus auch dem Aspekt der Humanität gerecht wird, genügt es aus der Sicht von RICHTER (1997) nicht, das ganze Arbeitssystem nur aus der Perspektive des sozio-technischen Systemansatzes zu betrachten, sondern es sollten darüber hinaus auch die Humankriterien zur Aufgabengestaltung mit einfließen.

2.4.5.4 Humankriterien der Aufgabengestaltung

Generell muss die Arbeitsaufgabe derart gestaltet sein, dass die Entstehung von Aufgabenorientierung im Sinne von EMERY (1959) begünstigt wird. Diese Forderung wird im Konzept der „Humanen Arbeitstätigkeit“ impliziert. BAITSCH, KATZ, SPINAS & ULICH (1989) geben folgende Definition von humaner Arbeitstätigkeit:

„Als human werden Arbeitstätigkeiten bezeichnet, die die psychophysische Gesundheit der Arbeitstätigen nicht schädigen, ihr psychosoziales Wohlbefinden nicht – oder allenfalls vorübergehend – beeinträchtigen, ihren Bedürfnissen und Qualifikationen entsprechen, individuelle und/oder kollektive Einflussnahme auf Arbeitsbedingungen und Arbeitssysteme ermöglichen und zur Entwicklung ihrer

Persönlichkeit im Sinne der Entfaltung ihrer Potentiale und Förderung ihrer Kompetenzen beizutragen vermögen“ (BAITSCH, KATZ, SPINAS & ULICH, 1989; S. 27).

Diese Definition humaner Arbeitstätigkeit beinhaltet, dass neben den persönlichkeitsförderlichen Kriterien aus der Systemgestaltung auch Einflussfaktoren beachtet werden müssen, die die Gesundheit generell am BSAP beeinträchtigen können. Die Erkenntnisse aus den verschiedenen Untersuchungen lassen einige Faktoren erkennen, deren gemeinsame Beachtung der o. g. Forderung gerecht werden (vgl. EMERY & EMERY, 1974; CHERNS, 1976; HACKMAN & LAWLER, 1971; HACKMAN & OLDHAM, 1980; EMERY & THORSRUD, 1982). Die wichtigsten Aufgabengestaltungsmerkmale bei der Bildschirmarbeitstätigkeit und ihre beobachteten Wirkungen auf den Menschen werden in der folgenden Tabelle 2 zusammengefasst und finden allgemeine Anerkennung:

Merkmale der Arbeitsgestaltung	**Beobachtete Wirkungen**
Anorderungsvielfalt und vollständige anspruchs-volle Arbeitsaufgaben	• Fördern und ermöglichen den Erwerb und Erhalt von Fähigkeiten, Kenntnissen und Fertigkeiten. • Vermeiden dysfunktionale und fördern funktionale, leistungssteigernde psychische Beanspruchungen. • Erhöhen die Leistungsbereitschaft.
Autonomie (Handlungs-, Gestaltungs- und Entscheidungs-spielraum)	• Fördert die Bereitschaft zur eigenständigen Aufgabenbearbeitung. • Steigert die Selbstsicherheit und das Selbstwertgefühl. • Fördert kreative Problemlösungsstrategien.
Vermeidung von Regulations-behinderungen	• Verringert unnötige, zusätzliche psychische bzw. kognitive Belastungen durch Arbeitsbehinderungen oder –unterbrechungen. • Ermöglicht eine reibungslose Aufgabenerledigung. • Reduziert unnötige Wartezeiten. • Reduziert Ärger und Gereiztheit aufgrund häufiger Arbeitsunterbrechungen.
Leistungs- und Zeitvorgaben	• Fördern bei angemessener Dosierung klare Zielsetzungen und die Zielerreichung. • Liefern Anreize zur Einhaltung von Leistungszielen.
Möglichkeit der Kooperation und sozialen Interaktion	• Fördern die Bereitschaft zur fachlichen und sozialen Unterstützung. • Erfüllen menschliches Grundbedürfnis nach Kommunikation.

Tabelle 2: Arbeitsgestaltungsmerkmale und ihre beobachteten Wirkungen auf den Menschen (WIELAND-ECKELMANN ET AL., 1996).

2.4.5.5 Anforderungsvielfalt und Vollständige Tätigkeit

Aufgaben, die sich durch eine Anforderungsvielfalt auszeichnen, ermöglichen ~~es~~ dem Mitarbeiter bei der Ausführung der (Arbeits-)Tätigkeit, seine Fähigkeiten, Kenntnisse und Fertigkeiten mit einzubringen. Dies dient sowohl dem Erhalt dieser Faktoren, als auch der Förderung. Dadurch können einseitige Beanspruchungen vermieden und die Leistungsbereitschaft gesteigert werden. Dieses Prinzip wird nach HACKER (1998) durch vollständige Tätigkeiten verwirklicht.

Das Konzept der Vollständigen Tätigkeit leitet sich aus der Handlungsregulationstheorie von HACKER (1973) ab und formuliert Merkmale, die begünstigend auf das oben erwähnte Arbeitsgestaltungskriterium der Humanen Arbeitstätigkeit wirken. Dies ist dann der Fall, „wenn Bedingungen in der Arbeitstätigkeit und in der Arbeitssituation vorliegen, die objektiv wenig Restriktionen aufweisen und das Ausüben von Kontrolle – der unterschiedlichsten Facetten – im Arbeitsprozess ermöglichen“ (BÜSSING & GLASER; 1991; S. 122). Somit wird die Vollständige Tätigkeit zum Leitprinzip der Aufgabengestaltung. Damit eine Arbeitstätigkeit als vollständig gelten kann, müssen nach HACKER (1998) folgende Kriterien erfüllt sein:

- „Ausreichende Tätigkeitserfordernisse (im Unterschied zu Aktivitätsmangel),
- mögliche Kooperationen (im Unterschied zu Kooperativitätsmangel),
- selbständige individuelle bzw. kooperative Zielfindungs-/stellungs- und Entscheidungsmöglichkeiten auf der Grundlage von Freiheitsgraden (im Unterschied zu Zielbildungs- und Entscheidungsmangel mit der Folge des Verantwortungsmangels),
- kognitive Vorbereitungsschritte der Tätigkeiten mit nicht algorithmischen, „produktiven“ Teilen (im Unterschied zu Denkanforderungsmangel),
- Lern- und Übertragungsmöglichkeiten von Leistungsvoraussetzungen auf andere (Arbeits- und Freizeit-)Tätigkeiten (im Unterschied zu Lernanforderungs- und Disponibilitätsmangel)“. (a. a. O., S. 253)

Im Gegensatz zu Vollständigen Tätigkeiten verhindern Unvollständige Tätigkeiten Lern- und Entwicklungsmöglichkeiten und führen zu Gesundheitsgefährdungen (vgl. HACKER (1998). Des Weiteren kann es zu Verlernprozessen und Intelligenzabbau kommen (vgl. HACKER & RICHTER, 1990).

2.4.5.6 Autonomie bzw. Tätigkeitsspielraum

Stehen dem Mitarbeiter Dispositions- und Entscheidungsmöglichkeiten zur eigenständigen Lösung von Problemen zur Verfügung, so spricht man von Autonomie. FREI (1993) bzw. FREI ET AL. (1984) akzentuieren dabei die Möglichkeit der Selbstregulation, wodurch eine positive Entwicklung der Kompetenz erst möglich ist (vgl. ULICH, 1992). Die folgende Abbildung 9 soll den Zusammenhang zwischen Autonomie, Kontrolle und Selbstregulation veranschaulichen:

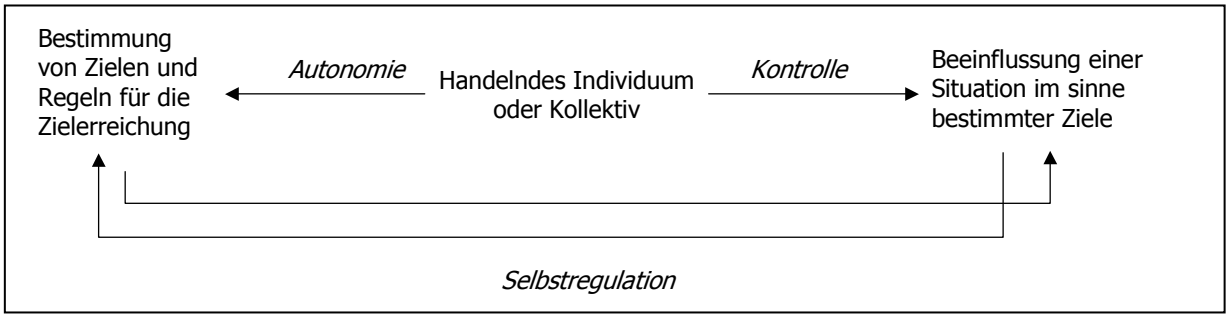


Abbildung 9: Beziehungen zwischen Autonomie, Kontrolle und Selbstregulation (aus: GROTE 1997a).

Die positive Entwicklung der Kompetenz ist unabhängig von der Richtigkeit der getroffenen Entscheidung. Auch falsche Entscheidungen tragen zur Persönlichkeitsentwicklung bei, da durch die resultierenden Konsequenzen Einblicke in komplexe Systeme gewonnen werden können. Die hieraus entstandenen Erfahrungen stehen für spätere Problemsituationen zur Verfügung und erhöhen die Kontrollmöglichkeit. Dies steigert wiederum das Verantwortungs- und Selbstwertgefühls (vgl. HACKER, 1998). Der Grad der Kontrolle hängt vom Wissen und der Kompetenz des Mitarbeiters ab. Aufgaben mit hoher Kontrollmöglichkeit zeichnen sich durch einen entsprechenden Tätigkeitsspielraum aus.

BÜSSING & GLASER (1991) untersuchten in diesem Zusammenhang die Beziehung zwischen der Persönlichkeitsförderlichkeit von Arbeitstätigkeiten und dem Tätigkeitsspielraum. Sie konnten dabei zeigen, dass Arbeitszufriedenheit, individuelle und kollektive Kontrolle sowie die generelle Kontrollmotivation am Arbeitsplatz mit dem Umfang des Tätigkeitsspielraums steigen. Fehlt ein angemessener Tätigkeitsspielraum, können psychische Belastungen mit weit reichenden Beanspruchungsfolgen auftreten. So beeinflusst der Tätigkeitsspielraum nachweislich:

- Die Wahrnehmung und Beurteilung der (Arbeits-)Situation positiv (vgl. LANKENAU; 1984),
- die intrinsische Arbeitsmotivation (Erhöhung der Arbeitsmotivation) (vgl. HACKMAN & OLDHAM; 1974),
- die Qualifizierungsbereitschaft und den Lerntransfer (wird gesteigert) (vgl. LANKENAU, 1984; FRESE, 1989),
- das Wohlbefinden (wird gesteigert) und das Risiko von arbeitsbedingten psychischen Fehlbeanspruchungen (wird reduziert) (vgl. KARASEK & THEORELL, 1990; WARR, 1990; WALL, JACKSON, MULLARKEY & PARKER, 1996).

2.4.5.7 Regulationsbehinderungen

Ein weiteres wichtiges Merkmal gesundheitsförderlicher Aspekte am BSAP ist die Vermeidung von Regulationsbehinderungen, die aus den unterschiedlichsten Arbeitsplatzbedingungen entstehen können (z. B. Arbeitsplatzumgebung, ergonomische Gestaltung des Arbeitsplatzes und den Arbeitsmitteln, den technischen und arbeitsorganisatorischen Bedingungen etc.). Das Konzept der Regulationsbehinderungen wurde von LEITNER et al. (1987) entwickelt und subsumiert kontraproduktive Arbeitsbedingungen, auf die der Arbeitsplatzinhaber keinen bzw. nur geringen Einfluss nehmen kann. Mögliche Folgen davon können sein:

- Erhöhte Anstrengung bzw. Fehlhandlungen (vgl. LEITNER ET. AL, 1987),
- Mangelhaft bzw. verzerrte Beurteilungs- und/oder Schlussfolgerungsprozesse (vgl. REASON, 1994).

Es wird bei den Regulationsbehinderungen zwischen Regulationshindernissen und –überforderungen unterschieden. Diese Unterscheidung wird in der nächsten Tabelle 3 visualisiert:

Regulationsbehinderungen				
Regulationshindernisse		**Regulationsüberforderungen**		
Erschwerungen	Unterbrechungen	aufgabenimmanent		aufgabenunspezifisch
informatorische motorische	Person Funktionsstörungen Blockierung	Monotone Bedingungen	Zeitdruck	Lärm Beleuchtung Raumklima Schadstoffe ergonomische Probleme

Tabelle 3: Klassifikation der Regulationsbehinderungen nach LEITNER (1999). (In R. OESTERREICH & W. VOLPERT, 1999; S. 89)

Unter den *Regulationshindernissen* werden die auf dem Weg des zu realisierenden Arbeitsergebnisses bezogenen Hindernisse bzw. Behinderungen zusammengefasst. Dies kann sich darin äußern, dass das Arbeitshandeln entweder aufgrund von mangelhaften Informationen oder zusätzlichen Arbeitsschritten erschwert wird oder Unterbrechungen einen Neubeginn der Arbeitsschritte erfordern. (vgl. LEITNER (1999).

Regulationsüberforderungen beinhalten ungünstige Arbeitsbedingungen, die sich durch das zeitimmanente Vorhandensein negativ auswirken. Kurzfristige Störungen hingegen würden das Arbeitsergebnis nicht negativ beeinflussen, da erst das langfristige Vorhandensein von Störungen menschliche Ressourcen ausschöpft und psychische Prozesse überfordert (a. a. O., 1999). LEITNER (1999) unterscheidet aufgabenimmanente und aufgabenunspezifische Überforderungen. Ersteres beinhaltet zwei Aspekte: a) Aufgaben, die trotz stereotyper Handlungsfolge eine hohe Konzentration erfordern und b) aufgrund von Zeitvorgaben ist eine konstant hohe Arbeitsgeschwindigkeit erforderlich. Der zweite Punkt beinhaltet die Umgebungsvariablen, die mit der Arbeitsaufgabe nicht direkt in Verbindung stehen.

Treten Regulationsbehinderungen auf, müssen nach LEITNER (1999) folgende Punkte geprüft werden:

- Sind alle notwendigen Informationen verfügbar, erkennbar und eindeutig interpretierbar?

- Sind die benötigten Hard- und Softwarekomponenten verfügbar, geeignet und funktionstüchtig?
- Ist die Handhabung der Betriebsmittel ohne räumliche Barrieren, Einengungen oder Widerstände ausführbar?

2.4.5.8 Leistungs- und Zeitvorgaben

Zeitelastizität und stressfreie Regulierbarkeit – darunter werden Arbeitsbedingungen verstanden, die die „Möglichkeit eines angemessenen Zeitmanagements aufweisen und die keine unangemessenen Arbeitsverdichtung beinhalten“ (WIELAND-ECKELMANN ET AL.; 1996; S. 52). Diese sind durch Leistungs- und Zeitvorgaben bei der Aufgabenbewältigung gekennzeichnet. Müssen Arbeiten in einer selbst- oder fremd vorgegebenen Zeit durchgeführt werden, dann spricht man von „Zeitdruck“ (vgl. NACHREINER & WUCHTERPFENNIG (1975). Es konnte in verschiedenen Untersuchungen gut nachgewiesen werden, wie die Aufgabenbewältigung unter Zeitdruck zu Überforderungssymptomen führte. So steigen defizitäre, arbeitsbezogene Verhaltensweisen bei verminderter Produktivität bzw. Leistung. Dies spiegelt sich vor allem in der Zunahme der Fehlerrate (vgl. SCHULZ & HÖFERT; 1981).

2.4.5.9 Kooperation bzw. soziale Interaktion

Der Mensch ist ein soziales Wesen. Kooperation und unmittelbarer Kontakt erfüllen das menschliche Grundbedürfnis nach Kommunikation. Die Kooperation sieht HACKER (1998) dabei als Grundlage der sozial bedingten Entwicklung der Persönlichkeit an. Die sozialen Interaktionen beziehen sich auf die fachliche, persönliche und kollegiale Unterstützung bei der Bewältigung von Arbeitsaufgaben (vgl. WIELAND-ECKELMANN; 1996). Dies trägt dazu bei, dass Schwierigkeiten gemeinsam bewältigt werden können bzw. die Erfahrung vorhanden ist, sich bei Problemen auf die Unterstützung der Kollegen und Vorgesetzten verlassen zu können. So sehen KÖNIG ET AL. (1995) eine Verringerung der Kommunikationsmöglichkeiten durch BSAP in Verbindung mit einer negativen Beeinflussung sozialer Beziehungen

zwischen den Beschäftigten. LEITNER (1999) hebt den direkten Zusammenhang zwischen dem Austausch von Informationen, dem Abstimmungsprozess über gemeinsame Ziele und Vorgehensweisen mit der Weiterentwicklung sozialer Kompetenzen hervor (vgl. LEITNER, 1999).

Der Einfluss der aufgeführten Faktoren auf das menschliche Wohlbefinden, konnte in vielen Untersuchungen bestätigt werden (vgl. GREIF et. al, 1994; WIELAND ET AL., 1999; LEITNER, 1999). Werden bei der Aufgabengestaltung die genannten Kriterien berücksichtigt, so stellen sie Lern- und Entwicklungsmöglichkeiten für den Mitarbeiter bereit. „Die individuell verfügbaren Ressourcen werden dadurch erhalten und weiterentwickelt bzw. die verfügbaren Leistungsvoraussetzungen werden optimal beansprucht“ (WIELAND-ECKELMANN ET AL.; 1996).

In diesem Kapitel wurde die Bedeutung der Arbeitsaufgabengestaltung am BSAP verdeutlicht. Die Einhaltung dieser Gestaltungskriterien stellt dem Mitarbeiter weitere kognitive Ressourcen beim Arbeitsbewältigungsprozess zur Verfügung. Diese sind notwendig, um zusätzlichen Arbeitsanforderungen motiviert entgegentreten zu können. Die Einhaltung der Gestaltungskriterien bildet die Grundlage eines „gelebten“ und nicht von „oben“ festgesetzten IT-Sicherheitsystems. Des Weiteren beinhaltet die Einhaltung der aufgeführten Gestaltungskriterien Regulationsmöglichkeiten, um psychische Belastungen entgegenzuwirken. Das wirksam werden der Gestaltungskriterien am BSAP liegt im Aufgabenbereich der Belastungs- und Beanspruchungsforschung. Was das für die Tätigkeit am BSAP konkret bedeutet, wird im Kapitel Belastung und Beanspruchung am BSAP erläutert.

2.5 Belastung und Beanspruchung am BSAP

2.5.1 Die Humane Arbeitstätigkeit als Nutzenfaktor

Das jahrelange Interesse zur Bewältigung von gesundheitsschädigenden Einflüssen am Arbeitsplatz lag darin, belastende Ereignisse zu reduzieren. Interindividuelle Verhaltensdispositionen wurden vernachlässigt. Der Grund hierfür liegt darin, dass bei überwiegend körperlicher Arbeitstätigkeit es einfacher ist, die Umgebungsvariablen bzw. Situationsbedingungen zu untersuchen und zu verändern anstatt auf die innere Struktur der Person einzugehen. Doch mit der Veränderung der Arbeitsformen rückt das Konzept der „Salutogenese“ von ANTONOVSKY (1979) verstärkt in den Vordergrund. Darin richtet sich der Fokus auf die Etablierung gesundheits- und persönlichkeitsförderlicher Arbeitsinhalte und –bedingungen (vgl. HACKER, 1991), die zur humanen Arbeitstätigkeitsgestaltung beitragen. Die Umsetzung der Arbeitsgestaltungsmerkmale setzt Mittel und Ressourcen frei, die den Menschen trotz Belastung und Stress bei der Arbeit gesund halten und stellt somit den „Nutzenaspekt“ der Beanspruchung dar. Sie werden als „notwendige Voraussetzung für die Erzeugung des geforderten Arbeitsergebnisses gesehen“ (WIELAND-ECKELMANN, 1992; S. 484), wodurch verschiedene Leistungsfunktionen erhalten und trainiert werden. Somit haben Belastungen resultierend aus der Arbeitstätigkeit nicht nur negative, sondern auch positive Wirkungen. Sie können je nach Gestaltung der Bildschirmaufgabe sinnbildlich mit einem Januskopf verglichen werden.

Abbildung 10: Januskopf der Beanspruchung (modifiziert nach WIELAND-ECKELMANN ET AL., 1996; S. 43)

Bezogen auf die Gestaltung des BSAP heißt das, dass auch hier die Gesamtaufgabe in Verbindung mit den Schnittstellen im Mittelpunkt des Interesses steht (siehe Abbildung 11). Belastungen mit negativen Wirkungen sollten verringert bzw. vermieden werden und Belastungen mit positiven Wirkungen dagegen intensiviert werden (vgl. WIELAND-ECKELMANN, 1992). WIELAND-ECKELMANN (1992) spricht dabei von der „*Beanspruchungsoptimalität*“

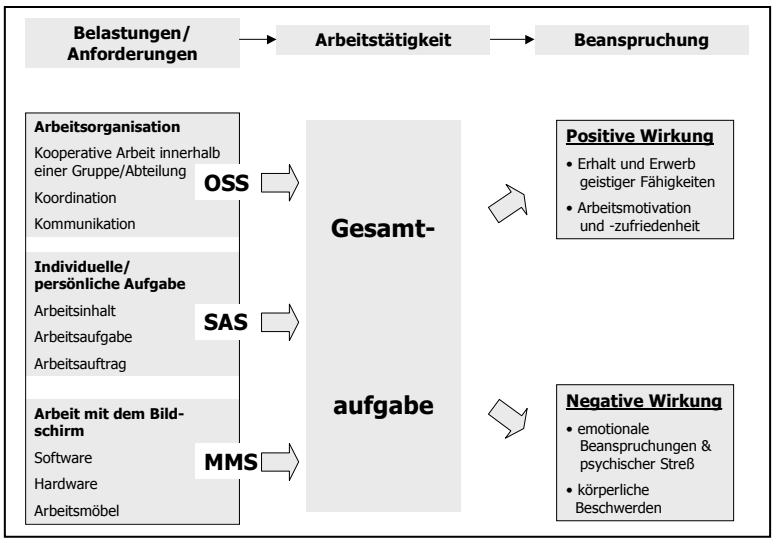


Abbildung 11: Ein ganzheitliches Belastungs- und Beanspruchungsmodell zur Analyse, Bewertung und Gestaltung beanspruchungsoptimaler und funktionaler Büroarbeit (In R. WIELAND-ECKELMANN ET AL., 1996; S. 65)

Bei dieser Betrachtungsweise bedarf es einem Modell, das sowohl kognitive und motivationale Aspekte der Stressregulation beinhaltet, aber auch emotionale und physiologische Auswirkungen mit einschließt. Doch zuerst werden die Begrifflichkeiten definiert.

2.5.1.1 Vom „Stress“-Begriff zur „psychischen Belastung“ und „psychischen Beanspruchung“

Das Wort „Stress“ wurde 1914 von CANNON mit dem Modell der Notfallreaktion in der psychophysiologischen Fachliteratur eingeführt. SEYLE (1950) verlieh mit der Annahme einer biologisch funktionalen Anpassungsreaktion („Allgemeines Adaptionssyndrom) dem Begriff „Stress“ Popularität. Seither gleicht dem Verständnis, was nun eigentlich unter Stress zu verstehen ist, einem „semantischen Morast“

(HACKER & RICHTER, 1998; S. 15). Dies insofern, da der Stressbegriff gleichermaßen als Reiz (unabhängige Variable), als auch als Reaktion (abhängige Variable) zu verstehen ist. Um ihn für die psychologische Arbeitswissenschaft transparent zu machen, bediente man sich den aus der Technik und Physik stammenden Begriffen „Belastung“ (load) und „Beanspruchung“ (strain).

In der deutschsprachigen Arbeitswissenschaft hat sich für die Begriffe psychische Belastung und psychische Beanspruchung eine einheitliche, normative Sprachregelung durchgesetzt (vgl. ROHMERT & RUTENFRANZ (1975). Dabei definiert die Internationale Norm ISO 10075 auf Grundlage von ROHMERT & RUTENFRANZ (1975) den Begriff „psychische Belastung“ folgendermaßen:

- „Die Gesamtheit aller erfassbaren Einflüsse, die von außen auf den Menschen zukommen und psychisch auf ihn einwirken“ (In: HACKER & RICHTER; 1998; S. 32).

Mit „psychischer Beanspruchung“ wird verstanden:

- „Die zeitlich unmittelbar und nicht langfristige Auswirkung der psychischen Belastung auf die Einzelperson in Abhängigkeit von ihren eigenen habituellen und augenblicklichen Voraussetzungen einschließlich der individuellen Auseinandersetzungsstrategie“ (a. a. O.; 1998; S. 32).

2.5.1.2 Belastungs- und Beanspruchungskonzepte

Die klassischen Belastungs-Beanspruchungs-Modelle gehen von einem linearen Ursache-Wirkungs-Zusammenhang zwischen der Belastung als Anforderung (Reiz) und der Beanspruchung als Auswirkung (Reaktion) aus. Des Weiteren gibt es Modelle, in denen das Hauptaugenmerk auf den individuellen Verarbeitungsmechanismus (Transaktion)[12] gerichtet ist. Ursprünglich dienten die Konzepte zur Bestimmung von Belastungen überwiegend körperlicher Arbeit und den darauf folgenden

[12] Vgl. Person-Environment-Fit-Modell von FRENCH, RODGERS & COBB (1981); Imbalance-Theorie von MCGRATH (1970); Transaktionale-Streß-Modell von LAZARUS & LAUNIER (1981); Demand control Support (DCS) von KARASEK (1979) bzw. KARASEK & THEORELL (1990).

Auswirkungen auf den Menschen (vgl. ROHMERT & RUTENFRANZ, 1975; ROSEMEIER, 1981; HACKER & RICHTER, 1998). Dies erfolgte aus dem einfachen Grund, dass sich Beanspruchungen aus körperlichen Tätigkeiten einfacher messen und erklären lassen, als psychische Beanspruchungen bei mentalen Arbeitstätigkeiten. Im ersten Fall sind die physiologischen Ressourcen bzw. Leistungsvoraussetzungen direkt beobachtbar und erfassbar. Doch auf Grund der o. g. Problemverschiebung durch das Arbeitssystem „Computer" rücken neben physischen Belastungen und Beanspruchungen auch psychische Belastungs- und Beanspruchungsfaktoren verstärkt in den Vordergrund. Zur Verarbeitung dieser neuartigen Form der Arbeitsbelastung wächst das Interesse an den möglichen individuellen Ressourcen und Leistungsvoraussetzungen.

2.5.1.3 Stimulus-Response-Konzepte

Zur reizzentrierten Betrachtungsweise zählt man Umgebungsbedingungen, die eine unspezifische Stressreaktion auslösen können (vgl. FRESE & SEMMER, 1984). Eine genaue Übersicht bietet die Klassifikation nach DIN EN ISO 10075-1. Hier werden vier Gruppen von Anforderungen unterschieden, die in der folgenden Tabelle 4 veranschaulicht sind:

Anforderungen der Arbeitsaufgabe	**Soziale und Organisationsfaktoren**
▪ Daueraufmerksamkeit ▪ Informationsverarbeitung ▪ Verantwortlichkeit ▪ Dauer und Verlauf der Tätigkeit ▪ Aufgabeninhalt ▪ Gefahren	▪ Organisationstyp ▪ Betriebsklima ▪ Gruppenmerkmale ▪ Führung ▪ Konflikte ▪ Kontakte
Physikalische Bedingungen	**Gesellschaftliche Faktoren**
▪ Beleuchtung ▪ Klima ▪ Lärm ▪ Wetter ▪ Gerüche	▪ Gesellschaftliche Anforderungen ▪ Kulturelle Normen ▪ Wirtschaftliche Lage

Tabelle 4: Anforderungsbeispiele nach DIN EN ISO 10075-1 (In: M. STAPP, 1999; S. 20).

Die Belastungsfaktoren sind unabhängige Variablen, die auf den arbeitenden Menschen einwirken. Sie wirken kumulativ und können sich negativ auf den Arbeitsprozess auswirken. Diese Auswirkungen werden in den

Responsekonzepten akzentuiert. Dabei werden die spezifischen Reaktionen untersucht, die durch unterschiedliche Reize ausgelöst wurden. Die Auswirkungen können auf der subjektiven Ebene (durch Fragebögen etc.), auf der Leistungsebene (durch Produktivität, Krankenstand etc.) und auf der physiologischen Ebene (durch Herzrate, Adrenalinausschüttung, Blutdruck etc.) erfasst werden. In der unternehmerischen Praxis werden Belastungen und mögliche Beanspruchungen anhand von Tätigkeitsanalysen (z. B. RHIA, TBS, VERA und REBA) erhoben. In der Tabelle 5 ist eine Klassifikation von negativen Beanspruchungsfolgen dargestellt:

	Kurzfristige, aktuelle Reaktionen	**Mittel- und langfristige Reaktionen**
Physiologisch, somatisch	▪ Erhöhte Herzfrequenz ▪ Blutdrucksteigerung ▪ Adrenalinausschüttung ▪ Katecholamin-/Kortisolausschüttung	▪ Psychosomatische Beschwerden und Erkrankungen ▪ Koronarerkrankungen
Psychisch (Erleben)	▪ Anspannung ▪ Frustration ▪ Ärger ▪ Ermüdung-, Monotonie-, Sättigungsgefühle ▪ Stress	▪ Unzufriedenheit, Resignation, Depression ▪ Gereiztheit/ Belastetheit, Nervosität
	Kurzfristige, aktuelle Reaktionen	**Mittel- und langfristige Reaktionen**
Verhaltens-mäßig: individuell	▪ Leistungsschwankung ▪ Nachlassen der Konzentration ▪ Fehler ▪ Schlechte sensumotorische Koordination	▪ Vermehrter Nikotin-, Alkohol-, Tablettenkonsum ▪ Arbeitsunfähigkeit ▪ Fernbleiben vom Arbeitsplatz
Verhaltens-mäßig: sozial	▪ Konflikte ▪ Streit ▪ Aggression gegen andere Rückzug (Isolierung innerhalb und außerhalb der Arbeit)	

Tabelle 5: Beanspruchungsfolgen nach KAUFMANN, PORNSCHLEGEL & UDRIS (1982).

Bei den reiz- bzw. reaktionsorientierten Belastungs-Beanspruchungs-Modellen werden die Bedingungen für Beanspruchung und deren Folgen in der Situation gesucht. Diese Zusammenhänge konnten in mehreren empirischen Untersuchungen bestätigt werden. So sind vor allem die Arbeiten von KARASEK (1979) bzw. KARASEK & THEORELL (1990) hervorzuheben. Die Autoren konnten in einer Längsschnittstudie bei der schwedischen Automobilindustrie die Bedeutung der Faktoren „Handlungskontrolle“, „Unterstützung am Arbeitsplatz“ und „psychologische und physiologische

Anforderungen“ und dem damit verbundenen Risiko einer Koronarerkrankung aufzeigen[13].

Kritiken an den gängigen Stimulus-Response-Konzepten werden aber auch von mehreren Seiten laut. So sind vor allem folgende Kritikpunkte hervorzuheben:

- Aufgrund individueller Differenzen kann praktisch jeder Stimulus eine negative, für die Situation unspezifische Reaktion auslösen (SEMMER, 1984).
- Die reiz-, als auch reaktionszentrierten Stressmodelle gehen von einem linearen Ursache-Wirkungs-Zusammenhang zwischen Belastung und Beanspruchung aus, wobei die persönlichen Leistungsvoraussetzungen und die Art der Bewältigung außer Acht gelassen werden (BACHMANN, 1990; GROS, 1994; RICHTER, 1997).
- Aus dieser Betrachtungsweise heraus lassen sich keine gezielten Präventionsmöglichkeiten zur Vermeidung oder Reduzierung von dysfunktionalen Belastungsquellen ableiten (BACHMANN, 1990; RICHTER, 1997).

In den eben beschriebenen Konzepten fehlt die aktive Rolle der arbeitenden Person im „Stress“-Bewältigungsprozess. Diese entscheidende Erweiterung gelang mit den transaktionalen Konzepten.

2.5.1.4 Transaktionale Stresskonzepte

Neben der „Imbalance Theory“ von McGrath (1970) und dem „Person-Environment-Fit Model“ von French, Rodgers & Cobb (1981) ist es vor allem LAZARUS (1966) bzw. LAZARUS & LAUNIER (1981) mit deren „transaktionalen Stressmodell“ gelungen, diejenigen Prozesse und Eigenschaften hervorzuheben, die in der Person liegen. In diesem Modell wird die subjektive (emotionale) Bewertung der Stresssituation, die Kontrolle über die Situation und die Bewältigungsmöglichkeiten des Individuums (kognitive Bewertung) hervorgehoben, wobei der Mensch nicht passiv den Belastungen ausgesetzt ist, sondern aktiv belastende Situationen mit beeinflussen

[13] Weitere Untersuchungsergebnisse bzgl. Situationsbedingungen und Beanspruchungsfolgen vgl. FRESE & SEMMER (1991)

kann. Dies geschieht durch problemlösende kognitive Bewertungsprozesse der Situation (appraisal). Sie beinhalten einerseits gezielte Informationssuche von Bewältigungsmöglichkeiten, direkte Aktionen gegen die Bedrohung bzw. Unterlassungen von Handlungen, die die Gefährdung verstärken könnten (instrumentelles coping). Andererseits kann eine vorübergehende Entlastung der Bedrohung durch Emotionsregulationen ermöglicht werden, ohne die Ursachen des Stresses zu verändern (pallitatives coping). Zu dieser Klasse symptomorientierter Verhaltensweisen gehören z. B. die Einnahme von Psychopharmaka, Alkoholkonsum, Entspannungsübungen, kognitive Umbewertungen durch Ablenkung, Bagatellisierung oder Wunschdenken.

So schön sich die transaktionalen Konzepte anhören, so schwer sind sie in der Anwendung. Denn zum einen führt die Komplexität des Modelle dazu, dass „[...] die Gültigkeit kaum noch durch eindeutige, theoretisch abgeleitete Prognosen oder empirische Untersuchungen vollständig erfasst und getestet werden kann“ (GREIF, BAMBERG & SEMMER; 1991). Zum anderen gingen die transaktionalen Modelle zwar auf die Problematik der inneren Struktur der Person ein, doch präzise Aussagen über die Koordination internaler und externaler Regulationen fehlen. Aus diesem Grund steht die Frage im Mittelpunkt, welche Arten von Ressourcen bzw. Regulationsmechanismen die Auftretenswahrscheinlichkeit und Intensität von Stressempfindungen erhöhen bzw. vermindern können. Eine Annäherung zur Lösung soll mit dem Mehrkomponenten-Modell gelingen.

Eine Annäherung zur Lösung dieser Problematik kann mit einem Modell bewerkstelligt werden, in dem motivationale, emotionale und kognitive (Regulations-) Aspekte gleichermaßen berücksichtigt werden – dem Mehrkomponenten-Modell von WIELAND-ECKELMANN (1992). ES „stellt den Versuch dar, ein allgemeines Rahmenmodell zur Verfügung zu stellen, das die Möglichkeit bietet, jene Mechanismen und Prozesse genauer zu analysieren, die zwischen der Belastung als Ausgangszustand und der psychischen Beanspruchung als einen Endzustand vermittelt“ (a. a. O., 1992, S. XVII). In dieser Modellvorstellung steht, analog den transaktionalen Modellen, der Mensch mit seinen Verhaltensdispositionen und

–strategien im Mittelpunkt der „Stressbewältigung“. Dabei folgt es dem Prinzip von arbeitspsychologischen Belastungs-Beanspruchungskonzepten. WIELAND-ECKELMANN (1991) akzentuiert die „Inanspruchnahme von individuellen Leistungsvoraussetzungen oder Ressourcen“ (a. a. O., 1991; S. 8) als ausschlaggebend bei der strategischen Ausführungskontrolle. Dadurch hebt er den Prozess des Zeit- und Ressourcenmanagements hervor.

2.5.1.5 Das Zeit- und Ressourcenmanagement zur Regulation psychischer Beanspruchung

Aufgrund der Begrenztheit individueller kognitiver Ressourcen des Menschen kann die Bewältigung der Arbeitsaufgabe zu einer Belastungsgröße heranwachsen. Im Hinblick auf Arbeitstätigkeiten im Allgemeinen und bezogen auf die Bildschirmarbeitstätigkeit im Speziellen kann man von drei voneinander unabhängigen Anforderungsarten ausgehen (vgl. Wieland-Eckelmann, 1992):

Mentale Anforderungen: Sie ergeben sich aus der Aufgabe und lassen sich über die Dimensionen Informationsaufnahme, -verarbeitung und –abgabe beschreiben.

Emotionale Anforderungen: Sie resultieren aus den Kenntnissen, Fähigkeiten und Möglichkeiten bei der Bewältigung der Arbeitsaufgabe. Ihr Grad der Ausprägung wird u. a. durch soziale Kompetenzen und dem Arbeitsklima beeinflusst.

Motivationale Anforderungen: Sie richtet sich danach, wie stark die Arbeitsleistung intrinsisch oder extrinsisch motiviert ist.

Die folgende Abbildung 12 soll das eben Beschriebene veranschaulichen:

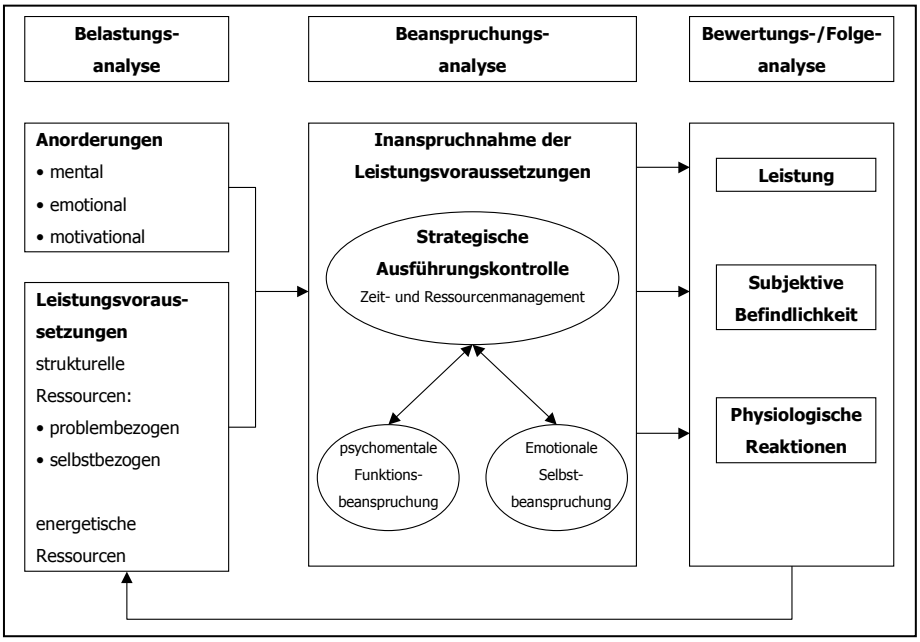


Abbildung 12: Das Mehrkomponentenmodell für psychische Belastung/Beanspruchung (nach WIELAND-ECKELMANN, 1992; S. 35).

Bei der Bewältigung von Anforderungen aus Tätigkeiten am BSAP wird eine emotional-motivationale und kognitive Regulationskoordination erforderlich. Dies gelingt durch die Inanspruchnahme von psychophysischen Leistungsfunktionen (Fertigkeiten, Wissen, Fähigkeiten etc.) und Selbstregulationsfunktionen (z. B. Anstrengung, Anspruchsniveausenkung). Die Ausführung von Leistungen bzw. Handlungen beinhaltet immer die Verwendung von Ressourcen und stellt damit eine Beanspruchung dar. UDRIS ET AL. (1992) definieren den Begriff „Ressourcen" folgendermaßen: Ressourcen sind „... das Insgesamt der einer Person zur Verfügung stehenden, von ihr genutzten oder beeinflussten gesundheitsschützenden und –fördernden Kompetenzen und äußeren Handlungsmöglichkeiten." (a. a. O., 1992; S. 25).

Diese in der Person liegenden Ressourcen stehen als prozesshafte, personale Bedingungen zur Verfügung. Um die Leistungsvoraussetzungen bei der Regulation des Beanspruchungsprozesses in Anspruch nehmen zu können, bedarf es nach WIELAND-ECKELMANN (1992) der strategischen Ausführungskontrolle, d. h., man muss sich über das Vorhandensein und der Nutzbarmachung der Ressourcen bewusst sein. Zudem sollte kein Zeitdruck bestehen. Die Beanspruchung liegt dabei weniger in

der Auswirkung der Anforderung, sondern ist viel mehr die Folge der erbrachten Leistung, determiniert durch den „Grad der Ausschöpfung von Ressourcen“ (vgl. KUHMANN, 1994).

2.5.2 Belastungsfaktoren und Beanspruchungsfolgen durch BSAP

Zur Prävention von Beanspruchungsfolgen durch BSAP wird der Arbeitgeber durch den Gesetzgeber verpflichtet, bei der Gestaltung des BSAP arbeitswissenschaftliche Erkenntnisse zu berücksichtigen, damit der Arbeitnehmer bei der Ausübung seiner Tätigkeit nicht zu Schaden kommt. Dies bedeutet konkret, dass die Arbeitsbedingungen am BSAP auf der Grundlage einer Arbeitsplatzanalyse nach bestimmten Gesichtspunkten ermittelt, bewertet und ggf. verändert werden müssen. Dies wird u. a. in der Bildschirmarbeitsverordnung (BildschArbV) geregelt. Die Kernpunkte der BildschArbV über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten wird in Tabelle 6 dargestellt:

Beurteilung der Arbeitsbedingungen bzgl. Gerät, Arbeitsumgebung, Gefährdung des Sehvermögens sowie körperlicher Probleme und psychischer Belastungen	§ 3 BildschArbV § 5 ArbSchG
Gestaltung von Bildschirmgerät, Tastatur, sonstige Arbeitsmittel und Arbeitsumgebung (Hardware)	Anhang der BildschArbV
Untersuchung der Augen und des Sehvermögens	§ 6 BildschArbV
Arbeitsgestaltung: Pausen, Tätigkeitswechsel	§ 5 BildschArbV
Softwaregestaltung (Zusammenwirken von Mensch-Arbeitsmittel)	Anhang der BildschArbV

Tabelle 6: Kernpunkte der BildschArbV (In M. BURMESTER, 1997; S. 3).

Damit die Bildschirmarbeitstätigkeit als Nutzenfaktor in der Belastungs-Beanspruchungs-Beziehung gesehen wird, kommt vor allem dem letztgenannten Punkt „Softwaregestaltung“ eine Sonderstellung zu. Sie stellt die Dialogschnittstelle in der Mensch-Computer-Interaktion dar und muss nach folgenden Punkten bewertet werden:

- Darstellung und Anordnung der benötigten Informationsobjekte am Bildschirm,
- Art und Ablauf des Dialogs zwischen System und Benutzer,
- Abstimmung und Verknüpfung der funktionellen Anforderungen mit der eingesetzten Anwendungssoftware.

Im Speziellen heißt das, dass zur Bewertung der Software-Ergonomie bestimmte Anforderungen erfüllt sein müssen. Diese werden nach ISO 9241 folgendermaßen klassifiziert (siehe Tabelle 7):

Anforderungen	**Ein interaktives Software-System ist...**
Aufgabenange-messenheit/ Brauchbarkeit/ Funktionalität:	...**aufgabenangemessen**, wenn es die Benutzer bei der Durchführung ihrer Arbeitsaufgaben effektiv und effizient unterstützt, d. h. die Benutzer durch die Eigenschaften von Interaktionshilfsmittel nicht unnötig belastet werden.
Selbstbeschreibungs-fähigkeit:	... **selbstbeschreibungsfähig**, wenn Benutzer auf Wunsch der Einsatzzweck sowie der Leistungsumfang des Computersystems erläutert werden können und wenn jeder einzelne Interaktionsschritt durch Rückmeldung des Computersystems unmittelbar verständlich ist oder die Benutzer auf Wunsch dem jeweiligen Interaktionsschritt entsprechende Erläuterungen erhalten können.
Steuerbarkeit/ Bedienbarkeit	... **steuerbar**, wenn die Benutzer die Geschwindigkeit des Ablaufs der Interaktion sowie die Auswahl und Reihenfolge von Arbeitsgegenständen und Interaktionshilfsmitteln, sowie darüber hinaus die Art und den Umfang von Ein- und Ausgaben beeinflussen können.
Erwartungs-konformität/ benutzerbezogene Zuverlässigkeit	... **erwartungskonform**, wenn es Erwartungen von Benutzern erfüllt. Diese Erwartungen rekrutieren sich aus Kenntnissen bisheriger (Arbeit-) Abläufe, der Ausbildung und Erfahrungen, die Benutzer aufgrund der Systemtransparenz und –konsistenz während des Umgangs mit Computersystemen erwerben.
Fehlerrobustheit/ Fehlertoleranz und –transparenz	... **fehlerrobust**, wenn trotz erkennbarer fehlerhafter Eingaben das beabsichtigte Arbeitsergebnis ohne oder mit minimalem Korrekturaufwand erreicht wird. Dazu müssen Benutzern die Fehler zum Zwecke der Behebung verständlich gemacht werden.
Adaptivität/ Flexibilität/ Individualisier-barkeit	... **adaptiv**, wenn es Mechanismen für Entwickler und Benutzer bietet, auf geänderte Anforderungen dynamisch zu reagieren. ... **individualisierbar**, wenn es Anpassungen an individuelle Benutzerbedürfnisse bzw. –fähigkeiten im Hinblick auf eine gegebene Aufgabe zulässt.
Erlernbarkeit	... **erlernbar**, wenn es den Benutzern ermöglicht, die Aufgabenbewältigung in einer angemessenen Zeitspanne zu erlernen. ...**lernförderlich**, wenn es den Benutzern während des Lernens Unterstützung und Anleitung gibt
Kooperations- und Kommunikations-förderlichkeit	... **kooperationsförderlich**, wenn es den Benutzern möglich ist, die Aufgaben gemeinsam zu bewältigen. ... **kommunikationsförderlich**, wenn es den Benutzern möglich ist, soziale Beziehungen untereinander zu entwickeln und zu pflegen.
Datensicherheit	... **sicher**, wenn es unbefugten Benutzern unmöglich ist, auf Daten zuzugreifen und diese zu manipulieren.

Tabelle 7: Klassifikation von Bewertungskriterien zur Software-Ergonomie. (In: Das Sanus-Handbuch, 1997; S. 26).

Besonders hervorzuheben sind in diesem Zusammenhang die negativen Auswirkungen am BSAP (vgl. SCHMID, 1995). Auf der physiologischen Ebene wirken überwiegend sitzende Tätigkeiten, geringe körperliche Bewegungen und damit verbunden seltener Haltungswechsel schädigend. Die Auswirkungen sind vor allem auf den Sehapparat und das Muskel-Skelett-System zu spüren. Einen Überblick der Belastungsarten und damit verbunden Folgen wird in folgender Tabelle 8 dargestellt:

Belastungsfaktoren durch BSAP	**Beanspruchungsfolgen**	**Autoren**
- Sehvermögen und Sehanforderung durch schlechte Bildschirmqualität, Beleuchtung, Blendung, Spiegelung, Kontrast, Helligkeit oder ungünstige Gestaltung der Informationsdarstellung - ungünstige Arbeitsorganisation (z. B. Arbeitszeit, kurzzyklische und fremdbestimmte Arbeitsaufgaben)	• Verschwommensehen, Augentränen, -brennen, -rötung, Lidflattern, Schulter-Nacken-Schmerzen, Rückenschmerzen, Kopfschmerzen und Konzentrationsstörungen • Peripheren Anhangsgebilde des Auges (Lider, Bindehaut), Ermüdung, Leistungsabfall	MAINTZ (1995) SCHWANINGER et al. (1992) SCHMID (1995) und ÖSTBERG & HÖGBERG (1990) und NIBEL & GEHM (1990)
Muskel-Skelett-System - durch ungünstige Körperhaltung, kleiner Bewegungsraum, ungünstige Sehbedingungen und emotionale Verspannung - durch einförmige repetitive Arbeitsanforderungen	• Rücken, Hals, Schulter, Hand, Handgelenk • Schmerzhafte Bewegungsweinschränkungen, Muskelpartien und Sehnenansatzstellen • Dauernde Anspannung der Rückenmuskulatur, Muskelverspannung und –versteifungen, Gefühle der Kraftlosigkeit an Kopf, Hals, Nacken, Schultern, Rücken und Armen (sog. RSI-Syndrom – Repetititve-Strain-Injury) • Kopf-/Rückenschmerzen, Augenbeschwerden	SCHMID (1995) SCHWANINGER et al. (1992) und BOIKAT (1986) KÖSSLER & HEUCHERT (1993) und PATKIN (1990) LOERZER (1991)
Atmungsorgane, Verdauungsorgane - aufgrund sitzender Tätigkeit	• Verminderte Sauerstoffaufnahme, Konzentrationsstörungen, vorzeitige Ermüdung, verminderte Beanspruchung des Herz-Kreislauf-Systems	ERTEL et al. (1997)

Tabelle 8: Belastungen und Beanspruchungsfolgen bei Bildschirmarbeitsplätzen (zusammengestellt aus ERTEL ET AL. (1997).

Um eine Integration von sowohl arbeits- und software-ergonomischer Kriterien als auch den psychologischen Humankriterien bei der Arbeitstätigkeit zu ermöglichen, richtet WIELAND-ECKELMANN (1996) seine Herangehensweise am Januskopf der Beanspruchung aus. Er konnte nachweisen, dass unter Berücksichtigung der o. g. Beanspruchungsdimensionen „Mental", „Motivational", „Emotional" und „Physisch" solche Arbeitsaufgaben funktionale Beanspruchungsfolgen haben, bei denen die mentalen und motivationalen Aspekte im Vordergrund stehen und emotionale und physische Einflüsse eher als gering bewertet werden. Umgekehrt liegt der Fall bei dysfunktionalen Beanspruchungswirkungen, d. h., es gilt das individuelle Optimum zwischen äußeren Belastungsfaktoren und inneren Regelungsmechanismen herzustellen. In einer Vorstudie wurde bei der Beanspruchungsanalyse die Arbeitsaufgabe am BSAP nach den Humankriterien der Arbeitsaufgabe und unter Hinzunahme der vier Beanspruchungsdimensionen untersucht. Das Ergebnis zeigt das folgende Bewertungsschema (Tabelle 9; vgl. WIELAND-ECKELMANN, 1996):

Kriterien der humanen Arbeits-platzgestaltung	**Belastungsfaktoren**	**Mindestanforderungen** Der Belastungsfaktor sollte...
Aufgaben-anforderung	Gedächtnisanforderungen	... oft zutreffen
	Verarbeitungsoperationen	... oft zutreffen
	Routinisierte Handlungen	... manchmal zutreffen
	Kurzzyklische Tätigkeiten	... selten zutreffen
Tätigkeitsspiel-raum	Großer Entscheidungsspielraum	... oft zutreffen
	Großer Gestaltungsspielraum	... oft zutreffen
	Einseitige Arbeit ohne Handlungsspielraum	...selten zutreffen
Regulations-behinderungen	Wartezeit	... selten zutreffen
	Mangelnde Rückmeldung	... selten zutreffen
	Schlechte Arbeitsbedingungen	... selten zutreffen
	Mangelnde Transparenz	... selten zutreffen
Leistungskontrolle	Leistungsvorgaben	... manchmal zutreffen
	Zeitvorgaben	... manchmal zutreffen
Kooperation & Kommunikation	Einzelarbeit	... oft zutreffen
	Kooperative Arbeit	... oft zutreffen

Tabelle 9: Belastungsfaktoren am BSAP nach Wieland-Eckelmann et al. (1996)

In diesem Bewertungsschema werden die oben beschriebenen Schnittstellen bzw. deren Einflussfaktoren aus der Sicht des Mitarbeiters berücksichtigt. Gerade im Hinblick auf zunehmende Vernetzung des BSAP durch Intranet und Internet, bilden diese drei Aspekte einen Ansatzpunkt, um den Mitarbeitern gesundheits- und persönlichkeitsförderliche Arbeitsbedingungen zu liefern. Werden diese Aspekt vernachlässigt, kann dies sowohl „negative Folgen für das Engagement und die Arbeitszufriedenheit der Beschäftigten haben“ (WEIßGERBER, 1998; S. 7), als auch negative Folgen für die Gesundheit und Umsetzung von Sicherheitsmaßnahmen.

3 Fragestellung

Der vorrangige und damit erste Schwerpunkt der vorliegenden Arbeit bildet die Konstruktion und Überprüfung eines Fragebogens als Instrument zur Erhebung und Bewertung des betrieblichen IT-Sicherheitniveaus auf individueller Ebene der Mitarbeiter. Die Bestimmungsgrößen des IT-sicherem Verhaltens und das Führungsverhalten der Vorgesetzten sollen funktional als qualitative Leistungsindikatoren für ein IT-Sicherheitsmanagement genutzt werden. Der Entwicklung des Fragebogens liegen die Theorie des geplanten Verhaltens, die Zielsetzungstheorie und die Soziale Unterstützung am Arbeitsplatz zugrunde. Dabei werden folgende Schritte durchgeführt:

1. Schritt: Hier werden die theoretisch abgeleiteten Bestimmungsgrößen der Mitarbeiterführung, des IT-Sicherheitverhaltens und der Sozialen Unterstützung am Arbeitsplatz hinsichtlich der testtheoretischen Gütekriterien „Objektivität“, „Reliabilität“ und „Validität“ überprüft.
2. Schritt: Hier werden Typenprofile mit Hilfe einer Cluster- & Diskriminanzanalyse gebildet, um statistische Zusammenhänge bzgl. des wahrgenommenen Führungsstils, dem IT-sicherem Verhalten, der psychischen Belastung und psychischen Beanspruchung am BSAP und der BSAP-Gestaltung bzgl. der softwareergonomischen Kriterien herauszuarbeiten (siehe Abbildung 13).
3. Schritt: Dies umfasst die Analyse der Zusammenhänge zwischen den Ausprägungen der Skalen des Fragebogens zum IT-sicherem Verhalten und anderen individuellen Leistungsindikatoren (siehe Abbildung 14).

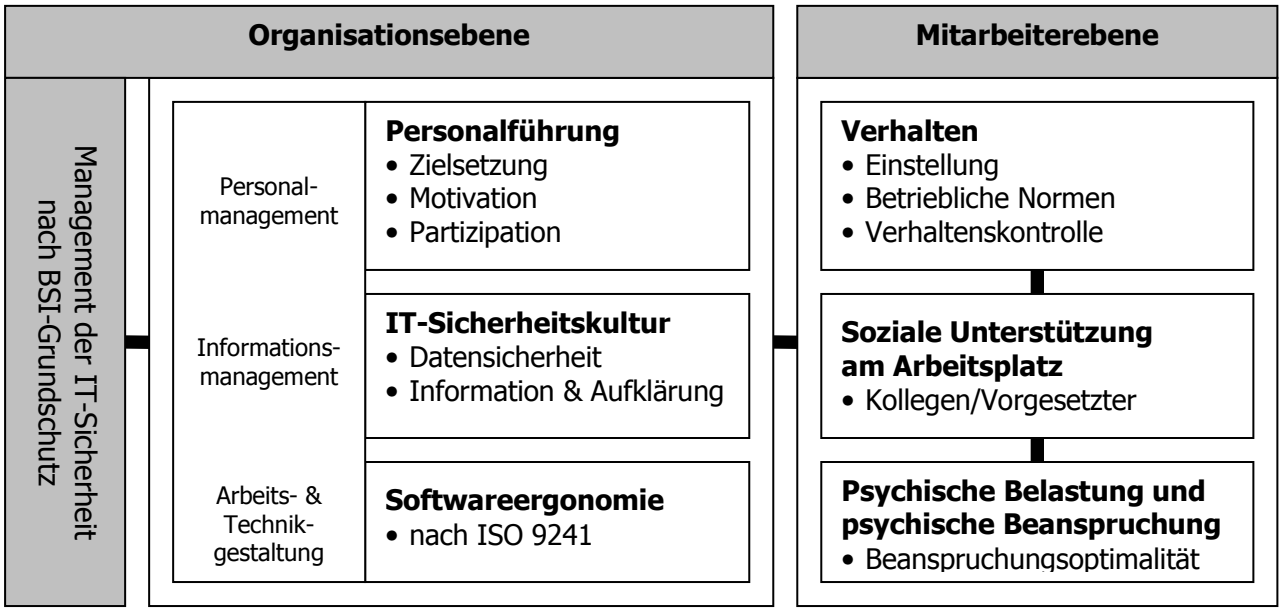


Abbildung 13: Untersuchungsdesign 1 (Modifiziert nach ZIMOLONG, 1995)

Der zweite Schwerpunkt beinhaltet den Vergleich IT-sicherheitsgerechtem Verhalten zwischen einer Gruppe von „IT-Anwendern“ und „IT-Experten“. Hier sollen Mittelwertunterschiede herangezogen werden um Aussagen machen zu können, ob spezielle IT-Kenntnisse das IT-sichere Verhalten beeinflussen.

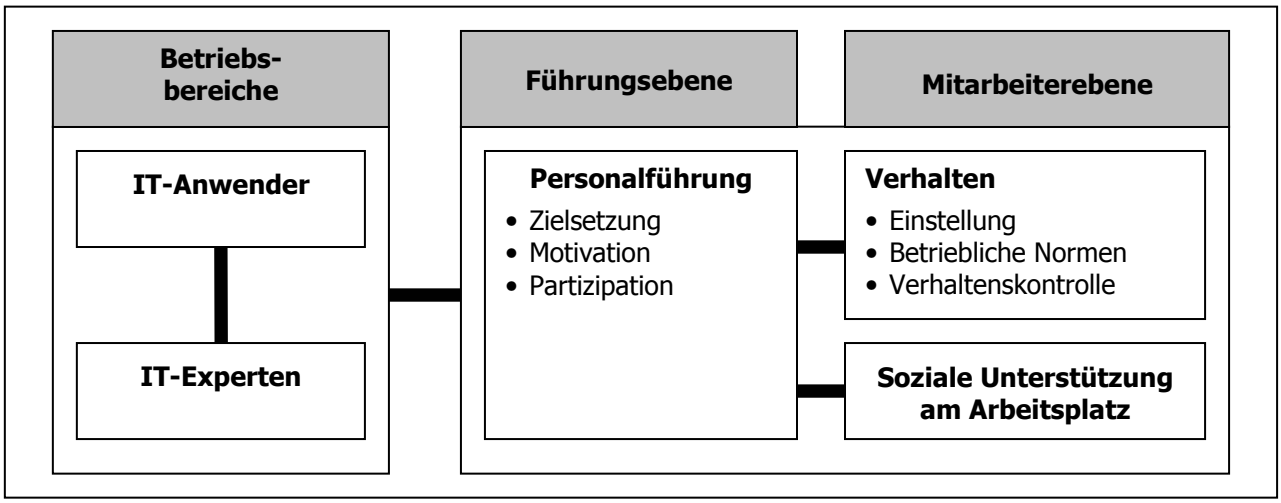


Abbildung 14: Untersuchungsdesign 2

Als Indikator zum Vergleich der Bezugsgrößen werden die Kriterien nach BSI-Grundschutzkatalog herangezogen. Die Erhebung hierfür erfolgt mittels eines zusammengestellten Fragenkatalogs nach BSI-Grundschutz und wird mit dem IT-Sicherheitsmanager des Unternehmens durchgeführt. Die Zusammenhänge zwischen den Ausprägungen der Skalen zur Mitarbeitführung und denen des IT-Sicherheitverhaltens und den Ergebnissen des Interviews können als kriteriumsorientierte Validität des Messinstruments bewertet werden.

Die Hypothesen für den jeweiligen Untersuchungsschwerpunkt und das spezielle Vorgehen bei den einzelnen Analysen werden vor den entsprechenden Ergebnisdarstellungen präzisiert.

4 Konstruktion und Überprüfung des Fragebogens

Bei der Konstruktion und Gestaltung des Fragebogeninstruments wurden folgende Ziele verfolgt:

1. Adäquate Abbildung des entwickelten Modellansatzes.
2. Vergleichbarkeit der Ergebnisse.
3. Einhaltung der Gütekriterien.

Um das Kriterium 1 zu erfüllen, muss das Verfahren die einzelnen Modellkomponenten als Skalen abbilden können. Punkt 2 wird verfolgt, indem zur Itemsammlung auf Literatur und Expertenbefragungen zurückgegriffen wird. Der letzte Punkt wird durch die statistische Überprüfung nach testmethodischen Kriterien erreicht.

4.1 Methodik

4.1.1 Durchführung der Untersuchung

Die vorliegende Untersuchung wurde bei einem großen Finanzdienstleister[14] in Nordrhein-Westfalen durchgeführt. Die Erhebung der Daten fand in zwei Bereichen statt:

- In dem „Service“-Bereich mit Mitarbeitern ohne tiefergreifender Qualifikation bzgl. der Thematik IT (ohne IT-bezogenem Studium, ohne spezielle Ausbildung etc.) – „IT-Anwender“.
- In der IT-Abteilung. D. h hier wurden qualifizierte Mitarbeiter bzgl. der „IT-Sicherheitsthemen“ befragt (mit IT-bezogenem Studium, mit spezieller Ausbildung etc.) – „IT-Experten“.

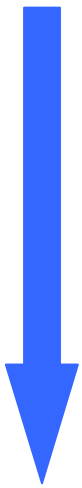
[14] Das Unternehmen möchte nicht genannt werden, ist aber der Universität bekannt.

Die schriftlichen Befragungen fanden in einem Zeitraum von Dezember 2003 bis Februar 2004 statt. Die standardisierte Instruktion zur Ausfüllung des Fragebogens findet sich im Anhang.

Für die 1. Fragebogenaktion im Bereich „Service“ wurden 13 Bereiche per Zufallsprinzip ausgewählt. Davon nahmen 11 Bereiche an der Fragebogenaktion teil. Aus diesen 11 Bereichen wurden insgesamt 470 Fragebögen an die Mitarbeiter ausgeteilt. 203 Fragebögen wurden zurückgeschickt, von denen 192 Fragebögen in die Auswertung einflossen. Die 2. Fragebogenaktion im Bereich „IT-Abteilung“ startete im Februar 2004 bei allen ca. 300 Mitarbeitern. Hier wurden 103 Fragebögen zurückgesendet, von denen 100 Fragebögen in die Auswertung einflossen. Die Auswertung erfolgte anonym und extern an der Universität in Wuppertal

Die Erhebung des „objektiven“ IT-Sicherheitniveaus nach BSI-Grundschutz fand in Form eines Interviews mit den jeweiligen Spezialisten statt.

Der Projektablauf soll mit folgender Tabelle 10 verdeutlicht werden:

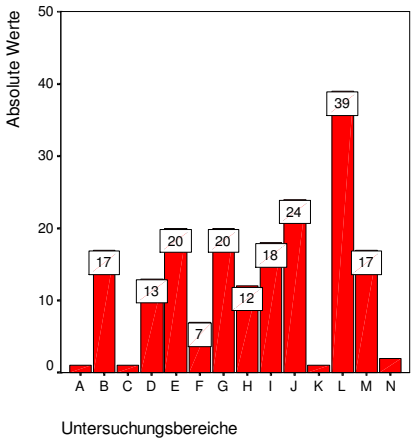


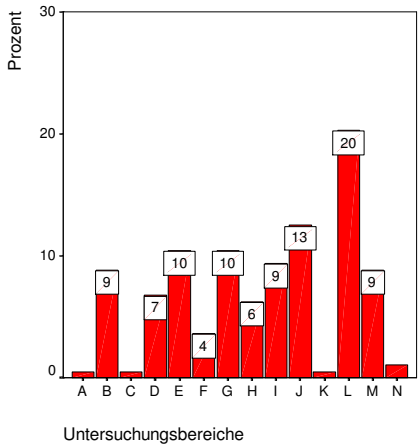
Kick-Off Meeting	Vorstellung des Projektteams; Auswahl der Untersuchungsbereiche
Information aller Betroffenen über die Fb-Aktion	Absprache mit dem Betriebsrat (BR); Benachrichtigung der Betriebsleiter (BL)
IST-Aufnahme	Interview; Fragebogenaktion
Auswertung	Externe Auswertung der Fragebögen
Vorab-Dokumentation	Berichtsentwurf und Information des BR
Abstimmung der Abschlussdokumentation	Feststellung offener Punkte
Abschlusspräsentation	Übergabe der Untersuchungsergebnisse

Tabelle 10: Projektablauf

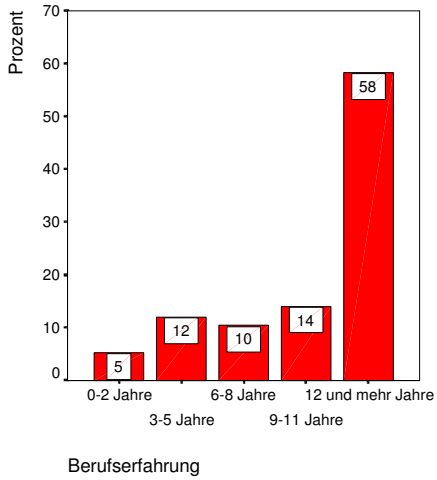
4.1.2 Die Stichprobe

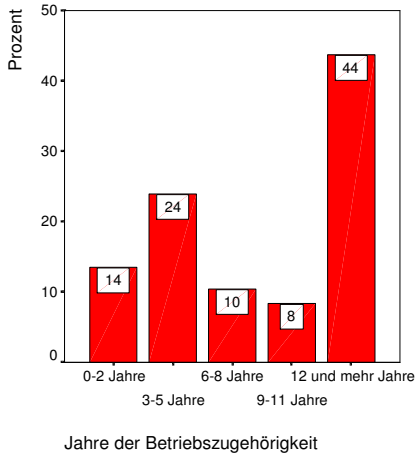
In der folgenden Abbildung sind die Daten, die zur Konstruktion und Validierung des Fragebogens erhoben wurden nach absoluter Häufigkeit und prozentualem Anteil

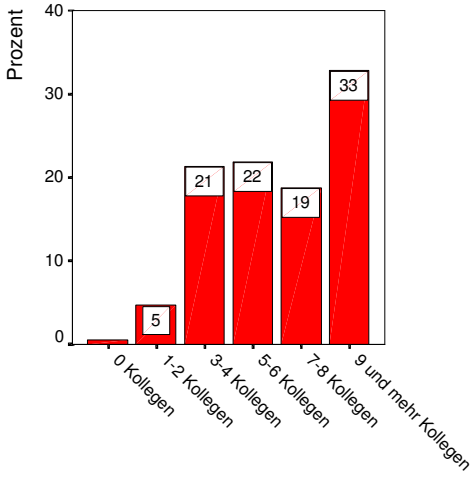


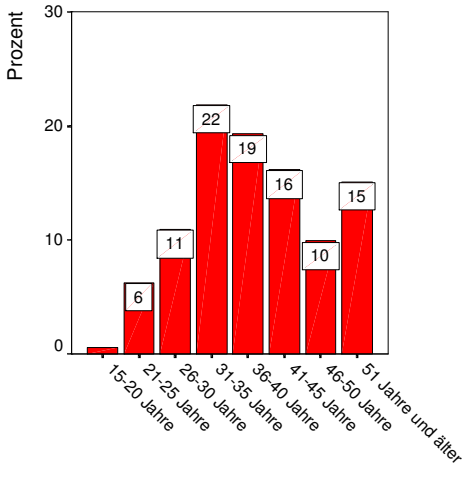


Zur weiteren Beschreibung der Befragungsstichprobe sind in der folgenden Tabelle die demographischen Variablen „Berufserfahrung“, „Jahre der Betriebszugehörigkeit“, Anzahl der engen Kollegen“ und „Alter“ dargestellt:









Die Eckdaten der untersuchten Stichprobe sind in ihrer Verteilung den Realverteilungen kongruent, so dass die Aussage möglich ist, dass die vorliegende Stichprobe repräsentativ ist.

4.1.3 Konzepte und Operationalisierung

Die Konstruktion des Fragebogens zur Messung des subjektiven IT-Sicherheitniveaus basiert auf folgenden theoretischen Konzepten[15]:

- Führungsverhalten: Hier werden insgesamt fünf Skalen zur Lenkung und Koordination des Mitarbeiterverhaltens erfasst (siehe Theoretischer Teil):
- Vorgesetztenverhalten: Die hier erhobenen drei Skalen basieren auf den im „Theoretischen Teil" erörterten Theorien der „Zielsetzung" von LOCKE & LATHAM (1990a) und weiteren Konzepten zur „Partizipation" und „Motivation"
- Unternehmerische Tätigkeit: Die hier erhobenen zwei Skalen ergaben sich aus der praktischen Tätigkeit im IT-Sicherheitsbereich und sollen die Bewertung der unternehmerischen Tätigkeit zur Aufklärung und Information bzgl. Themen der IT-Sicherheit und die unternehmerische Tätigkeit zum Erhalt der Daten messen.
- IT-Sicherheitseinstellung: Die hier erhobenen Skalen resultieren aus der „Theorie des geplanten Verhaltens" von AJZEN & MADDEN (1986). Das IT-sicherheitsbezogene Verhalten wird über das Ausmaß der Intention, sich auch IT-sicherheitsgerecht verhalten zu wollen und deren zugrundeliegenden Bestimmungsgrößen erfasst.

[15] Die Konstruktion des Fragebogens wurde modifiziert nach Stapp et al. (1999).

4.1.4 Skalen des Fragebogens

4.1.4.1 Skalen zum IT-Sicherheitsverhalten

Nach dem zugrunde liegenden Modell und Konzept des Fragebogens wird das Verhalten durch die Verhaltensbereitschaft bestimmt. Diese Bereitschaft ist das Ergebnis folgender Dimensionen:

Einstellung: Die „Einstellung“ soll sich über die Dimensionen „Wissen über Gefahren“ (WÜG), „Persönliche Bedeutung“ (PB), „Verantwortung“ (VA) und „Einschätzung des Stellenwerts IT-Sicherheit für das Unternehmen“ (ESU).

- Die Skala „WÜG“ erfasst die Einschätzung wie wahrscheinlich Daten verändert oder gelöscht werden können. Die Einschätzung von Gefahren am BSAP bildet die Basis zur Bewertung der Konsequenz um IT-Sicherheitsmaßnahmen auch umzusetzen. (9 Fragen)
- Die Skala „PB“ erfasst den emotionalen und kognitiven Aspekt der IT-Sicherheitsmaßnahmen. Zum einen wird erhoben, wie sehr die Themen der IT-Sicherheit die eigentliche Arbeitstätigkeit beeinflussen (emotional), zum anderen wird erhoben, wie sehr sich der Mitarbeiter mit den Themen zur IT-Sicherheit beschäftigt. (6 Fragen)
- Die Skala „VA“ erfasst, wie sehr sich der Mitarbeiter verantwortlich für die Umsetzung der IT-Sicherheitsthemen und den Erhalt der Arbeitsmittel sieht. (3 Fragen)
- Die Skala „ESU“ erfasst die Einschätzung, wie ernst das Unternehmen die Themen der IT-Sicherheit behandelt. (4 Fragen)

Subjektive Norm: Die „Subjektive Norm“ wird über die Skalen „Normative Überzeugung“ (NÜ) und der „Einwilligungsbereitschaft“ (EW) erfasst.

- Die Skala „NÜ“ erfasst den Stellenwert, der das Thema IT-Sicherheit sowohl bei den Kollegen als auch beim Vorgesetzten einnimmt. (11 Fragen)

- Die Skala „EB“ erfasst den Grad der möglichen Einflussnahme durch die Kollegen.
  D. h. wie hoch die Meinungen der Kollegen angesehen werden. (5 Fragen)

Verhaltenstontrolle: Die Dimension „Verhaltenskontrolle“ resultiert aus den Skalen „Fähigkeiten“ (FK), „Internale Kontrollüberzeugung“ (IK) und „Externale Kontrollüber-zeugung“ (EK).

- Die Skala „FK“ erfasst die Einschätzung, geeignete Strategien zum Erhalt der Datensicherheit zu haben. (2 Fragen)
- Die Skala „IK“ erfasst die Überzeugung, selbst Kontrolle über die Gefahrenabwehr am BSAP zu besitzen und dieses durch das eigene Verhalten steuern zu können. (2 Fragen)
- Die Skala „EK“ erfasst die Überzeugung, keine Kontrolle über Gefahrenabwehr am BSAP zu besitzen. Man hat auch keine Möglichkeit der Steuerung und Beeinflussung. (4 Fragen)

Bereitschaft zur IT-Sicherheitsumsetzung: Die Dimension Bereitschaft zur IT-Sicherheitsumsetzung setzt sich zusammen aus der Skala „Intention“ (I) und den Skalen „Soziale Unterstützung/Vorgesetzter“ (SUV) und „Soziale Unterstützung/ Kollegen“ (SUK).

- Die Skale „I“ erfasst die Handlungsbereitschaft die zur Verfügung stehenden Handlungsstrategien zur Sicherung von Daten einzusetzen. (15 Fragen)
- Sie Skalen „SUK“ und „SUV“ werden weiter unten erklärt. (4 & 2 Fragen)

4.1.4.2 Skalen zum Führungsverhalten

Vorgesetztenverhalten: Die Dimension „Vorgesetztenverhalten“ setzt sich zusammen aus den Skalen „Zielsetzung“ (ZS), „Partizipation“ (P) und „Motivation“ (M).

- Die Skale „ZS“ setzt sich zusammen aus Fragen bzgl. IT-Sicherheitsvorgaben, Kontrolle der Umsetzung durch den Vorgesetzten und dem Gespräch über Themen der „IT-Sicherheit“ (3 Fragen)

- Die Skale „P“ bezieht sich darauf, in wieweit der Vorgesetzte an der Weiterbildung und Qualifizierung seiner Mitarbeiter zum Thema interessiert ist. (5 Fragen)
- Die Skala „M“ resultiert überwiegend aus der Bewertung des vorbildlichen Verhaltens des Vorgesetzten und dem Gespräch über die Themen der IT-Sicherheit. (8 Fragen)

Unternehmerische Tätigkeit: Die Dimension „Unternehmerische Tätigkeit“ setzt sich aus den Skalen „Aufklärung & Information“ (AI) und der Skala „Datensicherheit“ (DS) zusammen.

- Die Skala „AI“ bildet sich ab über Fragen bzgl. der Angebote des Informationsflusses durch die Unternehmung. (6 Fragen)
- Die Skala „DS“ setzt sich zusammen aus Fragen, wie sehr die Aktivitäten des Unternehmens zum Erhalt von Daten eingeschätzt werden. (4 Fragen)

4.1.4.3 Skalen zur Sozialen Unterstützung am Arbeitsplatz

Soziale Unterstützung durch die Kollegen (SUK): Die Dimension setzt sich nicht aus verschiedenen Skalen zusammen. Die hier zugehörigen Fragen zielen darauf ab, ob die Kollegin bzw. der Kollege zu Themen der IT-Sicherheit bereitwillig Fragen beantworten. (4 Fragen)

Soziale Unterstützung durch den Vorgesetzten (SUV): Die Dimension setzt sich nicht aus verschiedenen Skalen zusammen. Die hier zugehörigen Fragen zielen darauf ab, ob die Vorgesetzten zu Themen der IT-Sicherheit bereitwillig Fragen beantworten. (2 Fragen)

4.2 Fragebogenkonstruktion

4.2.1 Itemanalyse

Im ersten Schritt werden zum einen die Trennschärfe und zum anderen die Kreuztrennschärfe mit den Items berechnet. Diese Berechnungen erfolgen getrennt zwischen den Fragen des Führungsverhaltens und den Fragen zum IT-sicherheitsgerechtem Verhalten.

4.2.1.1 Trennschärfe (TS) & Kreuztrennschärfe (KTS) für das IT-Sicherheitsverhalten

Die Trennschärfe ist die Korrelation des Items mit dem um das Item reduzierte Summenwert der Skala. Als Kriterium für die Item-Total-Korrelation schlagen LIENERT & RAATZ (1994) eine untere Grenze von .20 vor.

Für die Kreuztrennschärfe gilt, dass es die Korrelation des Items mit dem Summenwert der anderen Skalen ist. Diese sog. Quadrierte Multiple Korrelation sollte den Wert von .30 nicht überschreiten. Diese Forderung unterstellt allerdings die Unabhängigkeit der erhobenen Skalen. Da bei der Fragebogenkonstruktion auf der Modellebene die unabhängigen Skalen „Einstellung“, „Subjektive Normen“ und „Verhaltenskontrolle“ das Ausmaß der abhängigen Skala „Bereitschaft zur Umsetzung von IT-sicherem Verhalten“ bestimmen, wird als Ausschlusskriterium der Kreuztrennschärfe der max. Wert der Trennschärfe definiert. Die Tabellen 11 & 12 zeigen die Ergebnisse der Trennschärfe- und der Kreuztrennschärfeberechnung:

Skala	.	MW	SD	TS
	Item-Nr			
WÜG	EV_0023	2,28	1,09	0,613
	EV_0031	2,50	1,16	0,639
	EV_0056	3,23	1,19	0,518
	EV_0016	2,73	1,04	0,642
	EV_0042			**-0,159**
	EV_0003			**0,128**
	EV_0009	2,46	1,01	0,561
	EV_0065	3,79	1,02	0,508
	EV_0038	3,48	0,96	0,601
PB	EV_0030	2,87	0,97	0,696
	EV_0047	3,33	1,10	0,643
	EV_0022			**0,044**
	EV_0019	3,33	1,00	0,636
	EV_0028	1,63	0,71	0,291
	EV_0069			**0,098**
ESU	EV_0032	2,41	0,91	0,629
	EV_0053	1,86	0,91	0,700
	EV_0048	2,08	0,98	0,765
	EV_0055	2,97	1,03	0,459
VA	EV_0007	1,79	0,95	0,348
	EV_0063	2,01	0,84	0,303
	EV_0050	1,90	0,69	0,312
NÜ	EV_0002	2,31	0,81	0,670
	EV_0046	2,19	0,97	0,767
	EV_0044	2,54	1,09	0,719
	EV_0072	2,40	0,85	0,541
	EV_0040			**0,102**
	EV_0052	2,15	1,07	0,277
	EV_0015	2,65	0,97	0,701
	EV_0024	2,24	0,84	0,825
	EV_0033	2,92	1,15	0,634
	EV_0068			**-0,098**
	EV_0071	3,31	1,11	0,522
EW	EV_0062	1,87	0,79	0,604
	EV_0035	2,18	0,89	0,609
	EV_0017	2,65	0,89	0,677
	EV_0051	2,58	0,89	0,587
	EV_0057	2,51	0,80	0,693
FK	EV_0020	2,65	0,97	0,456
	EV_0029	1,98	0,72	0,456

Skala		MW	SD	TS
	Item-Nr.			
IK	EV_0058	2,78	1,06	0,392
	EV_0054	3,28	1,13	0,392
EK	EV_0070	2,60	1,02	0,270
	EV_0018	1,69	0,89	0,281
	EV_0026	2,86	1,20	0,448
	EV_0010	3,90	0,89	0,230
I	EV_0061	2,71	1,03	0,572
	EV_0014	2,25	0,96	0,377
	EV_0060	1,48	0,88	0,540
	EV_0041			**0,189**
	EV_0073	1,74	1,22	0,217
	EV_0012	3,03	1,32	0,492
	EV_0037	1,67	0,96	0,511
	EV_0066	2,13	0,97	0,500
	EV_0045	1,46	0,67	0,345
	EV_0025			**0,156**
	EV_0059	1,94	0,95	0,437
	EV_0021	1,21	0,55	0,205
	EV_0008	2,97	1,15	0,591
	EV_0034	2,00	1,38	0,417
	EV_0013	1,40	0,85	0,409

Tabelle 11: Trennschärfe zum IT-Sicherheitsverhalten (PB = persönliche Bedeutung, ESU = Einschätzung der Sicherheitsumsetzung des Unternehmens, VA = Verantwortung, NÜ = normative Überzeugung, EW = Einwilligungsbereitschaft, FK Fähigkeiten, IK = internale Kontrollüberzeugung, EK = externale Kontrollüberzeugung, I = Intention)

Nach der o. g. Ausschlussmethode verfehlen folgende Items das Kriterium:

EV_03,_22,_25,_40,_41,_42,_50,_63,_68,_69

Skala	Item-Nr.	MW	SD	TS	KTS WÜG	KTS PB	KTS ESU	KTS VA	KTS NÜ	KTS EW	KTS FK	KTS IK	KTS EK	KTS I
WÜG	EV_0023	2,28	1,09	0,613		-0,019	-0,157	0,136	-0,097	-0,056	-0,091	0,153	0,229	-0,057
	EV_0031	2,50	1,16	0,639		-0,141	-0,161	0,130	-0,320	-0,167	-0,192	-0,028	0,191	-0,196
	EV_0056	3,23	1,19	0,518		-0,266	-0,321	-0,272	-0,513	-0,441	-0,280	-0,011	0,085	-0,331
	EV_0016	2,73	1,04	0,642		-0,151	-0,202	-0,036	-0,296	-0,247	-0,208	-0,143	0,174	-0,244
	EV_0009	2,46	1,01	0,561		-0,274	-0,277	0,048	-0,335	-0,215	-0,305	-0,098	0,043	-0,244
	EV_0065	3,79	1,02	0,508		-0,209	-0,215	-0,130	-0,348	-0,318	-0,137	-0,065	0,072	-0,448
	EV_0038	3,48	0,96	0,601		-0,149	-0,316	-0,050	-0,364	-0,298	-0,403	0,070	0,126	-0,191
PB	EV_0030	2,87	0,97	0,696	-0,216		0,221	0,282	0,501	0,308	0,461	0,317	0,312	0,418
	EV_0047	3,33	1,10	0,643	-0,137		0,005	0,148	0,346	0,175	0,239	0,168	0,179	0,308
	EV_0019	3,33	1,00	0,636	-0,239		0,093	0,178	0,491	0,324	0,459	0,169	0,203	0,314
	EV_0028	1,63	0,71	0,291	-0,183		0,193	0,260	0,211	0,116	0,285	0,174	0,167	0,283
ESU	EV_0032	2,41	0,91	0,629	-0,376	-0,072		0,321	0,451	0,339	0,224	0,055	0,001	0,113
	EV_0053	1,86	0,91	0,700	-0,252	-0,008		0,221	0,363	0,232	0,280	0,078	0,093	0,204
	EV_0048	2,08	0,98	0,765	-0,332	0,137		0,265	0,448	0,257	0,359	0,177	0,180	0,373
	EV_0055	2,97	1,03	0,459	-0,312	0,246		0,153	0,435	0,373	0,201	0,261	0,049	0,319
VA	EV_0007	1,79	0,95	0,348	0,059	0,197	0,090		0,146	0,270	0,218	0,169	0,247	0,274
	EV_0063	**2,01**	**0,84**	**0,303**	**-0,062**	**0,323**	**0,122**		**0,220**	**0,341**	**0,208**	**0,271**	**0,189**	**0,391**
	EV_0050	**1,90**	**0,69**	**0,312**	**-0,076**	**0,092**	**0,124**		**0,180**	**0,338**	**0,168**	**0,100**	**0,013**	**0,314**
NÜ	EV_0002	2,31	0,81	0,670	-0,205	0,333	0,241	0,409		0,604	0,138	0,177	0,036	0,424
	EV_0046	2,19	0,97	0,767	-0,275	0,500	0,345	0,423		0,626	0,319	0,125	0,187	0,430
	EV_0044	2,54	1,09	0,719	-0,264	0,469	0,365	0,296		0,632	0,340	0,185	0,169	0,293
	EV_0072	2,40	0,85	0,541	-0,349	0,075	0,502	0,176		0,368	0,265	-0,027	-0,011	0,217
	EV_0052	**2,15**	**1,07**	**0,277**	**-0,296**	**-0,002**	**0,537**	**0,194**		**0,245**	**0,203**	**0,146**	**0,065**	**0,134**
	EV_0015	**2,65**	**0,97**	**0,701**	**-0,477**	**0,241**	**0,319**	**0,462**		**0,707**	**0,367**	**0,181**	**0,149**	**0,551**
	EV_0024	2,24	0,84	0,825	-0,444	0,367	0,294	0,423		0,776	0,448	0,217	0,111	0,629
	EV_0033	2,92	1,15	0,634	-0,222	0,432	0,408	0,189		0,443	0,324	0,147	0,225	0,378
	EV_0071	3,31	1,11	0,522	-0,236	0,488	0,295	0,230		0,431	0,274	0,251	0,290	0,474
EW	EV_0062	1,87	0,79	0,604	-0,285	0,128	0,162	0,299	0,389		0,126	0,042	-0,093	0,300
	EV_0035	2,18	0,89	0,609	-0,259	0,101	0,148	0,191	0,380		0,122	-0,033	-0,086	0,145
	EV_0017	2,65	0,89	0,677	-0,313	0,356	0,400	0,441	0,666		0,380	0,101	0,166	0,451
	EV_0051	2,58	0,89	0,587	-0,255	0,457	0,406	0,466	0,583		0,310	0,211	0,094	0,401
	EV_0057	2,51	0,80	0,693	-0,433	0,465	0,315	0,439	0,626		0,386	0,237	0,104	0,528
FK	EV_0020	2,65	0,97	0,456	-0,291	0,437	0,239	0,219	0,413	0,267		0,218	0,208	0,316
	EV_0029	1,98	0,72	0,456	-0,160	0,325	0,171	0,240	0,241	0,134		0,219	0,222	0,198
IK	EV_0058	2,78	1,06	0,392	-0,007	0,248	0,094	0,224	0,207	0,083	0,175		0,323	0,307
	EV_0054	3,28	1,13	0,392	-0,087	0,175	0,145	0,241	0,185	0,080	0,219		0,194	0,208

Tabelle 12: Kreuztrennschärfe zum IT-Sicherheitsverhalten (PB = persönliche Bedeutung, ESU = Einschätzung der Sicherheitsumsetzung des Unternehmens, VA = Verantwortung, NÜ = normative Überzeugung, EW = Einwilligungsbereitschaft, FK Fähigkeiten, IK = internale Kontrollüberzeugung)

Skala	Item-Nr.	MW	SD	TS	KTS WÜG	KTS PB	KTS ESU	KTS VA	KTS NÜ	KTS EW	KTS FK	KTS IK	KTS EK	KTS I
EK	EV_0070	2,60	1,02	0,270	0,135	0,200	0,084	0,190	0,202	0,024	0,207	0,263		0,106
	EV_0018	1,69	0,89	0,281	0,067	0,237	0,024	0,229	0,197	0,064	0,186	0,095		0,199
	EV_0026	2,86	1,20	0,448	0,156	0,213	0,048	0,206	0,017	0,031	0,208	0,231		0,121
	EV_0010	3,90	0,89	0,230	0,108	0,160	-0,089	0,159	0,064	0,119	0,061	0,229		0,115
I	**EV_0061**	**2,71**	**1,03**	**0,572**	**-0,266**	**0,546**	**0,229**	**0,356**	**0,641**	**0,477**	**0,267**	**0,342**	**0,206**	
	EV_0014	2,25	0,96	0,377	-0,327	0,197	0,135	0,321	0,186	0,295	0,180	0,078	-0,045	
	EV_0060	1,48	0,88	0,540	-0,102	0,203	0,071	0,155	0,112	0,108	0,119	0,118	0,056	
	EV_0073	1,74	1,22	0,217	-0,053	-0,023	0,008	0,027	-0,049	0,034	0,030	0,125	-0,002	
	EV_0012	3,03	1,32	0,492	-0,277	0,383	0,219	0,280	0,345	0,223	0,202	0,239	0,092	
	EV_0037	1,67	0,96	0,511	-0,093	0,256	-0,029	0,290	0,157	0,109	0,123	0,131	0,081	
	EV_0066	2,13	0,97	0,500	-0,286	0,261	0,029	0,189	0,215	0,178	0,264	0,135	-0,048	
	EV_0045	**1,46**	**0,67**	**0,345**	**-0,095**	**0,299**	**0,122**	**0,429**	**0,255**	**0,190**	**0,260**	**0,166**	**0,225**	
	EV_0059	1,94	0,95	0,437	-0,303	0,181	0,187	0,242	0,304	0,190	0,200	0,152	0,026	
	EV_0021	1,21	0,55	0,205	-0,016	0,049	-0,055	0,112	-0,028	0,205	0,183	-0,030	0,068	
	EV_0008	2,97	1,15	0,591	-0,188	0,501	0,196	0,444	0,571	0,470	0,252	0,303	0,247	
	EV_0034	2,00	1,38	0,417	-0,253	0,267	0,241	0,352	0,371	0,412	0,218	0,286	0,000	
	EV_0013	1,40	0,85	0,409	-0,135	0,150	0,047	0,040	0,089	0,075	0,061	0,096	0,107	

Tabelle 12: (Fortsetzung): Kreuztrennschärfe zum IT-Sicherheitsverhalten (EK = externale Kontrollüberzeugung, I = Intention)

Hier verfehlen folgende Items das Auswahlkriterium: EV_15,_45,_52,_61.
Die Skala „Verantwortung“ (VA) wird ganz herausgenommen.

4.2.1.1.1 Trennschärfe und Kreuztrennschärfe für die Einschätzung der unternehmerischen Tätigkeit

In den Tabellen 13 & 14 werden die Ergebnisse der Trennschärfe und Kreuztrennschärfe für die Einschätzung der unternehmerischen Tätigkeit zur IT-Sicherheit dargestellt:

Skala	Item-Nr.	MW	SD	TS
AI	FO_0005	2,13	0,98	.3449
	FO_0012	2,96	1,15	.6889
	FO_0015	2,94	1,23	.5768
	FO_0017	2,87	1,05	.6841
	FO_0019	2,23	0,91	.5449
	FO_0010	3,13	1,57	.5067
DS	FO_0002	2,47	1,02	.4159
	FO_0003	2,03	0,99	.4903
	FO_0016	2,18	1,13	.5972
	FO_0021	3,01	1,28	.4618

Tabelle 13: Trennschärfeergebnis der unternehmerischen Tätigkeit zur IT-Sicherheit (AI = Aufklärung & Information, DS = Datensicherheit).

Alle Items bleiben in den Skalen

Skala	Item-Nr.	MW	SD	TS	KTS AI	KTS DS
AI	FO_0005	2,1	1	.3449		0,281
	FO_0012	3	1,2	.6889		0,432
	FO_0015	2,9	1,2	.5768		0,425
	FO_0017	2,9	1,1	.6841		0,465
	FO_0019	2,2	0,9	.5449		0,513
	FO_0010	3,1	1,6	.5067		0,248
DS	FO_0002	2,5	1	.4159	0,275	
	FO_0003	2	1	.4903	0,354	
	FO_0016	2,2	1,1	.5972	0,480	
	FO_0021	3	1,3	.4618	0,467	

Tabelle 14: Kreuztrennschärfeergebnis der unternehmerischen Tätigkeit zur IT-Sicherheit (AI = Aufklärung & Information, DS = Datensicherheit).

Auch nach der Betrachtung der Kreuztrennschärfe verbleiben alle Items in den Skalen.

Die Tabellen 15 & 16 zeigen die Trennschärfe- & Kreuztrennschärfeergebnisse des Vorgesetztenverhaltens:

Skala	Item-Nr.	MW	SD	TS
ZS	FO_0007	3,13	1,09	.7110
	FO_0004	3,05	1,16	.7024
	FO_0009	3,82	1,04	.5704
P	FO_0011	3,19	1,29	.6036
	FO_0018	2,92	1,24	.5404
	FO_0020	2,81	1,08	.5799
	FO_0001	4,45	0,82	.2665
	FO_0014	3,09	1,27	.6056
M	FO_0006	2,11	0,93	.7478
	FO_0022	1,96	1,05	.6521
	FO_0025	2,41	1,17	.7486
	FO_0026	2,3	1,21	.4249
	FO_0013	2,64	1,08	.7157
	FO_0023	2,68	0,93	.4532
	FO_0024	1,57	0,92	.4815
	FO_0027	2,89	1,09	.5874

Tabelle 15: Trennschärfeergebnisse des Vorgesetztenverhaltens (ZS = Zielsetzung, P = Partizipation, M = Motivation).

Skala	Item-Nr.	MW	SD	TS	KTS ZS	KTS P	KTS M
ZS	FO_0007	3,1	1,1	.7110		0,692	0,615
	FO_0004	3,1	1,2	.7024		0,645	0,623
	FO_0009	3,8	1	.5704		0,539	0,422
P	FO_0011	3,2	1,3	.6036	0,584		0,565
	FO_0018	2,9	1,2	.5404	0,536		0,532
	FO_0020	2,8	1,1	.5799	0,526		0,561
	FO_0001	**4,5**	**0,8**	**.2665**	**0,282**		**0,265**
	FO_0014	3,1	1,3	.6056	0,472		0,536
M	FO_0006	2,1	0,9	.7478	0,659	0,589	
	FO_0022	2	1,1	.6521	0,410	0,429	
	FO_0025	2,4	1,2	.7486	0,620	0,623	
	FO_0026	2,3	1,2	.4249	0,317	0,381	
	FO_0013	2,6	1,1	.7157	0,684	0,712	
	FO_0023	2,7	0,9	.4532	0,216	0,278	
	FO_0024	1,6	0,9	.4815	0,248	0,327	
	FO_0027	**2,9**	**1,1**	**.5874**	**0,677**	**0,699**	

Tabelle 16: Kreuztrennschärfeergebnis des Vorgesetztenverhaltens (ZS = Zielsetzung, P = Partizipation, M = Motivation).

Es werden die Items FO_01_27 ausgeschlossen

4.2.2 Relative Informationsgehalt der Items

Um die Differenzierungsfähigkeit eines Items bei Mehrfachwahlantworten ohne Bestantwort zu berechnet, wird der relative Informationsgehalt nach Mittenecker & Raab (1973) berechnet. Dieses Maß gilt als Index der darüber Auskunft gibt, wie die vorgegebenen Antwortstufen ausgenutzt wurden (vgl. Shannon, 1949). Der Relative Informationsgehalt variiert zwischen 0 – es wird nur eine Skalenstufe angekreuzt – und 1 – es werden alle Skalenstufen gleich häufig angekreuzt. Der Index errechnet sich aus dem Verhältnis des tatsächlichen Informationsgehalts und des max. möglichen. Die Tabelle zur Berechnung des Relativen Informationsgehalts wird in der folgenden Formel dargestellt:

h(x) $$h(x) = \frac{H(X)}{H(\max)}$$

wobei H (X) = ldN - $\frac{1}{N}\sum_{i-1} N$ (xi)ldN (xi) und H (max) = ld (q)

mit N (xi) = absolute Häufigkeit der i-ten Skalenstufe und q = Anzahl der Skalenstufen

Als Kriterium wird festgelegt, dass mehr als die Hälfte der möglichen Informationen genutzt werden sollten. D. h. der Wert von .50 sollte nicht unterschritten werden.
Alle in dem Fragebogen verbliebenen Items erfüllen das oben beschriebene Kriterium.

4.2.3 Skalenanalyse

4.2.3.1 Reliabilitätsanalyse

Zur Bestimmung der inneren Konsistenz der Skalen werden Konsistenzanalysen durchgeführt. Damit wird die Messgenauigkeit eines Tests bestimmt. Nach Lienert & Raatz (1994) bildet die Reliabilitätsanalyse nach Cronbach auf Grund der Unabhängigkeit der Bedingungen bei der Testdurchführung – im Gegensatz zu Parallel- oder Retestreliabilität – das geeignete Maß zu Bewertung der Leistungsfähigkeit eines Tests als Messinstrument. Als Kriterium werden

Reliabilitätskoeffizienten mit >.50 als zufriedenstellend akzeptiert. Das Ergebnis wird in der Tabelle 17 dargestellt:

Skalen	Item	Cronbach´s Alpha
Vorgesetztenverhalten (V)		
V:ZS	fo_04, fo_07, fo_09	.810
V:P	fo_11, fo_14, fo_18, fo_20	.777
V:M	fo_06, fo_13, fo_22, fo_23, fo_24, fo_25, fo_26	.837
Unternehmerische Tätigkeit (U)		
U:AI	fo_05, fo_10, fo_12, fo_15, fo_17, fo_19	.790
U:DS	fo_02, fo_03, fo_16, fo_21	.702
IT-Sicherheitsverhalten		
WÜG	ev_09, ev_16, ev_23, ev_31, ev_38, ev_56, ev_65	.833
PB	ev_19, ev_28, ev_30, ev_47	.761
ESU	ev_32, ev_48, ev_53, ev_55	.815
NÜ	ev_02, ev_24, ev_33, ev_44, ev_46, ev_71, ev_72	.836
EW	ev_17, ev_35, ev_51, ev_57, ev_62	.833
FK	ev_20, ev_29	.609
IK	ev_54, ev_58	.562
EK	ev_10, ev_18, ev_26, ev_70	.514
I	ev_08, ev_12, ev_13, ev_14, ev_21, ev_34, ev_37, ev_59, ev_60, ev_66, ev_73	.745
Soziale Unterstützung		
SUK	ev_05, ev_27, ev_36, ev_64	.681
SUV	ev_01, ev_43	.759

Tabelle 17: Reliabilitätskennwerte nach Cronbach (ZS = Zielsetzung, P = Partizipation, M = Motivation, AI = Aufklärung & Information, DS = Datensicherheit, WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, I = Intention, SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).

4.2.3.2 Weitere Skalenwerte

Um einen Überblick über die Mittelwerte, Standardabweichungen und anderen statistischen Kennwerten der Skalen zur erhalten, wurden diese in der folgenden Tabelle 18 zusammengestellt:

	Bereich	Min	Max	MW	SD	Schiefe	Kurtosis
Vorgesetztenverhalten							
V:ZS	1 bis 5	1,00	5,00	3,32	1,00	-0,05	-0,57
V:P	1 bis 5	1,40	5,00	3,30	0,79	0,12	-0,47
V:M	1 bis 5	1,00	4,63	2,32	0,60	0,73	1,17
Unternehmerische Tätigkeit							
U:AI	1 bis 5	1,00	4,67	2,71	0,77	-0,05	-0,29
U:DS	1 bis 5	1,00	5,00	2,37	0,88	0,74	0,36
IT-Sicherheitsverhalten							
WÜG	1 bis 5	1,14	4,86	2,92	0,62	-0,02	0,69
PB	1 bis 5	1,00	4,50	2,79	0,70	0,09	-0,16
ESU	1 bis 5	1,00	5,00	2,33	0,58	0,96	3,41
NÜ	1 bis 5	1,10	4,10	2,58	0,48	0,00	1,17
EB	1 bis 5	1,67	4,00	2,59	0,42	0,61	0,52
FK	1 bis 5	1,00	5,00	2,31	0,71	0,35	0,37
IK	1 bis 5	1,00	5,00	3,03	0,85	0,14	0,14
EK	1 bis 5	1,25	4,75	2,76	0,62	0,08	-0,02
I	1 bis 5	1,08	3,23	2,00	0,49	0,33	-0,46

Tabelle 18: Zusammenfassung der statistischen Kennwerte (ZS = Zielsetzung, P = Partizipation, M = Motivation, AI = Aufklärung & Information, DS = Datensicherheit, WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, I = Intention).

4.2.4 Validität des Fragebogens

Es wird bei der Validität eines Tests zwischen der inhaltlichen, der kriterienbezogenen und der Konstruktvalidität unterschieden.

Bei der inhaltlichen Validität wird nach HÄCKER, LEUTNER & AMELANG (1998) „das Ausmaß, in dem eine Stichprobe von Items, Leistungsaufgaben oder Fragen eines Test eine definierte inhaltliche Grundgesamtheit repräsentiert“ (o. o. A., 1998, S. 342) verstanden. Dabei wird häufig auf die Einschätzung von Experten zurückgegriffen. Da bei der Erstellung, Formulierung und Konstruktion der Skalen eine Reihe von Experten aus der Wirtschaft und Wissenschaft beteiligt waren, kann von einer ausreichenden inhaltlichen Validität ausgegangen werden.

Zur Überprüfung der Konstruktvalidität wird nach LIENTER & RAATZ (1994) schwerpunktmäßig eine inhaltlich-logische Analyse der einzelnen Fragebogenelemente durchgeführt. Dies dient der Ermittlung bzgl. der Aussagekraft eines Testwerts bzw. um den Ausprägungsgrad der interessierenden psychologischen Eigenschaft zu messen. Hierfür werden zum einen Analysen der Skaleninterkorrelationen durchgeführt, um Zusammenhänge auf der Skalenebene zu untersuchen. Zum anderen kann mit Hilfe einer Kovarianzstrukturanalyse die Passung zwischen dem theoretischen Konzept und den empirischen Daten überprüft werden.

Der Zusammenhang zwischen dem Testpunktwert und dem Kriterienpunktwert wird mit Hilfe der kriterienbezogenen Validität bestimmt. Dabei wird der einzelne Testpunktwert mit einem Außenkriterium korreliert. Zur Überprüfung der kriterienbezogenen Validität gelten die Daten aus der BSI-Grundschutzanalyse. Diese erfolgte systematischer Form mit Hilfe eines Expertenratings. Die relevanten Themenbereiche aus dem vom BSI vorgegebenen IT-Grundschutzkatalog wurden mit dem IT-Sicherheitsexperten ausgewählt und zu einem Fragenkatalog zusammengefasst. Es gingen folgende Themenbereiche in den Fragebogen ein:

- IT-Sicherheitsmanagement: Dieser Bereich umfasst Fragen zur Erstellung und Durchführung aller relevanten Schritte zur Bildung und Etablierung eines umfassenden IT-Sicherheitsprozesses. Z. B. den Aufbau einer geeigneten Organisationsstruktur (Planung, Einführung und Pflege), Erstellung, Umsetzung und Dokumentation eines IT-Sicherheitskonzepts etc.
- Organisation: Dieser Bereich umfasst die Festlegung von Verantwortlichkeiten, Regelung des Gebrauchs von Zugriffsrechten, IT-Sicherheitsbestimmungen (z. B. Passwort, Bildschirmschoner, e-Mail-Nutzung, Computer-Viren-Programme etc.), Kommunkationspartnern, Sicherheitspolitik usw.
- Personal: Dieser Bereich umfasst die Einarbeitung, Schulung und Sensibilisierung der Mitarbeiter über Gesetze, Vorschriften und Regelungen zur Umsetzung relevanter IT-Sicherheitsthemen am BSAP.

Die folgende Tabelle 19 zeigt die Anzahl der Kategorien und die Anzahl der Fragen zu den einzelnen Bereichen:

Bereich	Kategorien	Fragen insgesamt
IT-Sicherheitsmanagement	13	88
Organisation	17	101
Personal	8	36

Tabelle 19: Anzahl der Kategorien und der Fragen für die einzelnen Bereiche.

Die Beantwortung der einzelnen Fragen erfolgte nach folgendem Schema:

1 = Die Aussage ist erfüllt

2 = Die Aussage ist teilweise erfüllt

3 = Die Aussage ist nicht erfüllt

x = Keine Beantwortung möglich/Frage ist nicht relevant

Die Formulierung der Frage wurde so gewählt, dass die Nichterfüllung einer Aussage die Maßnahme zur Erfüllung der Aussage beinhaltet. Das Ergebnis der Analyse kann dem Anhang entnommen werden.

4.2.5 Skaleninterkorrelationen

	PB	ESU	NÜ	EW	FK	IK	EK	I	AI	DS	ZS	P	M
WÜG	-0,232*	-0,358*	-0,427*	-0,378*	-0,283*	-0,079	0,227*	-0,343*	-0,311*	-0,310*	-0,300*	-0,324*	-0,310*
PB		0,127	0,528*	0,296*	0,465*	0,271*	0,190*	0,415*	0,301*	0,083	0,358*	0,431*	0,300*
ESU			0,520*	0,373*	0,283*	0,156	-0,006	0,218*	0,535*	0,410*	0,464*	0,498*	0,540*
NÜ				0,627*	0,417*	0,237*	0,074	0,429*	0,643*	0,437*	0,680*	0,724*	0,692*
EW					0,289*	0,119	-0,037	0,391*	0,385*	0,319*	0,433*	0,411*	0,510*
FK						0,257*	0,223*	0,295*	0,438*	0,326*	0,317*	0,408*	0,410*
IK							0,285*	0,293*	0,197	0,068	0,277*	0,276*	0,051
EK								0,086	0,147	-0,108	0,062	0,178	0,066
I									0,259*	0,323*	0,348*	0,316*	0,352*
AI										0,507*	0,596*	0,783*	0,692*
DS											0,470*	0,370*	0,566*
ZS												0,723*	0,596*
P													0,656*

Tabelle 20: Skaleninterkorrelationen mit Darstellung der Spearman Korrelations-koeffizienten; fett= p ≤ 0,01; (WÜG= Wissen über Gefahren,PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, I = Intention, AI = Aufklärung & Information, DS = Datensicherheit, ZS = Zielsetzung, P = Partizipation, M = Motivation).

4.2.5.1 Einstellung

Die Dimension „Einstellung“ wird abgebildet über die Skalen „Wissen über Gefahren“ (WÜG), „Persönliche Bedeutung“ (PD) und „Einschätzung des Stellenwertes für das Unternehmen“ (ESU). Die Skale „WÜG“ weist eine negative statistisch bedeutsam Korrelation mit der Skale „ESU“ und „PB“ auf. Nur die Skale „PB“ zeigt keinen Zusammenhang mit der Skala „ESU“.

4.2.5.2 Subjektive Normen

Die Dimension „Subjektive Normen“ wird abgebildet über die Skalen „Normative Überzeugung“ und „Einwilligungsbereitschaft“. Der statistische Zusammenhang ist hier mit r=.672 sehr hoch.

4.2.5.3 Verhaltenskontrolle

Die Dimension „Verhaltenskontrolle“ wird abgebildet über die Skalen „Fähigkeiten“ (FK), „Internale Kontrollüberzeugung“ (IK) und „Externale Kontrollüberzeugung“ (EK). Alle drei Skalen weisen positive statistisch bedeutsame Korrelationen zwischen r= .212 und r= .306 auf.

4.2.5.4 Verhaltensbereitschaft/ Intention

Diese Dimension setzt sich nicht aus einzelnen Skalen zusammen.

4.2.5.5 Einschätzung des Führungsverhaltens

Die Dimension „Führungsverhalten“ wird abgebildet über die Skalen „Zielsetzung“ (ZS), „Partizipation“ (P) und „Motivation (M). Die Skalen korrelieren mit Werten zwischen r= .652 und r= .728 sehr hoch miteinander.

4.2.5.6 Einschätzung der betrieblichen Aktivitäten

Die Dimension „Unternehmerische Aktivitäten“ wird abgebildet über die Skalen „Aufklärung & Information“ (AI) und „Datensicherung“ (DS). Dies beiden Skalen korrelieren mit r= .518 sehr stark

4.2.6 Weitere Zusammenhänge

Bis auf die Skale „EK“ korrelieren alle anderen Skalen hoch signifikant mit der Dimension „Intention“ (I). Alle drei Skalen zur Abbildung des „Vorgesetztenverhaltens“ weisen hoch bedeutsame Ergebnisse zu den Einstellungs- und Verhaltensskalen zur „IT-Sicherheit“ auf (außer „ZS“ mit „EK“ und „M“ mit „IK und „EK“). Die Skale „WÜG“ korreliert mit allen Skalen negativ. Das statistisch bedeutsame Ergebnis zeigt sich nur bei den Skalen „IK“ und „EK“ nicht.

4.3 Kovarianzstruktur: IT-Sicherheitsverhalten & IT-Sicherheitspolitik

Mit Hilfe der Kovarianzstrukturanalyse wird die Passung zwischen dem theoretischen Modellen und den empirischen Daten überprüft. Dies wird auch als Hinweis für die Konstruktvalidität des Fragebogens betrachtet. Mit Zuhilfenahme des Programms Amos (Analysis of moment structures) ist es möglich, die Datenanalysen über Struktur- und Kausalmodelle sowie Kovarianzstrukturen durchzuführen. Um Hypothesen zu testen und Schätzprobleme zu lösen, stehen die Instrumentarien GLM (general linear model) und CFA (connom factor analysis) zur Verfügung.

Im Gegensatz zu LISREL-Programmen (JÖRESKOG & SÖRBOM, 1992) ist bei Amos das konstruierte Pfaddiagramm das Modell – es ist hier nicht erforderlich, dass als Vorstufe vor der eigentlichen Analyse aufwendige Gleichungssysteme entwickelt werden müssen. Als den Hauptgrund für die Entwicklung von Strukturgleichungsmodellen nennen JACCARD & WAN (1996) die „Messfehler-

Problematik“ und die daraus resultierende geringe statistische Power (a. a. O., S.1). Über die Anwendung von Strukturgleichungsmodellen lassen sich die Interaktionseffekte zwischen kontinuierlichen Variablen in multiplen Regressionen analysieren, so dass die „Messfehler-Problematik“ weitestgehend minimiert wird.

Generell gilt für Pfadanalysen: Postulierte Theoriemodelle können an einem Datensatz überprüft, die Passung über Ergänzung zusätzlicher oder Entfernung überflüssiger Pfade verbessert und somit das Modell auf diesen Datensatz bezogen modifiziert werden.

Das Ausgangsmaterial für die Amos-Analyse ist eine Kovarianz- und eine Korrelationsmatrix aller beobachteten Variablen (Datenmatrizen). Das spezifizierte Modell wird ebenfalls in Matrixform dargestellt (Modellmatrix). Daten- und Modellmatrix laufen über SPSS und sind für den Amos-Anwender nicht sichtbar – der Anwender manipuliert direkt über das Pfadmodell auf dem Bildschirm. Durch Parametervariation wird die Modellmatrix den Datenmtrizen möglichst ähnlich gemacht – beispielsweise durch Maximum-Likelihood- oder Least-Square-Schätzungen. Von der resultiernden optimierten Modellmatrix aus ergeben sich nun neben Parametermatrizen, die detaillierten Aufschluss über die Zusammenhänge geben, sowohl die Modellgütekriterien als auch die Modifikationsindizes.

Ein allgemeines Testgütemaß ist z. B. der χ^{2}-Test mit der Modellmatrix als erwartete und der Datenmatrix als beobachtete Werte. Ein Modell wird als gut gefittet angesehen, wenn laut KELLOWAY (1998) der Quotient aus χ^2 und den Freiheitsgraden (CMIN/DF) zwischen 2 und 5 liegt. Bei Werten, die kleiner als 2 sind, spricht man von einem „overfitting model“ (a. a. O., S. 28). Allerdings sollte man diesen Index auch nicht überschätzen: „Interpretartive standards for the chi2/df ratio have very little justification other than modelers´ experience, and as a result, use of the index appears to be unwise and in decline.“ (A. a. O., S. 28).

Ein simples aber brauchbareres Maß für die Modellgüte ist das RMR-Maß (Root-Mean-Squared-Residual = Wurzel des Mittelwertes der Abweichungsquadrate) als

Anhalspunkt, wie groß die Abweichung vom gefitteten Modell ist. Der RMR-Index schwankt zwischen 0 und 1 und sollte möglichst nahe der 0 sein. Ist der Wert kleiner als .05, so zeigt er eine ausreichende Modellgüte an.

Der GFI (Goodness-of-fit-Index = Index der Modellpassungsgüte) beschreibt, wie viel besser das Modell im Vergleich zu gar keinem Modell ist. Er liegt zwischen 0 und 1 und sollte möglichst nahe der 1 liegen. Laut KELLOWAY (1998) gelten Werte üb er .90 als zufriedenstellend – allerdings ist dieser Grenzwert als Erfahrungswert zu interpretieren.

Ein weiterer relevanter Index ist der AGFI (Adjusted-goodness-of-fit-Index = Korrigierter Index der Modellpassungsgüte), der die Freiheitsgrade des Modells berücksichtigt. Genauso wie der RMR und GFI schwankt auch der AGFI zwischen 0 und 1 und sollte analog dem GFI möglichst über .90 liegen. Quantitative Unterschiede zwischen dem AGFI und dem GFI sind so zu interpretieren, dass triviale bzw. nicht signifikante Variablen im Modell wirken. GERBING & ANDERSON (1993) schlagen darüber hinaus vor, den DELTA2-Index zu berücksichtigen. Je höher die DELTA2-Werte sind, desto besser ist das Modell gefittet.

Bei allen Versuchen, die o. g. Indizes durch Modifikationen zu optimieren, ist jedoch abzuschätzen, inwieweit die Veränderungen das Modell inkonsistens oder unlogisch werden lassen, oder aber den Erklärungswert schmälern – d. h. neben den statistischen Kennwerten ist auch ein hohes Maß an inhaltlicher Überprüfung notwendig.

In den Abbildungen 15 und 16 sind die Strukturmodelle mit den entsprechenden Indikatorvariablen dargestellt:

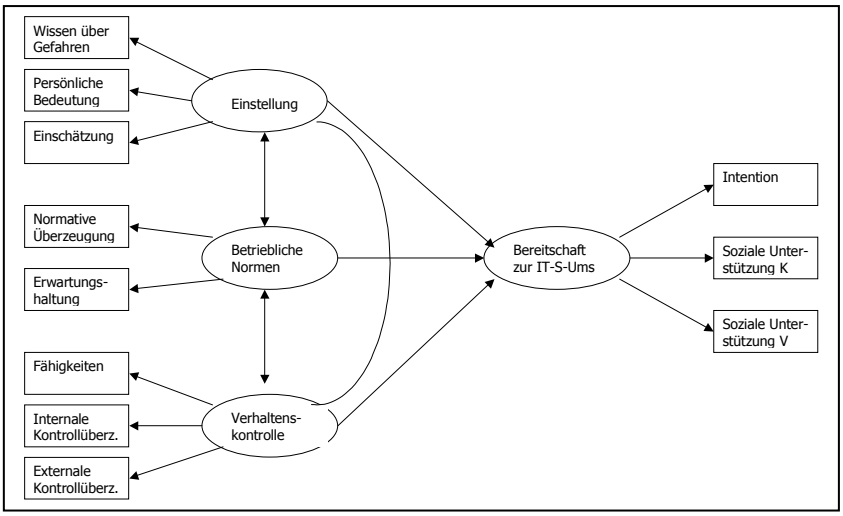


Abbildung 15: Strukturmodell zur IT-Sicherheitsumsetzung durch die Mitarbeiter.

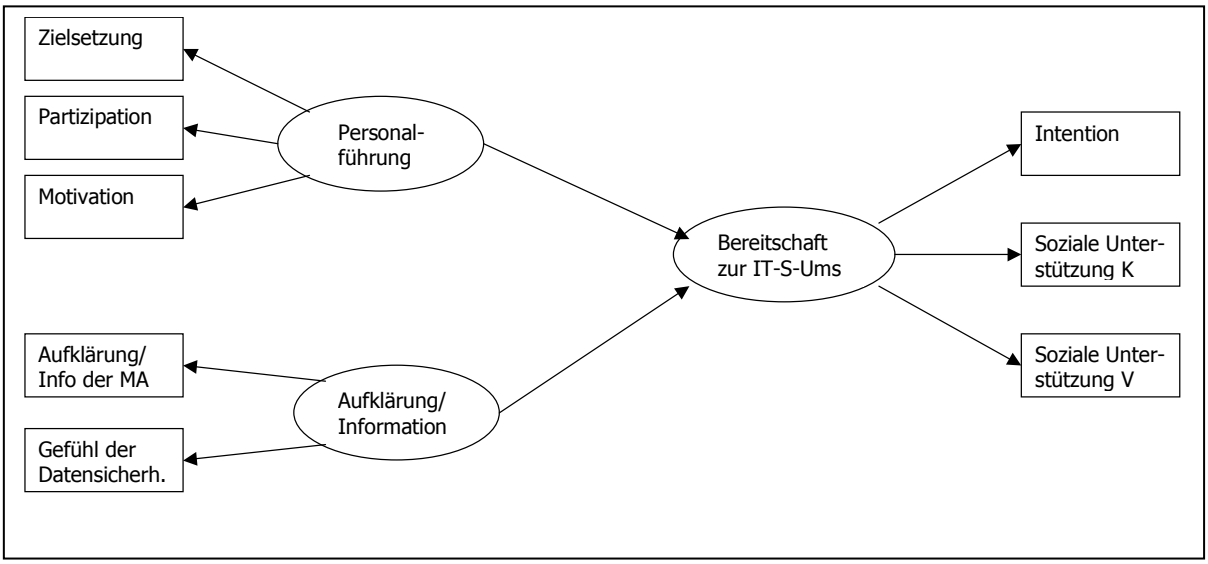


Abbildung 16: Strukturmodell zur IT-Sicherheitspolitik.

Die Notation der Kovarianzstrkturmodelle unterscheidet sich von den bisher verwendeten Bezeichnungen. Die bisher als Skalen definierten Itemzusammenfassungen bilden nun die Indikatorvariablen für die latenten, nicht messbaren Variablen. Die latenten exogenen Variablen erklären dabei die latenten endogenen Variablen im Strukturmodell. Die Kennwerte an den gerichteten Pfeilen zwischen exogenen und endogenen Variablen sind die Pfadkoeffizienten und die Koeffizienten an den ungerichteten Pfeilen zwischen den exogenen Variablen sind

Korrelationen. Die latenten Variablen „Einstellung“, „Betriebliche Normen“, „Verhaltenskontrolle“, Bereitschaft zur IT-Sicherheitsumsetzung“, „Personalführung“ und „Aufklärung und Information durch das Unternehmen“ sind mit den jeweiligen messbaren Indikatorvariablen dargestellt.

Die Modellparameter, die die Passung der theoretischen Modelle mit den empirischen Daten beschreiben sind wie folgt:

Kriterien der Modellgüte für die IT-Sicherheitsumsetzung durch die Mitarbeiter:

- Das RMR-Maß liegt mit .054 geringfügig über den geforderten Wert von .05 und kann somit als zufrieden stellend angesehen werden.
- Der GFI kann mit .905 als gut bezeichnet werden.
- Der korrigierte GFI (AGFI) kann auch als gut bezeichnet werden (.805).
- Der DELTA2-Wert entspricht mit .817 im Bereich der Erwartungen
- Der χ^2-Wert beträgt 199 mit df=38 Freiheitsgrade und ist statistisch hochsignifikant. Auch der Quotient aus χ^2 und Freiheitsgraden liegt mit 3,27 in dem von KELLOWAY (1998) geforderten Intervall zwischen 2 und 5.

Kriterien der Modellgüte für die IT-Sicherheitspolitik durch das Unternehmen:

- Das RMR-Maß liegt mit .031 unterhalb den geforderten Wert von .05 und kann als sehr zufriedenstellend angesehen werden.
- Der GFI kann mit .928 als gut bezeichnet werden.
- Der korrigierte GFI (AGFI) kann auch als gut bezeichnet werden (.848).
- Der DELTA2-Wert entspricht mit .93 den Erwartungen
- Der χ^2-Wert beträgt 92 mit 17 Freiheitsgraden und ist statistisch hochsignifikant. Auch der Quotient aus χ^2 und Freiheitsgraden liegt mit 2,98 in dem von KELLOWAY (1998) geforderten Intervall zwischen 2 und 5.

Insgesamt kann das Modell auf Basis der resultierenden Güteparameter als „gut und passend“ beurteilt werden.

4.4 Zusammenfassung und Diskussion der Fragebogenkonstruktion

Bei der Konstruktion des Fragebogens wurde auf der Ebene der Organisation auf die Theorien der „Zielsetzung“, „Motivation“ und „Partizipation“ zurückgegriffen. Dies aus dem Grund, da generell kann gesagt werden, dass sich die aus der Prozesstheorie entstammten Konzepte näher am tatsächlichen Verhalten bewegen als die Konzepte aus der Inhaltstheorie. Sie berücksichtigen die Verbindungen zwischen den Ergebnissen und deren Bewertung. In den Prozesstheorien wird darüber hinaus nicht unterstellt, dass alle Menschen von denselben Motiven geleitet werden, sondern betonen die individuellen Bedürfnisse des Menschen.

Auf der individuellen Ebene wurde auf die „Theorie des geplanten Verhaltens“ von AJZEN & MADDEN (1986) zurückgegriffen. Sie erhebt den Anspruch, eine allgemein gültige Theorie zur Erklärung jeglichen Verhaltens zu sein (VGL. BAMBERG ET AL., 1999). Darüber hinaus stellt sie einen theoretischen Ansatz dar, mit dessen Hilfe die durch die Situation determinierten Verhaltensweisen analysiert werden können und bietet damit einen direkten Ansatzpunkt für die systematische Entwicklung und Evaluation von Interventionsmaßnahmen. – indirekt sind Erwartungs-x-Wert-Annahmen enthalten.

Die vorliegenden Analysen zu den Testgütekriterien Objektivität, Reliabilität und Validität des Fragebogens zur Messung des betrieblichen IT-Sicherheitsniveaus der Mitarbeiter erheben nicht den Anspruch der Vollständigkeit. Die vorliegenden Daten und Analysen ergeben aber, dass dieses entwickelte Messinstrument einen Beitrag zur Verbesserung der IT-Sicherheit leisten kann.

Die Messgenauigkeit des Fragebogens kann insgesamt als gegeben angesehen werden. Die erzielten Reliabilitätskoeffizienten liegen bei > .68. Eine Ausnahme bilden die Skalen der Dimension „Verhaltenskontrolle“ deren Konsistenzkennwerte zwischen .514 und .609 liegen. Bei dieser Bewertung ist zu berücksichtigen, dass es ich im engeren Sinne um die Überprüfung einer eng umschriebenen Handlungsfähigkeit

handele, bei der die Validität höher zu bewerten ist als die Reliabilität (vgl. LIENERT & RAATZ, 1994).

Die Konstruktvalidität des Fragebogens konnte nach LIENERT & RAATZ (1994) durch eine ausreichende innere Konsistenz der Konstrukte bestätigt werden. Die kriteriumsorientierte Validität wurde durch die Erhebung der IT-Sicherheitsmaßnahmenumsetzung nach dem BSI-Grundschutz gewährleistet.

Die Skaleninterkorrelationen unterstützen die angenommenen Dimensionen „Einstellung“, „Betriebliche Normen“ und „Verhaltenskontrolle“ zur IT-Sicherheitsumsetzung durch die Mitarbeiter. Die Interkorrelationen der Skalen der Dimension „Einstellung“ sind signifikant, aber fallen zwischen r= .127 und r= -0.358 relativ gering aus. Das gilt auch für die Skalen der Dimension „Verhaltenskontrolle“ mit Werten zwischen r= .223 und r= .285. Nur bei der Dimension „Betriebliche Normen“ korrelieren die Skalen mit r= .627 relativ hoch. Die Zusammenhänge zwischen den Skalen sind auf Grund der inhaltlichen Logik zu interpretieren.

Die Skaleninterkorrelationen zum Vorgesetztenverhalten korrelieren sehr stark mit Werten zwischen r= .596 und r= .723 miteinander. Sie zeigen auch sehr hohe Korrelationen mit den Skalen der Dimension „Betriebliche Normen“ und den Skalen der Dimension „Unternehmerische Tätigkeit“, die ebenso einen hohen Zusammenhang mit der Dimension „Betriebliche Normen“ aufweist. Auch hier sind die Zusammenhänge zwischen den Skalen wegen der inhaltlichen Logik zu interpretieren.

Die Ergebnisse der Kovarianzstrukturanalyse unterstützen die Zusammenhänge zwischen den Dimensionen „Einstellung“, „Betriebliche Normen“, „Verhaltenskonstrolle“ und der „Bereitschaft zur IT-Sicherheitsumsetzung“ auf der Seite des IT-Sicherheitsverhaltens ebenso wie die Dimensionen „Personalführung“, „Aufklärung/Information“ und „Bereitschaft zur IT-Sicherheitsumsetzung“ auf der Seite der IT-Sicherheitspolitik.

Die Skala „Verantwortung“ (VA) wurde auf Grund der bisherigen Analysen herausgenommen.

Die Durchführungs- und Auswertungsobjektivität kann aufgrund der standardisieren Befragungssituation, der schriftlichen Instruktion und der verwendeten geschlossenen Fragen als gegeben betrachtet werden.

5 Zusammenhänge zwischen den erhobenen Skalen

5.1 Ermittlung von Typenprofilen mittels Cluster- und Diskriminanzanalysen

5.1.1 Clusteranalysen zur Ermittlung von Typenprofilen

Im ersten Schritt zur Ermittlung von statistischen Zusammenhängen zwischen den erhobenen Skalen werden Gruppen über die Gesamtstichprobe gebildet. Dies hat zum Ziel, homogene und voneinander gut trennbare Gruppen zu ermitteln und zu beschreiben. Da die erhobenen Skalen auf Intervallskalenniveau basieren, kann nach BORTZ (1993) das Agglomerationsverfahren nach Ward als Mittel der Wahl herangezogen werden. Dieses Verfahren genießt den Vorteil einer guten Diskriminierung zwischen den Partitionen, so dass eine „adäquate“ Zuordnung von „guten“ vs. „schlechten“ Mitarbeitern erfolgt (vgl. BORTZ, 1993). Nach BACKHAUS et al., (1994) zählt darüber hinaus der hierarchische Ward-Algorithmus zu den polythetischen Verfahren, die in der Lage sind bei der Fusionierung der zu klassifizierenden Objekte mehrere relevante Merkmale gleichzeitig zu berücksichtigen. Dies ist insofern ausschlaggebend, da eine Clusterung auf der Grundlage von mehreren Skalen erfolgen soll und somit die Anwendung rechtfertigt. Die Grundlage der weiteren Schritte dieser „Fusionierung“ bildet bei diesem Verfahren die „feinste Patition“. Dabei bildet jedes einzelne Untersuchungsobjekt auf der ersten Stufe der Fusion eine Gruppe, die im weiteren Verlauf der Fusionierung mit den anderen Gruppen zusammengefasst wird (vgl. BACKHAUS et al., 1994). Das Fusionierungsprinzip folgt der Intragruppen-Varianz. D. h., dass die Skalen sukzesssiv nach dem geringsten Zuwachs der Fehlerquadratsumme zusammengeschmolzen werden.

Bei den hier vorliegenden intervallskalierten Daten wird die Ähnlichkeit bzw. Unähnlichkeit zweier Skalen durch die Euklidische Distanz beschrieben (vgl. STEINHAUSEN & LANGER, 1977; BORTZ, 1993). Durch Verwendung der quadrierten Euklidischen Distanz als Summe der quadrierten Variablendifferenzen wird der Größe der Differenzwerte stärker Rechnung getragen (vgl. BROSIUS, 1989; BACKHAUS et al.,

1994). STEINHAUSEN & LANGER (1977) empfehlen, die minimale Clusteranzahl als Beurteilungskriterium zur Auswahl einer geeigneten Clusterlösung Zugrundezulegen. Bei Berücksichtigung dieser Empfehlung und der Betrachtung des resultierenden Dendorgramms, erscheint für den vorliegenden Datensatz eine 2-Clusterlösung sinnvoll zu sein.

5.1.2 Diskriminanzanalysen zur Überprüfung der Clusterlösungen

Als strukturprüfendes Verfahren erlaubt das Verfahren der Diskriminanzanalyse in einem zweiten Schritt vorgegebene Gruppen bzgl. der Unterschiedlichkeit einer Mehrzahl von Variablen zu untersuchen (vgl. STEINHAUSEN & LANGER, 1977; BACKHAUS et al., 1994). Mit Hilfe der Diskriminanzanalyse ist es möglich, die Abhängigkeit einer nominal skalierten Variablen von metrisch skalierten Variablen zu untersuchen (vgl. BACKHAUS et al., 1994). Da durch die Clusteranalyse solche Gruppen erzeugt wurden, kann die Diskriminanzanalyse hier eine Ergänzung darstellen, um die Zuordnung der Personen zu den Clustern aufgrund der Eigenschaften auf den erhobenen Skalen zu überprüfen. Auf der Grundlage von Clustergruppen lässt sich nun eine Diskriminanzfunktion bilden, die eine optimale Trennung zwischen den Gruppen ermöglicht. Dabei sind folgende Kennwerte von besonderer Relevanz:

Kanonische Korrelationskoeffizient: Er misst den Anteil der gesamten Streuung, der durch die Streuung zwischen den Gruppen entsteht. Somit resultiert ein Maß für die Strenge des Zusammenhangs zwischen den Diskriminanzfunktionswerten und den betreffenden Gruppen. Die vorgenommene Trennung zwischen den Gruppen ist umso besser, je näher der Koeffizient an dem Wert „1“ liegt (vgl. BROSIUS, 1989).

Eigenwert: Laut BROSIUS (1989) handelt es sich bei dem angegebenen Eigenwert um ein Maß für die Güte der Diskriminanzfunktion, die mit der Größe des Eigenwertes zunimmt.

Wilks´ Lambda: Dieses Maß prüft die beiden Gruppen hinsichtlich einer signifikanten Unterscheidung der mittleren Werte der Diskriminanzfunktion. Somit sind Aussagen über die Streuung der Funktionswerte innerhalb der Gruppen möglich (vgl. BROSIUS, 1989). Die vorgenommene Trennung ist umso besser, je näher Wilks´ Lambda an dem Wert „0“ liegt.

In den folgenden Abschnitten werden für die einzelnen Untersuchungsgruppen „Vorgesetztenverhalten“, „IT-Sicherheitskultur“ und „Softwareergonomie“ Typenprofile mittels Cluster- & Diskriminazanalysen erstellt um Unterschiede in den Untersuchungsskalen „IT-Sicherheitsverhalten“ und „Soziale Unterstützung am Arbeitsplatz“ mittels t-Test für Mittelwertunterschiede zwischen den ermittelten Gruppen herauszufinden.

5.2 Ermittlung von Typenprofilen bei der Personalführung

5.2.1 Clusteranalyse zur Ermittlung von Typenprofilen der Personalführung

Als erstes werden Typenprofile hinsichtlich der Personalführungsstrategien „Zielsetzung“, „Partizipation“ und „Motivation“ gebildet. Es wird untersucht, ob Mitarbeiter die die drei Führungsstrategien überwiegend positiv bewerten von Mitarbeitern unterscheiden die diese Führungsstrategien hauptsächlich negativ wahrnehmen, sich hinsichtlich der Wahrnehmung bzw. Bewertung des „IT-Sicherheitsverhaltens“ und der „Sozialen Unterstützung am Arbeitsplatz“ unterscheiden.

Hierzu wird eine 2-Clusterlösung mit einer anschließenden Trennfähigkeitsberechnungen und ein t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen des IT-Sicherheitsverhaltens durchgeführt. Die folgende Abbildung 17 gibt das Profil der beiden Clustergruppen in Bezug auf die zugrundegelegten Skalen zur Messung des Führungsverhaltens wider:

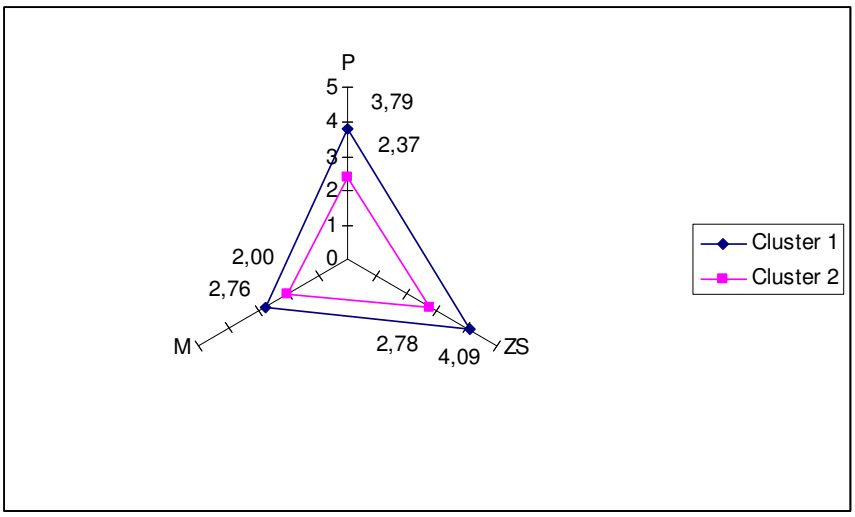


Abbildung 17: 2-Clusterlösung auf den Skalen „Zielsetzung", „Partizipation" und „Motivation" (Cluster 1= hohe Bewertung des Führungsverhaltens, Cluster 2= niedrige Bewertung des Führungsverhaltens; ZS= Zielsetzung, P= Partizipation, M= Motivation).

Cluster 1 schließt 107 Mitarbeiter und Cluster 2 84 Mitarbeiter ein. Es resultieren folgende Gruppenmittelwerte auf den drei Skalen:

Skala	Cluster 1 (N=107)	Cluster 2 (N= 84)
Zielsetzung	2,78	4,09
Partizipation	2,37	3,79
Motivation	2,00	2,76

Tabelle 21: Gruppenmittelwerte der gebildeten Cluster auf den Skalen zum Führungsverhalten.

Die Mitarbeiter der ersten Clusterlösung zeigen eine wesentlich niedrigere Wahrnehmung auf das Führungsverhalten als die Mitarbeiter der zweiten Clusterlösung. D. h., die Clusterlösung ist aussagefähig. Zur Beantwortung des qualitativen Unterschieds zwischen der ersten und der zweiten Clusterlösung, erfolgt eine Diskriminanzanalyse.

5.2.2 Diskriminanzanalysen zur Überprüfung der 2-Clusterlösungen

Die folgende Tabelle 22 zeigt die isolierte Trennfähigkeit der einzelnen Variablen in Bezug auf die zwei Clustergruppen unter Angabe der Testgrößen Wilks´ Lambda und einer univariaten Varianzanalyse, d. h. es wird zunächst einmal getestet, inwieweit die einzelnen Skalen jeweils isoliert zwischen den beiden Gruppen trennen.

Skala	Wilks´ Lambda	F	Sign.
Zielsetzung	,455	227,383	,000
Partizipation	,415	267,467	,000
Motivation	,611	121,094	,000

Tabelle 22: Univariate Trennfähigkeit der einzelnen Skalen zum Führungsverhalten.

Die resultierende Trennfähigkeit ist für alle Skalen signifikant.

Die relevanten Koeffizienten sind in Tabelle 23 widergegeben:

Funktion	Kanonische Korrelation	Eigenwert	% der Varianz	Wilks´ Lambda	χ^2-Wert	Df	Signif.
1	,834	2,278	100	0,305	222,585	3	,000

Tabelle 23: **Gütemaße der kanonischen Diskriminanzfunktion.**

Der ermittelte Wert der Kanonischen Korrelation von ,834 erlaubt die Aussage, dass man hier von einer „zufriedenstellenden" Trennung der beiden Clustergruppen ausgehen kann.

Der angegebene Eigenwert von 2,278 trennt signifikant mit einem Varianzanteil von 100% zwischen den beiden Clustergruppen.
Die Betrachtung von Wilks´ Lambda von ,305 und dem zugehörigen χ^2-Wert von 222,585 mit dem Freiheitsgrad 3 stimmt auch in dieser Hinsicht zufrieden. Die vorgenommene Klassifizierung in zwei Gruppen kann hiermit als bestätigt gelten.

Die folgende Klassifikationsmatrix gibt an, wie hoch die erzielte „Treffergenauigkeit" in der Untersuchungsstichprobe ist:

		Vorhergesagte Gruppenzugehörigkeit	
Aktuelle Gruppe	N a priori	Cluster 1	Cluster 2
1	107	106 (99,1%)	1 (0,9%)
2	84	2 (2,4%)	82 (97,6%)

Tabelle 24: Klassifikationsmatrix auf der Basis der Skalen zum Führungsverhalten.

Bei diesen Klassifizierungsergebnissen werden 98,5% der ursprünglich gruppierten Fälle korrekt klassifiziert. Dieser Wert kann nach STEINHAUSEN & LANGER (1977), die einen Toleranzbereich von 90 bis 95 Prozent angeben, als äußerst zufriedenstellend bezeichnet werden. Dieses Ergebnis muss vor dem Hintergrund gesehen werden, dass

bei zwei vorhandenen Gruppen, ohne Berücksichtigung der unterschiedlichen Gruppengröße, eine a priori Wahrscheinlichkeit von 50% existiert. D. h., die Wahrscheinlichkeit einer richtigen Zuordnung einer Person zu einer Gruppe beträgt 50%. Hier liegt die per Diskriminanzanalyse gefundene korrekte Zuordnung von 98,5% deutlich über diesem Zufallswert. Die gesamte Fehlerklassifizierung beträgt demnach nur 1,5%. D. h., dass von den 191 Mitarbeitern 188 richtig bzw. 3 falsch zugeordnet wurden.

Zusammenfassend lässt sich feststellen, dass die durch die Clusteranalyse vorgenommene Klassifizierung durch die im Anschluss durchgeführte Diskriminanazanalyse bestätigt wird.

Um zu überprüfen, ob sich die Mittelwerte der Skalen signifikant voneinander unterscheiden, wird ein t-Test auf Mittelwertunterschiede über die Skalen des Führungsverhaltens gerechnet. Als abhängige Variable dienen die drei Skalen und als unabhängige Variable werden die Clusterzugehörigkeiten verwendet.

Tabelle 25 gibt einen Überblick über die relevanten Zusammenhänge:

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
ZS	Varianzen sind gleich	-15,079	190	,000	-1,3038
	Varianzen sind nicht gleich	-15,256	179,312	,000	-1,3038
P	Varianzen sind gleich	-16,354	190	,000	-1,4220
	Varianzen sind nicht gleich	-16,506	178,010	,000	-1,4220
M	Varianzen sind gleich	-11,004	190	,000	-,7535
	Varianzen sind nicht gleich	-10,343	129,368	,000	-,7535

Tabelle 25: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen des Führungsverhaltens. (ZS = Zielsetzung, P = Partizipation, M= Motivation).

Der t-Test auf Mittelwertgleichheit dokumentiert, dass es signifikante Unterschiede zwischen den Gruppen auf allen zugrundeliegenden Skalen gibt.

Es konnte gezeigt werden, dass die 2-Clusterlösung hinreichend zufriedenstellend ist. Das bedeutet, dass sich die gefundenen Gruppen in sämtlichen Aspekten der subjektiven Wahrnehmung des Führungsverhaltens unterscheiden. Die Gruppe 1 ist durch eine signifikant niedrigere empfundene Personalführung gekennzeichnet als die Gruppe 2.

5.2.3 Zusammenhänge zwischen dem Führungsverhalten und dem IT-Sicherheitsverhalten

Hypothese Nr. 1:
Die Mitarbeiter, die das Führungsverhalten Ihrer Vorgesetzten in den Bereichen „Zielsetzung“, „Motivation“ und „Partizipation“ hoch einschätzen, bewerten auch die Skalen zum „IT-Sicherheitsverhalten“ höher ein als Mitarbeiter die das Führungsverhalten Ihrer Vorgesetzten niedrig einschätzen.

Abbildung 18: Untersuchungsdesign zur Überprüfung der Hypothese 1.

Zur Verifizierung bzw. Falsifizierung der Hypothese wird ein t-Test bei unabhängigen Stichproben für Mittelwertgleichheit gerechnet. Das Ergebnis zeigt folgende Tabelle 26:

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
WÜG	Varianzen sind gleich	3,653	185	,000	,4110
	Varianzen sind nicht gleich	3,714	181,005	,000	,4110
PB	Varianzen sind gleich	-5,147	189	,000	-,5235
	Varianzen sind nicht gleich	-5,194	183,798	,000	-,5235
ESU	Varianzen sind gleich	-5,182	166	,000	-,0849
	Varianzen sind nicht gleich	5,116	141,683	,000	-,0849
NÜ	Varianzen sind gleich	-10,363	186	,000	-,1219
	Varianzen sind nicht gleich	-10,566	182,418	,000	-,1219
EW	Varianzen sind gleich	-5,078	188	,000	-,0652
	Varianzen sind nicht gleich	-4,953	156,819	,000	-,0652
FK	Varianzen sind gleich	-4,361	188	,000	-,4391
	Varianzen sind nicht gleich	-4,312	169,440	,000	-,4391
IK	Varianzen sind gleich	-2,321	177	,021	-,3304
	Varianzen sind nicht gleich	-2,317	164,587	,022	-,3304
EK	Varianzen sind gleich	-1,600	189	,031	-,1721
	Varianzen sind nicht gleich	-1,591	174,562	,033	-,1721
I	Varianzen sind gleich	-4,732	189	,000	-,3499
		-4,663	167,172	,000	-,3499

Tabelle 26: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen des IT-Sicherheitsverhaltens (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK = internale Kontrollüberzeugung, EK = externale Kontrollüberzeugung, I = Intention).

Auf allen Skalen gibt es über die 2-Clusterlösung signifikante Mittelwertunterschiede. D. h., Mitarbeiter die einen hohen Ausprägungsgrad an den Personalführungsstrategien „Zielsetzung“, „Motivation“ und „Partizipation“ wahrnehmen, sind den Skalen des IT-Sicherheitsverhaltens signifikant positiver eingestellt als die Mitarbeiter, die das Führungsverhalten mit niedrigem Ausprägungsgrad wahrnehmen.

Die folgende Abbildung 19 gibt die Mittelwertunterschiede graphisch wider:

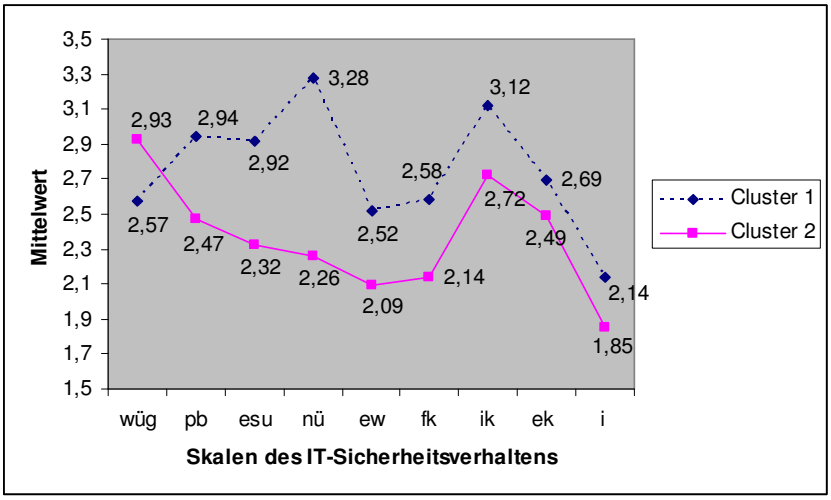


Abbildung 19: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen des IT-Sicherheitsverhaltens (Cluster 1= hohe Bewertung des Führungsverhaltens, Cluster 2= niedrige Bewertung des Führungsverhaltens, WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK = internale Kontrollüberzeugung, EK = externale Kontrollüberzeugung, I = Intention).).

Die Abbildung 19 ist wie folgt zu interpretieren. Auf der X-Achse sind die relevanten Skalen abgetragen, deren Mittelwerte auf der Y-Achse zwischen 1,00 und 5,00 schwanken können. Das Intervall von 1 bis 5 entspricht der in dem Fragebogen vorgegebenen Antwortskala – mit folgender Transformation:

„++ = die Aussage trifft völlig zu“

„+ = die Aussage trifft zu“

„+/- = die Aussage trifft manchmal zu“

„- = die Aussage trifft selten zu“

„- - = die Aussage trifft gar nicht zu“.

Die Hypothese Nr. 1 konnte bestätigt werden. D. h. Mitarbeiter, die einen hohen Ausprägungsgrad der Personalführung angeben, bewerten auch die Skalen des IT-Sicherheitsverhaltens signifikant höher.

5.2.4 Zusammenhänge zwischen dem Führungsverhalten und der Sozialen Unterstützung am Arbeitsplatz

Hypothese Nr. 2:
Die Mitarbeiter, die das Führungsverhalten Ihrer Vorgesetzten in den Bereichen „Zielsetzung", „Motivation" und „Partizipation" hoch einschätzen, bewerten auch die Skalen der „Sozialen Unterstützung am Arbeitsplatz" höher ein als Mitarbeiter die das Führungsverhalten Ihrer Vorgesetzten niedrig einschätzen.

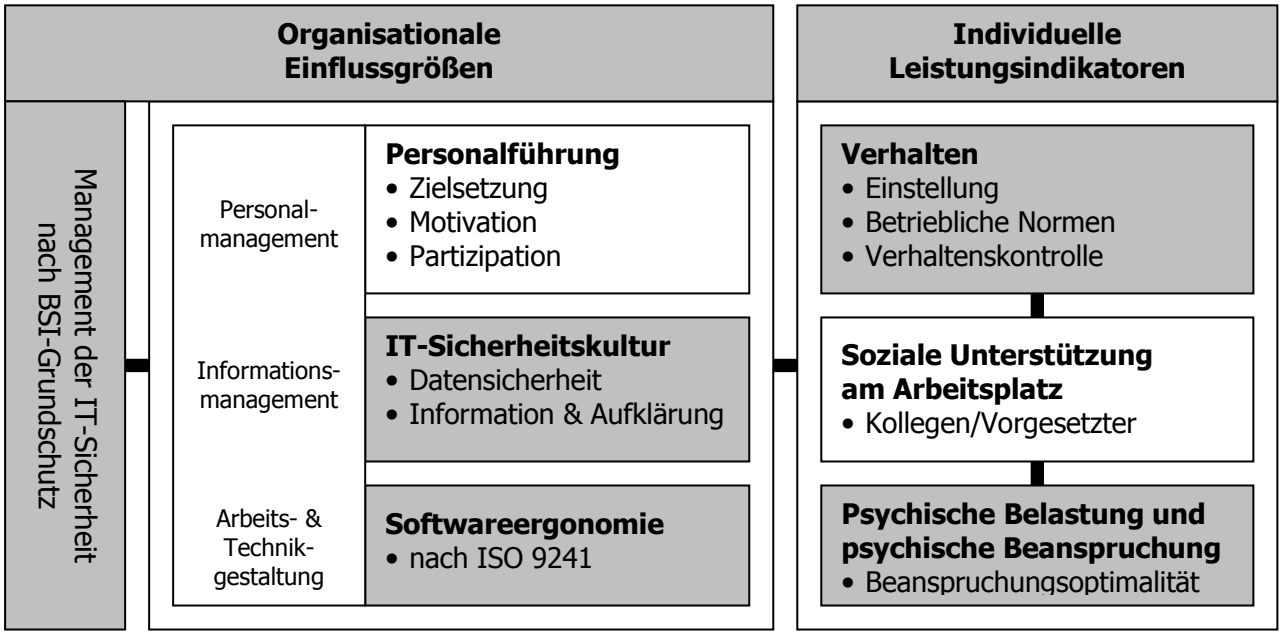


Abbildung 20: Untersuchungsdesign zur Überprüfung der Hypothese 2.

Zur Verifizierung bzw. Falsifizierung der Hypothese wird ein t-Test bei unabhängigen Stichproben für Mittelwertgleichheit gerechnet.

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
SUK	Varianzen sind gleich	-5,603	289	,000	-,39664
	Varianzen sind nicht gleich	-5,237	191,032	,000	-,39664
SUV	Varianzen sind gleich	-8,375	287	,000	-,74547
	Varianzen sind nicht gleich	-7,751	182,051	,000	-,74547

Tabelle 27: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen der Sozialen Unterstützung am Arbeitsplatz (SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).

Auf allen Skalen gibt es über die 2-Clusterlösung signifikante Mittelwertunterschiede. D. h., Mitarbeiter die einen hohen Ausprägungsgrad an den Personalführungsstrategien „Zielsetzung“, „Motivation“ und „Partizipation“ wahrnehmen, bewerten die Skalen der „Sozialen Unterstützung am Arbeitsplatz“ signifikant höher als Mitarbeiter, die das Führungsverhalten niedrig einschätzen.

Die folgende Abbildung 21 gibt die Mittelwertunterschiede graphisch wider:

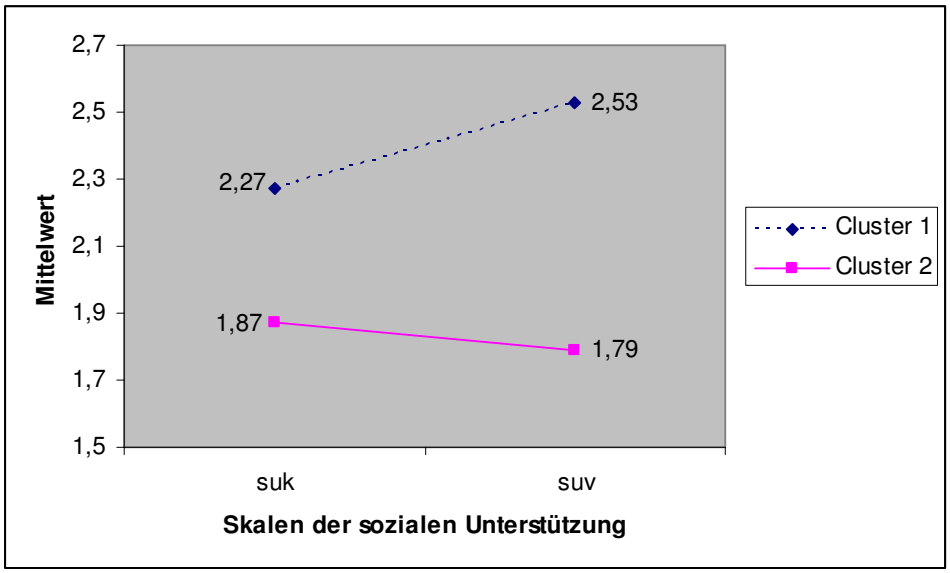


Abbildung 21: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen der Sozialen Unterstützung (Cluster 1= hohe Bewertung des Führungsverhaltens, Cluster 2= niedrige Bewertung des Führungsverhaltens, suk= Soziale Unterstützung am Arbeitsplatz durch die Kollegen, suv= Soziale Unterstützung am Arbeitsplatz durch den Vorgesetzten).

Die Hypothese Nr. 2 konnte bestätigt werden. D. h. Mitarbeiter, die einen hohen Ausprägungsgrad der Personalführung angeben, bewerten auch die Skalen der Sozialen Unterstützung am Arbeitsplatz signifikant höher.

5.3 Ermittlung von Typenprofilen bei der IT-Sicherheitskultur

5.3.1 Clusteranalyse zur Ermittlung von Typenprofilen der IT-Sicherheitskultur

Cluster 1 schließt 107 Mitarbeiter und Cluster 2 84 Mitarbeiter ein. Es resultieren folgende Gruppenmittelwerte auf den zwei Skalen:

Skala	Cluster 1 (N=63)	Cluster 2 (N= 129)
Datensicherheit (DS)	3,41	2,29
Aufklärung & Information (AI)	3,09	1,89

Tabelle 28: Gruppenmittelwerte der gebildeten Cluster auf den Skalen zur IT-Sicherheitskultur.

Die Mitarbeiter der ersten Clusterlösung zeigen eine wesentlich höhere Wahrnehmung der IT-Sicherheitskultur als die Mitarbeiter der zweiten Clusterlösung. D. h., die Clusterlösung ist aussagefähig. Zur Beantwortung des qualitativen Unterschieds zwischen der ersten und der zweiten Clusterlösung, erfolgt eine Diskriminanzanalyse. Die folgende Abbildung 22 gibt das Profil der beiden Clustergruppen in Bezug auf die zugrunde gelegten Skalen zur Messung des Führungsverhaltens wider:

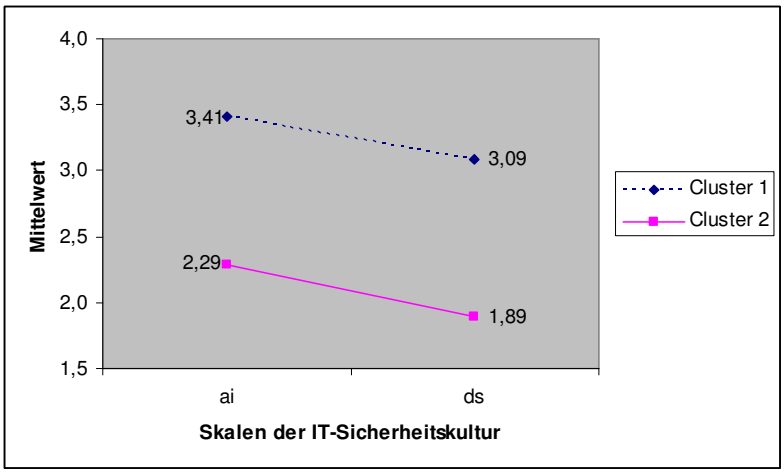


Abbildung 22: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen der IT-Sicherheitskultur (Cluster 1 = hohe Bewertung des Führungsverhaltens, Cluster 2 = niedrige Bewertung des Führungsverhaltens, ai = Aufklärung/Information, ds = Datensicherheit)

Cluster 1 schließt 63 Mitarbeiter und Cluster 2 126 Mitarbeiter ein. Es resultieren folgende Gruppenmittelwerte auf den zwei Skalen:

Skala	Cluster 1 (N=63)	Cluster 2 (N= 126)
Aufklärung & Information (AI)	3.41	2,29
Datensicherheit (DS)	3,09	1,89

Tabelle 29: Gruppenmittelwerte der gebildeten Cluster auf den Skalen zum Führungsverhalten.

5.3.2 Diskriminanzanalysen zur Überprüfung der 2-Clusterlösungen

Die folgende Tabelle 30 zeigt die isolierte Trennfähigkeit der einzelnen Variablen in Bezug auf die zwei Clustergruppen unter Angabe der Testgrößen Wilks´ Lambda und einer univariaten Varianzanalyse, d. h. es wird zunächst einmal getestet, inwieweit die einzelnen Skalen jeweils isoliert zwischen den beiden Gruppen trennen.

Skala	Wilks´ Lambda	F	Sign.
Datensicherheit (DS)	,836	56,863	,000
Aufklärung & Information (AI)	,339	565,852	,000

Tabelle 30: Univariate Trennfähigkeit der einzelnen Skalen zur IT-Sicherheitskultur.

Die resultierende Trennfähigkeit ist für alle Skalen signifikant.

Die relevanten Koeffizienten sind in Tabelle 31 wiedergegeben:

Funktion	Kanonische Korrelation	Eigenwert	% der Varianz	Wilks´ Lambda	χ^2-Wert	Df	Signif.
1	,792	1,687	100	0,372	285,678	2	,000

Tabelle 31: Gütemaße der kanonischen Diskriminanzfunktion.

Der ermittelte Wert der Kanonischen Korrelation von ,792 erlaubt die Aussage, dass man hier von einer „ausreichenden“ Trennung der beiden Clustergruppen ausgehen kann.

Der angegebene Eigenwert von 1,687 trennt signifikant mit einem Varianzanteil von 100% zwischen den beiden Clustergruppen.

Die Betrachtung von Wilks´ Lambda von ,3725 und dem zugehörigen χ^2-Wert von 285,678 mit dem Freiheitsgrad 2 stimmt auch in dieser Hinsicht zufrieden. Die vorgenommene Klassifizierung in zwei Gruppen kann hiermit als bestätigt gelten.

Zusammenfassend lässt sich feststellen, dass die durch die Clusteranalyse vorgenommene Klassifizierung durch die im Anschluss durchgeführte Diskriminanzanalyse bestätigt wird.

Um zu überprüfen, ob sich die Mittelwerte der Skalen signifikant voneinander unterscheiden, wird ein t-Test auf Mittelwertunterschiede über die Skalen des Führungsverhaltens gerechnet. Als abhängige Variable dienen die drei Skalen und als unabhängige Variable werden die Clusterzugehörigkeiten verwendet.

Tabelle 32 gibt einen Überblick über die relevanten Zusammenhänge:

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
AI	Varianzen sind gleich	15,232	190	,000	1,11821
	Varianzen sind nicht gleich	15,070	129,902	,000	1,11821
DS	Varianzen sind gleich	16,5941	190	,000	1,19681
	Varianzen sind nicht gleich	15,292	178,612	,000	1,19681

Tabelle 32: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen der IT-Sicherheitskultur (AI = Aufklärung & Information, DS = Datensicherheit).

Der t-Test auf Mittelwertgleichheit dokumentiert, dass es signifikante Unterschiede zwischen den Gruppen auf allen zugrunde liegenden Skalen gibt.

Es konnte gezeigt werden, dass die 2-Clusterlösung hinreichend zufrieden stellend ist. Das bedeutet, dass sich die gefundenen Gruppen in sämtlichen Aspekten der subjektiven Wahrnehmung der IT-Sicherheitskultur unterscheiden. Die Gruppe 1 ist durch eine signifikant höhere empfundene Aufklärungs- & Informationspolitik bzw. der Einschätzung der Datensicherheit gekennzeichnet als die Gruppe 2.

5.3.3 Zusammenhänge zwischen der IT-Sicherheitskultur und dem IT-Sicherheitsverhalten

Hypothese Nr. 3:
Die Mitarbeiter, die die IT-Sicherheitskultur Ihres Unternehmens in den Bereichen „Aufklärung & Information“ und „Datensicherheit“ hoch einschätzen, bewerten auch die Skalen des „IT-Sicherheitsverhaltens““ höher ein als Mitarbeiter die die IT-Sicherheitskultur niedrig einschätzen.

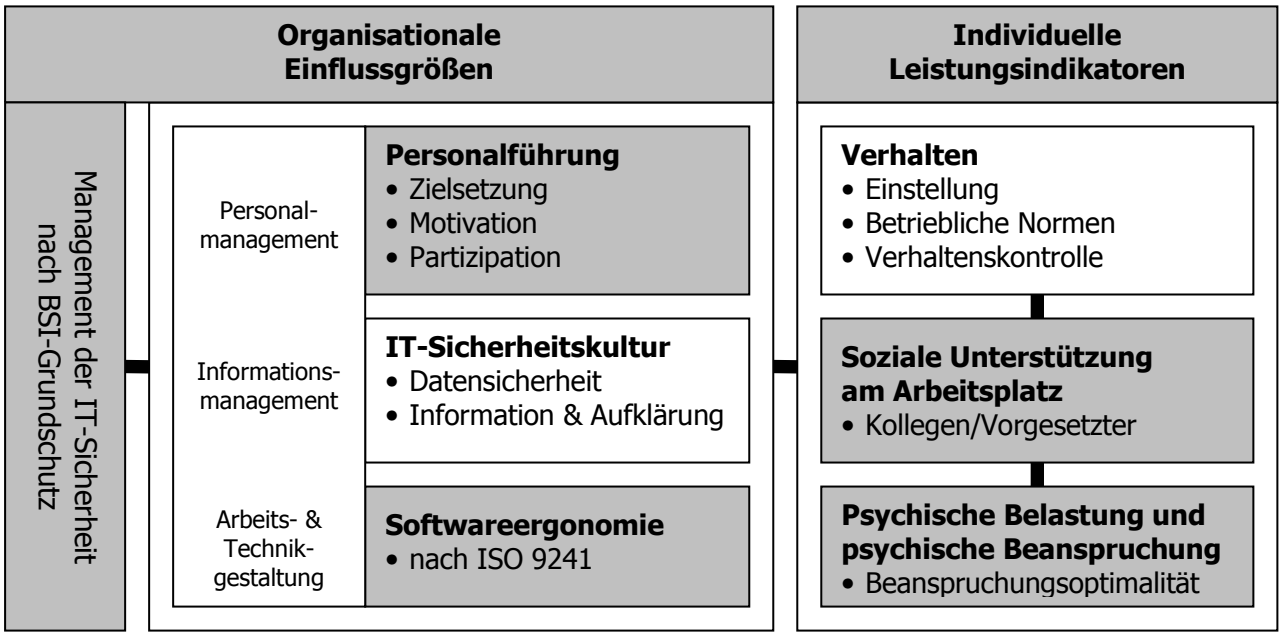


Abbildung 23: Untersuchungsdesign zur Überprüfung der Hypothese Nr. 3

Zur Verifizierung bzw. Falsifizierung der Hypothese wird ein t-Test bei unabhängigen Stichproben für Mittelwertgleichheit gerechnet:

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
WÜG	Varianzen sind gleich	-3,222	185	,001	-,31042
	Varianzen sind nicht gleich	-3,300	164,096	,001	-,31042
PB	Varianzen sind gleich	2,936	189	,004	,28690
	Varianzen sind nicht gleich	3,004	181,065	,003	,28690
ESU	Varianzen sind gleich	5,850	166	,000	,65081
	Varianzen sind nicht gleich	5,762	121,812	,000	,65081
NÜ	Varianzen sind gleich	8,156	185	,000	-,1219
	Varianzen sind nicht gleich	7,730	143,948	,000	-,1219
EW	Varianzen sind gleich	5,802	188	,000	,43248
	Varianzen sind nicht gleich	5,401	153,616	,000	,43248
FK	Varianzen sind gleich	4,993	188	,000	,41068
	Varianzen sind nicht gleich	5,027	163,848	,000	,41068
	Varianzen sind nicht gleich				
IK	Varianzen sind gleich	2,195	177	,029	,25894
	Varianzen sind nicht gleich	2,253	163,668	,025	,25894
EK	Varianzen sind gleich	,781	190	,436	,07326
	Varianzen sind nicht gleich	,782	153,355	,436	,07326
I	Varianzen sind gleich	4,646	190	,000	,28949
		4,432	162,235	,000	,28949

Tabelle 33: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen des IT-Sicherheitsverhaltens (WÜG = Wissen über Gefahren, PB = Persönliche Bedeutung, ESU = Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ = Normative Überzeugung, EW = Einwilligungsbereitschaft, FK = Fähigkeiten, IK = Internale Kontrollüberzeugung, EK = Externale Kontrollüberzeugung, I = Intention).).

Bis auf die Skale „EK“ gibt es über die 2-Clusterlösung signifikante Mittelwertunterschiede. D. h., Mitarbeiter die einen hohen Ausprägungsgrad an den der unternehmerischen „Aufklärung & Information“ und „Datensicherheit“

wahrnehmen, sind den Skalen des IT-Sicherheitsverhaltens signifikant positiver eingestellt als die Mitarbeiter, die die unternehmerische Aufklärungs- und Informationsarbeit mit niedrigem Ausprägungsgrad wahrnehmen.

Die folgende Abbildung 24 gibt die Mittelwertunterschiede graphisch wider:

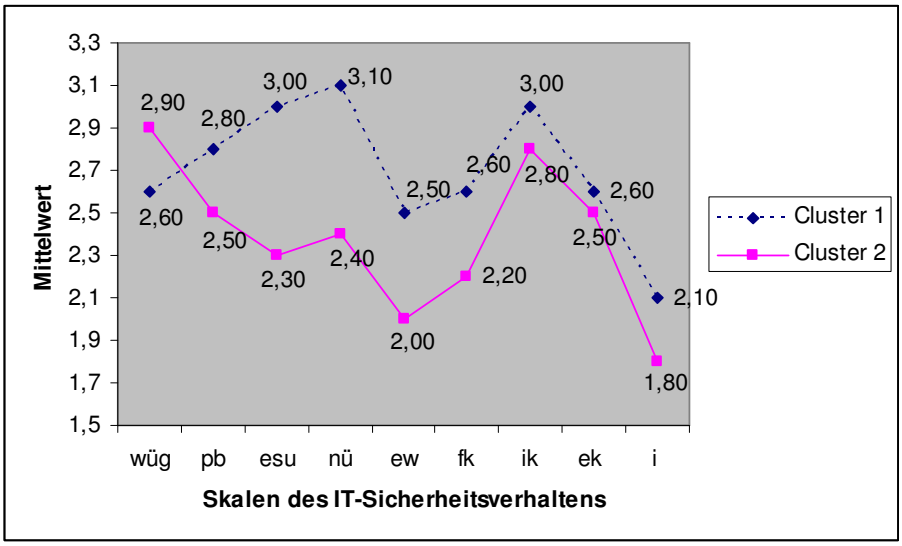


Abbildung 24: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen des IT-Sicherheitsverhaltens (Cluster 1= hohe Bewertung der IT-Sicherheitskultur, Cluster 2= niedrige Bewertung der IT-Sicherheitskultur; wüg= Wissen über Gefahren, pb= Persönliche Bedeutung, esu= Einschätzung der Sicherheitsumsetzung des Unternehmens, nü= Normative Überzeugung, ew= Einwilligungsbereitschaft, fk= Fähigkeiten, ik= Internale Kontrollüberzeugung, ek= Externale Kontrollüberzeugung, i= Intention).

Die Hypothese Nr. 3 konnte bestätigt werden. D. h. Mitarbeiter, die einen hohen Ausprägungsgrad der IT-Sicherheitskultur angeben, bewerten auch die Skalen des IT-Sicherheitsverhaltens signifikant höher.

5.3.4 Zusammenhänge zwischen der IT-Sicherheitskultur und der Sozialen Unterstützung

Hypothese Nr. 4:

Die Mitarbeiter, die die IT-Sicherheitskultur Ihres Unternehmens in den Bereichen „Aufklärung & Information“ und „Datensicherheit“ hoch einschätzen, bewerten auch die Skalen der „Sozialen Unterstützung am ‚Arbeitsplatz““ höher ein als Mitarbeiter die die IT-Sicherheitskultur niedrig einschätzen.

Abbildung 25: Untersuchungsdesign zur Überprüfung der Hypothese Nr. 4

Zur Verifizierung bzw. Falsifizierung der Hypothese wird ein t-Test bei unabhängigen Stichproben für Mittelwertgleichheit gerechnet.

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
SUK	Varianzen sind gleich	3,491	190	,001	,25575
	Varianzen sind nicht gleich	3,265	163,231	,001	,25575
SUV	Varianzen sind gleich	5,217	188	,000	,49679
	Varianzen sind nicht gleich	4,792	155,142	,000	,49679

Tabelle 34: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen der IT-Sicherheitskultur.

Die folgende Abbildung 26 gibt die Mittelwertunterschiede graphisch wider:

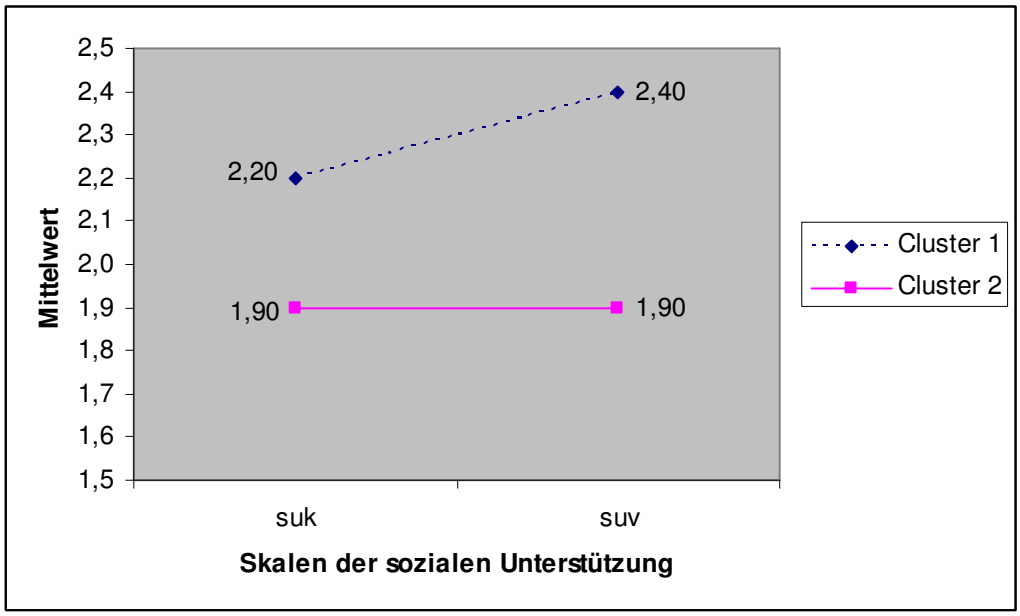


Abbildung 26: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen der Sozialen Unterstützung am Arbeitsplatz (Cluster 1= hohe Bewertung der IT-Sicherheitskultur, Cluster 2= niedrige Bewertung der IT-Sicherheitskultur; suk= Soziale Unterstützung am Arbeitsplatz durch die Kollegen, suv= Soziale Unterstützung am Arbeitsplatz durch den Vorgesetzten).

Die Hypothese Nr. 4 konnte bestätigt werden. D. h. Mitarbeiter, die einen hohen Ausprägungsgrad der IT-Sicherheitskultur angeben, bewerten auch die Skalen des Sozialen Unterstützung am Arbeitsplatz signifikant höher.

5.4 Ermittlung von Typenprofilen der Softwareergonomie

5.4.1 Clusteranalysen zur Ermittlung von Typenprofilen der Softwareergonomie

Die folgende Abbildung 25 gibt das Profil der beiden Clustergruppen hinsichtlich der Dimension „Softwareergonomie“ in Bezug auf die zugrunde gelegten Skalen wider:

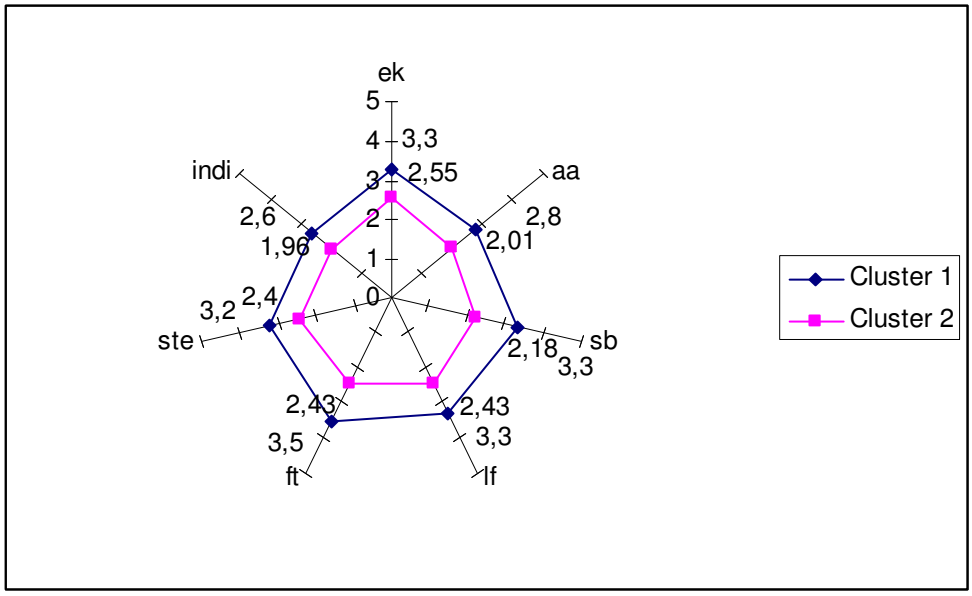


Abbildung 27: 2-Clusterlösung auf den Skalen der Softwareergonomie nach ISO 9241 (Cluster 1 = hohe Bewertung der Softwareergonomie, Cluster 2 = niedrige Bewertung der Softwareergonomie; (ek = Erwartungskonformität, aa =Aufgabenangemessenheit; sb = Selbstbeschreibungsfähigkeit; lf = Lernförderlichkeit; ft = Fehlertoleranz; ste = Steuerbarkeit; indi = Individualisierbarkeit).

Cluster 1 schließt 80 Mitarbeiter und Cluster 2 schließt 94 Mitarbeiter ein. Es resultiert folgende Gruppenmittelwerte auf den Skalen:

Skala	Cluster 1 (N=80)	Cluster 2 (N= 94)
ek	2,55	3,28
aa	2,01	2,78
sb	2,18	3,32
lf	2,43	3,28
ft	2,43	3,52
ste	2,4	3,23
indi	1,96	2,61

Tabelle 35: Gruppenmittelwerte der gebildeten Cluster auf den Skalen der Softwareergonomie nach ISO 9241 (ek = Erwartungskonformität, aa =Aufgabenangemessenheit; sb = Selbstbeschreibungs-fähigkeit; lf = Lernförderlich-keit; ft = Fehlertoleranz; ste = Steuerbarkeit; indi = Indi-vidualisierbarkeit).

Die Mitarbeiter der ersten Clusterlösung zeigen eine wesentlich niedrigere Wahrnehmung der Umsetzung der Softwareergonomischen Kriterien am Arbeitsplatz als die Mitarbeiter der zweiten Clusterlösung. D. h., die Clusterlösung ist aussagefähig. Zur Beantwortung des qualitativen Unterschieds zwischen der ersten und der zweiten Clusterlösung, erfolgt eine Diskriminanzanalyse.

5.4.2 Diskriminanzanalysen zur Überprüfung der 2-Clusterlösungen

Die folgende Tabelle 36 zeigt die isolierte Trennfähigkeit der einzelnen Variablen in Bezug auf die zwei Clustergruppen unter Angabe der Testgrößen Wilks Lambda und einer univariaten Varianzanalyse, d. h. es wird zunächst einmal getestet, inwieweit die einzelnen Skalen jeweils isoliert zwischen den beiden Gruppen trennen.

Skala	Wilks´ Lambda	F	Sign.
ek	,833	34,366	,000
aa	,691	76,809	,000
sb	,640	96,810	,000
lf	,715	68,394	,000
ft	,564	133,215	,000
ste	,707	71,140	,000
indi	,787	46,690	,000

Tabelle 36: Univariate Trennfähigkeit der einzelnen Skalen zur Softwareergonomie (ek = Erwartungskonformität, aa =Aufgabenangemessenheit; sb = Selbstbeschreibungsfähigkeit; lf = Lernförderlichkeit; ft = Fehlertoleranz; ste = Steuerbarkeit; indi = Individualisierbarkeit).

Die resultierende Trennfähigkeit ist für alle Skalen signifikant.

Auf der Grundlage von zwei Clustergruppen lässt sich nun eine Diskriminanzfunktion bilden, die eine optimale Trennung zwischen den Gruppen ermöglicht. Die relevanten Koeffizienten sind in Tabelle 37 wiedergegeben:

Funktion	Kanonische Korrelation	Eigenwert	% der Varianz	Wilks´ Lambda	χ^2-Wert	Df	Signif.
1	,755	1,323	100	0,431	141,996	7	,000

Tabelle 37: Gütemaße der kanonischen Diskriminanzfunktion.

Kennwerte:

- Der Wert der Kanonischen Korrelation beträgt ,755.
- Der Eigenwert liegt bei 1,323 und trennt signifikant zwischen den Gruppen mit einem Varianzanteil von 100%.
- Wilks´ Lambda beträgt ,431.

Die vorgenommene Klassifizierung in die zwei Gruppen kann als ausreichend bestätigt werden.

5.5 Operationalisierung und Erhebung weiterer Leistungsindikatoren

Auf der individuellen Ebene werden die subjektiv wahrgenommenen psychischen Belastungen und psychischen Beanspruchungen der Befragten erfasst. Die Leistungsindikatoren werden mit Hilfe des Fragebogens SynBA-GA von WIELAND-ECKELMANN (1992) erhoben. Bei diesem Fragebogen handelt es sich um ein Verfahren, mit dessen Hilfe sowohl eine Gesamtanalyse zur Beurteilung von psychischen Belastungs- und psychischen Beanspruchungsfaktoren von informationsverarbeitenden Tätigkeiten durchzuführen ist, als auch Gestaltungsmaßnahmen ableiten lassen. Das Verfahren wurde für die Analyse, Bewertung und Gestaltung von BSAP entwickelt. Das Gestaltungskriterium und –ziel ist die Beanspruchungsoptimalität und richtet sich nach der Doppelrolle der Beanspruchung. Aus methodischer Perspektive hinsichtlich der Gütekriterien und bzgl. seines Einsatzes im Betrieb, handelt es sich bei dem SynBA-GA um ein kompaktes, ökonomisches und effizientes Fragebogeninstrument für den Einsatz im betrieblichen Kontext. Die Auswertung des Fragebogens SynBA-GA erfolgt hinsichtlich der einzelnen Dimensionen. Damit ist eine „feinere“ Betrachtung bzw. Interpretation der Untersuchungsergebnisse möglich.

5.5.1 Zusammenhänge zwischen der Beanspruchungsoptimalität und der Softwareegonomie nach ISO 9241

Hypothese Nr. 5:
Die Mitarbeiter, die die Kriterien der Softwareergonomie hoch einschätzen, bewerten die Kriterien der Beanspruchungsoptimalität besser ein bzw. weisen einen geringen Gestaltungsbedarf in den einzelnen Kriterien der psychischen Belastung und psychischen Beanspruchung auf.

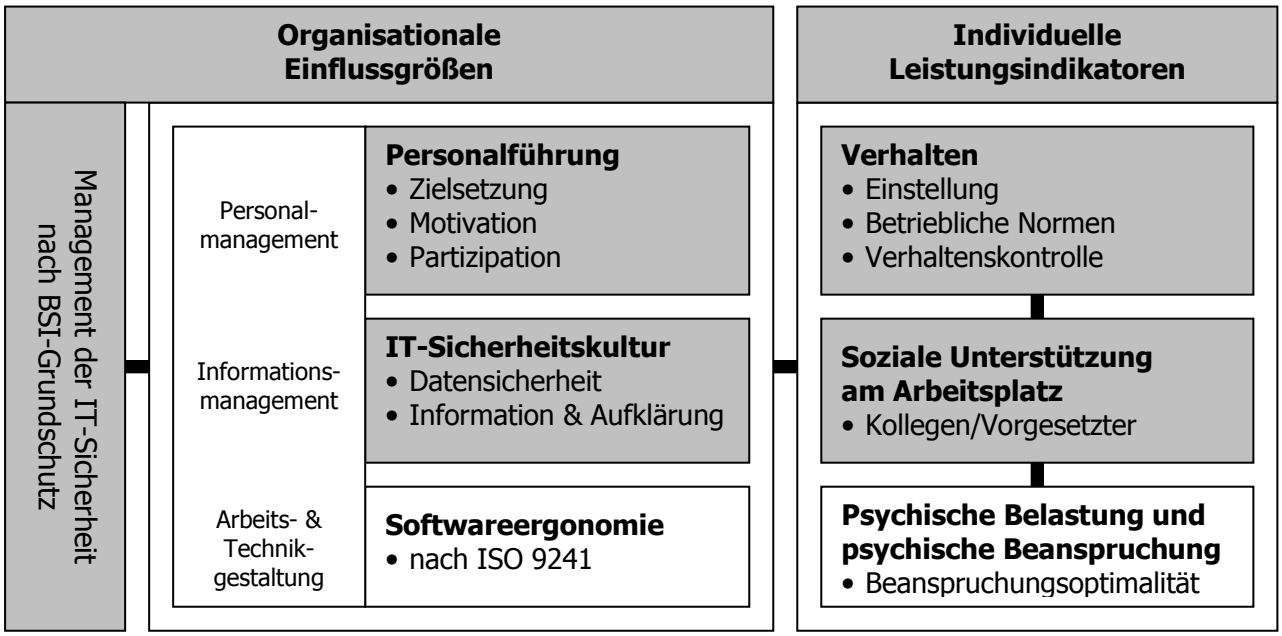


Abbildung 28: Untersuchungsdesign zur Überprüfung der Hypothese Nr. 5

Zur Verifizierung bzw. Falsifizierung der Hypothese wird ein t-Test bei unabhängigen Stichproben für Mittelwertgleichheit auf den Skalen der Beanspruchungsoptimalität gerechnet:

Skalen		t-Test für die Mittelwertvergleiche			
		t	df	sign. (2-seitig)	Mittlere Differenz
AA	Varianzen sind gleich	2,845	171	,005	,16653
	Varianzen sind nicht gleich	2,821	160,020	,005	,16653
TS	Varianzen sind gleich	3,377	170	,001	,14741
	Varianzen sind nicht gleich	3,307	142,935	,001	,14741
RB	Varianzen sind gleich	4,481	170	,000	,24077
	Varianzen sind nicht gleich	4,400	147,080	,000	,24077
LK	Varianzen sind gleich	1,025	170	,307	,07283
	Varianzen sind nicht gleich	1,030	169,053	,307	,07283
KK	Varianzen sind gleich	,219	169	,827	,01676
	Varianzen sind nicht gleich	,220	166,041	,826	,01676

Tabelle 38: t-Test auf Mittelwertunterschiede zwischen den beiden Clusterlösungen über die Skalen der Beanspruchungsoptimalität (AA= Arbeitsaufgabe, TS= Tätigkeitsspielraum, RB= Regulationsbehinderung, LK= Leistungskontrolle, KK= Kommunikation & Kooperation).

Bis auf die Skalen „LK“ und „KK“ gibt es über die 2-Clusterlösung signifikante Mittelwertunterschiede. D. h., Mitarbeiter die einen hohen Ausprägungsgrad nach den Kriterien der Softwareergonomie an ihrem BSAP wahrnehmen, bewerten die Skalen „AA“, „TS“ und „RB“ höher ein als die Mitarbeiter, die den Umsetzungsgrad der Softwareergonomischen Kriterien niedriger wahrnehmen.

Die folgende Abbildung 29 gibt die Mittelwertunterschiede graphisch wider:

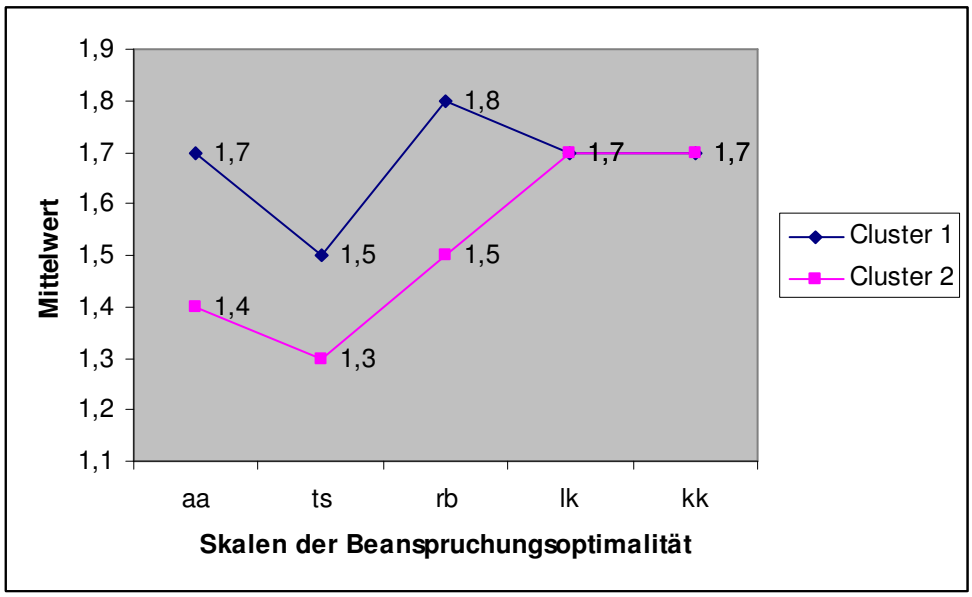


Abbildung 29: Mittelwertunterschiede zwischen den beiden Clustergruppen über die Skalen der Beanspruchungsoptimalität (Cluster 1 = hohe Bewertung der Beanspruchungsoptimalität, Cluster 2 = niedrige Bewertung der Beanspruchungsoptimalität, aa= Arbeitsaufgabe; ts = Tätigkeitsspielraum; rb = Regulationsbehinderung; lk = Leistungskontrolle; kk = Kommunikation & Kooperation).

Die Hypothese Nr. 5 konnte teilweise bestätigt werden. D. h. Mitarbeiter, die einen hohen Ausprägungsgrad der Umsetzung an softwareergonomischen Kriterien angeben, bewerten auch die Skalen der Beanspruchungsoptimalität in den Bereichen „AA“, „TS“ und „RB“ signifikant höher.

5.5.2 Zusammenhang zwischen Beanspruchungsoptimalität und IT-Sicherheitsverhalten

Hypothese Nr. 6:
Die Mitarbeiter, die ihren Arbeitsplatz und –tätigkeit beanspruchungsoptimal einschätzen, bewerten auch die Skalen zum „IT-Sicherheitsverhalten“ höher als Mitarbeiter die eine hohe psychische Belastung bzw. psychische Beanspruchung aufweisen.

Abbildung 30: Untersuchungsdesign zur Überprüfung der Hypothese Nr. 6.

In dem folgenden Abschnitt werden Mittelwertunterschiede zwischen einzelnen Gruppen, die nach dem Kriterium der Beanspruchungsoptimalität auf Grund der SynBA-Analyse eine geringe oder einen hohe Beanspruchung und damit einen geringen bzw. hohen Gestaltungsbedarf aufweisen und den Skalen des IT-sicherem Verhaltens auf Signifikanz überprüft. Das Mittel der Wahl ist die multivariate Varianzanalyse. Dabei gehen die Skalen des IT-Sicherheitsmanagements-Fragebogens als unabhängige Variablen und die Gruppen der Gestaltungsbereiche als abhängige Variablen in die Berechnung ein:

Testname	Wert	F	Hypothese df	Fehler df	Signifikanz
Pillai-Spur	,991	3722,580	5	165	.000
Wilks-Lambda	.009	3755,580	5	165	.000
Hotelling-Spur	112,805	3755,580	5	165	.000
Größte charakteristische Wurzel nach Roy	112,805	3755,580	5	165	.000

Tabelle 39: **Multivariater Signifikanztest der Skalen des IT-Sicherheitsverhalten**.

Variable	Mittel der Quadrate	F	Signifikanz
WÜG	-,30165	3,676	,020
PB	-,15717	6,620	,209
ESU	,17951	7,157	,267
NÜ	,08597	4,902	,538
EW	,06569	9,313	,546
FK	-,02634	3,370	,829
IK	-,18750	,256	,238
EK	-,03015	6,253	,804
I	,02762	4,215	,753

Tabelle 40: **Univariater F-Test mit (9; 192) df der Skalen zum IT-Sicherheitsverhalten (WÜG = Wissen über Gefahren, PB = Persönliche Bedeutung, ESU = Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ = Normative Überzeugung, EW = Einwilligungsbereitschaft, FK = Fähigkeiten, IK = Internale Kontrollüberzeugung, EK = Externale Kontrollüberzeugung, I = Intention).**

Um den Einfluss der Gruppenunterschiede bzgl. der einzelnen Skalen auf die Gesamtvarianz hin zu überprüfen, bietet sich ein Mittelwertvergleich der einzelnen Gruppen auf den jeweiligen Skalen mit Hilfe eines Scheffé-Tests an. Damit wird eine a-posteriori-Überprüfung der Mittelwertunterschiede unterschiedlicher Gruppengrößen möglich. In Tabelle 41 werden die Skalen den Gruppen gegenübergestellt und auf Signifikanz überprüft. Das Signifikanzkriterium lautet hierbei $p<.05$:

	Mittelwerte der Gestaltungsbereiche	
Skalen	geringer Gestaltungsbereich (N=117)	Hoher Gestaltungsbereich (N=54)
WÜG	2,7	3,0
PB	2,7	2,8
ESU	2,6	2,4
NÜ	2,8	2,7
EW	2,4	2,3
FK	2,3	2,3
IK	2,8	3,1
EK	2,7	2,7
I	2,0	2,0

Tabelle 41: **Mittelwerte der Gestaltungsbereiche in den Skalen des IT-Sicherheitsverhaltens (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK= Internale Kontrollüberzeugung, EK= Externale Kontrollüberzeugung, I= Intention)**.

Bis auf die Skala „WÜG“ weist keine der aufgeführten Skalen zum IT-Sicherheitsverhalten einen signifikanten Unterschied zwischen den beiden Gruppen des Gestaltungsbedarfs auf.

Die Hypothese Nr. 6 konnte nicht bestätigt werden.

5.5.3 Zusammenhang zwischen Beanspruchungsoptimalität und der Sozialen Unterstützung am Arbeitsplatz

Hypothese Nr. 7:
Die Mitarbeiter, die ihren Arbeitsplatz und ihre Arbeitstätigkeit beanspruchungs-optimal einschätzen, bewerten auch die Skalen zur „Sozialen Unterstützung am Arbeitsplatz“ höher als Mitarbeiter die eine hohe psychische Belastung bzw. psychische Beanspruchung aufweisen.

Abbildung 31: Untersuchungsdesign zur Überprüfung der Hypothese Nr. 7.

In dem folgenden Abschnitt werden Mittelwertunterschiede zwischen einzelnen Gruppen, die nach dem Kriterium der Beanspruchungsoptimalität auf Grund der SynBA-Analyse eine geringe oder einen hohe Beanspruchung und damit einen geringen bzw. hohen Gestaltungsbedarf aufweisen und den Skalen der Sozialen Unterstützung am Arbeitsplatz auf Signifikanz überprüft. Das Mittel der Wahl ist die multivariate Varianzanalyse. Dabei gehen die Skalen der Sozialen Unterstützung als

unabhängige Variablen und die Gruppen des Gestaltungsbedarfs als abhängigen Variablen in die Berechnung ein.

Testname	Wert	F	Hypothese df	Fehler df	Signifikanz
Pillai-Spur	,974	3638,433	2	187	.000
Wilks-Lambda	,026	3638,433	2	187	.000
Hotelling-Spur	37,928	3638,433	2	187	.000
Größte charakteristische Wurzel nach Roy	37,928	3638,433	2	187	.000

Tabelle 42: **Multivariater Signifikanztest der Skalen der Sozialen Unterstützung am Arbeitsplatz**.

Variable	Mittel der Quadrate	F	Signifikanz
SUK	,28680	41,092	,006
SUV	,20259	12,939	,143

Tabelle 43: **Univariater F-Test mit (2; 192) df der Skalen zur Sozialen Unterstützung am Arbeitsplatz (SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).**

Um den Einfluss der Gruppenunterschiede bzgl. der einzelnen Skalen auf die Gesamtvarianz hin zu überprüfen, bietet sich ein Mittelwertvergleich der einzelnen Gruppen auf den jeweiligen Skalen mit Hilfe eines Scheffé-Tests an. Damit wird eine a-posteriori-Überprüfung der Mittelwertunterschiede unterschiedlicher Gruppengrößen möglich. In Tabelle 44 werden die Skalen den Gruppen gegenübergestellt und auf Signifikanz überprüft. Das Signifikanzkriterium lautet hierbei $p<.05$:

	Mittelwerte der Gestaltungsbereiche	
Skalen	geringer Gestaltungsbereich (N=117)	Hoher Gestaltungsbereich (N=54)
SUK	2,30	2,01
SUV	2,25	2,05

Tabelle 44: **Mittelwerte der Gestaltungsbereiche in den Skalen der Sozialen Unterstützung am Arbeitsplatz(SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).**.

Nur die Skala „Soziale Unterstützung am Arbeitsplatz durch die Kollegen“ weist einen signifikanten Unterschied hinsichtlich des Bewertungskriteriums „Beanspruchungsoptimalität auf. Die Skala „Soziale Unterstützung am Arbeitsplatz durch den Vorgesetzten“ weist zwar keinen signifikanten Unterschied, ab eine Tendenz hinsichtlich des Ausmaßes der Beanspruchungsoptimalität auf.

Die Hypothese Nr. 7 konnte nur für den Bereich der „Sozialen Unterstützung am Arbeitsplatz durch die Kollegen“ bestätigt werden.

6 Unterschiede zwischen „IT-Experten“ und „IT-Anwendern“ hinsichtlich der Fragebogenskalen und -dimensionen

Die Hypothese Nr. 8:

A) „IT-Experten“ bewerten die Dimensionen „Einstellung“ und „Verhaltenskontrolle“ auf Grund ihres spezifischen Wissens höher als „IT-Anwender“.

B) Die Dimension „Betriebliche Normen“ wird auf Grund der allgemeingültigen „Unternehmenskultur“ sowohl von „IT-Experten“ als auch „IT-Anwendern“ gleich eingeschätzt.

Die Hypothese Nr. 9:

Das Führungsverhalten hinsichtlich den Dimensionen “Zielsetzung“, „Partizipation“, „Motivation“ und „Aufklärung und Information“ wird auf Grund der allgemeingültigen „Unternehmenskultur“ von den Gruppen „IT-Experten“ und „IT-Anwendern“ gleich eingeschätzt.

Zur Überprüfung der Hypothesen 8A, 8B und 9 folgt eine varianzanalytische Überprüfung mit anschließender Testung auf Mittelwertunterschiede. Zuvor werden die beiden Gruppe auf Normalverteilung getestet, um die Vergleichbarkeit der Gruppen zu garantieren.

6.1 Kolmogorov-Smirnov-Test

Mit Hilfe des K-S-Test werden die erhobenen Skalen auf Normalverteilung überprüft. Der Test nach Kolmogorov-Smirnov arbeitet auf Grundlage der maximalen absoluten Differenz zwischen den beobachteten kumulativen Verteilungsfunktionen für beide Stichproben. Wenn diese Differenz signifikant groß ist ($p>.05$), werden die beiden Verteilungen als verschieden betrachtet.

K-S-Test für Gruppe A:

	WÜG	PB	ESU	NÜ	EW	FK	IK	EK	I	AI	DS	ZS	P	M
N	188	192	169	189	191	191	180	192	192	192	192	191	192	192
K-S-Z	0,957	0,980	1,350	1,018	1,422	1,955	2,138	1,150	1,172	0,757	1,379	1,378	1,086	1,021
Asym. Sig.	0,319*	0,292*	0,052*	0,251*	0,065*	0,001	0,000	0,142*	0,128*	0,615*	0,052*	0,055*	0,189*	0,249*

Tabelle 45: Kolmogorov-Smirnov-Test für die Gruppe A (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK= Internale Kontrollüberzeugung, EK= Externale Kontrollüberzeugung, I= Intention).

K-S-Test für Gruppe B:

	WÜG	PB	ESU	NÜ	EW	FK	IK	EK	I	AI	DS	ZS	P	M
N	99	100	94	98	99	100	99	100	100	100	100	100	100	100
K-S-Z	1,287	1,232	0,823	0,827	1,339	1,619	1,152	1,361	1,154	0,778	1,357	0,992	1,072	0,863
Asym. Sig.	0,073*	0,096*	0,507*	0,501*	0,056*	0,011	0,141*	0,051*	0,140*	0,580*	0,050*	0,279*	0,201*	0,446*

Tabelle 46: Kolmogorov-Smirnov-Test für die Gruppe B. (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK= Internale Kontrollüberzeugung, EK= Externale Kontrollüberzeugung, I= Intention).

Außer den Skalen FK und IK in der Gruppe A (IT-Anwender) und der Skala FK in der Gruppe B (IT-Spezialisten) sind alle normalverteilt und somit für Mittelwertsunterscheidungen geeignet.

6.2 Varianzanalytische Überprüfung der Gruppenunterschiede „IT-Experten“ vs. „IT-Anwender“

In dem folgenden Abschnitt sollen Mittelwertunterschiede zwischen den Gruppen „IT-Anwender“ und „IT-Experten“ und dem IT-Sicherheitsverhalten auf Signifikanz überprüft werden. Das Mittel der Wahl ist hier eine multivariate Varianzanalyse. Dabei gehen die Skalen des Fragebogens als unabhängige Variablen und die beiden untersuchten Gruppen als abhängige Variablen in die Berechnung ein.

Als Indikator hierfür kann u. a. die multivariate Prüfgröße Pillai´s Trace gelten, der unter den angeführten Prüfmaßen die größte Robustheit zugesprochen werden kann. Aber auch die nachfolgenden univariaten Tests weisen signifikante Unterschiede zwischen den Gruppen auf allen zugrundeliegenden Skalen aus.

Die nachfolgenden Tabellen 47 und 48 zeigen das Untersuchungsergebnis:

Testname	Wert	F	Hypothese df	Fehler df	Signifikanz
Pillai-Spur	.201	6,409	11	280	.000
Wilks-Lambda	.799	6,409	11	280	.000
Hotelling-Spur	.252	6,409	11	280	.000
Größte charakteristische Wurzel nach Roy	.252	6,409	11	280	.000

Tabelle 47: Multivariater Signifikanztest der Gruppen zu den Skalen des IT-Sicherheitsverhaltens.

Variable	Mittel der Quadrate	F	Signifikanz
WÜG	10,787	17,848	.000
PB	3,730	5,580	.019
ESU	3,288	4,291	.039
NÜ	.852	1,162	.282
EW	2,239	5,383	.021
FK	6,337E-02	.125	.724
IK	10,942	12,807	.000
EK	17,334	31,421	.000
I	1,188E-02	.041	.839
SUK	1,667	4,370	.037
SUV	.510	.755	.386

Tabelle 48: **Univariater F-Test der Gruppen „IT-Experten“ und „IT-Anwender“ zu den Skalen des IT-Sicherheitsverhaltens (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK= Internale Kontrollüberzeugung, EK= Externale Kontrollüberzeugung, I= Intention, SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).**

Um den Einfluss der Gruppenunterschiede bzgl. der einzelnen Skalen auf die Gesamtvarianz hin zu überprüfen, bietet sich ein Mittelwertvergleich der einzelnen Gruppen auf den jeweiligen Skalen mit Hilfe eines Scheffé-Tests an. Damit wird eine a-posteriori-Überprüfung der Mittelwertunterschiede unterschiedlicher Gruppengrößen möglich. In Tabelle 49 werden die Skalen den Gruppen gegenübergestellt und auf Signifikanz überprüft. Das Signifikanzkriterium lautet hierbei $p < .05$:

	Mittelwerte der Gruppen	
Skalen	„IT-Anwender“ (N=192)	„IT-Experten“ (N=100)
WÜB*	2,92	2,51
PB*	2,75	2,51
ESU*	2,48	2,70
NÜ	2,71	2,60
EW*	2,33	2,14
FK	2,31	2,34
IK*	3,03	2,62
EK*	2,75	2,24
I	1,96	1,98
SUK*	2,09	1,93
SUV	2,12	2,03

Tabelle 49: Mittelwerte der Gruppen „IT-Anwender“ und „IT-Experten“ in den Skalen des IT-Sicherheitsverhaltens (*= signifikant bei p<.05) (WÜG= Wissen über Gefahren, PB= Persönliche Bedeutung, ESU= Einschätzung der Sicherheitsumsetzung des Unternehmens, NÜ= Normative Überzeugung, EW= Einwilligungsbereitschaft, FK= Fähigkeiten, IK= Internale Kontrollüberzeugung, EK= Externale Kontrollüberzeugung, I= Intention, SUK = Soziale Unterstützung Kollegen, SUV = Soziale Unterstützung Vorgesetzter).

Bis auf die Skalen „NÜ“, „FK“, „I“ und „SUV“ weisen alle anderen aufgeführten Skalen signifikante Unterschiede zwischen den Gruppen „IT-Anwender“ vs. „IT-Experten“ auf. Dabei zeigt sich, dass die „IT-Anwender“ die aufgeführten Skalen stärker einschätzen als die „IT-Experten“.

Der Gruppenvergleich soll im Folgenden für das Führungsverhalten vorgenommen werden. Die Ergebnisse lassen sich folgendermaßen darstellen:

Testname	Wert	F	Hypothese df	Fehler df	Signifikanz
Pillai-Spur	.034	2,015	5	286	.077
Wilks-Lambda	.966	2,015	5	286	.077
Hotelling-Spur	.035	2,015	5	286	.077
Größte charakteristische Wurzel nach Roy	.035	2,015	5	286	.077

Tabelle 50: Multivariater Signifikanztest der Gruppen zu den Skalen des Führungsverhaltens.

Variable	Mittel der Quadrate	F	Signifikanz
AI	,232	,345	,557
DS	,189	,269	,605
ZS	5,363E-02	,053	,818
P	3,261	3,553	,060
M	1,334	2,417	,121

Tabelle 51: Univariater F-Test der Gruppen „IT-Experten“ und „IT-Anwender“ zu den Skalen des Führungsverhaltens (AI = Aufklärung & Information, DS = Datensicherheit, ZS = Zielsetzung, P = Partizipation, M = Motivation).

	Mittelwerte der Gruppen	
Skalen	„IT-Anwender“ (N=192)	„IT-Experten“ (N=100)
AI	2,75	2,69
DS	2,37	2,32
ZS	3,32	3,29
P	3,01	2,78
M	2,30	2,16

Tabelle 52: Mittelwerte der Gruppen „IT-Anwender“ und „IT-Experten“ in den Skalen des Führungsverhaltens (AI = Aufklärung & Information, DS = Datensicherheit, ZS = Zielsetzung, P = Partizipation, M = Motivation).

Bzgl. der Unternehmenspolitik zeigen die Gruppen „IT-Anwender“ und „IT-Experten“ keine signifikanten Unterschiede. Auch hier zeigen die „IT-Anwender“ eine tendenziell stärkere Bewertung der Skalen.

Die Hypothese Nr. 9 konnte bestätigt werden.

Um die Unterschiede der Dimensionen aufzuzeigen, wird die varianzanalytische Überprüfung mit anschließender Testung auf Mittelwertunterschiede mit den Dimensionen „Einstellung“, „Betriebliche Normen“ und „Verhaltenskontrolle“ durchgeführt. Die folgenden Tabellen zeigen das Untersuchungsergebnis:

Testname	Wert	F	Hypothese df	Fehler df	Signifikanz
Pillai-Spur	.063	6,416	3	288	.000
Wilks-Lambda	.937	6,416	3	288	.000
Hotelling-Spur	.067	6,416	3	288	.000
Größte charakteristische Wurzel nach Roy	.067	6,416	3	288	.000

Tabelle 53: Multivariater Signifikanztest der Gruppen zu den Dimensionen des IT-Sicherheitsverhaltens.

Dimensionen	Mittel der Quadrate	F	Signifikanz
Einstellung	1,286	7,429	,007
Betriebliche Normen	1,463	3,301	,070
Verhaltenskontrolle	5,791	17,960	,000

Tabelle 54: Univariater F-Test der Gruppen „IT-Experten“ und „IT-Anwender“ zu den Dimensionen des IT-Sicherheitsverhaltens.

	Mittelwerte der Gestaltungsbereiche	
Dimensionen	„IT-Anwender“ (N=192)	„IT-Experten“ (N=100)
Einstellung	2,72	2,58
Betriebliche Normen	2,52	2,37
Verhaltenskontrolle	2,70	2,40

Tabelle 55: Mittelwerte der Gruppen „IT-Anwender“ und „IT-Experten“ in den Dimensionen des IT-Sicherheitsverhaltens.

Die Hypothesen Nr. 8A und 8B konnten bestätigt werden.

7 Zusammenhänge zwischen dem IT-Sicherheitsverhalten und den soziodemographischen Daten

In der Tabelle 56 sind die Ergebnisse der multivariaten Varianzanalyse mit den abhängigen Variablen des „IT-Sicherheitsverhalten“ dargestellt. Die unabhängigen Variablen sind die soziodemographischen Variablen „Berufszugehörigkeit“, „Betriebszugehörigkeit“, „Anzahl der Kollegen“ und „Altersgruppe“:

Unabhängige Variable	Art des Effekts	Pillai-Spur	df Hypothese/Fehler	F	Signifikanz
Berufserfahrung	Kein Effekt	.077	12/405	.890	.557
Betriebszugehörigkeit	Kein Effekt	.081	12/405	.933	.513
Anzahl der Kollegen	Kein Effekt	.067	15/405	.619	.860
Altersgruppe	Kein Effekt	.119	21/405	.798	.723

Tabelle 56: Multivariate Varianzanalyse des IT-Sicherheitsverhaltens und den soziodemographischen Variablen.

Keine der erhobenen Variablen zeigen einen signifikanten Einfluss auf das „IT-Sicherheitsverhalten“ auf. Somit kann bei der Überarbeitung des Fragebogens auf die Erhebung der soziodemographischen Daten verzichtet werden.

8 Diskussion der Ergebnisse und Ausblick

Ein großer Wettbewerbsvorteil der IT resultiert aus der hohen strategischen und operativen Bedeutung bei der Erfüllung von Unternehmenszielen. Dies insofern, da mittlerweile nahezu alle Geschäftsprozesse IT-gestützt ablaufen. Wesentliche Entscheidungen hängen von der Richtigkeit, Aktualität, Verfügbarkeit und Vertraulichkeit von Informationen ab, die mittels IT erarbeitet werden. Insbesondere werden durch die IT Geschwindigkeit, Kapazität, Zuverlässigkeit und Flexibilität der Geschäftsprozesse gewährleistet. Um diesen Wettbewerbsvorteil effektiv nutzen zu können, ist es wichtig, auf dem vernetzten multimedialen Kommunikationsweg den Transfer von sensiblen Daten so sicher als möglich zu gestalten.

Befragungen im Mittleren und Top Management haben gezeigt, dass Angriffe auf IT-Systeme weniger außerhalb eines Unternehmens zu suchen sind. So werden Einschätzungen zur Folge ca. 70% der „Systemangriffe“ durch die eigenen Mitarbeiter verursacht (vgl. COLE & MATZER, 1999). Dabei stehen Nachlässigkeit, Irrtum, fehlendes Wissen und Verständnislosigkeit bzgl. IT-Sicherheitsthemen im Vordergrund. Da der Datenschutz und die Datensicherheit eine zentrale Aufgabe des Managements und des Mitarbeiters ist, müssen auf der Ebene der Organisation Bedingungen geschaffen werden, um auf der einen Seite technische Standards umsetzen zu können und auf der anderen Seite die Mitarbeiter hinsichtlich der Thematik zu sensibilisieren und zu motivieren. Dies bedarf eines IT-Sicherheitsprozesses, der sowohl Platz für Fehler, als auch Spielraum für Veränderungen zulässt. Auf diesem Hintergrund sind Rahmenbedingungen zu definieren, die in einer allgemein anerkannten IT-Sicherheitsphilosophie fußen. Des Weiteren müssen die betrieblichen Teilsysteme Organisation, Technik und Mensch in ihrer Wechselbeziehung zueinander betrachtet werden.

Im Rahmen der vorliegenden Arbeit wurde der Fragebogen zum IT-Sicherheitsniveau zur Erfassung von individuellen Leistungsindikatoren nach Testkriterien überprüft und die Zusammenhänge nach dem oben genannten Prinzip der Teilsysteme mit anderen

Leistungsindikatoren untersucht. In den folgenden Abschnitten werden die Zusammenhänge der Indikatoren auf der Ebene der Organisation und der individuellen Ebene zusammengefasst und diskutiert.

Als Indikator auf der Ebene der Organisation sind die Umsetzungskriterien nach IT-Grundschutz des BSI und das Führungsverhalten analysiert worden. Die einzelnen Maßnahmenempfehlungen werden gesondert in einem eigenen Kapitel aufgelistet.

8.1 Bewertung des IT-Sicherheitsmanagements nach BSI-Grundschutz

Der Fragenkatalog des BSI-Grundschutzes wurde vor der endgültigen Zusammenstellung mit dem kommissarisch berufenen IT-Sicherheitsbeauftragten besprochen, relevante Fragen ausgewählt und in Form eines Interviews bewertet.

Der detaillierte Bewertungsbogen befindet sich im Anhang. Jeder Fragenkategorie wurden die vom BSI empfohlenen Umsetzungsmaßnahmen und Erläuterungen ergänzt. Die Fragen sind dergestalt aufgebaut, dass die Nichterfüllung einer Frage die jeweilige Umsetzungsmaßnahme beinhaltet. Im Folgenden wird der Fragenkomplexe kurz dargestellt und beurteilt:

8.1.1 Etablierung des IT-Sicherheitsprozesses

„Die Durchsetzung und Aufrechterhaltung eines angemessenen und ausreichenden IT-Sicherheitsniveaus können für einen komplexen IT-Verbund nur durch geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet werden. Es sind strategische Leitaussagen zu formulieren, konzeptionelle Vorgaben zu erarbeiten und die organisatorischen Rahmenbedingungen zu schaffen, um das ordnungsgemäße und sichere IT-gestützte Arbeiten des Unternehmens zu ermöglichen. Sinnvollerweise wird durch die Unternehmensleitung ein gesteuerter IT-Sicherheitsprozess initiiert, der die Voraussetzungen für die durchdachte Gestaltung sowie sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen gewährleistet. Da mit der allgemeinen

Verantwortung für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation auch die Gewährleistung der IT-Sicherheit der obersten Leitungsebene obliegt, muss diese den IT-Sicherheitsprozess initiieren, steuern und kontrollieren.“ (BSI, 2002; S. 1130).

Die Untersuchung zeigte, dass organisatorische Rahmenbedingungen nur zum Teil geschaffen wurden. Die Initiative zur Etablierung des IT-Sicherheitsprozesses ist nicht Gegenstand der Unternehmensleitung und wird nur in unzureichendem Maß unterstützt.

8.1.2 Erstellung einer IT-Sicherheitsrichtlinie

„Die IT-Sicherheitsleitlinie definiert das angestrebte IT-Sicherheitsniveau, mit dem die Aufgaben durch die Organisation erfüllt werden. Die IT-Sicherheitsleitlinie beinhaltet die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie. Sie ist somit Anspruch und zugleich die Aussage, dass das IT-Sicherheitsniveau auf allen Ebenen der Organisation erreicht werden soll.“ (BSI, 2002; S. 1135).

Für das untersuchte Unternehmen besteht zwar eine IT-Sicherheitspolicy. Diese ist aber erst nach einer gründlichen Suche im Intranet zu finden. Des Weiteren wurde die bestehende IT-Sicherheitspolicy in der englischen Sprache abgefasst und umfasst 63 Seiten. Somit ist nachvollziehbar, dass sich die Mitarbeiter nicht mir dieser Literatur befassen.

8.1.3 Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit

„IT-Sicherheit ist für jedes IT-Projekt, jedes IT-System und alle IT-Benutzer innerhalb einer Organisation von besonderer Bedeutung. Das angestrebte IT-Sicherheitsniveau kann nur erreicht werden, wenn das IT-Sicherheitskonzept unternehmensweit umgesetzt wird. Dieser übergreifende Charakter des IT-Sicherheitsprozesses macht es notwendig, die Rollen innerhalb des Unternehmens festzulegen. Den Rollen sind die

entsprechenden Aufgaben zuzuordnen, die wiederum von qualifizierten Mitarbeitern ausgeführt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effizient und effektiv erledigt werden. Das IT-Sicherheitsmanagement hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Organisation ab.“ (BSI, 2002;S. 1142).

Die Umsetzung von IT-Sicherheit beinhaltet den konkreten Aufbau einer eigenständigen Organisationsstruktur für IT-Sicherheit. Dies befand sich zum Zeitpunkt der Untersuchung in der Planungsphase. Die Leitung des IT-Sicherheitsmanagements wurde bis dahin nur kommissarisch von der Leitung der IT-Abteilung übernommen.

8.1.4 Erstellung eines Schulungskonzepts für IT-Sicherheit

„Die sachgerechte Erfüllung der Gemeinschaftsaufgabe "IT-Sicherheit" kann nur dann gelingen, wenn alle am IT-Sicherheitsprozess beteiligten Personen einen angemessenen Kenntnisstand über IT-Sicherheit im Allgemeinen und insbesondere über die Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet haben. Obwohl letztlich jeder Benutzer dazu motiviert werden sollte, sich auch in Eigeninitiative auf dem notwendigen Kenntnisstand zu halten, bleibt es in der Verantwortung der Organisationsleitung, durch geeignete Schulungsmaßnahmen die nötigen Voraussetzungen zu schaffen. Angesichts des Umfangs der möglichen Schulungsthemen und der Bedeutung der IT-Sicherheit ist bei der Auswahl der Schulungsinhalte ein koordiniertes Vorgehen erforderlich. Dieses ist in Schulungskonzepten darzulegen und zu dokumentieren.

Bei größeren Organisationen mit heterogenen Arbeitsplätzen wird *ein* Konzept in der Regel nicht ausreichen. Vielmehr sind Schulungskonzepte nach Umfang und Inhalt auf die Bedeutung und Komplexität des IT-Einsatzes bei den jeweiligen Zielgruppen abzustimmen. So muss der IT-Sicherheitskenntnisstand eines IT-Administrators oder Softwareentwicklers deutlich höher sein, als der eines kaufmännischen Mitarbeiters oder einer Schreibkraft. Erster Schritt bei der Abfassung von Schulungskonzepten zur

IT-Sicherheit ist daher die Einteilung der Mitarbeiter einer Organisation in Zielgruppen, für die jeweils ein eigenes Konzept erstellt wird. Hierbei ist zu gewährleisten, dass sich jeder Mitarbeiter, dessen Arbeitsbereich mittelbar oder unmittelbar mit der IT zusammenhängt, in einer für ihn passenden Gruppe wieder findet. Weiter ist zu gewährleisten, dass dieses Konzept nachprüfbar umgesetzt wird und die Schulungsnachweise aufbewahrt werden. Somit wird sichergestellt, dass eine umfassende Schulung in jeweils angemessener Tiefe stattfindet.

Die Schulungskonzepte zur IT-Sicherheit müssen in enger Abstimmung mit den sonstigen Schulungskonzepten eines Unternehmens, insbesondere mit der IT-Anwenderschulung erstellt werden. Dabei sollte überlegt werden, inwieweit es möglich ist, Schulungsthemen zur IT-Sicherheit in Letztere zu integrieren. Eine solche Einbindung hat den Vorteil, dass IT-Sicherheit unmittelbar als Bestandteil des IT-Einsatzes wahrgenommen wird. Voraussetzung hierfür ist zunächst eine ausreichende und nachgewiesene Qualifikation der Dozenten. Entscheidend bei der Gestaltung der Schulung selbst ist ein hinreichender Umfang des Teils "IT-Sicherheit" innerhalb des Gesamtplans.“ (BSI, 2002; S. 1157).

Es bestehen keine eigenen Schulungskonzepte zur IT-Sicherheit. Die relevanten Sicherheitsthemen werden nur am Rande von fachspezifischen Schulungen erwähnt.

8.1.5 Sensibilisierung der Mitarbeiter für IT-Sicherheit

„In der Praxis bestätigt sich immer wieder, dass ein Großteil der Sicherheitsvorfälle bei der IT-Nutzung nicht durch organisationsfremde Außenstehende, sondern durch unsachgemäßes Verhalten eigener Mitarbeiter hervorgerufen wird. Daher können die Verbesserung der IT-Sicherheitskenntnisse der eigenen Mitarbeiter und die Erhöhung der Eigenverantwortung jedes IT-Benutzers als eine besonders wirksame und überdies relativ kostengünstige Maßnahme zur Erhöhung der IT-Sicherheit gelten. Ebenso sind gute IT-Sicherheitskenntnisse Voraussetzung dafür, dass sicherheitsrelevante Zwischenfälle frühzeitig als solche erkannt werden. Es sollte bei allen Mitarbeitern ein

hinreichender Kenntnisstand über die Belange der IT-Sicherheit und das Bewusstsein für die Risiken im alltäglichen Umgang mit der IT vorhanden sein. Zur Erreichung dieses Ziels trägt neben einem Schulungskonzept für IT-Sicherheit insbesondere die wiederholte Sensibilisierung aller Mitarbeiter durch IT-Sicherheits-Verantwortliche, Vorgesetzte oder Kollegen wesentlich bei.

Im Mittelpunkt der Sensibilisierungsmaßnahmen sollten stets die Zielsetzungen der IT-Sicherheitsleitlinie stehen. Jedem Mitarbeiter muss im täglichen Umgang mit der IT bewusst sein und bewusst gemacht werden, dass die Einhaltung der Sicherheitsziele, die gewissenhafte Umsetzung der Sicherheitsmaßnahmen sowie die Erhaltung und Steigerung des erlangten Sicherheitsniveaus zu selbstverständlichen Pflichten innerhalb des Unternehmens gehören.“ (BSI, 2002; S. 1159).

Alle gut gemeinten Maßnahmen versanden, wenn der Vorgesetzte nicht mit gutem Beispiel voran geht. Leider trifft dies in der Praxis häufig zu – so auch in dem untersuchten Unternehmen.

8.1.6 Aufrechterhaltung der IT-Sicherheit

„Im IT-Sicherheitsprozess geht es nicht nur darum, das angestrebte IT-Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende IT-Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle IT-Sicherheitsmaßnahmen regelmäßig überprüft werden.

Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens alle zwei Jahre) durchgeführt werden und können bei gegebenem Anlass auch zwischenzeitlich erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden IT-Sicherheitsmaßnahmen. Die in den einzelnen Überprüfungen erlangten Ergebnisse zu dokumentieren, ist von großem Vorteil. Dabei wird festgelegt, wie mit den Überprüfungsergebnissen zu verfahren ist. Hervorzuheben

ist hierbei, dass Überprüfungen nur dann wirksam die IT-Sicherheit aufrechterhalten können, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden.

Es sollte im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Dazu ist zu regeln, welche IT-Sicherheitsmaßnahmen wann und von wem zu überprüfen sind. Somit wird zum einen unnötige Doppelarbeit vermieden und zum anderen verhindert, dass bestimmte Bereiche innerhalb einer Organisation unberücksichtigt bleiben.“ (BSI, 2002; S. 1161).

8.1.7 Dokumentation des IT-Sicherheitsprozesses

„Der Ablauf des IT-Sicherheitsprozesses und die Arbeitsergebnisse in seinen einzelnen Phasen sollten dokumentiert werden. Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der IT-Sicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist dabei, dass nicht nur die jeweils aktuelle Version der betreffenden Unterlagen rasch verfügbar ist, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst hierdurch ist eine kontinuierliche Rückverfolgung der Entwicklung im Bereich IT-Sicherheit, bei der die getroffenen Entscheidungen nachvollziehbar werden, gewährleistet.“ (BSI, 2002; S. 1168).

Die Untersuchung zeigte, dass sich die regelmäßigen Überprüfungen auf ein bis zwei sporadische Kontrollen im Jahr beschränken. Die Einhaltung der IT-Sicherheits-maßnahmen wird mit der Verpflichtung auf Einhaltung der Vorschriften durch die geleistete Unterschrift des Arbeitsvertrages, der Verpflichtung auf Geheimhaltung von unternehmensbezogenen Daten und der Information über den korrekten Umgang mit Passwörtern vorausgesetzt.

8.1.8 Erstellung eines Handbuches zur IT-Sicherheit

„Im Laufe des IT-Sicherheitsprozesses werden nicht nur die in den vorstehenden Maßnahmen erwähnten Dokumente produziert, darüber hinaus entstehen in der Umsetzungsphase weitere Regelungen für sämtliche oder spezielle Arbeitsplätze. Es werden Verhaltensregeln oder Handlungsanleitungen formuliert, die jedem Mitarbeiter als Basis für seine Handlungen oder Nicht-Durchführungen am Arbeitsplatz zur Verfügung stehen können. Es ist daher Aufgabe der Organisation, diese Regelungen zusammenzutragen und in geeigneter Form der jeweiligen Zielgruppe an die Hand zu geben. Während die Dokumentation des IT-Sicherheitsprozesses ein wesentliches Arbeitsmittel für das IT-Sicherheitsmangement-Team ist, dient das Handbuch der IT-Sicherheitsorganisation als Leitfaden für alle vom IT-Sicherheitsprozess betroffenen Mitarbeiter. In der Praxis werden Teile dieser Handreichung unter Bezeichnungen wie "PC-Richtlinie" oder "IT-Benutzerrichtlinie" verwendet. Es gilt, für die verschiedenen Zielgruppen innerhalb der Organisiation zu unterschiedlichen Regelungen zu kommen, die sich an den gleichen Leitaussagen orientieren, daneben aber auch speziell auf Rechte und Pflichen aus der jeweiligen Funktion eingehen. So entstehen Regelwerke, in denen Aufgaben und Verantwortlichkeiten für unterschiedliche Zielgruppen zu beschreiben sind.

Das Erstellen eines Handbuches zur IT-Sicherheit als Leitfaden für alle vom IT-Sicherheitsprozess betroffenen Mitarbeiter wird erst unter Mitwirkung des IT-Sicherheitsbeauftragten und der Einberufung eines IT-Sicherheits-Teams in Auftrag gegeben und durchgeführt.“ (BSI, 2002; S. 1169).

8.2 Ergebnisse der auf Organisationsebene erhobenen Einflussgrößen auf die individuellen Leistungsindikatoren

8.2.1 Personalmanagement

Die drei dargestellten Führungsinstrumente „Zielsetzung“, „Partizipation“ und „Motivation“ dienen der persönlichen Weiterentwicklung des Mitarbeiters. Ihr Einsatz soll sowohl intrinsische Motivation fördern als auch den Mitarbeiter zu einem verantwortungsbewussten, mitdenkenden Menschen machen, auf dessen Wissen und Fähigkeiten eine Organisation aufbauen und sich (weiter-)entwickeln kann. Sie tragen ein großes Stück dazu bei, IT-Sicherheitsbewusstsein zu fördern und IT-sicheres Handeln zu realisieren. Doch die Effizienz der oben beschriebenen Führungsstrategien ist nicht allein von der inhaltlichen Umsetzung abhängig, sondern genauso von der Persönlichkeitseigenschaft der Führungsperson, dessen Wertvorstellung, Vorbildfunktion und der wirtschaftlichen Situation des Unternehmens. Die Führungsstrategien bilden einen wichtigen Ansatzpunkt, um Mitarbeiter zur Umsetzung von Sicherheitsvorkehrungen in der IT zu motivieren. „Langfristig betrachtet, hat jeder Vorgesetzte die Mitarbeiter, die er verdient“ (COMELLI & VON ROSENSTIEL, 2001; S. 85).

Mit Hilfe der Clusteranalyse konnten Typenprofile erstellt werden, die zwischen Mitarbeitern diskriminieren, die auf der einen Seite das Führungsverhalten ihrer Vorgesetzten bzgl. den Führungsstrategien „Zielsetzung“, „Motivation“ und „Partizipation“ hoch bewerten sowie Mitarbeitern, die das Führungsverhalten hinsichtlich der Strategien niedrig einschätzen.

8.2.1.1 Personalführung vs. IT-Sicherheitsverhalten

Der Vergleich der Gruppen „hohe Bewertung der Personalführung“ und „niedrige Bewertung der Personalführung“ mit Hilfe eines t-Test bei unabhängigen Stichproben für Mittelwertgleichheit zeigten die erhobenen Skalen des Fragebogens zur Messung

des IT-Sicherheitverhaltens bis auf die Skala „Externale Kontrollüberzeugung“ (EK) signifikante Unterschiede. Dies lässt den Schluss zu, dass die Wahrnehmung eines positiven Führungsstils einen positiven Einfluss auf die Sensibilität der Mitarbeiter bzgl. der IT-Sicherheitsthemen hat. Der fehlende Unterschied bei der Skala EK lässt die Vermutung zu, dass die Mitarbeiter unabhängig des Führungsverhaltens ihrer Vorgesetzten Einflussmöglichkeiten bei der Beeinflussung und Steuerung bei der Gefahrenabwehr am BSAP wahrnehmen, die Motivation dazu aber gering ausfallen kann.

8.2.1.2 Personalführung vs. Soziale Unterstützung

Beim Vergleich der Gruppen „hohe Bewertung der Personalführung“ mit der Gruppe „niedrige Bewertung der Personalführung“ mit Hilfe des t-Test bei unabhängiger Stichproben für Mittelwertgleichheit zeigen die erhobenen Skalen des Fragebogens zur Messung der Sozialen Unterstützung am Arbeitsplatz sowohl signifikante Unterschiede bei den Vorgesetzten (SUV) als auch bei den Kollegen (SUK). Dabei zeigt sich eine deutlich höhere Bewertung bei der Skala SUV. Dies kann ein Hinweis dafür sein, dass der positive Einsatz der Führungsstrategien auch zu einem offeneren und positiven Betriebs- bzw. Sozialklima beiträgt. So kann vor „unsicheren“ Entscheidungen eher auf die Hilfe der Kollegen bzw. des Vorgesetzten vertraut und zurückgegriffen werden.

8.2.2 Informationsmanagement

Die beiden Bereiche „Aufklärung und Information durch das Unternehmen“ und „Einschätzung der Aktivitäten des Unternehmens zum Erhalt von Daten“ sollen darüber Auskunft geben, wie sehr Informationen bzw. Aufklärungsarbeit durch das Unternehmen stattfinden bzw. von den Mitarbeitern wahrgenommen werden. Dies wird darüber erreicht, indem Mitarbeiter über mögliche Risiken und gängige Sicherheitsstandards zur Abwehr dieser Risiken informiert werden. Dies wiederum dient als Beitrag zur Schaffung einer „sich sicher fühlenden Arbeitsumgebung“.

Mit Hilfe der Clusteranalyse konnten Typenprofile erstellt werden, die zwischen Mitarbeitern diskriminieren die sich „gut“ vs. „schlecht“ informiert betrachten.

8.2.2.1 IT-Sicherheitskultur vs. IT-Sicherheitsverhalten

Der Vergleich der Gruppe 1 „hohe Bewertung der Aufklärungsarbeit durch das Unternehmen“ und der Gruppe 2 „niedrige Bewertung der Aufklärungsarbeit durch das Unternehmen“ mit Hilfe eines t-Test bei unabhängiger Stichprobe für Mittelwertgleichheit zeigt signifikante Unterschiede zwischen diesen beiden Gruppen. Dabei bewertet die Gruppe 1 ihr IT-Sicherheitsverhalten signifikant höher als die Gruppe 2. Eine Ausnahme bildet hier die Skala „wüg“. Hier liegt der signifikante Unterschied in umgekehrter Richtung, d. h., Gruppe 1 bewertet die Skala „wüg“ bedeutend niedriger als Gruppe 2. Somit kann eine positive Einschätzung der IT-Sicherheitskultur zu der Überzeugung führen, dass noch nicht genügend Wissen über die drohenden Gefahren und der Abwehrmaßnahmen dieser Gefahren vorhanden ist. Dieses Wissensdeifzit kann mit geeigneten Schulungsmaßnahmen und Wissenstransfer via Intranet erfolgen.

Keinen Unterschied weist die Skala „EK“ in den beiden Gruppen auf. Mit einer mittleren Bewertung von 2,5 bzw. 2,6 sehen sich die Mitarbeiter unabhängig der Bewertung der unternehmerischen Aufklärungsarbeit keiner bedrohlichen Situation ausgesetzt.

8.2.2.2 IT-Sicherheitskultur vs. Soziale Unterstützung

Ähnlich wie bei dem Vergleich der Personalführung und der Sozialen Überstützung zeigt sich auch hier, dass eine hohe Bewertung der IT-Sicherheitskultur zu einer hohen Bewertung der Sozialen Unterstützung am Arbeitsplatz durch die Kollegen bzw. den Vorgesetzten erfolgt. Auch hier kann dies als Zeichen eines positiven Betriebs- bzw. Sozialklimas gedeutet werden.

8.2.3 Arbeitsgestaltung

Als Kriterium zur Ermittlung von Kennwerten zur Messung der Arbeitsgestaltung wurde die Bewertung von softwareergonomischen Kriterien nach ISO 9241 herangezogen. Auch hier wurden Gruppenprofile hinsichtlich der subjektiven Bewertung der Einzelkriterien gebildet.

8.2.3.1 Softwareergonomie vs. Beanspruchungsoptimalität

Es zeigt sich, dass ein nach den Kriterien der Beanspruchungsoptimalität gestalteter BSAP auch mit einer positiven Einschätzung der softwareergonomischen Kriterien in Verbindung steht.

8.2.3.2 Softwareergonomie vs. IT-Sicherheitsverhalten

Ähnlich den anderen Untersuchungsergebnissen lässt sich auch hier schlussfolgern, dass eine positive Bewertung der softwareergonomischen Kriterien auch eine positive Bewertung der Skalen zum IT-Sicherheitsverhalten beinhaltet.

8.3 Ergebnisse auf der individuellen Ebene

Auf der individuellen Ebene wurden die Leistungsindikatoren „Beanspruchungsoptimalität“, „Soziale Unterstützung“, „Softwareergonomie“ und das „IT-Sicherheitsverhalten“ analysiert und in Beziehung zueinander gesetzt.

8.3.1 Beanspruchungsoptimalität vs. IT-Sicherheitsverhalten

Mit Hilfe des Fragebogens SynBA-GA wurde auf der individuellen Ebene die subjektiv wahrgenommene psychische Belastung gemessen. Die Auswertung der Fragebogenergebnisse erfolgte bzgl. der Einteilung nach der Kriterien

„Beanspruchungsoptimalität“ nach WIELAND-ECKELMANN (1992). Es wurden zwei Gruppen mit der Clusteranalyse gebildet. Die erste Gruppe fasst Mitarbeiter zusammen, die die Leistungskriterien positiv bewerteten und damit auch keinen bzw. einen geringen Gestaltungsbedarf aufwiesen. Die zweite Gruppe beinhaltet Mitarbeiter, die die Leistungskriterien negativ bewerteten und damit einen hohen Gestaltungsbedarf zeigten. Der t-Test auf Mittelwertunterschiede zwischen diesen beiden Gruppen ergab, dass Mitarbeiter, die einen geringen Gestaltungsbedarf hatten, die Skalen des IT-Sicherheitsverhaltens auch signifikant höher bewerten. Ausnahmen bildeten die Skalen „Einschätzung des Stellenwerts IT-Sicherheit für das Unternehmen“ (ESU) und „Externale Kontrollüberzeugung“ (EK). Eine Erklärung wäre, dass unabhängig der Beanspruchungsoptimalität am BSAP sowohl das Wissen über die Wichtigkeit des Erhalts der Daten (Sicherung der Arbeitsleistung) bei den Mitarbeitern vorhanden ist, aber auch das Wissen über die Abhängigkeit der Datensicherung durch „Externe“ (IT-Abteilung) zu gewährleisten ist.

8.4 Ergebnisse zwischen „IT-Experten“ vs. „IT-Anwender“

8.4.1.1 Personalführung

Die Datenauswertung zwischen den beiden Gruppen „IT-Anwender“ und „IT-Experten“ zeigt, dass es keinen Unterschied hinsichtlich des wahrgenommen Führungsstils gibt. Dies kann vor allem daran liegen, dass IT-Sicherheitsthemen nicht über den Vorgesetzten kommuniziert werden, sondern als Aufgabe der IT-Abteilung bzw. übergeordneter oder unabhängiger Strukturen (Abteilungen) betrachtet wird. Somit sieht sich der Vorgesetzte nicht verantwortlich bei der Einhaltung, Umsetzung und Motivation der Mitarbeiter hinsichtlich IT-Sicherheitsthemen. Er definiert diese nicht zu seinem Aufgabenbereich gehörend.

8.4.1.2 IT-Sicherheitsverhalten

Bei einem Vergleich der wahrgenommen IT-Sicherheit zwischen „IT-Anwendern“ und „IT-Experten“ zeigt sich ein signifikanter Unterschied zwischen den Gruppen in den Dimensionen „Einstellung“ und „Verhaltenskontrolle“. Dabei erhalten die „IT-Anwender“ eine positivere Bewertung als die „IT-Experten“. Dies zeigt sich auch auf Skalenniveau. Dabei kann die Frage aufgeworfen werden, ob „IT-Anwender“ nicht einem subjektiven Fehlschluss erliegen, da sie auf Grund fehlenden Fachwissens keinen Einblick über die Vielzahl an „Angriffsmöglichkeiten“ am BSAP haben. Die Bewertung des IT-Sicherheitsfragebogens erfolgt immer aus der subjektiven Sicht der eigenen Realität und dem damit verbundenen Wissen, Kenntnissen und Schlussfolgerungen. Die Dimension „Betriebliche Normen“ zeigt in den Gruppen keinen signifikanten Unterschied auf. Auf Grund der einheitlichen IT-Sicherheitspolitik bzw. –kultur, kennen die Mitarbeiter die Bestimmungen und Anweisungen, und damit haben sie Wissen über den Wissensstand der Kolleginnen und Kollegen.

8.5 IT-Sicherheitsverhalten vs. Soziodemographische Daten

Die Betrachtung der Zusammenhänge zwischen dem Verhalten und den soziodemographischen Daten weisen keinen signifikanten Zusammenhang auf. Somit kann zur Freude des Betriebsrats beim weiteren Einsatz des Fragebogeninstruments auf diese Erhebungskriterien verzichtet werden. Dies lässt auf eine höhere Beteiligung der Mitarbeiter bei zukünftigen Untersuchungen hoffen.

8.6 Schlussfolgerung und Ausblick

Die zuvor diskutierten Ergebnisse resultieren aus Querschnittdaten und können streng genommen keine Aussage über die Wirkrichtung der Zusammenhänge klären. Zur Spezifizierung der dargestellten Beziehung wäre demnach eine Längsschnittstudie mit Kontrollgruppendesign wünschenswert. Dies birgt allerdings unter Feldbedingung wegen der notwendigen Kontrolle möglicher Störvariablen weitere Probleme mit sich.

Ziel des Fragebogens ist die Erfassung von Leistungsmaßen des IT-Sicherheitsprozesses auf individueller Ebene in Form von Bestimmungsgrößen zum IT-sicherheitsgerechten Verhalten und Aspekte der Personalführung zur Umsetzung von IT-Sicherheit.

Unterstellt man, dass kontinuierlich gute Sicherheitsleistung ein Resultat bestimmter Steuerungssysteme ist, so ist der Fragebogen durch die Erfassung einiger Bestimmungsgrößen des IT-Sicherheitsverhaltens und der Personalführung in der Lage, einen zusätzlichen Indikator für die Güte solcher Steuerungssysteme zu liefern. Während bei den Maßen auf der Ebene der Organisation die Aussage möglich ist, „Welches?“ Leistungsniveau besteht, bietet der Fragebogen zusätzliche Ansatzmöglichkeiten, indem er durch die Bestimmungsgrößen des sicherheitsgerechtem Verhaltes auch das „Warum?“ des entsprechenden Niveaus näher bestimmt.

Die betriebswirtschaftlichen Gründe zur Verbesserung der IT-Sicherheit bestehen zum einem im Erhalt der unternehmensbezogenen Daten und zum anderen mit der durch Fehlerbehebung verbundenen Zeiten und Kosten. Aufgrund der Notwendigkeit einer Intervention seitens des Unternehmens kann durch den Einsatz von Verfahren und Instrumenten versucht werden, die Defizite im IT-Sicherheitsverhalten zu beseitigen, bevor Datenverluste oder IT-Ausfälle verursacht worden sind. Vor allem im Einsatz von IT muss dem Gedanken präventiven Handelns Vorschub gewährt werden.

Datenverluste können Unternehmen schädigen und damit Wettbewerbsvorteile zunichte machen.

Die Verbesserung von IT-Sicherheit ist auf der Prozess- oder Managementebene genauso zu handhaben wie Konzepte zur Verbesserung der Qualität und Produktivität. Im Rahmen eines ganzheitlichen Managements des Arbeits- und Gesundheitsschutzes kann das IT-Sicherheitsmanagement einen weiteren Beitrag zur Förderung und Erhaltung psychischer Gesundheit leisten. Durch den Fragebogen ist eine Leistungsermittlung auf individueller Ebene möglich.

Um die Sicherheit am BSAP nachhaltig im betrieblichen Alltag implementieren zu können, ist es wichtig, den Mitarbeiter als Produktionsfaktor mit Hilfe der Arbeitsaufgabengestaltung zu fördern und zu motivieren. Die Arbeitsaufgabe soll derart gestaltet werden, dass intrinsische Motivation durch Aufgabenorientierung geschaffen bzw. gefördert wird. Die praktische Konsequenz hieraus formulieren TURNER & KARASEK (1984), nämlich, dass es erforderlich sei, die „psychische Arbeitsbelastung zu ermitteln, zu beurteilen und letztendlich durch Maßnahmen der Arbeitsgestaltung zu beeinflussen“ (zit. Nach WIELAND-ECKELMANN, 1996; S.15). Wird der Aspekt der Arbeitsgestaltung vernachlässigt, kann dies sowohl negative Folgen für die psychische und physische Gesundheit, als auch „negative Folgen für das Engagement und die Arbeitszufriedenheit der Beschäftigten haben“ (WEIßGERBER, 1998; S. 7). Dies kann im gleichen Sinne auch die Bereitschaft, die Maßnahmen zur Umsetzung von IT-Sicherheit am BSAP, die Gefahrenkognition, –bewertung und die Weitergabe der Informationen an die zuständige Stelle betreffen.

Es wäre für die Ergebnisinterpretation hilfreich gewesen, die subjektiven Beschwerden der Mitarbeiter zu erheben, um diese mit der jeweiligen Aufgabengestaltung in korrelative Beziehung zu setzen. Eine exakte Aufgabenbeschreibung hätte weitere Differenzierungen ermöglicht, so dass man in auf die Detailebene hätte gehen können. Aus organisatorischen und Betriebsrat bedingten Gründe konnten derartige Daten nicht erhoben werden. Dies kann Ansatzpunkte für weitere Untersuchungen ergeben.

Wie gezeigt werden konnte, kann das Führungspersonal durch adäquaten Einsatz expliziter Führungsstrategien das Verhalten direkt und positiv – d. h. seinen bzw. den unternehmerischen Zielen entsprechend – beeinflussen. Durch das „richtige" Definieren bzw. Vereinbaren von Zielen, entsprechender Kontrolle sowie regelmäßiger und effizienter Rückmeldung über die Arbeitsleistung, ist eine Operationalisierung dieser Führungsstrategien möglich (vgl. STAPP, ELKE & ZIMOLONG, 1999).

Leider zeigt die Realität oft ein anderes Bild, vor allem, was das IT-Sicherheitsbewusstsein im Mittleren und Top-Management betrifft. Umfragen zufolge sehen die Manager die Ursachen von Datenverlusten überwiegend beim Mitarbeiter. Dabei sind es weniger Absichten als viel mehr Irrtum und Nachlässigkeiten (vgl. KOSSAKOWSKI & SCHINDLER, 2002; Zeitschrift KES 2002/3, S. 6-23). Obwohl dies den Managern bewusst ist, wird ein sehr geringer Teil des Budgets für IT-Sicherheitsmaßnahmen in die Sensibilisierung und Schulung der Mitarbeiter verwendet (vgl. COOLE & MATZER, 2000). Dieses Bild konnte bei der Erhebung der IT-Sicherheitsumsetzung nach dem BSI IT-Grundschutz bestätigt werden. Zum einen fließen – wenn überhaupt – Sicherheitssensibilisierungsmaßnahmen indirekt bei anderen IT-bezogenen Weiterbildungsmaßnahmen (z. B. Programmschulung) mit ein, oder werden mit einer Verpflichtungserklärung zur Einhaltung von datensichernden Maßnahmen abgetan. Meist betrachtet das Management die Umsetzung von IT-Sicherheitsbestimmungen als Sache der IT-Abteilung. Diese ist in großen Unternehmen noch nicht einmal ein Bestandteil des eigenen Unternehmens, sondern an Externe vergeben, die eine eigene Unternehmenskultur und –philosophie besitzen.

Das Bewusstsein wird erst dann geschärft, wenn IT-Anlagen ausfallen und Mitarbeiter unter Umständen stunden, oder sogar tagelang nicht ihrer Arbeitstätigkeit nachkommen können. Dies macht auch die Messung eines IT-Sicherheitsniveaus schwierig, da keine Leistungsdaten bzgl. einer Vergleichbarkeit gewonnen werden können. Somit entzieht sich IT-Sicherheit der genauen Messbarkeit. Dies bildet weitere Ansatzpunkte, um die Forschung in diesem Bereich fortzuführen.

9 Maßnahmenempfehlung

Im Folgenden werden stichpunktartig Maßnahmenempfehlungen vorgeschlagen, um das IT-Sicherheitsbewusstsein in den Arbeitsprozess bei Vorgesetzen und deren Mitarbeitern einfließen zu lassen und somit zu einer positiven IT-Sicherheitskultur beizutragen:

9.1 IT-Sicherheitspolicy bzw. IT-Sicherheitsleitlinie

Die Erstellung und Veröffentlichung einer IT-Sicherheitspolicy bzw. IT-Sicherheitsleitlinie mit Verpflichtung zur Initiative „IT-Sicherheit“ sollte durch die Unternehmensleitung und in „angemessener“ Form mit folgendem Inhalt erfolgen:

- Verantwortung und aktive Unterstützung durch die Unternehmensleitung für die IT-Sicherheitsleitlinie.
- Einberufung einer Entwicklungsgruppe für die IT-Sicherheitsleitlinie.
- Bestimmung der IT-Sicherheitsziele.
- Inhalt der IT-Sicherheitsleitlinie.
- Bekanntgabe der IT-Sicherheitsleitlinie.
- Erstellung zusätzlicher IT-System-Sicherheitsleitlinien.

Die IT-Sicherheitspolicy sollte stichpunktartig und auf das Wesentliche für die Mitarbeiter abgefasst sein. Sie sollte in der jeweiligen Landessprache des Unternehmens geschrieben sein und allen Mitarbeitern zugeschickt werden.

9.2 Bestimmung von Funktionsträgern

- **IT-Sicherheitsbeauftragten**, der eine eigene Fachkompetenz für IT-Sicherheit aufbaut und für alle IT-Sicherheitsfragen in der Organisation zuständig ist, sowie
- **IT-Sicherheitsmanagement-Teams**, welches in größeren Organisationen sämtliche übergreifenden Belange der IT-Sicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet.
- Einbezug der Vorgesetzten in sicherheitsbezogene Aktivitäten.

Der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement-Team, sollte sich bei den Mitarbeitern vorstellen (E-Mail) und die Mitarbeiter regelmäßig über ihre Tätigkeit berichten.

9.3 Erstellung eines eigenen Schulungskonzepts zur IT-Sicherheit für alle IT-Nutzer mit mindestens folgenden Punkten

- Risiken und Bedrohungen bei der IT-Nutzung.
- Grundbegriffe und Grundwerte der IT-Sicherheit.
- Die organisationsweite IT-Sicherheitsleitlinie - Was bedeutet sie in meinem Arbeitsalltag?
- Verantwortlichkeiten und Meldewege in unserer Organisation (mit persönlicher Vorstellung der IT-Sicherheitsbeauftragten).
- Wie kann ich zur IT-Sicherheit beitragen?
- Wie erkenne ich sicherheitsrelevante Vorfälle und was ist zu tun?
- Wie kann ich mich selbst in Fragen der IT-Sicherheit fortbilden und informieren?
- Gezielte Sensibilisierung der Vorgesetzten zum Thema „IT-Sicherheit“.
- Nutzung unterschiedlicher Schulungstechniken (Veranschaulichung).

Bei der Durchführung der Schulungsmaßnahmen sollte auf eine kurze, aber präzise Darstellung der Themen geachtet werden. Die Maßnahmen sollten praxisnah und veranschaulichend sein. Dabei ist es hilfreich, auch einen privaten Nutzen der vermittelten Informationen für die Teilnehmer herauszustellen.

9.4 Zielgerichtete Schulungen für Vorgesetzte und Mitarbeiter mit folgendem Inhalt

- Tipps und Tricks für die Erstellung eines „einfachen“ aber sicheren Passwortes.
- Aufzeigen von Hackermöglichkeiten wie schnell ein Passwort „geknackt“ werden kann.
- Einführung in das Thema „Computerviren“ und ihre Wirkungsweise.
- Sinn und Zweck von Computervirensuchprogrammen.
- Gefahren bei der Nutzung des Internets und deren Abwehr.
- Gefahren bei der Nutzung von E-Mails und deren Abwehr.
- Neuste Entwicklungen.

9.5 Weitere wirksame Möglichkeiten zur Sensibilisierung

- Mitarbeiter-Workshops zum Thema "Wie trägt die IT-Sicherheit zu unserer Arbeitsaufgabe bei?",
- Sprechstunden des IT-Sicherheitsbeauftragten,
- Einrichtung eines "Sicherheitsforums" im Intranet,
- Veröffentlichung von "IT-Sicherheitsreports" im Intranet,
- Sichtbare Förderung des IT-Sicherheits-Gedankens durch die Leitungsebene,
- Aushang von (Presse-) Informationen über IT-Sicherheitsvorfälle und
- Lösungsansätze am Schwarzen Brett o. Ä.,
- Auslegen von Fachzeitschriften zur IT-Sicherheit und
- Gespräche am Arbeitsplatz und in Arbeitspausen zu Themen der IT-Sicherheit.
- Aufbau eines eigenen Portals zum Thema „IT-Sicherheit“ für Mitarbeiter im Intranet mit laufend aktualisierten Informationen über Gefahren, Bedrohungen und Aktivitäten im Bereich Internet.

9.6 Treffen von Zielvereinbarungen zwischen dem Vorgesetzten und den Mitarbeitern

- Was ist das beabsichtigte Ziel? Ist es präzise beschrieben? Was ist als Ergebnis, Endprodukt bzw. erwünschte Verhaltensweise definiert worden? (Wege zu diesen Ergebnissen sind keine Ziele!)
- Wie ist das angestrebte Ziel (Ergebnis, Endprodukt, erwünschte Verhaltensweise) zu kontrollieren?
- Wie kann man hinreichend genau feststellen, ob das Ziel erreicht wurde?
- Wie ist es messbar bzw. beobachtbar?
- Lässt sich das Ziel mit den Zielen...
  - des Mitarbeiters
  - seiner Stellenbeschreibung,
  - seiner Abteilung und
  - seines Unternehmens vereinbaren? (Ggf. Zielhierarchie entwickeln: Was hat im Zweifelsfall Vorrang?)
- Wird das Arbeitsgebiet durch Ziele vollständig abgedeckt oder gibt es Lücken?

- Ist das Ziel wirklich wichtig? Was passiert, wenn es nicht erreicht wird?
- Ist das Ziel eine Herausforderung?
- Ist das Ziel positiv formuliert? („Ich soll ...“, nicht „Ich darf nicht ...“)
- Wer muss mitwirken, um das Ziel erreichen zu können?

Die Zielformulierungen sollten vom direkten Vorgesetzten ausgehen. So sieht sich der Vorgesetzte in der unmittelbaren Verantwortung zur Umsetzung der IT-Sicherheits-maßnahmen und er erhält dadurch eine Vorbildfunktion.

9.7 Maßnahmen zur Förderung der Motivation

- Lob und Anerkennung bei sicherer Arbeitsausführung.
- Aktive Gefahrenerkennung durch Plakate oder Anzeigen.
- Vorbildfunktion des Vorgesetzten klar herausstellen.
- Vorschlagswesen zum Thema „IT-Sicherheit am Arbeitsplatz“
- Übermittlung von Maßnahme und Standards im Bereich „IT-Sicherheit“ direkt über den Vorgesetzten (via E-Mail). Dies wirkt näher und der Vorgesetzte erhält Vorbildfunktion.

9.8 Maßnahmen zur Förderung der Partizipation

- Einbezug der Mitarbeiter bei:
- der Entscheidung, ob eine neue Technik eingeführt wird,
- der Entscheidung, welche neue Technik eingeführt wird,
- der Entscheidungen, wenn die neue Technik gekauft wird, welches Training man dabei besucht, ob sich jemand zum lokalen Experten ausbilden lässt etc.
- der Erstellung von Alternativen zur Ist-Situation,
- der Ermittlung von Qualifikationsdefiziten,
- der Auswahl geeigneter Schulungsmaßnahmen.

9.9 Maßnahmen zur Förderung der IT-Sicherheitskultur

- Aufklärung und Information über den Einsatz von Budget, Arten der Technik, Projekte zur Erhaltung der Datensicherheit.
- Einführung in das Datensicherungssystem
- Führung durch das Rechenzentrum.

9.10 Maßnahmen zur Förderung des IT-Sicherheitsbewusstseins

- Veranschaulichung genereller Hackermethoden und Möglichkeiten eines Systemangriffs.
- Darstellung über Methoden und Aktivitäten im Unternehmen über die Gefahrenabwehr.
- Darstellung und Übung der Abwehrmöglichkeit am Arbeitsplatz.
- Thematisierung von Sicherheitspunkten („Monatsmotto“).
- Schnelle Information über Sicherheitsrelevante Themen im Unternehmen durch den Vorgesetzten um der „Gerüchteküche“ vorzubeugen.
- Macht der gewohnten Verhaltensweisen vorbeugen bzw. entgegenwirken.

9.11 Weitere Maßnahmen

- Monatliche Sicherheitsthemen
- Erstellung einer Checkliste mit relevanten arbeitsplatzbezogenen IT-Sicherheitszielen und Umsetzungsmöglichkeiten am Arbeitsplatz
- 3-4 Qualitätskontrollen pro Jahr zur Überprüfung der Effektivität und Effizienz der durchgeführten Maßnahmen
- Tiefergreifende Arbeitsplatzanalysen bzw. –befragungen hinsichtlich hardware- und softwareergonomischer Kriterien nach Bildschirmarbeitsverordnung bzw. ISO 9241

10 Literatur

Ajzen, I. & Fishbein, M. (1980). Understandig Attitudes and Predictiong Social Behavior. Engelwood Cliffs, NJ: Prentice-Hall

Ajzen, I. & Madden; T. J. (1986). Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. Journal of Experimental Social Psychology, 22, pp. 453-474.

Ajzen, I. (1991). The theory of planned behavior. Organizationsal Behavior and Human Decision Processe, 50, S. 179-211.

Alioth, A. (1980). Entwicklung und Einführung alternativer Arbeitsformen. In: E., Ulich (1980). Schriften zur Arbeitspsychologie. Band 27. Bern: Huber.

Antonovsky, A. (1980). Health, stress and coping. San Francisco, Calif.: Jossey-Bass.

Atkinson, J. W. (1975). Einführung in die Motivationsforschung. Stuttgart: Klett.

Bachmann, W., Heinroth, H. & Renner, K. (1978). Psychohygienische Probleme der Berufsarbeit. Zeitschrift für die gesamte Hygiene, 24, S. 588-594.

Backhaus, K., Erichson, B., Plinke, W. & Weiber, R. (1994). Multivariate Analysemethoden. (7. Aufl.). Berlin: Spinger.

Badura, B. (1981b). Sozialpolitik und Selbsthilfe aus tradtioneller und sozialepidemiologischer Sicht. In: Badura, B.; Ferber, C. V. (Hrsg.): Selbsthilfe und Selbstorganisation. Die Bedeutung nichtprofessioneller Sozialsysteme für Krankheitsbewältigung: München.

Bagozzi, R. P. & Warshaw, P. R. (1992). An examination of the etiology of the attitude-behavior relation for goal-directed behaviors. Multivariate Behavioral Research, 27, S. 601-634.

Bagozzi, R. P. & Yi, Y. (1989). The degree of intention formation as a moderator of the attitude-behavior relationship. Social Psychology Quarterly, 52, S. 266-279.

Baitsch, C., Katz, C., Spinas, P. & Ulich, E. (1989). Computerunterstützte Büroarbeit. Ein Leitfaden für Organisation und Gestaltung. Zürich: Verlag der Fachvereine.

Baitsch, C., Knoepfel, P. & Eberle, A. (1996). Prinzipien und Instrumente organisationalen Lernens. Organisationsentwicklung 15 (3), S. 4-21.

Bamberg, S. & Lüdemann, C. (1996). Eine Überprüfung der Theorie des geplanten Verhaltens in zwei Wahlsituationen mit dichotomen Handlungsalternativen: Rad vs. PKW und Container vs. Hausmüll. Zeitschrift für Sozialpsychologie, S. 32-46.

Bamberg, S. & Schmidt, P. (1999). Die Theorie geplanten Verhaltens von Ajzen. Ansätze zur Reduktion des motorisierten Individualverkehrs in einer Kleinstadt. Zeitschrift für Umweltpsychologie, 3 (2), S. 24-31.

Bamberg, S. (1996). Allgemeine oder spezifische Einstellungen. Zeitschrift für Sozialpsychologie. S. 47-60.

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review, 1977, Vol. 84, No. 2, pp. 191-215.

Beck, L. & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. Journal of Research in Personality, 25, S. 285-301.

Bell, D. E. (1982). Regret in decision making under uncertainty. Operations Researach, 30, S.961/981.

BGBI, (1990). Bürgerliches Gesetzbuch. Bundesanzeiger. Verlagsges. mbH.

Bortz, J. (1993). Statistik für Sozialwissenschaftler. (4. Aufl.). Heidelberg: Springer.

Brodbeck, F. C. (1991). Fehlerbewältigungsdauer und die Nutzung von Unterstützungsmöglichkeiten. In: M. Frese & D. Zapf (Hrsg.). Fehler bei der Arbeit mit dem Computer. Bern; Göttingen; Toronto: Huber. S. 80-95

Brosius, G. (1989). SPSS/PC+ Advanced Statistics und Tables. Hamburg. McGraw-Hill.

BSI (2000). IT-Grundschutzhandbuch. Schriftenreihe zur IT-Sicherheit. Band 3.

BSI (2000). Sicherheit in der Informationstechnik. Studien des Bundesamtes für Sicherheit in der Informationstechnik. München: Oldenbourg.

Burmester, M. (1997). Das SANUS-Handbuch: Bildschirmarbeit EU-konform; Information, Analyse, Gestaltung. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Bremerhaven: Wirtschaftsverl. NW, Verl. für Neue Wiss.

Büssing, A. & Glaser, J. (1991). Zusammenhänge zwischen Tätigkeitsspielräumen nd Persönlichkeitsförderung in der Arbeitstätigkeit. Zeitschrift für Arbeits- und Organisationspsychologie, 35 (N.F. 9) 3; S. 122-136.

Cacciabue, P. C. (1998). Modelling and simultation of human behaviour for safety analysis and control of complex systems. Safety science, 28, 2, S. 97-110.

Cakir, A. (1981). Belastung und Beanspruchung bei Bildschirmtätigkeiten. In: M. Frese (Hrsg.). Streß im Büro. Schriftenreihe zur Arbeitspsychologie. 34. Bern: Huber. S. 46-71

Caplan, G. (1976). The family as a support system. In: G. Caplan & M. Killilea (Hrsg.).

Charng, H.-W., Piliavin, J. A. & Callero, P. L. (1988). Role identity and reasoned action in the prediction of repeated behavior. Social Psychology Quarterly, 51, S. 303-317.

Cobb, S. (1976). Social support as a moderator of life stress. Psychosomatic Medicine, 38, 5, S. 300-314.

Cole, T. & Matzer, M. (1999). Managementaufgabe Sicherheit. Schützen Sie Ihr Unternehmen gegen die Risiken im Online-Zeitalter. Wien: Hanser.

Comelli, G. & von Rosenstiel, L. (2001). Führung durch Motivation. Mitarbeiter für Organisationswziele gewinnen. München: Vahlen.

Dedobbeleer, N. & Béland, F. (1991). A safety climate measure for construction sites. Journal of Safety Research, 22, S. 97-103.

DeVries, H., Dijkstra, M. & Kuhlman, P. (1988). Self-efficiacy: The third factor besides attitude and subjective norm as a predictor of behavioural intentions. Health-Education-Research, Vol. 3 (3), S. 273-282.

Diewald, M. (1991). Soziale Beziehungen: Verlust oder Liberalisierung? Soziale Unterstützung in informellen Netzwerken.

Dunkel-Schetter, C. & Bennett, T. L. (1990). Differentiating the cognitive and behavioral aspects of social support. In: B. R. Sarason, I. G. Sarason & G. R. Pierce, (Hrsg.). Social Support: An interactional view. New York: Wiley & Sons, S. 267-296.

Eisfeller, G.; Lorenz, D. & Schubert, P. (1999). Integration der Bildschirmarbeitsverordnung in die betriebliche Praxis. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin: Dortmund.

Emery, F. E. & Emery, M. (1974). Participative Design. Canberra: Centre for Continuing Education, Australian National University.

Emery, F. E. & Thorstrud, E. (1982). Industrielle Demokratie. Schriften zur Arbeitspsychologie (Hrsg. E. Ulich), Band 25. bern: Huber.

Emery, F. E. & Trist, E. L. (1960). Socio-technical Systems. In F. E. Emery (Ed.). System Thinking. Harmondsworth. Pengain Books.

Emery, F. E. (1959). Characteristics of Socio-Technical Systems. In: L. E. Davis & J. C. Taylor, (1972). Design of Jobs. Australia: Penguin Books. S. 177-198.

Ertel, M.; Junghanns, G.; Pech, E. & Ullsperger, P. (1997). Auswirkungen der Bildschirmarbeit auf Gesundheit und Wohlbefinden. Ergebnisse betrieblicher Untersuchungen mit dem Fragebogen „Gesundheit am Bildschirmarbeitsplatz“. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin: Dortmund.

Faber, U. (1998). Management des neuen Arbeits- und Gesundheitsschutzes nach dem neuen Arbeitsschutzgesetz. In: Burhardt, F. & Winklmeier, C. (Hrsg.). (1998). Psychologie der Arbeitssicherheit. 9. Workshop 1997. Heidelberg: Roland Asanger Verlag.

Fazio, R. H. (1986). How do attitudes guide behavior? In: R. M. Sorrentino & E. T. Higgins (Eds.). The handbook of motivation and cognition: Foundations for social behavior (S. 204-243). New York: Guiolford Press.

Fazio, R. H. (1990). Multiple processes by which attitudes guide behavior: The MODE-model as an integrative framework. In: M. P., Zanna (Hrsg.). Advances in experimental social psychology. Vol. 23. San Diege, CA: Academic Press. S. 75-109.

Fischer, M. T. (1982). Arbeitsplatzgestaltung im Büro: Handbuch für die Büropraxis. Ludwigshafen (Rhein): Kiel.

Fishbein, M. & Ajzen, I. (1975). Belief, attitude, and behavior: An introduction to theory and research. Reading, Mass.: Addison-Wesley.

Frei, F. (1993). Partizipation und Selbstregulation bei CIM: das Baugruppenprojekt bei Alcatel STR. In: G. Cyranek & E. Ulich (Hrsg.), CIM – Herausforderung an Mensch, Technik, Organisation. Schriftenreihe Mensch – Technik – Organisation (Hrsg. E. Ulich), Band 1. Zürich: Verlag der Fachv ereine, Stuttgart: Teubner. S. 321-338:

Frei, F., Duell, W. & Baitsch, C. (1984). Arbeit und Kompetenzentwicklung. Theoretische Konzepte zur Psychologie arbeitsimmanenter Qualifizierung. In: E., Ulich (Hrsg.). Schriften zur Arbeitspsychologie. Band 39. Bern: Huber.

French, J. R. P., Rodgers, W. & Cobb, S. (1981). A model of person-environment fit. In L. Levi (Hrsg.). Society, stress and disease (Vol. 4: Working Life). Oxford: University Press. S. 39-44.

Frese, M. & Brodbeck, F. C., (1989). Computer im Büro und Verwaltung. Berlin: Springer-Verlag.

Frese, M. & Zapf, D. (1991). Fehlersystematik und Fehlerentstehung: Eine theoretische Einführung. In: M., Frese & D., Zapf (Hrsg.). Fehler bei der Arbeit mit dem Computer: Ergebnisse von Beobachtungen und Befragungen im Bürobereich. Bern; Göttingen, Toronto: Huber. S. 14-32.

Frese, M. (1989). Theoretical models of control and helath. In: S. C. Sauter, J. J. Hussel, & C. C. Cooper (Hrsg.). Job Control and Worker Helath. London: Wiley. S. 107-128.

Frey, D.; Stahlberg, D. & Gollwitzer, P. M. (1993). Einstellung und Verhalten: Die Theorie des überlegten Handelns und die Theorie des geplanten Verhaltens. In: D. Frey & M. Irle (Hrsg.). Theorien der Sozialpsychologie: Band I. Kognitive Theorien. S. 361-398. Bern: Huber.

Frieling, E. & Sonntag, K. (1987). Lehrbuch Arbeitspsychologie. Bern: Huber.

Gabler, E. (1997). Wirtschaftslexikon. Wiesbaden.

Gebert, D. (1978). Organisation und Umwelt: Probleme der Gestaltung innovationsfähiger Organisationen Stuttgart: Kohlhammer.

Geiger, G. (2000). (Hrsg.). Sicherheit der Informationsgesellschaft. Gefährdung und Schutz informationsabhängiger Infrastrukturen. Baden-Baden: Nomos Verlagsgesellschaft.

Gerbing, D. W. & Anderson, J. C. (1993). Monte Carlo evaluations of goodness of fit indices for structural equation models. In: K. Bollen & J. S. Long (Hrsg.). Testing Structural Equation Models. Newbury Park, CA: Sage. (S. 40-65).

Gollwitzer, P. M. (1993). Goal achievement: The role of intentions. In: W. Stroebe & M. Hewstone (Eds.). European Review of Social Psychology. Vol. 4. Chichester: Wiley. S. 141-185.

Greif, S. (1994). Die Arbeits- und Organisationspsychologie: Gegenstand und Aufgabenfelder, Lehre und Forschung, Fort- und Weiterbildung. Göttingen: Hogrefe.

Greif, S. Bamberg, E. & Semmer, N. (1991). Psychischer Stress am Arbeitsplatz. Göttingen. Hogrefe.

Grote, G. & Künzler, C. (1994). Safety culture and is reflections in job and organizational design: total safety management. In. G. Apostolakis (Hrsg.). (1994). Proceeding of the Conference PSAM II. San Diego, New York: Plenum Press.

Grote, G. (1997). Autonomie und Kontrolle. Zur Gestaltung automatisierter und risikoreicher Systeme. Schriftenreihe Mensch, Technik, Organisation (Hrsg. E. Ulich). Band 16, Zürich: vdf Hochschulverlag.

Grote, G., Weik, S.; Wäfler, T., Zölch, M. & Ryser, C. (1999). KOMPASS (Komplementäre Analyse und Gestaltung von Produktionsaufgaben in soziotechnischen Systemen). In H. Dunckel (Hrsg.), Handbuch der psychologischen Arbeitsanalyseverfahren. Schriftenreihe Mensch, Teachnik, Organisation (Hrsg. E. Ulich). Band 14, S. 255-284. Zürich. Vdf Hochschulverlag.

Gusy, B. (1994). Stressoren in der Arbeit, Soziale Unterstützung und Burnout. Eine Kausalanalyse. München, Wie: Profil Verlag.

Häcker, H., Leutner D. & Amelang, M. (1998). Standards für pädagogisches und psychologisches Testen. Supplementum 1/1998 der Diagnostica und der Zeitschrift für Differnetielle und Diagnostische Psychologie.

Hacker, W. & Richter, P. (1990). Psychische Regulation von Arbeitstätigkeiten – Ein Konzept in Entwicklung. In: F. Frei & I. Udris (Hrsg.). Das Bild der Arbeit. Bern: Huber. S. 125-142.

Hacker, W. & Richter, P. (1998). Belastung und Beanspruchung. Streß, Ermüdung und Burnout im Arbeitsleben. Heidelberg: Asanger.

Hacker, W. (1973). Allgemeine Arbeits- und Ingenieurspsychologie. Berlin: VEB Deutscher Verlag der Wissenschaft.

Hacker, W. (1980). Optimierung von kognitiven Arbeitsanforderungen. In: U. Kleinbeck & J. Rutenfranz (1987.). Arbeitspsychologie. Enzyklopädie der Psychologie, Themenbereich D, Serie III, Band 1.

Hacker, W. (1986). Arbeitspsychologie. In: E., Ulich (Hrsg.). Schriften zur Arbeitspsychologie, Band 41. Bern: Huber.

Hacker, W. (1991). Aspekte einer gesundheitsstabilisierenden und –fördernden Arbeitsgestaltung. Zeitschrift für Arbeits- und Organisationspsychologie, 35, S. 48-58.

Hacker, W. (1995). Arbeitstätigkeitsanalyse. Analyse und Bewertung psychischer Arbeitsanforderungen. Heidelberg: Asanger.

Hacker, W. (1998). Allgemeine Arbeitspsychologie. Psychische Regulation von Arbeitstätigkeiten. Bern: Huber.

Hackman, J. R. & Lawler, E. E. (1971). Employee reactions to job characteristics. Journal of Applied Psychology 55, S. 259-286.

Hackman, J. R. & Oldham, G. R. (1974). The job diagnosis survey: An instrument for the diagnosis of jobs and the evaluation of job redesign projects. Technical Report, 4. Yale University.

Hackman, J. R. & Oldham, G. R. (1980). Work redesign. Reading, M. A.: Kohlhammer.

Haller, M. (1997). Vom Wechselspiel der Sicherheiten. Ganzheitliches Risikomanagement anstatt isolierter Sicherheitsbereiche. In NZZ, 25.11.65.

Heckhausen, H. (1989). Motivation und Handeln (2. Aufl.). Berlin: Springer.

Hentze, J., Kammel, A. & Lindert, K. (1997). Personalführungslehre. (3., vollst. überarb. Aufl.). Bern: Haupt.

Herzberg, F., Mausner, B. & Snyderman, B. (1959). The motivation to work. New York, London: Wiley & Sons.

Hoffmann, B. (1991). Arbeitsschutz und Unfallstatistik. Bonn: Hauptverband der gewerblichen Berufsgenossenschaft.

Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method. CREAM. Oxfprd: Elseviel.

Hoyos, Graf C. & Ruppert, F. (1993). Der Fragebogen zur Sicherheitsdiagnose FSD. In: E. Ulich (Hrsg.). Schriften zur Arbeitspsychologie, Band 53. Bern: Huber.

Hoyos, Graf C. & Wenninger, G. (1995). Arbeitssicherheit und Gesundheitsschutz in Organisationen. (Beiträge zur Organisationspsycholgoe Bd. 11). Göttingen: Hogrefe.

Jaccard, J. & Wan, C. K. (1996). LISREL approaches to interaction effects in multiple regression. In: Sage University Papers, University at Albany, State University of New York. Thousand Oaks: Sage Publications.

Jonas, K. & Doll, J. (1996). Kritische Bewertung der Theorie überlegten Handelns und der Theorie geplanten Verhaltens. Zeitschrift für Sozialpsychologie, S. 18-31.

Jöreskog, K. G. & Sörbom, D. (1992). LISREL VIII: Analysis of linear structural relations. Mooresville, In: Scientific Software.

Kahnemann, R. A. & Tversky, T. (1979). Prospect theory. An analysis of decision under risk. Econometrica, 47, S. 263-291.

Karasek, R. A. & Theorell, T. (1990). Healthy work: Stress, productivity, and the reconstruction of working life. New York: Basic Books.

Karasek, R. A. (1979). Job demands, job descision latitude, and mental strain: Implications for job redesign. Administrative Science Quarterly, 24, S. 285-307.

Kastner, M. & Kreissel, S. (1999). Verhalten in Organisationen. In: Graf C. Hoyos,. & D. Frey (Hrsg.). Arbeits- und Organisationsppsychologie. Beltz: PsychologieVerlagsUnion.

Kaufmann, F. X. (1970). Sicherheit als soziologisches und sozialpolitisches Problem. Stuttgart: Emke.

Kelloway, E. K. (1998). Using LISREL for Structural Equation Modeling. A Researcher´s Guide. Thousand Oaks: Sage Publications.

Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. London: Taylor & Francis.

Klinbeck, U. (1996). Arbeitsmotivation: Entstehung, Wirkung und Förderung. Weinheim, München: Juventa Verlag.

König, D. H. (1995). Aspekte kombinierter Belastungen bei Tätigkeiten an Arbeitsplätzen mit modernen Kommunikationstechnologien. Schriftenreihe der Bundesanstalt für Arbeitsschutz . Forschung ; 724. Bremerhaven : Wirtschaftsverlag. NW, Verl. Für Neue Wiss.

Konrad, P. (1998). Geschäftsprozeß-orientierte Simulation der Informationssicherheit. Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmangements. Reihe: Wirtschaftsinformatik. Band 20. Lohmar, Köln: Eul Verlag.

Kossakowski & Schindler, 2002 ; Zeitschrift KES 2002/3, S. 6-23

Kuhl, J. (1985). Volitional mediators of cognition-behavior consistency: Self-regulatory processes and actions versus state orientation. In: J. Kuhl & J. Beckmann (Eds.). Action control: From cognition to behavior. Berlin: Springer. S. 101-128.

Kühlmann, T. M. (1993). Streßbewältigung bei computerunterstützter Arbeit. Ein prozeßorientierte Ansatz. Zeitschrift für Arbeitswissenschaft 47; S. 233-238.

Kuhmann, W. (1994). Leistungsgüte und Beanspruchung bei mentalen Tätigkeiten. Bern: Huber.

Künzler, C. (2002). Kompetenzförderliche Sicherheitskultur. Ganzheitlicher Gestaltung risikoreicher Arbeitssysteme. Vdf Hochschulverlag AG an der ETH Zürich.

Laireiter, A. (1993). Soziales Netzwerk und soziale Unterstützung. Konzepte, Methoden und Befunde. Bern: Huber.

Lankenau, K. (1984). Handlungsspielraum, Beurteilung der Arbeitstätigkeit und Qualifizierungsbereitschaft. Psychologie und Praxis, 28, S. 109-118.

Latham, G. P., Erez, M. & Locke, E. A. (1988). Resolving scientific disputes by the joint design of crucial experiments by the antagonists: Application of the Erez-Latham dispute regarding participation in goal-setting. Journal of Applied Psychology, 73, S. 753-772.

Latham, G.P. & Lee, T.W. (1986). Goal setting. In E. A. Locke (Ed.), Generalizing from laboratory to field settings. Lexington, MA: Lexington Books. S. 101-117.

Lazarus, R. S. & Launier, R. (1981). Streßbezogene Transaktionen zwischen Person und Umwelt. In J. R. Nitsch (Hrsg.). Streß, Theorien, Untersuchungen, Maßnahmen. Bern: Huber. S. 213-259.

Leitner, K. (1999). Kriterien und Befunde zu gesundheitsgerechter Arbeits – Was schädigt, was fördert die Gesundheit? In R. Oessterreich & W. Volpert (Hrsg.). Psychologie gesundheitsgerechter Arbeitsbedingungen.(S. 63-139). Schriften zur Arbeitspsychologie (Hrsg. E. Ulich), Band 59. Bern: Huber.

Leitner, K., Volpert, W., Greier, B., Weber, W.-G. & Hennes, K. (1987). Analyse psychischer Belastung in der Arbeit. Das RHIA-Verfahren. Handbuch. Köln: TÜV Rheinland.

Leontjew, A. (1977). Tätigkeit, Bewußtsein, Persönlichkeit. Beiträge zur Psychologie. Berlin: für die deutsche Ausgabe Volk und Wissen Volkseigener Verlag.

Leontjew, A. (1982). Psychologie des sprachlichen Verkehrs. Weinheim: Beltz.

Lewin, K. (1948). Resolving Social Conflicts. New York. Harper & Row.

Lienert, G. A. & Raatz, U. (1994). Testaufbau und Testanalyse. (5. Aufl.) Weinheim: Psychologie Verlags Union.

Liska, A. E. (1984). A critical examination of the causal structure of the Fishbein/Ajzen attitude-behavior model. Social Psychology Quarterly, 47, S. 61-74.

Locke & Latham (1968). In: Locke, E. A. & Latham, G. P. (1990a). A Theory of Goal Setting & Task Performance. New Jersey: Prentice Hall.

Locke (1968). In: Locke, E. A. & Latham, G. P. (1990a). A Theory of Goal Setting & Task Performance. New Jersey: Prentice Hall.

Locke, E. A. & Latham, G. P. (1984). Goal setting. A motivational technique that works. Prentice-Hall, Inc.: Engelwood Cliffs, NJ.

Locke, E. A. & Latham, G. P. (1990a). A Theory of Goal Setting & Task Performance. New Jersey: Prentice Hall.

Locke, E. A. (1976). The nature and causes of job satisfaction. In M. D. Dannette (Ed.), Handbook of Industrial and Organizational Psychology (S. 1297-1349). Chicago: Rand McNally.

Locke, E. A., Shaw, K. N., Saari, L. M. & Latham, G. P. (1981). Goal Setting and Task Performance: 1969-1980. Psychological Bulletin, 69, S. 125-152.

Locke, E.A. & Latham, G.P. (1990b). The high performance cycle. In U. Kleinbeck, H.-H. Quast, H. Thierry & H. Häcker: Work motivation. Hillsdale, NJ: Lawrence Erlbaum Ass.

Loerzer, S. (1991). Wohlfühlen am Arbeitsplatz. In: C., Lippmann (Hrsg.). Wohlfühlen am Computer, wertvolle Tipps, praktische Übungen. München: Gräfe und Unzer.

Loh, M. (1995). Reengineering at work. Aldershot-Hampshire.

Luczak, H. & Volpert, W. (1987). Psychophysiologische Methoden zur Erfassung psychophysischer Beanspruchungszustände. In: U. Kleinbeck & J. Rutenfranz (Hrsg.). Arbeitspsychologie. Enzyklopädie der Psychologie, Themenbereich D, Serie III, Band 1. Göttingen: Hogrefe. S. 185-259.

Macharzina, K. (1995). Unternehmungsführung. Das internationale Managementwissen. Wiesbaden. S. 207

Maintz, G. (1995). Sehen und Bildschirmarbeit. In: Schriftenreihe der Bundesanstalt für Arbeitsmedizin: Tagungsbericht; 6. Sehen und Bildschirmarbeit. Bremerhaven: Wirtschaftsverlag NW. S. 5-10.

Manstead, A. S. R. & Parker, D. (1995). Evaluationg and extending the theory of planned behaviour. In W. Stroebe & M. Hewstone (Eds.). European Review of Social Psychology (Vol. 6). Chickester, UK: Wiley. S. 69-95.

Marx, K. (1962). Das Kapital – Kritik der politischen Ökonomie (Erster Band, Marx Engels Werke 23). Berlin: Dietz.

Maslow, A. H. (1954). Motivation and Personality. New York: Harper.
McGrath, J. E. (1970). A conceptual formulation for research on stress. In J. E. McGrath (Hrsg.). Social and psychological factors in stress. New York: Holt, Rinehart and Winston. S. 10-21.
Meier, H. (1998). Unternehmensführung. Aufgaben und Techniken des betrieblichen Managements. Berlin: Verlag Neue Wirtschafts-Briefe.
Mento, A.J., Steel, R.P. & Karren, R.J. (1987). A meta-analytic study of the effects of goal setting on task performance: Organizational Behavior and Human Decision Processes, 39, S. 52-83.
Miller, G. A., Galanter, E. & Pribram, K. H. (1973). Strategien der Handlung. Stuttgart: Klett.
Mittenecker, E. & Raab, E. (1973). Informationstheorie für Psychologie. Göttingen: Hogrefe.
Mulder, M. (1977). The daily power game. Leiden: Nijhoff.
Nachreiner, F. & Wuchterpfennig, B (1975). Arbeits- und sozial-psychologische Aspekte der Arbeit unter Zeitdruck. Betriebsärztliches, 2, S. 22-36.
Nestmann, F. (1988). Die alltäglichen Helfer. Theorien sozialer Unterstützung und eine Untersuchung alltäglicher Helfer aus vier Dienstleistungsberufen: Berlin.
OECD (2001). conomic surveys / Luxembourg.
Östberg, O. & Högberg, Y. K. O. (1990). Perspectives on Ergonomics Issues in a VDT Office. In: S. L., Sauter, M. J., Dainoff, & M. J., Smith (Eds.). Promoting health and productivity in the computerized office: Models of successful ergonomic interventions. London: Taylor and Francis. S. 131-146.
Patkin, M. (1990). Neck and Arm Pain in Office Workers: Causes and Management. In: S. L., Sauter, M. J., Daianoff & M. J., Smith (Eds.). Promoting health and productivity in the computerized office: Models of soccussful ergonomic interventions. London: Taylor and Francis. S. 207-231.
Pfaff, H. (1989). Streßbewältigung und soziale Unterstützung. Zur sozialen Regulierung individuellen Wohlbefindens. Deutscher Studien Verlag: Weinheim.
Pohl, H. & Weck, G. (1995). Sicherheit in der Informationstechnik. Managementaufgaben im Bereich der Informationssicherheit. München: Oldenbourg Verlag.
Poy, A. & Weisbach, H.-J. (1994). Vom Sicherheitssystem zur Sicherheitskultur? In N. Beckenbach & W. van Treeck. (Hrsg.) Umbrüche gesellschaftlicher Arbeit, Soziale Welt, Sonderband 9. (S. 393-407). Göttingen: Otto Schwarz & Co.
Rasmussen (1985). New technology and human error. Chichester: Wiley.
Reason, J. (1993). Managing the management risk: New approaches to organisational safety. In B. Wilpert & T. Qvale (Eds.), Reliability and safety in hazardous work systems, S. 7-22, Hove: Lavraence Erlbaum.
Reason, J. (1994). Menschliches Versagen : psychologische Risikofaktoren und moderne Technologien. Heidelberg: Spektrum, Akad. Verlag.
Regnet, E. (1995). Der Weg in die Zukunft – Neue Anforderungen an die Führungskraft. In: L. V. Rosenstiel, E. Regnet & M. Domsch (Hrsg.). (1995). Führung von Mitarbeitern. Handbuch für erfolgreiches Personalmanagement. (3. Überarb. u. erw. Aufl.). Stuttgart: Schäffer-Poeschel Verlag.
Reinecke, J., Schmidt, P. & Ajzen, I. (1997). Kondom oder kein Kondom bei neuen sexuellen Kontakten? Erklärung und Vorhersage mit der Theorie geplanten Verhaltens im Längsschnitt. Zeitschrift für Sozialpsychologie, 28, S. 210-222.
Rice, A. K. (1958). Productivity and Social Organization. The Ahmedabad Experiment. London: Tavistock.
Richter, G. & Hacker, W. (1998). Belastung und Beanspruchung: Streß, Ermüdung und Burnout. Heidelberg: Asanger.

Richter, G. (1997). Psychische Belastung und Beanspruchung – Streß, psychische Ermüdung, Monotonie, psychische Sättigung. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. – Forschunganwendung – Fa 36.

Richter, G. (2001). Psychologische Bewertung von Arbeitsbedingungen. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin: Dortmund.

Rohmert, W. & Rutenfranz, J. (1975). Arbeitswissenschaftliche Beurteilung der Belastung und Beanspruchung an unterschiedlichen industriellen Arbeitsplätzen. Bonn: Der Bundesminister für Arbeit und Sozialordnung.

Rohmert, W. (1972). Aufgaben und Inhalt der Arbeitswissenschaft. Die berufsbildende Schule, 24, S. 3-14.

Röhrle, B. & Stark, W. (1985). Soziale Stützsysteme und Netzwerke im Kontext klinisch-psychologischer Praxis. In: A, Dies (Hrsg.): Soziale Netzwerke und Stützsysteme. Tübingen, S. 29-41.

Röhrle, B. (1987). Soziale Netzwerke und Unterstützung im Kontext der Psychologie. In: Deupp, H; Röhrle, B. (Hrsg.): Soziale Netzwerke. Frankfurt/New York, S. 54-108.

Röhrle, B. (1994). Soziale Netzwerke und soziale Unterstützung. Weinheim: Beltz.

Rosenstiel, L. & Regnet, E. (1999). Führung von Mitarbeitern. Handbuch für erfolgreiches Personalmanagement: Stuttgart.

Sarason, B. R., Shearin, E. N., Pierce, G. R. & Sarason, I. G. (1987). Interrelations of social support measures: Theoretical and practical implications. Journal of Personality and Social Psychology, 52, S. 813-832.

Savage, L. J. (1954). The foundations of statistics. New York: Wiley and Sons.

Schein, E. H. (1970). Organizational Psychology. Englewood Cliffs, N. J.: Prentice Hall.

Schein, E. H. (1984). Coming to a new awareness of organizational culture. Sloan Management Review, 25, S. 3-16.

Schenk, M. (1984). Soziale Netzwerke und Kommunikation. Tübingen.

Schifter, D. B. & Ajzen, I. (1985). Intention, perceived control, and weight loss: An application of the theory of planned behavior. Journal of Personality and Social Psychology, 49, S. 843-851.

Schmid, H. (1995). Computer und Gesundheit: Gesundheitspsychologische Betrachtungen von Beschwerden bei Computerarbeit. Münster: Waxmann.

Schmidt, K.H. & Kleinbeck, U. (1999). Funktionsgrundlagen der Leistungswirkung von Zielen bei der Arbeit. In: M. Jerusalem & R. Pekrum (Hrsg.). Emotion, Motivation und Leistung. Göttingen: Hogrefe. S. 291-304

Schmidt, K.-H. (1987). Motivation, Handlungskontrolle und Leistung in einer Doppelaufgabensituation. (Reihe 17, Biotechnik). Düsseldorf: VDI-Verlag.

Schuler, H. (1995). Organisationspsychologie. Bern: Huber.

Schulz, P. & Höfert, W. (1981). Wirkmechanismen und Effekte von Zeitdruck bei Angestelltentätigkeiten: Feld und Laborstudien. In M. Frese (Hrsg.). Streß im Büro. Bern: Verlag h. Huber. S. 72-93.

Schwaninger, U.; Thomas, C.; Nibel, H.; Menozzi, M.; Läubli, T. & Krueger, H. (1992). Auswirkungen der Bildschirmarbeit auf Augen sowie Stütz- und Bewegungsapparat. Schriftenreihe der Bundesanstalt für Arbeitsschutz: Forschung, Fb 601. Bremerhaven: Wirtschaftsverlaag NW.

Schwarzer, R. (1996). Psychologie des Gesundheitsverhaltens. (2., überarb. Und erw. Aufl.). Göttingen: Hogrefe.

Seligman, M. E. P. (1975). Helplessness: On depression, development and death. San Francisco, CA: Freeman.

Sellen, A. J. (1990). Four chapters on human error and human error detection. In: M. Frese & D. Zapf (Hrsg.). Fehler bei der Arbeit mit dem Computer. Bern, Göttingen, Toronto: Huber.

Seyle, H. (1953). Einführung in die Lehre von Adaptionssyndrom. Stuttgart: Enke.
Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28; S. 656.
Sheth, J. N. (1974). Models of buyer behavior: conceptual, quantitative and empirical. New York: Harper & Row.
Six, B. & Eckes, T. (1996). Metaanalyse in der Einstellungs-Verhaltens-Forschung. Zeitschrift für Sozialpsychologie, S. 7-17.
Sonntag, K. (1989). Trainingsforschung in der Arbeitspsychologie. Berufsbezogene Lernprozesse bei veränderten Tätigkeitsinhalten. Bern: Verlag H. Huber.
Sparks, P. & Shepherd, R. (1992). Self-identity and the theory of planned behavior: Assessing the role of identification with „green consumerism". Social Psychology Quarterly, 55, S. 388-399.
Stadelmann, M. (1996). Informationstechnologie als Hilfsmittel der Führung in KMU. Ansätze für die informationstechnologisch unterstützte organisatorische Gestaltung der Führungstätigkeit. Bern: Haupt.
Stapp, M., Elke, G. & Zimolong, B. (1999). Fragebogen zum Arbeits- und Gesundheitsschutz. In: Bochumer Berichte zur Angewandten Psychologie, Nr. 15/99.
Stary, Ch. & Riesenecker-Caba, Th. (1999). EU-CON II – Software-ergonomische Bewertung und Gestaltung von Bildschirmarbeit. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin: Dortmund.
Statistisches Bundesamt (2001). Leben und Arbeiten in Deutschland. Ergebnisse des Mikrozensus 2000. Statistisches Bundesamt: Wiesbaden.
Steinhausen, D. & Langer, K. (1977). Clusteranalyse. Einführung in Methoden und Verfahren der automatischen Klassifikation. Berlin: Walter de Gruyter.
Susman, G. I. (1976). Autonomy at Work. A Sociotechnical Analysis of Participative Management. New York: Praeger Publishers.
Toppinen, S. & Kalimo, R. (1996). Information overlaod. A risk factor in the information society. – Tyoterveiset – Newsletter of the Finnish Institute of Occupational Helth (1996), Special Issue: Information Society. S. 21-22.
Trist, E. L. & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coalgetting. Human Relations 4, S. 3-38.
Troy, N., Baitsch, C. & Katz, C. (1986). Arbeitswelt Bürocomputer – Chance für die Organisationsgestaltung? Zürich: Verlag für Fachvereine.
Tubbs, M.E. (1986). Goal setting: A meta-analytic examination of the empirical evidence. Journal of Applied Psychology, 71, S. 474-483.
Udris, I. & Frese, M. (1988). Belastung, Fehlbeanspruchung und ihre Folgen. In: D. Frey, C. Graf Hoyos & D. Stahlberg (Hrsg.), Angewandte Psychologie: Ergebnisse und neue Perspektiven. München: Urban & Schwarzenberg. S. 427-447.
Udris, I. & Frese, M. (1992). Arbeit und Gesundheit. Weinheim: Psychologie Verlags Union.
Udris, I. & Frese, M. (1999). Belastung und Beanspruchung. In. C. Graf Hoyos & D. Frey (Hrsg.). Arbeits- und Organisationspsychologie. Ein Lehrbuch (S. 429-445). Weinheim: Psychologie Verlags Union.
Ulich, E. (1991). Arbeitspsychologie. Zürich: Verl. Der Fachvereine.
Ulich, E. (1992). Arbeitspsychologie. Stuttgart: Poeschel Verlag.
Ulich, E. (1994). Arbeitspsychologie. Stuttgart: Schäffer-Poeschel.
Ulich, E. (2001). Arbeitspsychologie. Stuttgart: Schäffer-Poeschel.
Volpert, W. (1975). Die Lohnarbeitswissenschaft und die Psychologie der Arbeitstätigkeit. In P. Groskurth & W. Volpert, Lohnarbeitspsychologie. Berufliche Sozialisation: Emanzipation zur Anpassung (S. 11-196). Frankfurt am Main: Fischer.

Volpert, W. (1982). Das Modell der hierarchisch-sequentiellen Handlungsorganisation. In W. Hacker, W. Volpert & M. von Cranach (Hrsg.), Kognitive und motivationale Aspekte der Handlung. S. 38-58. Bern: Huber.

Volpert, W. (1987). Psychische Regulation von Arbeitstätigkeiten. In: u. Kleinbeck & J. Rutenfranz (Hrsg.). Arbeitspsychologie. Enzyklopädie der Psychologie, Themenbereich D, Serie III, Band 1. Göttingen: Hogrefe. S. 1-42.

Volpert, W. (1992). Welche Arbeit ist gut für den Menschen? Notizen zum Thema Menschenbild und Arbeitsgestaltung. In: F. Frei & I. Udris (Hrsg.). Das Bild der Arbeit. Bern: Huber. 23-40.

Vroom, V. H. & Jago, A. G. (1991). Flexible Führungsentscheidungen: Management der Partizipation in Organisationen. Stuttgart: Poeschel.

Vroom, V. H. (1964). Work and motivation. New York: Wiley.

Wall, T. D., Jackson, P.R., Mullarkey, S. & Parker, S. K. (1996). The demandscontrol model of job strain: A more specific test. Journal of Occupational Psychology, 69, S. 153-166.

Warr, P. B. (1990). Decision altitude, job demands and employee well-being. Work and Stress, 4, S. 285-294.

Warshaw, P. R. & Davis, F. D. (1985). Disentangling behavioral intention and behavioral expectation. Journal of Experimental Social Psychology, 21, S. 213-228.

Wehner, T. & Mehl, K. (1986). Über das Verhältnis von Handlungsteilen zum Handlungsganzen – Der Fehler als Indikator unterschiedlicher Bindungsstärken in „Automatismen“. Zeitschrift für Psychologie, 194, S. 231-245.

Wehner, T. (1984a). Im Schatten des Handlungsfehlers. Erkenntnisraum motorischen Geschehens. Bremer Beiträge zur Psychologie; 36: Reihe A, Psychologische Forschungsberichte. S. 61

Weinstein, N. D. (1988). The precaution adaption process. In: Health Psychology, 7, S. 355-386.

Weißgerber, B. (1998). Analyse psychischer Belastung. In: H. von Benda & D. Bratge (Hrsg.). Psychologie der Arbeitssicherheit. 9. Workshop 1997. Heidelberg: Asanger. S. 284-309

Wieland, R. & Koller, F. (1999). Bildschirmarbeit auf dem Prüfstand der EU-Richtlinien. Konzepte, Strategien und betriebliche Erfahrungen. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Forschung; 855. Arbeitsschutz Bremerhaven: Wirtschaftsverlag.

Wieland-Eckelmann, R. (1991). Strategien der Belastungsbewältigung im Spannungsfeld von Arbeit, Erholung und Persönlichkeit. In: H. Häcker & R. Wieland-Eckelmann (Hrsg.). Wuppertaler Psychologische Berichte. Band 2, Heft 2.

Wieland-Eckelmann, R. (1992). Kognition, Emotion und psychische Beanspruchung. Göttingen: Hogrefe.

Wieland-Eckelmann, R., Baggen, R., Saßmannshausen, A., Schwarz, R., Schmitz, U., Ademmer, C. & Rose, M. (1996). Gestaltung beanspruchungsoptimaler Bildschirmarbeit. Grundlagen und Verfahren für die Praxis (Schlussbericht). Bundesanstalt für Arbeitsmedizin. Berlin: Wirtschaftsverlag NW.

Wingert, B. (1984). CAD im Maschinenbau. Wirkungen, Chancen, Risiken. Berlin: Springer.

Womack, J. P., Jones, D. T. & Ross, D. (1992). Die zweite Revolution in der Automobilindustrie. Frankfurt/New York.

Wunderer, R. (1997). Führung und Zusammenarbeit. Beiträge zu einer unternehmerischen Führungslehre. (2., vollst. überarb. und erw. Aufl.). Stuttgart: Schöffer-Poeschel.

Zapf, D. (1991). In: M., Frese & D., Zapf (Hrsg.). Fehler bei der Arbeit mit dem Computer: Ergebnisse von Beobachtungen und Befragungen im Bürobereich. Bern; Göttingen, Toronto: Huber.

Zimolong, B. (1990). Fehler und Zuverlässigkeit. In C. Graf Hoyos & B. Zimolong (Hrsg.). Ingenierpssychologie. Enzyklopäie der Psychologie, Themenkreis D, Serie 3, Band 2, S. 313-345. Göttingen: Hogrefe.

Zimolong, B. (1995). Neue Perspektiven im Arbeits-,Gesundheits- und Umweltschutz: Rechtliche, arbeits- und organisationspsychologische Aspekte. In: C. Graf Hoyos & G. Wenninger (Hrsg.). (1995). Arbeitssicherheit und Gesundheitsschutz in Organisationen. Göttingen: Hogrefe.

Zimolong, B. (1998). Ganzheitliches Management des betrieblichen Arbeits- und Gesundheitsschutzes. In: Burkhradt, F. & Winklmeier, C. (Hrsg.). (1998). Psychologie der Arbeitssicherheit.. 9. Workshop 1997. Heidelberg: Roland Asanger Verlag.

Internetrecherche:

http://www.lenz-consult.com

http://www.phi-partner.com

Statistisches Bundesamt Deutschland (2001). http://www.statistik-bund.de/basis/d/evs/budtab2.htm

Zeitschrift: Business 2.0 (4/2001; S. 82)

Statistisches Bundesamt Deutschland (2001). http://www.statistik-bund.de/basis/d/evs/budtab2.htm

I)Abbildungsverzeichnis

II) Tabellenverzeichnis

III) Anhang

Teil 1: Organisation & Führung

Personalführung	
Zielsetzung (3)	zs
Partizipation (5)	p
Motivation (8)	m

Unternehmensführung	
Aufklärung & Information (6)	ai
Datensicherheit (4)	ds

Teil 2: Einstellung und Verhalten

IT-Sicherheitsverhalten	wüg
Wissen über Gefahren (9)	pb
Persönliche Bedeutung (6)	esu
Einschätzung des Stellenwerts IT-Sicherheit für das Unternehmen (4)	nü
Normative Überzeugunge (11)	ew
Einwilligungsbereitschaft (5)	fk
Fähigkeiten (2)	ik
Internale Kontrollüberzeugung (2)	ek
Externale Kontrollüberzeugung (4)	i
Intention (15)	
Soziale Unterstützung am Arbeitsplatz	
- durch die Kollegen (4)	suk
- durch die/den Vorgesetzten (2)	suv

Personalführung

Skala: **Zielsetzung**
4) Unser Vorgesetzter sagt uns klar und deutlich, welche IT-Sicherheitsvorkehrungen einzuhalten sind.
7) Unser Vorgesetzter informiert uns regelmäßig, welche IT-Sicherheitsvorkehrungen zu treffen sind.
9) Wir werden regelmäßig kontrolliert, ob wir die IT-Sicherheitsvorschriften einhalten.

Skala: **Partizipation**
11) Unser Vorgesetzter hält uns an, ihn auf IT-Sicherheitsmängel aufmerksam zu machen.
14) Ich wurde über die Gefahren von Computerviren ausführlich informiert.
18) Unser Vorgesetzter ist daran interessiert, dass wir uns im Bereich IT weiterbilden.
20) Über die IT-Sicherheitsvorschriften bin ich ausführlich belehrt worden.

Skala: **Motivation**
6) Unser Vorgesetzter schätzt es sehr, wenn man die IT-Sicherheitsbestimmungen beachtet.
13) Unser Vorgesetzter ist gut über IT-Sicherheit informiert und qualifiziert.
22) Unser Vorgesetzter sperrt immer seine Arbeitsstation, wenn er den Arbeitsplatz verlässt.
23) Ich bin mit meinen für die Arbeitsaufgabenerfüllung installierten Computerprogrammen sehr zufrieden.
24) Unserem Vorgesetzten ist es egal, ob wir eigene Software auf dem BSAP installiert haben.
25) Unser Vorgesetzter achtet darauf, dass keine Passwörter weitergegeben werden.
26) Für Probleme beim Umgang mit meinem PC habe ich eine zentrale Ansprechperson.
27) Mein Vorgesetzter unterstützt mich bei der Umsetzung der IT-Sicherheitsmassnahmen.

Unternehmensführung

Skala: **Aufklärung & Information**
5) Auf meinem BSAP wure nur die für meine Arbeitstätigkeit notwendige Software installiert.
10) Es gibt für meinen Arbeitsbereich einen IT-Sicherheitsbeauftragten, dessen Name und Telefonnummer mir bekannt ist.
12) Wir Mitarbeiter werden über Änderungen im IT-Sicherheitsbereich ausreichend informiert.
15) Ich wurde über die Gefahren von Computerviren ausführlich informiert.
17) Wir Mitarbeiter werden bei Problemen im IT-Sicherheitsbereich umfangreich informiert.
19) Unser Unternehmen interessiert sich sehr für das Thema IT-Sicherheit.

Skala: **Datensicherheit**
2) Unser Unternehmen hat alles veranlasst, dass auch im schlimmsten Fall die Daten erhalten bleiben (Backupsystem).
3) Ich wurde über den korrekten Umgang mit Passwörtern belehrt.
16) Sensible Daten werden in unserem Unternehmen immer mit Passwörter versehen.
21) Vertraulichen Daten werden nur verschlüsselt versendet.

IT-Sicherheitsverhalten

Skala: **Wissen über Gerfahren**
9) Die Gefahr, dass Daten versehentlich gelöscht oder unbrauchbar werden ist ausgeschlossen.
16) Die Gefahr, dass ich Dateien beschädige ist ausgeschlossen.
23) Die Gefahr meinen Computer mit einem Virus zu infizieren ist ausgeschlossen.
31) Die Gefahr, dass vertrauliche Daten abgefangen und verändert werden ist ausgeschlossen.
38) Gegen Computerviren bin ich ausreichend geschützt.
56) Meine gesendeten Daten sind anderen Personen nicht zugänglich.
65) Mein PC ist so gesichert, dass keine andere Person auf meine Daten zugreifen kann.

Skala: **Persönliche Bedeutung**
19) Ich informiere mich regelmäßig über den neusten Stand der IT-Sicherheit in meinem Unternehmen.
28) Ich bin der Meinung, dass das Thema „IT-Sicherheit“ generell in jedem Unternehmen einen hohen Stellenwert einnehmen muss.
30) Ich mache mir Gedanken, wie ich die IT-Sicherheitsrichtlinien an meinem Arbeitsplatz umsetzen kann.
47) Ich denke darüber nach, ob die IT-Sicherheitsvorkehrungen in meiner Firme ausreichend sind.

Skala: **Einschätzung des Stellenwerts IT-Sicherheit für das Unternehmen**
32) Unser Unternehmen investiert genügend Geld und Zeit in die IT-Sicherheit.
48) Die Maßnahmen zur IT-Sicherheits werden in meinem Unternehmen nicht konsequent genug umgesetzt.
53) Ich finde, dass mein Unternehmen IT-Sicherheit nicht ernst genug nimmt.
55) Unser Unternehmen ist daran interessiert, dass sich die Mitarbeiter hinsichtlich IT-Sicherheit laufend weiterbilden.

Skala: **Normative Überzeugung**
2) Meine Kollegen halten die IT-Sicherheitsmassnahmen für wichtig.
24) Mein Vorgesetzter hält die IT-Sicherheitsvorschriften immer ein.
33) Mein Vorgesetzter macht mich darauf aufmerksam, wenn ich die IT-Sicherheitsvorschriften nicht beachte.
44) Unsere Führungskraft interessiert sich sehr für den Bereich IT-Sicherheit.
46) Mein Vorgesetzter hält die IT-Sicherheitsmassnahmen für sehr wichtig.
71) Meine Kollegen machten mich darauf aufmerksam, wenn ich die IT-Sicherheitsvorschriften nicht beachte.
72) Die Regelung zur Umsetzung von IT-Sicherheitsmassnahmen ist in unserem Unternehmen sehr gut.

Skala: **Einwilligungsbereitschaft**
17) Meine Kollegen sind gut über IT-Sicherheit informiert und qualifiziert.
35) In meiner Arbeitsgruppe werden alle Mitarbeiter der Gruppe sehr geschätzt.
51) Meine Kollegen unterstützen mich bei der Umsetzung der IT-Sicherheitsmassnahmen.
57) Meine Kollegen schätzen es sehr, wenn man die IT-Sicherheitsbestimmungen beachtet.
62) Ich arbeite sehr gerne in meiner Arbeitsgruppe.

Skala: **Fähigkeiten**
20) Ich weiß ganz genau, wie ich die IT-Sicherheitsmassnahmen bei meiner Arbeitstätigkeit umsetzen muss.
29) Ich bin mit dem Umgang meiner Soft- und Hardware vertraut.

Skala: **Internale Kontrollüberzeugung**
54) Es liegt an mir, ob Daten frei von Computerviren bleiben.
58) Es liegt an mir, ob IT-Sicherheit auch im Betrieb umgesetzt wird.

Skala: **Externale Kontrollüberzeugung**
10) Die Umsetzung der IT-Sicherheitsmassnahmen werden durch andere geregelt (Administrator).
18) IT-Sicherheit und die Umsetzungs der Massnahmen betreffen mich nicht.
26) Die Umsetzung von IT-Sicherheit ist Sache anderer (z. B. Administrator).
70) Ich habe keinen Einfluss auf die IT-Sicherheit.

Skala: **Intention**
8) Wenn ich sehe, dass sich Kollegen nicht an die IT-Sicherheitsvorschriften halten, mache ich sie darauf aufmerksam.
12) Bevor ich Dateien auf meinen Computer lade überzeuge ich mich, ob diese Dateien frei von Viren sind.
13) Wenn es nötig ist, dann gebe ich mein Passwort auch weiter.
14) Bei der Ausführung meiner Arbeitstätigkeit „klicke“ ich nur, wenn ich mir über die Richtigkeit sicher bin.
21) Ich lade Software aus dem Internet auf meinen Computer.
34) Meine Kollegen geben ihre Passwörter nie weiter.
37) Bei Verlassen meines Arbeitsplatzes sperre ich immer die Arbeitsstation (Bildschirmschoner).
59) Die Auswahl meines Passwortes ist gut überlegt und schwer nachzuvollziehen.
60) Ich gebe Passwörter nie weiter.
66) Ich benutze das Internet nur für die Zwecke meiner Arbeit.
73) Ich habe mein Passwort nirgends notiert.

Skala: **Soziale Unterstützung am Arbeitsplatz durch die Kollegen**
5) Wenn es bei der Arbeit schwierig wird, dann kann ich mich auf meine Kollegen am Arbeitsplatz verlassen.
27) Ich kann auf die Hilfe meiner Kollegen bei Fragen im Umgang mit meinem Computer jederzeit zurückgreifen.
36) Meine Kollegen stört es, wenn ich Fragen bzgl. IT-Sicherheit und deren Umsetzungsmaßnahmen habe.
64) Meine Kollegen am Arbeitsplatz sind bereit, sich meine persönlichen Probleme anzuhören.

Skala: **Soziale Unterstützung am Arbeitsplatz durch den Vorgesetzten**
1) Mein Vorgesetzter ist bereit, sich meine persönlichen Probleme anzuhören.
43) Wenn es bei der Arbeit schwierig wird, dann kann ich mich auf meinen Vorgesetzten verlassen.

IV)Fragebogen zur Erhebung des IT-Sicherheitsbewusstseins

Sehr geehrte(r) TeilnehmerIn,

um das IT-Sicherheitsniveau in ihrer Firma laufend im Optimum zu halten sind wir auf Ihre Mitarbeit angewiesen. IT-Sicherheit ist nicht nur eine Frage der besten Hard- und Software, sondern darüber hinaus von Rahmen- und Randbedingungen durch die Organisation abhängig. Daher ist es für uns sehr wichtig, auf Ihren Einschätzungen und Erfahrungen aufbauen zu können.

Vor Ihnen liegt ein Fragebogen, de aus insgesamt 3 Teilbögen besteht. Alle Fragen sind durch einfaches Ankreuzen zu beantworten. Die Beantwortungszeit beträgt ca. 20 Minuten.

Es gelten bei der Beantwortung folgende Kriterien:

++ die Aussage trifft völlig zu
+ die Aussage trifft zu
+/- die Aussage trifft manchmal zu
- die Aussage trifft selten zu
-- die Aussage trifft gar nicht zu
x keine Aussage möglich

Sie sollten vor dem Ankreuzen oder Ausfüllen nicht lange überlegen, sondern nach Möglichkeit spontan antworten. Auch wenn Ihnen Fragen ähnlich oder doppelt erscheinen – lassen Sie bitte keine Frage unbeantwortet, es kommt bei der Beantwortung nur auf Ihre momentane Einschätzung an.

Die Auswertung des Fragebogens erfolgt anonym. Die beteiligten Personen unterliegen der Schweigepflicht, so dass die Bestimmungen des Datenschutzes eingehalten werden.

Wir danken Ihnen schon jetzt für Ihre Mitarbeit und Unterstützung!

Teil 1: Fragen zum Arbeitsplatz

Im Folgenden bitten wir Sie um einige allgemeine Angaben zu Ihrer Person und Ihrer derzeit ausgeübten Arbeitstätigkeit. Bitte kreuzen Sie die jeweils zutreffende Antwort an.

In welcher Organisationseinheit sind sie tätig?
O OE 1; O OE 3; O OE 5
O OE 2; O OE 4; O OE 6

Wie viele Jahre Berufserfahrung haben Sie?
O 0-2 Jahr; O 4-6 Jahre; O 8-10 Jahre
O 2-4 Jahre; O 6-8 Jahre; O 10 und mehr Jahre

Seit wann arbeiten Sie in Ihrer Firma?
O 0-2 Jahr; O 4-6 Jahre; O 8-10 Jahre
O 2-4 Jahre; O 6-8 Jahre; O 10 und mehr Jahre

Welcher Altersgruppe gehören Sie an?
O 15-20 Jahre; O 31-35 Jahre; O 46-50 Jahre
O 21-25 Jahre; O 36-40 Jahre; O 51 Jahre und
O 26-30 Jahre; O 41-45 Jahre

Teil 2: Führung & Organisation:

1) Ich erhielt eine ausführliche Einweisung im Umgang mit Virensuchprogrammen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

2) Unser Unternehmen hat alles veranlasst, dass auch im schlimmsten Fall die Daten erhalten bleiben (Backupsystem).

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

3) Ich wurde über den korrekten Umgang mit Passwörtern belehrt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

4) Unser Vorgesetzter sagt uns klar und deutlich, welche IT-Sicherheits-vorkehrungen einzuhalten sind.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

5) Auf meinem PC wurde nur die für meine Arbeitstätigkeit notwendige Software installiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

6) Unser Vorgesetzter schätzt es sehr, wenn man die IT-Sicherheits-bestimmungen beachtet.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

7) Wir Mitarbeiter werden über den Stand der IT-Sicherheit in unserem Betrieb ausreichend informiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

8) Unser Vorgesetzter verschlüsselt vertrauliche Informationen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

9) Unser Vorgesetzter kennt sich im Umgang mit dem Computer und den damit verbundenen Sicherheitsrisiken sehr gut aus.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

10) Unser Vorgesetzter informiert uns regelmäßig, welche IT-Sicherheits-vorkehrungen zu treffen sind.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

11) Unser Vorgesetzter gibt seine Passwörter nie weiter.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

12) Wir werden regelmäßig kontrolliert, ob wir die IT-Sicherheits-vorschriften einhalten.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

13) Es gibt für meinen Arbeitsbereich einen IT-Sicherheitsbeauftragten, dessen Name und Telefonnummer mir bekannt ist.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

14) Unser Vorgesetzter hält uns an, ihn auf IT-Sicherheitsmängel aufmerksam zu machen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

15) Wir Mitarbeiter werden über Änderungen im IT-Sicherheitsbereich ausreichend informiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

16) Unser Vorgesetzter ist gut über IT-Sicherheit informiert und qualifiziert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

17) Ich wurde über die Gefahren von Computerviren ausführlich informiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

18) Ich wurde ausführlich über die Gefahren bei der Nutzung des Internets aufgeklärt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

19) Sensible Daten werden in unserem Unternehmen immer mit Passwörtern versehen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

20) Wir Mitarbeiter werden bei Problemen im IT-Sicherheitsbereich umfangreich informiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

21) Unser Vorgesetzter ist daran interessiert, dass wir uns im Bereich IT weiterbilden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

22) Unser Unternehmen interessiert sich sehr für das Thema IT-Sicherheit.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

23) Über die IT-Sicherheitsvorschriften bin ich ausführlich belehrt worden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

24) Vertraulichen Daten werden nur verschlüsselt versendet.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

25) Unser Vorgesetzter sperrt immer seine Arbeitsstation, wenn er den Arbeitsplatz verlässt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

26) Ich bin mit meinen für die Arbeitsaufgaben-erfüllung installierten Computerprogrammen sehr zufrieden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

27) Unserem Vorgesetzten ist es egal, ob wir eigene Software auf dem PC installiert haben.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

28) Unser Vorgesetzter achtet darauf, dass keine Passwörter weitergegeben werden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

29) Unserem Vorgesetzten ist es egal, ob wir regelmäßig unser Virusupdate durchführen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

30) Für Probleme beim Umgang mit meinem PC habe ich eine zentrale Ansprechperson.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

31) Mein Vorgesetzter unterstützt mich bei der Umsetzung der IT-Sicherheitsmassnahmen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

Teil 3: Einstellung & Verhalten:

1) Mein Vorgesetzter ist bereit, sich meine persönlichen Probleme anzuhören.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

2) Meine Kollegen halten die IT-Sicherheitsmassnahmen für wichtig.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

3) Ich muss jederzeit damit rechnen, dass beim Öffnen von gesendeten Dateien auch ein Computervirus geladen wird.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

4) Ich bin gerne bereit, mir die Probleme meiner Kollegen anzuhören.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

5) Wenn es bei der Arbeit schwierig wird, dann kann ich mich auf meine Kollegen am Arbeitsplatz verlassen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

6) Ich bin für die Umsetzung der IT-Sicherheitsmassnahmen an meinem Arbeitsplatz verantwortlich.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

7) Wenn ich sehe, dass sich Kollegen nicht an die IT-Sicherheitsvorschriften halten, mache ich sie darauf aufmerksam.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

8) Die Gefahr, dass Daten versehentlich gelöscht oder unbrauchbar werden ist ausgeschlossen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

9) Die Umsetzung der IT-Sicherheitsmassnahmen wird durch andere geregelt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

10) Ich muss häufig auf die Hilfe meiner Kollegen zurückgreifen, weil ich Probleme mit meinem Computer habe.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

11) Bevor ich Dateien auf meinen Computer lade überzeuge ich mich, ob diese Dateien frei von Viren sind.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

12) Wenn es nötig ist, dann gebe ich mein Passwort auch weiter.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

13) Bei der Ausführung meiner Arbeitstätigkeit „klicke" ich nur, wenn ich mir über die Richtigkeit sicher bin.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

14) Ein Fehler bei der Dateneingabe (z. B. versehentliches Löschen etc.) kann ohne größere Probleme rückgängig gemacht werden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

15) Meine Kollegen halten die IT-Sicherheitsvorschriften immer ein.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

16) Die Gefahr, dass ich Dateien beschädige ist ausgeschlossen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

17) Meinen Bildschirmschoner habe ich passwortgeschützt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

18) Meine Kollegen sind gut über IT-Sicherheit informiert und qualifiziert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

19) IT-Sicherheit und die Umsetzungsmassnahmen betreffen mich nicht.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

20) Ich informiere mich regelmäßig über den neusten Stand der IT-Sicherheit in meinem Unternehmen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

21) Ich bin für die Umsetzung der IT-Sicherheitsmassnahmen an meinem Arbeitsplatz verantwortlich.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

22) Ich weiß ganz genau, wie ich die IT-Sicherheitsmassnahmen bei meiner Arbeitstätigkeit umsetzen muss.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

23) Ich lade Software aus dem Internet auf meinen Computer.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

24) Die Einhaltung der IT-Sicherheitsmassnahmen hält mich bei meiner Arbeit unnötig auf.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

25) Die Gefahr meinen Computer mit einem Virus zu infizieren ist ausgeschlossen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

26) Mein Vorgesetzter hält die IT-Sicherheitsvorschriften immer ein.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

27) Ich mache von meinen persönlichen Daten regelmäßig eine Sicherungskopie.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

28) Die Umsetzung von IT-Sicherheit ist Sache anderer (z. B. Administrator).

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

29) Ich kann auf die Hilfe meiner Kollegen bei Fragen im Umgang mit meinem Computer jederzeit zurückgreifen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

30) Ich bin der Meinung, dass das Thema „IT-Sicherheit" generell in jedem Unternehmen einen hohen Stellenwert einnehmen muss.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

31) Ich bin mit dem Umgang meiner Soft- und Hardware vertraut.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

32) Ich mache mir Gedanken, wie ich die IT-Sicherheitsrichtlinien an meinem Arbeitsplatz umsetzen kann.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

33) Mein Vorgesetzter ist bereit, sich meine Probleme im Zusammenhang mit der Arbeit anzuhören.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

34) Die Gefahr, dass vertrauliche Daten abgefangen und verändert werden ist ausgeschlossen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

35) Unser Unternehmen investiert genügend Geld und Zeit in die IT-Sicherheit.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

36) Mein Vorgesetzter macht mich darauf aufmerksam, wenn ich die IT-Sicherheitsvorschriften nicht beachte.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

37) Meine Kollegen geben ihre Passwörter nie weiter.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

38) Meine Kollegen am Arbeitsplatz sind bereit, sich meine Probleme im Zusammenhang mit der Arbeit anzuhören.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

39) In meiner Arbeitsgruppe werden alle Mitarbeiter der Gruppe sehr geschätzt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

40) Meine Kollegen stört es, wenn ich Fragen bzgl. IT-Sicherheit und deren Umsetzungsmassnahmen habe.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

41) Bei Verlassen meines Arbeitsplatzes sperre ich immer die Arbeitsstation.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

42) Gegen Computerviren bin ich ausreichend geschützt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

43) Die IT-Sicherheitsumsetzungsmassnahmen sind in unserem Unternehmen unsinnig oder unzureichend.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

44) Vor dem Öffnen von Dateien die per E-Mails versendet wurden, vergewissere ich mich über den Absender.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

45) Ich bin mir über die Risiken beim Herunterladen von Dateien aus dem Internet bewusst.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

46) Wenn es bei der Arbeit schwierig wird, dann kann ich mich auf meinen Vorgesetzten verlassen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

47) Unsere Führungskraft interessiert sich sehr für den Bereich IT-Sicherheit.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

48) Ich ändere regelmäßig mein Passwort.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

49) Mein Vorgesetzter hält die IT-Sicherheitsmassnahmen für sehr wichtig.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

50) Ich denke darüber nach, ob die IT-Sicherheitsvorkehrungen in meiner Firma ausreichend sind.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

51) Die IT-Sicherheitsumsetzungsmassnahmen werden in meinem Unternehmen nicht konsequent genug umgesetzt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

52) Es ist mir wichtig, was die Gruppemitglieder von mir halten.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

53) Bei unbekannten Problemen an meinem Computer frage ich lieber nach.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

54) Meine Kollegen unterstützen mich bei der Umsetzung der IT-Sicherheitsmassnahmen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

55) IT-Sicherheit wird in meinem Unternehmen unterschätzt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

56) Ich finde, dass mein Unternehmen IT-Sicherheit nicht ernst genug nimmt.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

57) Es liegt an mir, ob Daten frei von Computerviren bleiben.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

58) Unser Unternehmen ist daran interessiert, dass sich die Mitarbeiter hinsichtlich IT-Sicherheit laufend weiterbilden.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

59) Meine gesendeten Daten sind anderen Personen nicht zugänglich.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

60) Meine Kollegen schätzen es sehr, wenn man die IT-Sicherheits-bestimmungen beachtet.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

61) Es liegt an mir, ob IT-Sicherheit auch im Betrieb umgesetzt wird

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

62) Die Auswahl meines Passwortes ist gut überlegt und schwer nachzuvollziehen.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

63) Ich gebe Passwörter nie weiter.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

64) Mir sind die Gefahren und Risiken beim Umgang mit meinem Computer und deren installierten Programmen bewusst.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

65) Wenn ich sehe, dass sich ein Kollege über die IT-Sicherheits-vorschriften hinwegsetzt, mache ich ihn darauf aufmerksam.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

66) Ich arbeite sehr gerne in meiner Arbeitsgruppe.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

67) Ich bin für meine Arbeitsmittel verantwortlich.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

68) Meine Kollegen am Arbeitsplatz sind bereit, sich meine persönlichen Probleme anzuhören.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

69) Mein Computer ist so gesichert, dass keine andere Person auf meine Daten zugreifen kann.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

70) Ich benutze das Internet nur für die Zwecke meiner Arbeit.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

71) Ich werde häufig von Kollegen um Hilfe gebeten, weil diese Probleme mit Ihrem Computer haben.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

72) Ich bin der Meinung dass mein Unternehmen mehr in die Qualifizierung seiner Mitarbeiter zur Umsetzung und Verständnis für IT-Sicherheit investieren muss.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

73) Ich halte die IT-Sicherheitsumsetzungsmassnahmen an meinem Arbeitsplatz für übertrieben.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

74) Ich habe keinen Einfluss auf die IT-Sicherheit.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
O	O	O	O	O	O

75) Meine Kollegen machten mich darauf aufmerksam, wenn ich die IT-Sicherheitsvorschriften nicht beachte.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

76) Die Regelung zur Umsetzung von IT-Sicherheitsmassnahmen ist in unserem Unternehmen sehr gut.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

77) Ich habe mein Passwort nirgends notiert.

Grad der Zustimmung					
++	+	+/-	-	--	Keine Angabe möglich
○	○	○	○	○	○

Bitte beurteilen Sie die folgenden Situationsbeschreibungen in Bezug auf Ihre eigene tägliche Arbeit bzw. Ihren eigenen Arbeitsbereichen.

Geben Sie bitte an, ob und in welchem Ausmaß die Gegebenheiten der Situation auf Ihre Arbeitstätigkeit zutreffen.

Nach unseren Erfahrungen lassen sich Arbeitstätigkeiten in drei Bereiche unterteilen:

1. den **Arbeitsauftrag**, hierunter verstehen wir die Inhalte der Aufgaben, die Sie im Rahmen Ihrer Tätigkeit im Allgemeinen auszuführen haben.

2. die **Zusammenarbeit und Kommunikation mit anderen**, d. h. mit Vorgesetzten, Mitarbeitern, Kollegen und Außenstehenden Personen.

3. die **verwendeten Arbeitsmittel**, d. h. den Umgang mit Arbeitsmitteln – insbesondere mit Computern und Software -, die Sie zur Erledigung Ihrer Aufgaben verwenden.

Geben Sie bitte für die jeweils vorgegebene Situation an, inwieweit diese für die drei genannten Bereiche **Ihrer Arbeit** zutreffen.

Kreuzen Sie die Ziffern „0" an, wenn die jeweilige Situation in dem jeweiligen Bereich nicht vorkommt, also überhaupt nicht zutrifft. Die Ziffer „4" ist anzukreuzen, wenn die Situation vollständig zutrifft, d. h. Ihre Arbeit in dem entsprechenden Arbeitsbereich treffend beschreibt.

Wenn Sie für jeden Arbeitsbereich die zutreffende Ziffer angekreuzt haben, gehen Sie weiter zur nächsten Situation.

A1) Sie haben während der Arbeit auf mehrere Dinge gleichzeitig zu achten, wobei Sie vieles im Gedächtnis behalten müssen.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

A2) Sie haben schwierige Aufgaben zu bearbeiten, die eine hohe Konzentration und Genauigkeit erfordern.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

A3) Die Tätigkeit erfordert routinierte Handhabungen und geübte Bewegungsabläufe, ohne nachdenken zu müssen.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

A4) Die Arbeit besteht hauptsächlich aus kurzen, sich wiederholenden Teilaufgaben.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

T1) Sie müssen oft Entscheidungen treffen und tragen die Verantwortung dafür.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

T2) Sie müssen den optimalen Arbeitsablauf im Einzelnen selbst planen.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

T3) Die Arbeit ist meistens die gleiche und bietet wenig Handlungsspielraum.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

R1) Sie haben häufig Wartezeiten, in denen Sie nichts tun können und keine weiteren Informationen erhalten.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

R2) Sie erhalten keine Rückmeldung über Ihre Arbeits-ergebnisse.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

R3) Die Arbeitsbedingungen sind schlecht, der Arbeitsablauf ist häufig gestört.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

R4) Sie erhalten ungenaue und schwer durchschaubare Arbeitsaufträge.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

R5) Sie werden bei der Arbeit durch Lärm, schlechte Lichtverhältnisse oder unangenehme Temperaturen beeinträchtigt.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

L1) Sie erhalten Leistungsvorgaben, Ihre Arbeit wird kontrolliert.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

L2) Sie haben Zeitvorgaben einzuhalten.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

K1) Sie arbeiten vorwiegend alleine.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

K2) Die Arbeit erfordert häufig Absprachen und Abstimmungen mit Anderen.

	trifft **überhaupt nicht** zu	trifft **selten** zu	trifft **manchmal** zu	trifft **oft** zu	trifft **vollständig** zu
Dies hat etwas mit **Ihrem Arbeitsauftrag** zu tun	0	1	2	3	4
Dies hat etwas mit **der Zusammenarbeit und Kommunikation mit anderen** zu tun.	0	1	2	3	4
Dies hat etwas mit **den verwendeten Arbeitsmitteln (insbes. Computer und Software)** zu tun.	0	1	2	3	4

Fragebogen
zur Erhebung
des IT-Sicherheitsniveaus
nach BSI-Grundschutz

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
B 99.991	**IT-Sicherheitsmanagement**	1					
M 02.191	*Etablierung des IT-Sicherheitsprozesses*	1		X			Es ist wichtig, organisatorische Rahmenbedingungen zu schaffen, um das ordnungsgemäße und sichere IT-gestützte Arbeiten des Unternehmens zu ermöglichen. Sinnvollerweise soll durch die Unternehmensleitung ein gesteuerter IT-Sicherheitsprozess initiiert werden, der die Voraussetzungen für eine durchdachte Gestaltung sowie sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen gewährleistet. Wenn diese Randbedingungen in einer konkreten Situation nur teilweise gegeben sind, so sollte zunächst versucht werden, auf Arbeitsebene die Umsetzung der fehlenden IT-Sicherheitsmaßnahmen durchzuführen. In jedem Fall sollte aber darauf hingewirkt werden, die Unternehmensleitung für die Belange der IT-Sicherheit zu sensibilisieren, so dass sie zukünftig ihrer Verantwortung Rechnung trägt. Der vielfach zu beobachtende sich selbst auf Arbeitsebene initiierende IT-Sicherheitsprozess führt zwar zu einer Verbesserung der Sicherheitssituation, garantiert jedoch kein dauerhaftes Fortentwickeln des IT-Sicherheitsniveaus.
01003	Wenn ja, wurden organisatorische Rahmenbedingungen geschaffen,?			X			
02000	Wird der IT-Sicherheitsprozess in ausreichendem Maße von der Organisationsleitung unterstützt?			X			
02001	Wenn ja, geht die Initiative von der Unternehmensleitung aus?				X		Wichtig ist, dass die Unternehmensleitung in vollem Umfang hinter der IT-Sicherheitsleitlinie und den darin festgehaltenen Zielen steht. Selbst wenn einzelne Aufgaben im Rahmen des IT-Sicherheitsprozesses an Personen oder Organisationseinheiten delegiert werden, die dann für die Umsetzung zuständig sind, bleibt die Gesamtverantwortung bei der Unternehmensleitung.
02003	Wenn ja, wird die Aufgabe "IT-Sicherheit" durch die Unternehmenleitung aktiv unterstützt?			X			
M 02.192	*Erstellung einer IT-Sicherheitsrichtlinie*	1		X			Die IT-Sicherheitsleitlinie definiert das angestrebte IT-Sicherheitsniveau, mit dem die Aufgaben durch die Organisation erfüllt werden. Die IT-Sicherheitsleitlinie beinhaltet die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-icherheitsstrategie. Sie ist somit Anspruch und Aussage zugleich, dass das IT-Sicherheitsniveau auf allen Ebenen der Organisation erreicht werden soll.
01002	Wenn ja, beinhaltet diese die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie?			X			Die IT-Sicherheitsleitlinie beinhaltet die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie. Sie ist somit Anspruch und Aussage zugleich, dass das IT-Sicherheitsniveau auf allen Ebenen der Organisation erreicht werden soll.

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
01004	Wenn ja, wurde für die Formulierung eine Entwicklungsgruppe einberufen?			X			Sinnvollerweise sollte in dieser Entwicklungsgruppe Vertreter der IT-Anwender, Vertreter des IT-Betriebs und ein oder mehrere in Sachen IT-Sicherheit ausreichend vorgebildete Mitarbeiter mitwirken. Idealerweise sollte zeitweise auch ein Mitglied der Leitungsebene, das die Bedeutung der IT für das Unternehmen einschätzen kann, hinzugezogen werden.
01006	Wenn ja, ist darin eine Beschreibung der für die Umsetzung des IT-Sicherheitsprozesses etablierten Organisationsstruktur enthalten?			X			
01007	Wenn ja, wurde sie allen Mitarbeitern als verbindliche Richtlinie bekanntgegeben?				X		Es sollten alle Mitarbeiter darauf aufmerksam gemacht werden, dass nicht nur bei der Aufgabenerfüllung allgemein, sondern auch bei der Erfüllung der Aufgabe "IT-Sicherheit" von jedem Mitarbeiter ein engagiertes, kooperatives sowie verantwortungsbewusstes Handeln erwartet wird.
02000	Wurden zur Bestimmung von IT-Sicherheitszielen folgende Punkte berücksichtig?			X			Es ist wichtig, sich über den materiellen Wert der IT selbst hinaus klarzumachen, wie stark die Aufgabenerfüllung innerhalb der Organisation von der eingesetzten IT und deren reibungslosem Funktionieren abhängt.
02001	Welche kritischen Aufgaben des Unternehmens können ohne Unterstützung durch IT nicht, nur unzureichend oder mit erheblichem Mehraufwand ausgeführt werden können?				X		
02002	Welche wesentlichen Entscheidungen des Unternehmens auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationsverarbeitungssystemen beruhen?			X			
M 02.193	*Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit*	1		X			IT-Sicherheit ist für jedes IT-Projekt, jedes IT-System und alle IT-Benutzer innerhalb einer Organisation von besonderer Bedeutung. Das angestrebte IT-Sicherheitsniveau kann nur erreicht werden, wenn das IT-Sicherheitskonzept unternehmensweit umgesetzt wird. Dieser übergreifende Charakter des IT-Sicherheitsprozesses macht es notwendig, die Rollen innerhalb des Unternehmens festzulegen. Den Rollen sind die entsprechenden Aufgaben zuzuordnen, die wiederum von qualifizierten Mitarbeitern ausgeführt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effizient und effektiv erledigt werden.
01000	Existiert eine geeignete Organisationsstruktur für IT-Sicherheit (IT-Sicherheits-Beauftragter/-Team)?			X			In Abhängigkeit von der Organisationsgröße bieten sich nach BSI-Grundschutz drei Möglichkeiten für die Aufbauorganisation des IT-Sicherheitsmanagements an (siehe BSI-Grundschutzhandbuch)
01001	Wenn ja, wurden die einzelnen Rollen hinsichtlich IT-Sicherheit innerhalb des Unternehmens festgelegt?			X			
01002	Wenn ja, wurden diesen Rollen die entsprechenden Aufgaben zugeordnet?			X			
01003	Wenn ja, verfügen die Mitarbeiter, denen diese Aufgaben zugeteilt wurden über das entsprechende Fachwissen?			X			
02005	Wenn ja, wurden die Aufgaben, Verantwortungen und Kompetenzen von der Leitungsebene eindeutig festgelegt?			X			
02006	Wenn ja, kennen alle Organisationsmitglieder den IT-Sicherheitsbeauftragten namentlich?				X		

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
02010	Wenn ja, koordiniert er die Erstellung des Notfallvorsorge-Konzepts und anderer Teilkonzepte?			X			
03001	Wenn ja, sind die Mitglieder genügend qualifiziert (Kenntnisse über IT-Sicherheit, IT-Systeme, Organisation)?			X			
03002	Wenn ja, verfügt es über genügend Handlungs- und Entscheidungsspielraum um Belange der IT-Sicherheit zu regeln, bzw. Pläne, Vorgaben und Richtlinien zu erarbeiten?			X			
03005	Wenn ja, erstellt es die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit?			X			
03006	Wenn ja, kennen alle Organisationsmitglieder das IT-Sicherheitsmanagement-Team?			X			
M 02.194	*Erstellung einer Übersicht über vorhandene IT-Systeme*	1		X			Nicht nur für die Erstellung eines IT-Sicherheitskonzepts, sondern auch für die Überprüfung, Wartung, Fehlersuche und Instandsetzung von IT-Systemen ist eine vollständige und korrekte Erfassung der vorhandenen und geplanten IT-Systeme notwendig. Besonderer Wert ist auf die Vollständigkeit und Aktualität einer solchen Übersicht zu legen. Sie sollte insbesondere auch einen detaillierten Vernetzungsplan beinhalten
01000	Wurden alle vorhanden und geplanten IT-Systeme vollständig und korrekt in einer Übersichtsdokumentation erfasst?			X			Ist bereits ein vollständiges IT-Geräteverzeichnis sowie ein Netzplan vorhanden, so sind diesem die benötigten Informationen zu entnehmen. Existiert ein solches Verzeichnis nicht oder sind die Informationen dort nicht enthalten, so müssen sie zusätzlich erfasst werden.
01004	Wenn ja, wurden die Installationsorte der IT-Systeme aufgenommen?			X			
01005	Wenn ja, wurde die Vernetzung der IT-Systeme aufgenommen?			X			
01008	Wenn ja, wurden die Benutzer der IT-Systeme mit aufgenommen?				X		
01009	Wenn ja, wurden die Anwendungen aufgenommen, die auf dem IT-System laufen?			X			
01010	Wenn ja, wurden weitere Komponenten des Systems, wie z.B. Drucker, Diskettenlaufwerk, Monitor etc., aufgenommen?			X			
02000	Existiert ein Netzplan, aus dem die Vernetzungsstrukturen einschließlich der Verbindung nach außen ersichtlich ist?				X		Es sollte ein Netzplan verfügbar sein, aus dem die Vernetzungsstrukturen einschließlich der Verbindung nach außen ersichtlich sind.
03000	Wird das IT-Sicherheitsmanagement-Team über jede Veränderung im eingesetzten IT-Verbund informiert?				X		Wichtig ist die regelmäßige Überprüfung der Aktualität und Vollständigkeit einer solchen Übersicht. Um dies gewährleisten zu können, ist sicherzustellen, dass das IT-Sicherheitsmanagement-Team über jede Veränderung im eingesetzten IT-Verbund informiert wird.
M 02.195	*Erstellung eines IT-Sicherheitskonzepts*	1		X			Das IT-Sicherheitskonzept ist das "zentrale" Dokument im IT-Sicherheitsprozess eines Unternehmens. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen.
01000	Basieren alle konkreten Umsetzungsmaßnahmen auf einem IT-Sicherheitskonzept?			X			
01001	Wenn ja, beinhaltet es die Beschreibung des aktuellen Zustandes eines IT-Verbundes und der hier zu verarbeitenden Informationen?				X		

Anhalt	Frage	Ja	Entfällt teilweise	Nein	Nicht geprüft	Bemerkungen
02000	(bei Erfüllung von M 02.104): Wurde der Schutzbedarf des vorhandenen IT-Verbunds nach Erfassung aller IT-Systeme mit Bezug auf die Fachaufgaben festgelegt?			X		
02001	Wenn ja, wurde die Festlegung des Schutzbedarfs des vorhandenen IT-Verbunds begründet?				X	nicht zutreffend!
03000	Existiert ein IT-Sicherheitskonezpt? Und wurden bei der Erstellung des IT-Sicherheitskonzepts folgende Punkte beachtet?		X			Ein IT-Sicherheitskonzept enthält zunächst die Beschreibung des aktuellen Zustandes eines IT-Verbundes und der auf ihr zu verarbeitenden Informationen. Unter einem IT-Verbund ist die Gesamtheit der technischen Komponenten zu verstehen, die der Aufgabenerfüllung dienen. Dies beinhaltet die IT-Systeme und die IT-Anwendungen. Der aktuelle Zustand eines IT-Verbunds umfasst neben der Beschreibung der technischen Komponenten, der dort betriebenen IT-Anwendungen und dabei zu verarbeitenden Informationen auch eine Auflistung der vorhandenen Schwachstellen, möglicher Bedrohungen und bereits umgesetzter Maßnahmen.
03001	Wenn ja, wurden bei der Erstellung alle Mitarbeiter, die mit dem zu untersuchenden IT-Verbund und den darauf verarbeiteten Informationen befasst sind, in jeweils angemessener Art und Weise einbezogen?			X		
03002	Wenn ja, wurden vorhandene Sicherheitsmaßnahmen erfasst und analysiert (Soll-Ist-Vergleich des Sicherheits-Ist)?		X			
03003	Wenn ja, enthält es entsprechende Maßnahmeempfehlungen des IT-Grundschutzes?		X			
03004	Wenn ja, wurden für Systeme, für die der mittlere Grundschutz als nicht ausreichend erachtet wird, ergänzende Sicherheitsanalysen durchgeführt?				X	nicht zutreffend!
03005	Wenn ja, wurden für Systeme, für die im Grundschutzhandbuch keine Maßnahmeempfehlungen enthalten sind, ergänzende Sicherheitsanalysen durchgeführt?				X	nicht zutreffend!
03007	Wenn ja, wurde auf der Grundlage der Maßnahmeempfehlungen ein Kostenplan zur Vorlage und Genehmigung durch die Unternehmensleitung aufgestellt?			X		
03008	Wenn ja, wurde für den Fall fehlender Ressourcen an Personal und/oder Finanzmitteln für IT-Sicherheit eine Restrisikobetrachtung aufgestellt und der Unernehmensleitung zur Genehmigung vorgelegt?			X		
03009	Wenn ja, ist das IT-Sicherheitskonzept ausreichend dokumentiert, damit im Vertretungsfall ein Dritter sicherheitsspezifische Aufgaben übernehmen kann?			X		

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
M 02.196	*Umsetzung eines IT-Sicherheitskonzepts nach einem Realisierungsplan*	1					Nach der Erstellung des IT-Sicherheitskonzepts ist dieses in die Praxis umzusetzen. Hierbei ist zwischen einer Konzeptionsphase und der eigentlichen Realisierung zu unterscheiden. In der Konzeptionsphase ist die grundsätzliche Eignung jeder empfohlenen Maßnahme innerhalb des vorliegenden IT-Verbunds zu prüfen und die Maßnahmeempfehlungen derart zu konkretisieren, dass sie in organisationsspezifischen Regelungen münden. Im IT-Sicherheitskonzept erfolgt daher neben der Festlegung der Verantwortlichkeit für die Initiierung insbesondere die Festlegung der Verantwortung für die Umsetzung der Maßnahmen. Die Verantwortung für die Initiierung umfasst das Schaffen der Voraussetzungen für die wirksame Umsetzung sowie die Festlegung der Ziele. Diese Verantwortung setzt das Verfügungsrecht über die erforderlichen Ressourcen voraus.
01000	Wird bei der Umsetzung eines IT-Sicherheits-Konzepts nach einem Realisierungsplan vorgegangen?				X		
01001	Wenn ja, werden in der Konzeptionsphase die empfohlenen Maßnahmen innerhalb des vorliegenden IT-Verbunds geprüft?					X	nicht zutreffend!
01002	Wenn ja, werden diese überprüften Maßnahmen danach derart konkretisiert, dass sie in organisationsspezifischen Regelungen münden?					X	nicht zutreffend!
01003	Wenn ja, werden während der Erstellung die Verantwortlichkeiten für die Initiierung festgelegt?					X	nicht zutreffend!
01004	Wenn ja, verfügen die Verantwortlichen für die Initiierung über genügend Verfügungsrechte und über genügend Wissen hinsichtlich den Zielvorgaben?					X	nicht zutreffend!
01005	Wenn ja, werden die Zeitvorgaben zur Umsetzung der Maßnahmen realistisch vorgegeben?					X	nicht zutreffend!
01006	Wenn ja, verfügen die Verantwortlichen für die Initiierung über genügend Verfügungsrechte über die erforderlichen Ressourcen (Arbeitszeit, Finanzmittel etc.)?					X	nicht zutreffend!
01007	Wenn ja, werden während der Erstellung die Verantwortlichkeiten für die Umsetzung der Maßnahmen festgelegt?					X	nicht zutreffend!
01008	Wenn ja, verfügen die für die Umsetzung der Maßnahmen Verantwortlichen über genügend Entscheidungs- und Handlungsspielraum (Ausgestaltung der Regelungen, Beschaffung der Hilfsmittel, Gestaltung von Abläufen, Information der betroffenen Mitarbeiter etc.)?					X	nicht zutreffend!
01010	Wenn ja, kann bei der Umsetzung der Maßnahmen evtl. auch auf die Hilfe anderer Gruppen zurückgegriffen werden (Beschaffung, Installation, Pflege technischer Einrichtungen)?					X	nicht zutreffend!
01011	Wenn ja, findet ein regelmäßiger Informationsaustausch zwischen dem IT-Sicherheits-Beauftragten/-Management-Team und den Benutzern der betroffenen IT-Systeme statt?					X	nicht zutreffend!

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
01012	Wenn ja, weiß jeder Mitarbeiter, der von den Umsetzungsmaßnahmen betroffen ist, an wen er sich bei auftretenden Problemen wenden kann?					X	nicht zutreffend!
02000	Wurde vor Umsetzung eines IT-Sicherheitskonzets ein Realisierungsplan augestellt?				X		
02001	Wenn ja, sind darin die Namen der Personen enthalten, die für die Umsetzung der Maßnahmen verantwortlich sind?					X	nicht zutreffend!
02002	Wenn ja, sind darin die Prioritäten der umzusetzenden Maßnahmen enthalten?					X	nicht zutreffend!
02003	Wenn ja, sind darin Termine festgelegt, bis wann die Maßnahmen umzusetzen sind?					X	nicht zutreffend!
02004	Wenn ja, ist darin beschrieben, bei wem die vollzogene Umsetzung der Maßnahmen zu melden ist?					X	nicht zutreffend!
02005	Wenn ja, ist darin die Bereitstellung von Ressourcen dokumentiert (Mitarbeiterkapazitäten, Raumbedarf, Kosten)?					X	nicht zutreffend!
02006	Wenn ja, wird vor der Umsetzung der Maßnahmen geprüft, ob der Realisierungsplan realistisch ist?					X	nicht zutreffend!
M 02.197	*Erstellung eines Schulungskonzepts für IT-Sicherheit*	1		X			Die sachgerechte Erfüllung der Gemeinschaftsaufgabe "IT-Sicherheit" kann nur dann gelingen, wenn alle am IT-Sicherheitsprozess beteiligten Personen einen angemessenen Kenntnisstand über IT-Sicherheit allgemein und insbesondere über die Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet haben. Obwohl letztlich jeder Benutzer dazu motiviert werden sollte, sich auch in Eigeninitiative auf dem notwendigen Kenntnisstand zu halten, bleibt es in der Verantwortung der Organisationsleitung durch geeignete Schulungsmaßnahmen hierfür die nötigen Voraussetzungen zu schaffen. Angesichts des Umfangs der möglichen Schulungsthemen und der Bedeutung der IT-Sicherheit ist bei der Auswahl der Schulungsinhalte ein koordiniertes Vorgehen erforderlich. Dieses ist in Schulungskonzepten darzulegen und zu dokumentieren.
01000	Existieren explizite Schulungskonzepte zum Thema IT-Sicherheit?			X			
01002	Wenn ja, werden sie in enger Abstimmung mit den sonstigen Schulungskonzepten des Unternehmens erstellt?				X		
01006	(bei Erfüllung von M 02.192): Wenn ja, ist die Bedeutung der organisationsweiten IT-Sicherheitsleitlinie Inhalt der Schulungskonzepte?			X			
01007	Wenn ja, sind Verantwortlichkeiten und Meldewege in der Organisation Inhalte der Schulungskonzepte?			X			
01009	Wenn ja, ist darin enthalten, wie man sicherheitsrelevante Vorfälle erkennt und was in diesem Fall zu tun ist?						

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
M 02.198	*Sensibilisierung der Mitarbeiter für IT-Sicherheit*	1		X			In der Praxis bestätigt sich immer wieder, dass ein Großteil der Sicherheitsvorfälle bei der IT-Nutzung nicht durch organisationsfremde Außentäter, sondern durch unsachgemäßes Verhalten eigener Mitarbeiter hervorgerufen wird. Daher kann die Verbesserung der IT-Sicherheitskenntnisse der eigenen Mitarbeiter und die Erhöhung der Eigenverantwortung jedes IT-Benutzers als eine besonders wirksame und überdies relativ kostengünstige Maßnahme zur Erhöhung der IT-Sicherheit gelten. Ebenso sind gute IT-Sicherheitskenntnisse Voraussetzung dafür, dass sicherheitsrelevante Zwischenfälle frühzeitig als solche erkannt werden. Es sollte bei allen Mitarbeitern ein hinreichender Kenntnisstand über die Belange der IT-Sicherheit und das Bewusstsein für die Risiken im alltäglichen Umgang mit der IT vorhanden sein. Zur Erreichung dieses Ziels trägt neben einem Schulungskonzept für IT-Sicherheit insbesondere die wiederholte Sensibilisierung aller Mitarbeiter durch IT-Sicherheits-Verantwortliche, Vorgesetzte oder Kollegen wesentlich bei.
01001	Wenn ja, beinhalten diese Schulungen die Zielsetzungen der IT-Sicherheitsleitlinien?					X	nicht zutreffend!
04000	Gehen alle IT-Sicherheitsverantwortlichen und die Leitungsebene mit gutem Beispiel beim Thema IT-Sicherheit voran?				X		
M 02.199	*Aufrechterhaltung der IT-Sicherheit*	1		X			Im IT-Sicherheitsprozess geht es nicht nur darum, das angestrebte IT-Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende IT-Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle IT-Sicherheitsmaßnahmen regelmäßig überprüft werden.
01000	Werden alle IT-Sicherheitsmaßnahmen regelmäßig überprüft?			X			Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens alle zwei Jahre) durchgeführt werden und können bei gegebenem Anlass auch zwischenzeitlich erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden IT-Sicherheitsmaßnahmen.
01001	Wenn ja, sind die Zeitpunkte der Überprüfungen festgelegt?				X		
02000	Findet bei Veränderungen im technischen oder technisch-organisatorischen Umfeld eine Anpassung der bestehenden IT-Sicherheitsmaßnahmen statt?			X			
03001	Wenn ja, werden die Ergebnisse der Überprüfungen dokumentiert?			X			
03002	Wenn ja, wurde festgelegt, wie mit den Überprüfungsergebnissen zu verfahren ist?			X			
03003	Wenn ja, werden die Korrekturmaßnahmen auch umgesetzt?			X			
03004	Wenn ja, wurde festgelegt, wie die Tätigkeiten im Zusammenhang mit den Überprüfungen zu koordinieren sind?			X			

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
M 02.201	*Dokumentation des IT-Sicherheitsprozesses*	1		X			Der Ablauf des IT-Sicherheitsprozesses und die Arbeitsergebnisse in seinen einzelnen Phasen sollten dokumentiert werden. Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der IT-Sicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist dabei, dass nicht nur die jeweils aktuelle Version der betreffenden Unterlagen griffbereit gehalten wird, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst hierdurch ist eine kontinuierliche Rückverfolgung der Entwicklung im Bereich IT-Sicherheit, bei der die getroffenen Entscheidungen nachvollziehbar werden, gewährleistet.
03000	(bei Erfüllung M 02.195): Ist das IT-Sicherheitskonzept dokumentiert?			X			
04000	(bei Erfüllung M 02.196): Sind die Umsetzungspläne für IT-Sicherheitsmaßnahmen dokumentiert?			X			
04001	Wenn ja, sind Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz dokumentiert?				X		
04002	Wenn ja, existieren Dokumentationen von Überprüfungen?			X			
05000	(bei Erfüllung M 02.193): Sind die Sitzungsprotokolle und Beschlüsse des IT-Sicherheitsmanagement-Teams dokumentiert?				X		
07000	(bei Erfüllung M 02.197): Sind IT-Sicherheits-Schulungspläne dokumentiert?			X			
08000	Sind die Meldungen über sicherheitsrelevante Vorfälle dokumentiert?			X			
09000	Werden die Arbeitsergebnisse in ihren einzelnen Phasen dokumentiert?			X			
09001	Wenn ja, werden die Dokumentationen laufend aktualisiert und erneuert?			X			
09002	Wenn ja, werden die alten Dokumentationen zentral archiviert?			X			
09003	Wenn ja, sind die neusten Dokumentation für alle Mitarbeiter zugänglich?			X			

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
M 02.202	*Erstellung eines Handbuches zur IT-Sicherheit*	1		X			Im Laufe des IT-Sicherheitsprozesses werden nicht nur die in den vorstehenden Maßnahmen erwähnten Dokumente produziert, sondern in der Umsetzungsphase entstehen weitere Regelungen für sämtliche oder für spezielle Arbeitsplätze. Es werden Verhaltensregen oder Handlungsanleitungen formuliert, die jedem Mitarbeiter als Basis für seine Handlungen oder Unterlassungen am Arbeitsplatz zur Verfügung stehen müssen. Es ist daher Aufgabe der Organisation, diese Regelungen zusammenzutragen und in geeigneter Form der jeweiligen Zielgruppe an die Hand zu geben. Während die Dokumentation des IT-Sicherheitsprozesses ein wesentliches Arbeitsmittel für das IT-Sicherheitsmangement-Team ist, dient das Handbuch der IT-Sicherheitsorganisation als Leitfaden für alle vom IT-Sicherheitsprozess betroffenen Mitarbeiter. In der Praxis werden Teile dieser Handreichung unter Bezeichnungen wie "PC-Richtlinie" oder "IT-Benutzerrichtlinie" verwendet. Es gilt, für die verschiedenen Zielgruppen innerhalb der Organisiation zu unterschiedlichen Regelungen zu kommen, die sich an den gleichen Leitaussagen orientieren, daneben aber auch speziell auf Rechte und Pflichen aus der jeweiligen Funktion eingehen. So entstehen Regelwerke, in denen Aufgaben und Verantwortlichkeiten für unterschiedliche Zielgruppen zu beschreiben sind.
01000	Existiert ein Handbuch der IT-Sicherheitsorganisation als Leitfaden für alle vom IT-Sicherheitsprozess betroffenen Mitarbeiter?				X		
01001	Wenn ja, sind in dem Handbuch der IT-Sicherheitsorganisation die Verhaltensregeln oder Handlungsanleitungen für alle Arbeitsplätze formuliert worden?				X		
B 99.992	**Organisation**	1					
M 02.001	*Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz*	1		X			Für den "IT-Einsatz" ist eine Festlegung der Fachverantwortung und der Betriebsverantwortung vorzunehmen. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben, die es in einem IT-Verfahren umzusetzen gilt.
02002	Wenn ja, wird diese Bekanntgabe dokumentiert ?				X		Es empfiehlt sich, die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen. Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Mißverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu verhindern.
M 02.006	*Vergabe von Zutrittsberechtigungen für Räume*	1		X			

Nr.		Prio	ja	Entbehrlich	nein	Nicht zutreffend	Bemerkungen
02000	Ist festgelegt, welche Personen zur Ausübung der wahrzunehmenden Funktionen welches Zutrittsrecht benötigen?			X			Es ist festzulegen, welche Person zur Ausübung der wahrgenommenen Funktion welches Zutrittsrecht benötigt. Dabei ist die vorher erarbeitete Funktionstrennung zu beachten. Unnötige Zutrittsrechte sind zu vermeiden. Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte auch beim IT-Einsatz der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z. B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern den unerlaubten Zugriff eines Wartungstechnikers auf die Datenträger.
02001	Wenn ja, ist die Zutrittsberechtigung schutzbedürftiger Räume dokumentiert ?			X			Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muss die Rücknahme des Zutrittsmittels gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten.
02004	Wenn ja, wird der Zutritt zu schutzbedürftigen Räumen von nichtautorisierten Personen (z.B. Besucher) nur bei Anwesenheit und /oder Begleitung durch authorisierte Personen erlaubt ?			X			Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z. B. Besuchern) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.
M 02.007	*Vergabe von Zugangsberechtigungen für IT-Systeme*	1		X			
01001	Wenn ja, wurde bei der Vergabe von Zugangsberechtigungen auf Funktion und Funktionstrennung geachtet?						
01002	Wenn ja, werden personelle bzw. aufgabenbezogene Änderungen der Zugangsberechtigung unverzüglich berücksichtigt?			X			Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Anwender). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.
01003	Wenn ja, erfolgt der Zugang - sofern dv-technisch möglich - erst nach einer Identifikation (z.B. Name, User-ID, Chipkarte) und Authentisierung (z.B. Passwort) des Nutzungsberechtigten ?			X			Der Zugang soll - sofern DV-technisch möglich - erst nach einer Identifikation (z. B. durch Name, User-ID oder Chipkarte) und Authentisierung (z. B. durch ein Passwort) des Nutzungsberechtigten möglich sein und protokolliert werden.
01006	Wenn ja, gibt es Regelungen über die Handhabung von Zugangs- und Authentifikationsmittel ?			X			Die Ausgabe bzw. der Einzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentifikationsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung) müssen ebenfalls getroffen werden.
01007	Wenn ja, wird bei längerer Abwesenheit einer berechtigten Person, eine vorübergehende Sperre der Zugangsberechtigung durchgeführt ?				X		Die vorübergehende Sperrung einer Zugangsberechtigung sollte bei längerwährender Abwesenheit der berechtigten Person vorgenommen werden, um Missbräuche zu verhindern.
M 02.011	*Regelung des Paßwortgebrauchs*	1		X			

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
01003	Wenn ja, werden voreingestellte Passworte der Hersteller immer ersetzt ?			X			Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
M 02.017	*Zutrittsregelung und -kontrolle schutzbedürftiger Gebäudeteilen und Räume*	1		X			
01002	Wenn ja, ist die Zahl der Zutrittsberechtigten auf das notwendige Mindestmaß beschränkt ?			X			Die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können.
01003	Wenn ja, ist den berechtigten Personen untereinander die Zutrittsberechtigung bekannt (Fremde können so eindeutig identifiziert werden) ?			X			
02000	Wird der ungehinderte Zutritt (z.B. durch Schlösser, Kartenleser, etc.) verhindert ?						
03000	Gibt es Verhaltensregelungen über erkannte Berechtigungsüberschreitungen ?						
M 02.024	*Einführung eines PC-Checkheftes*	1					Um die durchgeführten IT-Sicherheitsmaßnahmen am PC zu dokumentieren, bietet es sich an, ein PC-Checkheft einzuführen.
01000	Existiert ein PC-Checkheft, um die IT-Sicherheitsmaßnahmen eines PC zu dokumentieren ?				X		
01001	Wenn ja, beinhaltet dieses Checkheft den Namen des PC-Benutzers?						
01002	Wenn ja, beinhaltet dieses Checkheft den Aufstellungsort des PC?						
01003	Wenn ja, beinhaltet dieses Checkheft die Beschreibung der Konfiguration?						
01004	Wenn ja, beinhaltet dieses Checkheft die Zugangsmittel?						
01005	Wenn ja, beinhaltet dieses Checkheft die eingesetzte Hard- und Software?						
01006	Wenn ja, beinhaltet dieses Checkheft durchgeführte Wartungen und Reparaturen?						
01007	Wenn ja, beinhaltet dieses Checkheft durchgeführte Viren-Kontrollen?						
01008	Wenn ja, beinhaltet dieses Checkheft durchgeführte Revisionen?						
01009	Wenn ja, beinhaltet dieses Checkheft Ansprechpartner für Problemfälle?						
M 02.026	*Ernennung eines Administrators und eines Vertreters*	1		X			
01002	Wenn ja, ist die Zuständigkeit so aufgeteilt, dass es nicht zu Lücken oder Überschneidungen kommt ?			X			Bei größeren Behörden bzw. Unternehmen mit einer Vielzahl verschiedener IT-Systeme und Teilnetzen muss außerdem sichergestellt sein, dass die Aufgaben zwischen den verschiedenen Administratoren so verteilt sind, dass es zu keinen Zuständigkeitsproblemen kommt, also weder zu Überschneidungen noch zu Lücken in der Aufgabenverteilung. Darüber hinaus sollte die Kommunikation zwischen den verschiedenen Administratoren möglichst reibungslos ablaufen. Hierzu können z. B. regelmäßige Administratoren-Treffen durchgeführt werden, bei denen typische Probleme und Lösungsmöglichkeiten bei der täglichen Arbeit thematisiert werden.

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
M 02.042	*Festlegung der möglichen Kommunikationspartner*	1					Sollen Informationen an einen Kommunikationspartner übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so soll für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat bzw. erhalten wird. Um die oben genannten Kriterien zu erfüllen, bedarf es einer Festlegung, welche Kommunikationspartner welche Informationen erhalten dürfen. Im Sinne des BDSG, Anlage zu § 9 Satz 1 (Übermittlungskontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenträgeraustausch erhalten können.
01000	Existiert eine Übersicht, mit welchen Kommunikationspartnern Daten ausgetauscht werden?				X		
01001	Wenn ja, ist bei Erstellung der Übersicht die Anlage zu § 9 des BDSG beachtet worden ?						
02000	Werden bei Austausch mit mehreren Partnern alle Beteiligten darüber informiert, wer die Daten erhalten hat?				X		
M 02.070	*Entwicklung eines Firewall-Konzeptes*	1		X			
01000	Liegt ein schriftlich fixiertes Firewall-Konzept vor?			X			
02000	Sind die Sicherheitsziele für den Einsatz einer Firewall formuliert?			X			

Inhalt	Pro	ja	entb.	nein	nicht zutref.	Bemerkungen
M 02.071 Festlegung einer Sicherheitspolitik für eine Firewall	1		X			Neben der sorgfältigen Aufstellung und Umsetzung der Filterregeln sind darüber hinaus folgende organisatorische Regelungen erforderlich: - Es müssen Verantwortliche sowohl für das Aufstellen als auch für die Umsetzung und das Testen der Filterregeln benannt werden. Es muss geklärt werden, wer befugt ist, die Filterregeln z. B. für Tests neuer Dienste zu verändern. - Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen. - Die Benutzer müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung umfassend informiert werden. - Angriffe auf die Firewall sollten nicht nur erfolgreich verhindert, sondern auch frühzeitig erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Die Firewall sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z. B. häufigen fehlerhaften Passworteingaben auf einem Application-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen. - Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z. B. der Angreifer verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt und die entsprechenden Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.
01003 Wenn ja, existieren organisatorische Regelungen über Reaktionen auf einen erkannten Angriff?				X		
04000 Wurde eine Risikoabschätzung für den Fall, dass die Firewall überwunden wird, durchgeführt?			X			
M 02.118 Festlegung einer Sicherheitspolitik für E-Mail Nutzung	1		X			E-Mails, die intern versandt werden, dürfen das interne Netz nicht verlassen. Dies ist durch die entsprechenden administrativen Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das Internet erfolgen. Grundsätzlich sollten Nachrichten, die an interne Adressen verschickt wurden, nicht an externe Adressen weitergeleitet werden. Sollen hiervon Ausnahmen gemacht werden, sind alle Mitarbeiter darüber zu informieren. Beispielsweise kann für Außendienstmitarbeiter oder andere Mitarbeiter, die viel unterwegs sind, die E-Mails an externe Zugriffspunkte weitergeleitet werden.

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
01004	Wenn ja, ist darin beschrieben, welche Handbücher beschafft werden?						
01005	Wenn ja, ist darin beschrieben, wie die Benutzer geschult werden?					X	nicht zutreffend
01006	Wenn ja, ist darin geregelt, wie jederzeit technische Hilfestellung für die Benutzer gewährleistet wird?					X	nicht zutreffend
03000	Ist sichergestellt, dass interne E-Mails das interne Netz auch nicht verlassen?				X		organisatorisch: JA
04000	Ist sichergestellt, dass interne E-Mails nicht an externe Adressen weitergeleitet werden (z.B. Weiterleitung von E-Mails an Außendienstarbeiter an externe Zugriffspunkte)?					X	nicht zutreffend; organisatorisch: JA
M 02.119	*Regelung für den Einsatz von E-Mail*	1		X			Sollen zwischen zwei oder mehreren Kommunikationspartnern Daten elektronisch ausgetauscht werden, so müssen diese zum ordnungsgemäßen Austausch folgende Punkte beachten: - Die Adressierung von E-Mail muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Innerhalb einer Organisation sollten Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Durch den Versand von Testnachrichten an neue E-Mailadressen ist die korrekte Zustellung von Nachrichten zu prüfen. - Wenn eine E-Mail an mehrere Empfänger geschickt wird, sollten hierfür nicht der "CC"-Eintrag benutzt werden, da hierdurch jeder Empfänger die komplette Empfängerliste sehen kann. Stattdessen sollten Verteilerlisten oder die "BCC"-Option benutzt werden. BCC steht für Blind Carbon Copy; hier eingetragene weitere Empfänger werden den anderen Empfänger nicht angezeigt.
01001	Wenn ja, ist darin enthalten, dass die Adressierung eindeutig erfolgen muss und durch Testmails an neue E-Mail-Adressen die korrekte Zustellung von Nachrichten zu prüfen ist?				X		
01002	Wenn ja, ist darin enthalten, dass bei Versand einer E-Mail an mehrere Empfänger nicht der "CC" Eintrag zu nutzen ist, sondern Verteilerlisten bzw. die "BCC"-Option?				X		
01004	Wenn ja, ist darin enthalten, dass die Betreffangabe sinnvoll genutzt werden soll?					X	nicht zutreffend; BO
01005	Wenn ja, ist darin enthalten, dass die korrekte Übertragung durch den Empfänger bestätigt werden soll?					X	nicht zutreffend, BO
01007	Wenn ja, ist darin enthalten, dass bei einem Datei-Anhang wesentliche Informationen dazu zusätzlich übermittelt werden sollen (z.B. Art der Datei)?					X	nicht zutreffend, BO
01008	Wenn ja, ist darin ein Hinweis enthalten, dass ein Passwort bzw. ein Schlüssel für eine geschützte Information NICHT in das E-Mail geschrieben wird?					X	nicht zutreffend, BO
01009	Wenn ja, sind die Regelungen und Bedienungshinweise zum Einsatz von E-Mail schriftlich fixiert?					X	nicht zutreffend, BO
01010	Wenn ja, stehen sie dem Mitarbeitern jederzeit zur Verfügung?					X	nicht zutreffend, BO
02000	Sind die Benutzer darüber informiert, dass sie mehrmals täglich den Eingang neuer E-Mails zu überprüfen haben?					X	nicht zutreffend, BO

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
04000	Werden die Benutzer vor dem Einsatz von E-Mail geschult und für die einzuhaltenden Sicherheitsmaßnahmen sensibilisiert?					X	nicht zutreffend, BO
05000	Sind die Mitarbeiter über potentielles Fehlverhalten informiert (z.B. Teilnahme an E-Mail-Kettenbriefen)?					X	nicht zutreffend, BO
M 02.154	*Erstellung eines Computer-Virenschutzkonzepts*	1		X			Zur Sensibilisierung und besseren Verständnis über Sinn und Zweck, sollten allen IT-Benutzern das Computer-Virenschutzkonzept bekannt gegeben werden.
01001	Wenn ja, ist dieses Computer-Virenschutzkonzept allen IT-Benutzern bekannt?			X			
01002	Wenn ja, kennt jeder IT-Benutzer seinen Ansprechpartner für die Umsetzung bzw. Einhaltung des Computer-Virenschutzkonzepts?					X	nicht bekannt
M 02.158	*Meldung von Computer-Virusinfektionen*	1		X			Für einen Überblick über die aktuelle Bedrohungslage durch Computer-Viren führt das BSI eine Statistik über alle aufgetretenen Viren-Infektionen. Dazu wurde ein Virus-Meldebogen herausgegeben, mit dem ein Viren-Vorfall erfasst wird. Diese Virus-Meldung wird vom BSI nur zu statistischen Zwecken verwendet; sie kann auch anonym abgegeben werden
01001	Wenn ja, ist dieser Ansprechpartner jedem IT-Benutzer bekannt?					X	TelNr. 20000
01004	Wenn ja, gibt der Verantwortliche im Bedarfsfall eine Aktualisierung der Computer-Viren-Suchprogramme an alle Benutzer?					X	nicht zutreffend
01005	Wenn ja, veranlaßt der Verantwortliche im Bedarfsfall eine Alarmierung der Betroffenen?					X	nicht zutreffend
02000	Werden bei einer Virusinfektion auch alle betroffenen "Externen" (diejenigen die den mutmaßlichen Virus weitergegeben oder erhalten haben) über das Problem informiert?					X	nicht zutreffend
03000	Werden alle Infektionen mit Computer-Viren dokumentiert?				X		
04000	Werden alle Auswirkungen, die durch Computer-Viren verursacht wurden, dokumentiert?				X		
05000	Werden alle Aufwendungen zur Beseitigung von Computer-Viren dokumentiert?				X		
M 02.160	*Regelungen zum Computer-Virenschutz*	1		X			Auf IT-Systemen, auf denen kein residentes Computer-Viren-Suchprogramm installiert worden ist, sind ersatzweise ein regelmäßiger Einsatz eines Computer-Viren-Suchprogramms, eine Virenkontrolle bei Datenträgeraustausch und Datenübertragung sowie eine Makro-Virenprüfung bei eingehenden Dateien festzulegen, um eine rasche Erkennung und Verhinderung der Weiterverbreitung von Computer-Viren sicherzustellen
01001	Wenn ja, wurde diese Regelung dokumentiert?						
01002	Wenn ja, ist darin enthalten wie die eingesetzten Computer-Viren-Suchprogramme aktualisiert werden?						
01003	Wenn ja, ist darin enthalten in welchen Zeitabständen die Computer-Viren-Suchprogramme aktualisiert werden?						
01004	Wenn ja, ist darin enthalten durch wen die Computer-Viren-Suchprogramme aktualisiert werden?						

Index	Prüfaussage	ja	nein	entbehrlich	zurück	Bemerkungen
01005	Wenn ja, wurden die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Computer-Virenschutz für den Ansprechpartner für Computer-Viren geregelt?					
01006	Wenn ja, wurden die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Computer-Virenschutz für den Administrator von Netzservern geregelt?					
01007	Wenn ja, wurden die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Computer-Virenschutz für den IT-Benutzer von Endgeräten geregelt?					
01008	Wenn ja, wurden die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Computer-Virenschutz für das IT-Sicherheitsmanagement geregelt?					
02001	Wenn ja, beinhaltet dies Gefahren durch Computer-Viren, Makro-Viren, Trojanische Pferde und Hoax?					
02002	Wenn ja, beinhaltet dies die notwendigen IT-Sicherheitsmaßnahmen?					
02003	Wenn ja, beinhaltet dies Verhaltensweise beim Auftreten von Computer-Viren?					
02004	Wenn ja, beinhaltet dies den Umgang mit dem eingesetzten Computer-Viren-Suchprogramm?					
03001	Wenn ja, gibt es eine Regelung bzgl. regelmäßiger Prüfungen auf Einhaltung dieses Verbots?					
05000	Wurde für jeden vorhandenen Rechnertyp eine Notfalldiskette angelegt?				X	nicht zutreffend
06000	Wird regelmäßig eine Datensicherung angelegt?				X	nicht zutreffend
06001	Wenn ja, wird bei dieser Datensicherung darauf geachtet, dass kein Computer-Virus mit aufgespielt wird?					
07000	Wurde darauf geachtet, dass keine IT-Systeme zum Einsatz kommen, auf denen kein residentes Computer-Viren-Suchprogramm installiert worden ist?		X			
07001	Falls doch, werden diese IT-Systeme regelmäßig auf Computer-Viren untersucht?		X			
07002	Falls doch, findet eine Virenkontrolle bei Datenträgeraustausch und Datenübertragung statt?		X			
07003	Falls doch, findet eine Makro-Virenprüfung bei eingehenden Dateien statt?		X			
08000	Wurde geregelt, wie bei Auftreten eines Computer-Virus zu verfahren ist?		X			
08001	Wenn ja, wurde geregelt, an wen ein entdeckter Computer-Virus unverzüglich zu melden ist?					
08002	Wenn ja, gibt es eine Regelung über die Form der Meldung entdeckter Computer-Viren?					
08003	Wenn ja, gibt es eine Regelung über den Übermittlungsweg entdeckter Computer-Viren?					
09002	Wenn ja, wurden diese Regelungen den Betroffenen zur Kenntnis gegeben?					
09003	Wenn ja, werden diese Regelungen sporadisch auf Einhaltung überprüft?					
09004	Wenn ja, werden diese Änderungen dokumentiert?					

Inhalt	Pro	ja	teilw.	nein	Nicht zutref.	Bemerkungen
M 02.173 Festlegung einer WWW-Sicherheitsstrategie	1		X			WWW-Server sind für einen Hacker sehr attraktive Ziele, da einem erfolgreichen Angriff oft sehr große Publizität zuteil wird. Daher muss der Absicherung eines WWW-Servers ein hoher Stellenwert eingeräumt werden. Vor dem Einrichten eines WWW-Servers sollte in einer WWW-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der WWW-Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind. In der WWW-Sicherheitsstrategie muss neben einer Sicherheitsstrategie für den Betrieb eines WWW-Servers auch eine Sicherheitsstrategie für die WWW-Nutzung enthalten sein. In der Sicherheitsstrategie für den Betrieb eines WWW-Servers sollten die folgenden Fragen beantwortet werden: - Wer darf welche Informationen einstellen? - Welche Randbedingungen sind beim Betrieb eines WWW-Servers zu beachten? - Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen? - Welche Dateien dürfen aufgrund ihres Inhaltes nicht auf dem WWW-Server eingestellt werden (z. B. weil die Inhalte vertraulich sind, nicht zur Veröffentlichung geeignet sind oder nicht der Firmen- bzw. Behördenpolitik entsprechen)? - Welche Zugriffsbeschränkungen auf den WWW-Server sollen realisiert werden (siehe auch M 2.175 Aufbau eines WWW-Servers)? Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potentielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. Neben den in M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems angesprochenen Informationsquellen ist für Sicherheitshinweise zur WWW-Nutzung besonderes die "World Wide Web Security FAQ" eine wertvolle Quelle. Die Master-Kopie dieses Dokumentes ist unter http://www.w3.org/Security/Faq/ zu finden. In der Sicherheitsstrategie für die WWW-Nutzung sollten die folgenden Fragen beantwortet werden: - Wer erhält WWW-Zugang? - Welche Randbedingungen sind bei der WWW-Nutzung zu beachten? - Wie werden die Benutzer geschult? - Wie wird technische Hilfestellung für die Benutzer gewährleistet? Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zu gewährleisten:

Inhalt		Prio	ja	teilw.	nein	n.zutreff.	Bemerkungen
01000	Existiert eine WWW-Sicherheitsstrategie bzw. -Leitlinie, in der beschrieben wird, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind?			X			
01001	Wenn ja, ist darin auch eine Sicherheitsstrategie für die WWW-Nutzung enthalten?						
01002	Wenn ja, wird darin behandelt, wer welche Informationen einstellen darf?					X	nicht zutreffend; BO
01003	Wenn ja, wird darin behandelt, welche Randbedingungen beim Betrieb eines WWW-Servers zu beachten sind?				X		
01004	Wenn ja, wird darin behandelt, wie die Verantwortlichen geschult werden, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen?				X		
01005	Wenn ja, wird darin behandelt, welche Dateien aufgrund ihres Inhaltes nicht auf dem WWW-Server eingestellt werden dürfen?					X	nicht zutreffend; BO
01006	Wenn ja, wird darin behandelt, welche Zugriffsbeschränkungen auf den WWW-Server realisiert werden sollen?						
01009	Wenn ja, wird darin behandelt, wie die Benutzer geschult werden?					X	nicht zutreffend, BO
02000	Werden regelmäßig Informationen über potentielle Sicherheitslücken beschafft?			X			
03000	Werden die Browser der Benutzer durch den Administrator so vorkonfiguriert, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann?				X		
04000	Wurde festgelegt, welche Inhalte auf dem WWW-Server aufgerufen werden dürfen bzw. welche Dateien nicht aufgerufen werden dürfen (z. B. Dateien, deren Inhalt Anstoß erregen könnte etc.)?						
07000	Wurden die WWW-Benutzer sowohl hinsichtlich der Nutzung ihrer WWW-Browser als auch des Internets geschult?					X	nicht zutreffend, SAS

Inhalt	Pro	Erfüllt ja	teilw.	nein	N/A zutreff.	Bemerkungen
M 02.182 Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen	1					Im IT-Grundschutzhandbuch werden eine Vielzahl von Regelungen vorgestellt, die für die Erreichung der angestrebten IT-Sicherheit notwendig sind. Es ist aber nicht ausreichend, diese Regelungen bekannt zu geben, es muss auch regelmäßig deren Einhaltung kontrolliert werden. Regelmäßig heißt hierbei aber nicht, dass die Kontrollen an vorhersagbaren Terminen stattfinden, da angekündigte Kontrollen meist ein verzerrtes Bild des Untersuchungsgegenstands ergeben. Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz von Kontrollen ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen nicht den Charakter von Schulmeisterei haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten. Wenn Mitarbeiter eine Regelung ignorieren oder umgehen, ist das meist ein Zeichen dafür, dass diese nicht mit den Arbeitsabläufen vereinbar ist oder durch die Mitarbeiter nicht umgesetzt werden kann. Beispielsweise ist eine Anweisung, vertrauliche Schreiben nicht unbeaufsichtigt am Drucker liegen zu lassen, unsinnig, wenn zum Drucken nur ein weit entfernter Netzdrucker zur Verfügung steht. Wenn bei Kontrollen Mängel festgestellt werden, kommt es nicht darauf an, nur die Symptome zu beseitigen. Vielmehr ist es wichtig, die Ursachen für diese Probleme festzustellen und Lösungen aufzuzeigen. Diese können beispielsweise in der Änderung bestehender Regelungen oder in der Hinzunahme technischer Maßnahmen bestehen. Kontrollen sollen helfen, Fehlerquellen abzustellen. Es ist für die Akzeptanz von Kontrollen extrem wichtig, dass dabei keine Personen bloßgestellt werden oder als "Schuldige" identifiziert werden. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.
01000 Werden die Sicherheitsregelungen im Unternehmen regelmäßig unangekündigt auf deren Einhaltung kontrolliert?						
01001 Wenn ja, zielen die Kontrollen darauf ab, dass Mängel beseitigt werden?						
01002 Wenn ja, werden diese Kontrollen von allen Mitarbeitern akzeptiert?						
01003 Wenn ja, wird während den Kontrollen mit den Mitarbeitern über mögliche Problemlösungen gesprochen?						
02000 Wird versucht, beim Auftreten von Problemen der Ursache auf den Grund zu gehen?						
B 99.993 Personal	1					

Index		Prio	ja	entbl. teilw.	nein	nicht zutr.	Bemerkungen
M 03.001	*Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*	1		X			Neuen Mitarbeitern müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner bzgl. IT-Sicherheit nicht, sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik die Behörde bzw. das Unternehmen betreibt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen. Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu. Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen: - Planung der notwendigen Schulungen; arbeitsplatzbezogene Schulungsmaßnahmen, - Vorstellung aller Ansprechpartner, insbesondere zu IT-Sicherheitsfragen, - Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit. Hilfreich zur Durchführung der Einarbeitung ist ein Laufzettel oder eine Checkliste, aus der die einzelnen Aktivitäten und der erreichte Stand der Einarbeitung ersichtlich sind.
05000	Werden einem neuen Mitarbeiter alle Ansprechpartner für IT-Sicherheitsfragen vorgestellt?			X			Vorstellung aller Ansprechpartner, insbesondere zu IT-Sicherheitsfragen
06000	Werden einem neuen Mitarbeiter die hausinternen Regelungen und Vorschriften zur IT-Sicherheit erläutert?			X			Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit.
M 03.002	*Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*	1		X			Bei der Einstellung von Mitarbeitern sollen diese verpflichtet werden, einschlägige Gesetze (z. B. § 5 BDSG "Datengeheimnis"), Vorschriften und interne Regelungen einzuhalten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme vorzuhalten. Alle Mitarbeiter sollten insbesondere darauf hingewiesen werden, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind.
01000	Wird ein neuer Mitarbeiter bei seiner Einstellung dazu verpflichtet einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten?						
02000	Werden einem neuen Mitarbeiter die entsprechenden Unterlagen über einschlägige Gesetze, Vorschriften und interne Regelungen zur Einsicht oder zum Verbleib ausgehändigt?			X			Es ist sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme vorzuhalten.

Nr.		Prio	ja	entbehrlich	nein	nicht zutref.	Bemerkungen
03000	Wird ein neuer Mitarbeiter darüber aufgeklärt, welcher rechtliche Rahmen seine Tätigkeit bestimmt?			X			Alle Mitarbeiter sollten insbesondere darauf hingewiesen werden, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind.
M 03.005	*Schulung zu IT-Sicherheitsmaßnahmen*	1		X			Die überwiegende Zahl von Schäden im IT-jeder einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die ein Verständnis für die IT-Sicherheitsmaßnahmen wecken. Insbesondere sollen folgende Themen in der Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden: - Sensibilisierung für IT-Sicherheit - Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen - Die produktbezogenen IT-Sicherheitsmaßnahmen - Das Verhalten bei Auftreten eines Computer-Virus auf einem PC - Der richtige Einsatz von Passwörtern - Die Bedeutung der Datensicherung und deren Durchführung - Der Umgang mit personenbezogenen Daten - Die Einweisung in Notfallmaßnahmen - Vorbeugung gegen Social Engineering Bei der Durchführung von Schulungen sollte immer beachtet werden, dass es nicht reicht, einen Mitarbeiter einmal während seines gesamten Arbeitsverhältnisses zu schulen. Für nahezu alle Formen von Schulungen, insbesondere Front-Desk-Schulungen, gilt, dass sehr viele neue Informationen auf die Teilnehmer einstürzen. Diese gelangen nur zu einem kleinen Teil ins Langzeitgedächtnis, 80% sind meist schon bei Schulungsende wieder vergessen. Daher sollten Mitarbeiter immer wieder zu Themen der IT-Sicherheit geschult bzw. sensibilisiert werden. Dies kann beispielsweise - in kürzeren Veranstaltungen zu aktuellen IT-Sicherheitsthemen, - im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen, oder - durch interaktive Schulungsprogramme, die allen Mitarbeitern zur verfügung stehen, erfolgen.
01003	Wenn ja, werden diese Sensibilisierungsmaßnahmen in regelmäßigen Zeitabständen wiederholt?				X		erfolgt aufgabenbezogen - Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z. B. in der Hauspost.
02001	Wenn ja, wird den Mitarbeitern gezeigt, wie man einen Computer-Virsubefall erkennt?				X		Es soll den Mitarbeitern vermittelt werden, woran das Auftreten eines Computer-Virus zu erkennen ist und wie mit Computer-Viren umzugehen ist
02002	Wenn ja, wird den Mitarbeitern die Wirkungsweise und Arten von Computer-Viren aufgezeigt?			X			

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
02004	Wenn ja, wird den Mitarbeitern Maßnahmen zur Eliminierung eine Computer-Virus gezeigt?				X		
05000	Werden Mitarbeiter, die mit personenbezogenen Daten arbeiten müssen, über die gesetzlich erforderlichen Sicherheitsmaßnahmen geschult? (z.B. Auskunftsersuchen, Änderungs- und Verbesserungswünsche der Betroffenen, gesetzlich vorgeschriebene Löschfristen, Schutz der Vertraulichkeit und die Übermittlung der Daten)			X			
07000	Werden alle Mitarbeiter auf die Gefahr des Social Engineering hingewiesen?				X		
07001	Wenn ja, werden alle Mitarbeiter regelmäßig darauf hingewiesen, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben? (Social Enginieering)				X		
07002	Wenn ja, werden alle Mitarbeiter über die typischen Muster des Social Engineering, über gezieltes Aushorchen um an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, aufgeklärt?				X		
08000	Werden die Mitarbeiter regelmäßig zu den Themen bzgl. IT-Sicherheitsmaßnahmen geschult?				X		
08001	Decken die Inhalte der Schulungsmaßnahmen die erforderlichen Gebiete ab?				X		
09000	Werden neue Mitarbeiter entsprechend in die IT-Sicherheitsmaßnahmen eingewiesen?						

Inhalt	Prio	ja	teilweise	nein	nicht zutref.	Bemerkungen
M 03.006 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	1		X			Scheidet ein Mitarbeiter aus, so ist zu beachten: - Vor dem Ausscheiden ist eine Einweisung des Nachfolgers durchzuführen. - Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT?Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen. - Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT?System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern. - Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen. - Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren. - Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über das Ausscheiden des Mitarbeiters zu unterrichten. - Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren. - Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden. Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.
02000 Wird vor Ausscheiden eines Mitarbeiters eine Einweisung des Nachfolgers durchgeführt?		X				
04000 Werden sämtliche für den Ausscheidenden eingerichtete Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht?		X				
06000 Wird vor Verabschiedung des ausscheidenden Mitarbeiters explizit auf die weiterhin in Kraft bleibende Verschwiegensheitserklärungen hingewiesen?		X				
07000 Wird vor Verabschiedung des ausscheidenden Mitarbeiters explizit darauf hingewiesen, dass keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen?		X				

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
09000	Werden sämtliche mit Sicherheitsaufgaben betrauten Personen (auch der Pförtnerdienst) über das Ausscheiden des Mitarbeiters unterrichtet?				X		
M 03.010	*Auswahl eines vertrauenswürdigen Administrators und Vertreters*	1		X			
01000	Wird der IT-Administrator regelmäßig darüber belehrt, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen?				X		Den IT-System- oder TK-Anlagen-Administratoren und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.
M 03.013	*Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen*	1					Die Mitarbeiter müssen über die mit dem Benutzen einer digitalen TK-Anlage verbundenen Gefährdungen informiert werden. Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein abnormes Verhalten der TK-Anlage gemeldet werden soll. Bei Manipulationen an der TK-Anlage sollte eine unabhängige Kontrollinstanz wie IT-Sicherheitsmanagement oder Datenschutzbeauftragte informiert werden.
01000	Werden die Mitarbeiter bzgl. der Gefährdungspotentiale bei der Benutzung der TK-Anlage informiert (z.B. Merkblätter, Unterweisung etc.)?						
02000	Wissen die Mitarbeiter, was bei einem abnormalen Verhalten der TK-Anlage zu machen ist?						
M 03.014	*Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches*	1		X			Mangelnde Information und Einweisung der Mitarbeiter führt in vielen Fällen dazu, dass Restriktionen der Informationsweitergabe nicht oder nur unzulänglich eingehalten werden. Die Festlegungen, welchen Kommunikationspartnern wann welche Daten übermittelt werden dürfen (M 2.42 Festlegung der möglichen Kommunikationspartner), ist den an einem Datenträgeraustausch Beteiligten daher zwingend bekannt zu geben. Außerdem sind die prinzipiellen Schritte für den Ablauf eines Datenträgeraustausches zu fixieren (eventuell als Dienstanweisung) und die Mitarbeiter zur Einhaltung zu verpflichten. Zusätzlich ist eine Sensibilisierung der am Datenträgeraustausch beteiligten Mitarbeiter hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen vor, während und nach dem Transport der Datenträger notwendig. Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung oder Checksummen-Verfahren), so sind diese Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

Inhalt		Prio.	Erfüllt ja	Erfüllt teilw.	Erfüllt nein	Nicht zutreff.	Bemerkungen
01000	Weiß jeder Mitarbeiter darüber Bescheid, welchen Kommunikationspartnern wann welche Daten übermittelt werden dürfen?						
02000	Wurden die prinzipiellen Schritte für den Ablauf eines Datenträgeraustausches fixiert (z.B. Dienstanweisung etc.)?						
02001	Wenn ja, werden die Mitarbeiter zur Einhaltung der Schritte für den Ablauf eines Datenträgeraustausches verpflichtet?						
03000	Haben die Mitarbeiter genügend Wissen bzw. Kenntnisse über mögliche Gefährdungen und einzuhaltenden Sicherheitsmaßnahmen vor, während und nach dem Transport der Datenträger?						
04000	Falls IT-gestützte Verfahren zum Schutz der Daten eingesetzt werden (Verschlüsselung, Checksummen-Verfahren), wurden dann die Mitarbeiter in diese Verfahren ausreichend eingearbeitet?						
M 03.015	*Informationen für alle Mitarbeiter über die Faxnutzung*	1		X			Alle Mitarbeiter sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen sowie darüber zu informieren, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Bei Verwendung herkömmlicher Faxgeräte sollte eine verständliche Bedienungsanleitung am Faxgerät zur Verfügung stehen. Beim Einsatz eines Faxservers sollten die Benutzer mindestens eine Kurzreferenz zur eingesetzten Faxclient-Software erhalten. Insbesondere ist, ggf. in Form einer Dienstanweisung, festzulegen, - wer der Fax-Verantwortliche ist und damit für die manuelle Verteilung eingehender Faxsendungen und als Ansprechpartner in Fax-Problemfällen zuständig ist, - wer das Faxgerät bzw. den Faxserver benutzen darf, - dass das Versenden von vertraulichen Informationen per Fax vermieden werden sollte, - dass ein einheitliches Faxvorblatt benutzt werden soll, - dass sich vor Austausch schutzbedürftiger Informationen über FaxVersand Empfänger und Absender hierüber telefonisch verständigen, - dass ggf. Einzelsendenachweise bzw. Übertragungsprotokolle für die korrekte Übertragung zu kontrollieren und diese den Unterlagen beizufügen und ggf. zu archivieren sind, - dass beim Einsatz eines Faxservers mit automatischer Eingangs-Fax-Verteilung für die Akten ein Ausdruck von Eingangs-Faxsendungen zu fertigen ist bzw. diese elektronisch zu archivieren sind, - dass bei Ausgangsfaxen, die über einen Faxserver versendet werden, für die Akten ein Ausdruck zu erstellen ist bzw. diese elektronisch zu archivieren sind, - dass die Adressbücher und Verteillisten regelmäßig kontrolliert werden, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden.
01000	Wurden die Mitarbeiter bzgl. der eingeschränkten Rechtsverbindlichkeit einer Faxsendung informiert?				X		

Inhalt	Frage	Ja	Entbehrlich	Nein	Nicht geprüft	Bemerkungen
02000	Falls ein Faxserver eingesetzt wird, wurden die Mitarbeiter über die eingesetzte Faxclient-Software eingewiesen?					
06000	Wurde festgelegt, dass ein einheitliches Faxvorblatt benutzt werden soll?					
07000	Wurde festgelegt, dass sich vor Austausch schutzbedürftiger Informationen über Faxversand Empfänger und Absender hierüber telefonisch verständigen?		X			
08000	Wurde festgelegt, ob gegebenenfalls zur Überprüfung der korrekten Übertragung Einzelsendenachweise bzw. Übertragungsprotokolle zu kontrollieren, den Unterlagen beizufügen und ggf. zu archivieren sind?			X		
09000	Wurde festgelegt, dass beim Einsatz eines Faxservers mit automatischer Eingangs-Fax-Verteilung für die Akten ein Ausdruck von Eingangs-Faxsendungen zu fertigen ist bzw. diese elektronisch zu archivieren sind?			X		
10000	Wurde festgelegt, dass bei Ausgangsfaxen, die über einen Faxserver versendet werden, für die Akten ein Ausdruck zu erstellen ist bzw. diese elektronisch zu archivieren sind?			X		
11000	Wurde festgelegt, dass die Adressbücher und Verteillisten regelmäßig kontrolliert werden, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden?		X			

ENDE IT-Verbund

Filterbedingungen für diese Liste:

Nicht zutreffende Maßnahmen ausblenden
Optionale Maßnahmen ausblenden
Erfüllte Maßnahmen ausblenden
Zusatzfragen ausblenden