HSW LUZERN

COMPETENCE CENTER
FORENSIK UND
WIRTSCHAFTSKRIMINALISTIK

Master of Advanced Studies Economic Crime Investigation (MAS ECI)

Ratgeber für Strafverfolgungsbehörden bei Abklärungen im IT-Umfeld

Gruppenarbeit

eingereicht am 13. Juni 2007 von

Christian de Raemy
Nicole Jerjen
Andreas Löwinger
Daniel Russenberger
Anita Tschopp

MAS ECI, Klasse 6

betreut von

Peter Cosandey (Tutor)

HSW LUZERN
CCFW
Zentralstrasse 9
CH—6002 Luzern

T: 041—228—41—70
F: 041—228—41—71
E: ccfw@hsw.fhz.ch
W: www.ccfw.ch

Inhaltsverzeichnis

2. Teil: Der Ratgeber

Literaturverzeichnis

Aepli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Zürich Basel Genf 2004. (zitiert: Aepli Michael)

BITKOM, Bundesamt für Informationswirtschaft, Kompass der IT Sicherheitsstandards, Leitfaden und Nachschlagewerk, Berlin-Mitte 2006. (zitiert: BITKOM)

BSI (2006), IT-Grundschutz-Kataloge, Version 2006, im Internet: „http://www.bsi.de“, abgerufen am 16. April 2007; Bonn 2006. (zitiert: BSI)

Dummer Stefan, Compliance durch Standrads für Informationssicherheit, Regendburg, 2006. (zitiert: Dummer Stefan)

Harris Shon (2003), CISSP Certification – Exam Guide, McGraw-Hill, Emeryville USA; 2003. (zitiert: Harris Shon)

Marfurt Konrad (2007), IT-Spurensuche, Skript MAS ECI, HSW Luzern; 2007. (zitiert: Marfurt Kurt)

Niggli Marcel A./**Riklin** F., www.unifr.ch/downloads/bt_skript/bt0t6/bt-skript_06_15.html. (zitiert: Niggli Marcel/Riklin F.)

Ochsenbein Andreas, Beweisbarkeit, Skript MAS ECI, HSW Luzern; 2007. (zitiert: Ochsenbein Andreas)

Pfefferli Peter W. (2005), Die Spur, Ratgeber für die spurenkundliche Praxis, 4. Auflage, Zürich / Heidelberg; 2005. (zitiert: Pfefferli Peter)

Riederer Carlos, Informationsicherheitsmanagement, Skript MAS ECI, HSW Luzern; 2007. (zitiert: Riederer Carlos)

Ryser Dominic, Internet-Recht und Strafrecht, Bern, 2005. (zitiert: Ryser Dominic)

Schmid Niklaus, Computer- sowie Check- und Kreditkarten-Kriminalität, Zürich, 1994. (zitiert: Schmid Niklaus)

Tuccillo Maurizio (2007), IT-Spurensuche / Einführung EnCase; Skript MAS ECI, HSW Luzern; 2007. (zitiert: Tuccillo Maurizio)

Trechsel, Stefan: Schweizerisches Strafgesetzbuch, Kurzkommentar, 2.Auflage, Zürich 1997.
(zitiert: Trechsel Stefan)

Abkürzungen siehe auch Glossar im Anhang I

Abs.	Absatz
Art.	Artikel
BankG	Bundesgesetz über die Banken und Sparkassen
bzw.	beziehungsweise
EDV	Elektronische Datenverarbeitung
IT	Informationstechnologie
i.V.m.	in Verbindung mit
lit.	littera
PC	Personal Computer
PDA	Personal Digital Assistant
TK	Telekommunikation
StGB	Schweizerisches Strafgesetzbuch
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte
WLAN	Wireless Local Area Network
Ziff.	Ziffer
z.B.	zum Beispiel

Kurzfassung

Der Umstand, dass wir heute in einer „digitalen“ Welt leben, hat dazu geführt, dass in den polizeilichen Kriminalstatistiken seit Jahren eine stetige Zunahme von Delikten der Computerkriminalität und von Strafdelikten mit IT-Bezug verzeichnet wird. Diese Entwicklung hat zu einer markanten Zunahme von Strafuntersuchungen mit IT-Bezug geführt und eine stetige Entwicklung der Computerforensik erforderlich gemacht.

Eine Umfrage in sieben Kantonen hat gezeigt, dass die Polizei die Zeichen der Zeit erkannt und auf die Zunahme der Strafuntersuchungen mit IT-Bezug reagiert hat. In allen Kantonen wird heute für IT-Ermittlungen Personal und eine gute technische Infrastruktur zur Verfügung gestellt. Die mit der IT-Ermittlung betrauten Polizisten sind für die Sicherstellung und Auswertung von digitalen Spuren zuhanden der Untersuchungsbehörden beziehungsweise der Staatsanwaltschaft zuständig. Zu diesem Zweck haben einige Polizeicorps aus ihren eigenen Reihen Polizisten im Bereich der Computerforensik ausbilden lassen, andere haben IT-Spezialisten für ihre IT-Ermittlungen eingestellt. Bei Bedarf wird in allen Kantonen auf externe Spezialisten aus dem Bereich der Computerforensik zurückgegriffen. Die Ergebnisse der polizeilichen IT-Ermittlungen werden in einem schriftlichen Bericht zuhanden der Untersuchungsbehörde beziehungsweise der Staatsanwaltschaft rapportiert.

Die Umfrage in den sieben Kantonen hat ergeben, dass an der Schnittstelle zwischen der jeweiligen Kantonspolizei und der Untersuchungsbehörde beziehungsweise der Staatsanwaltschaft eine gewisse Ineffizienz existiert, welche auf ein mangelndes IT-Knowhow auf Seiten der Untersuchungsbehörde beziehungsweise der Staatsanwaltschaft zurück zu führen ist. Der Kanton St. Gallen hat sich dieser Schnittstellenproblematik angenommen. Mit Hilfe von Richtlinien, Empfehlungen und Ausbildungsmassnahmen soll die Zusammenarbeit der Kantonspolizei und der Staatsanwaltschaft effizienter, einheitlicher und von besserer Qualität werden.

Die Untersuchungsrichter, Staatsanwälte und Richter wären heutzutage überfordert, ohne Hilfe von Spezialisten und Sachverständigen aus dem Bereich der Computerforensik in Straffällen mit IT-Bezug ein sachgemässes Urteil zu fällen. Umso erstaunlicher ist es, dass dem IT-Gutachten, dem Umgang des Richters mit IT-Gutachten und der richterlichen Beweiswürdigung von IT-Gutachten in Straffällen mit IT-Bezug sowohl in der juristischen Literatur als auch in der Rechtsprechung kaum Beachtung geschenkt wird. Diese Lücke ist zu schliessen.

Mit gezielten Umfeldabklärungen können die Ergebnisse eines IT-Gutachtens sowie die Beweise, auf die sich ein IT-Gutachten stützt, hinterfragt werden. Gezielte Umfeldabklärungen dienen bei Sachverhalten mit IT-Bezug dazu, die Zurechnung eines tatbestandsmässigen Verhaltens zu einer Person zu erleichtern, breit abgestützten Argumente für die Anklageerhebung zu finden oder zusätzliche Indizien und Beweise zu sammeln, welche die Ergebnisse eines IT-Gutachtens stützen.

Im Fokus solcher Umfeldabklärungen steht die Datenintegrität. Dabei geht es um die Frage, ob Daten makellos, unversehrt und nicht manipuliert sind. Da in den meisten Straffällen mit IT-Bezug die Datenintegrität in irgendeiner Weise verletzt wurde, lohnt es sich, im Rahmen eines Strafuntersuchungsverfahrens gezielte Fragen zur Datenintegrität zu stellen.

Anerkannte IT-Sicherheits-Standards geben umfassende Hinweise, was für Fragen zur Abklärung der Datenintegrität zu stellen sind. In der vorliegenden Arbeit wurden die IT-Grund-

schutz-Kataloge des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgewählt, da die vorgeschlagenen Massnahmen des BSI sehr konkret und anschaulich sind. Zudem sind die IT-Grundschutz-Kataloge international anerkannt und sowohl auf Deutsch als auch auf Englisch für jedermann frei über das Internet zugänglich. In den IT-Grundschutz-Katalogen des BSI werden jedoch 421 Gefährdungen und 954 Massnahmen bezüglich der Informationssicherheit diskutiert – eine zur Tätigung von Umfeldabklärungen im Rahmen eines Strafverfahrens nicht zu bewältigende Informationsmenge.

Im Rahmen der vorliegenden Arbeit wurde aus den 954 Massnahmen eine Checkliste mit den wichtigsten Fragen zum Thema der Datenintegrität ausgearbeitet. Bei der Checkliste wurde ein modularer Ansatz gewählt. Die Checkliste beinhaltet einerseits Fragen zur Computer-Basis, welche immer zu stellen sind, weil diese Fragen grundlegende Aspekte fokussieren, welche in der Regel bei jedem Computer zu beachten sind, und andererseits Fragen zu speziellen Modulen (Geschäftsarbeitsplatz, Heimarbeitsplatz, mobiler Einsatz, WLAN, Modem, Firewall/Router/Switch, Netzwerk-Komponenten-Basis, Datenbank/Anwendungsprogramm, Netzwerkanschluss), welche je nach den konkreten Gegebenheiten im Fall zu stellen sind. Jede Frage enthält eine Referenz zu den IT-Grundschutz-Katalogen vom BSI, wo im Bedarfsfall zusätzliche Informationen abgerufen werden können. Die Checkliste enthält zudem die wichtigsten Risiken hinsichtlich Datenintegrität.

Die Checkliste ist so aufgebaut, dass sie nach einem einfachen Muster bearbeitet werden kann. Zuerst werden die relevanten Bausteine festgelegt. Dann werden anhand dieser Bausteine die Fragen zur Computer-Basis, welche immer zu stellen sind, und diejenigen Fragen zu den festgelegten Bausteinen abgearbeitet. Falls eine Frage mit „nein“ beantwortet wird, ist zu prüfen, ob dieser Mangel für den konkreten Sachverhalt relevant ist.

Bei der Checkliste handelt es sich nicht um ein ausgefeiltes Expertensystem, welches dem Untersuchungsrichter oder Staatsanwalt nach Abarbeitung der Fragen die Täterschaft auf dem goldigen Tablett serviert. Vielmehr handelt es sich um ein Instrument, welches dem Untersuchungsrichter bei Straffällen mit IT-Bezug erlaubt, die richtigen Fragen zu stellen.

1. Teil: Der Hintergrund

1.1 Einleitung

Ergebnis der vorliegenden Arbeit ist eine Checkliste, die den Strafverfolgungsbehörden hilft, mit gezielten Fragen Umfeldabklärungen bei Strafuntersuchungen mit IT-Bezug vorzunehmen.

Im ersten Teil der Arbeit werden die Hintergründe, weshalb Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug überhaupt notwendig sind, dargelegt. Im zweiten Teil der Arbeit wird dargelegt, auf welchem Konzept und auf welchen Grundlagen die Checkliste basiert, wie die Checkliste aufgebaut ist, was sie beinhaltet und wie die Checkliste in der Praxis angewendet wird.

1.2 Die einzelnen Computertatbestände

Ausgangspunkt einer Strafuntersuchung sind in der Regel objektive Anhaltspunkte, die darauf hinweisen, dass eine bestimmte Person im Sinne des Schweizerischen Strafgesetzbuches oder eines Nebengesetzes tatbestandsmässig gehandelt hat. Unter Einhaltung der Regeln des Strafprozessrechts hat die Untersuchungsbehörde zu untersuchen, ob das fragliche Verhalten unter einen konkreten Tatbestand des Schweizerischen Strafgesetzbuches subsumiert werden kann. Wenn nicht, wird das Strafverfahren nach Abschluss der Untersuchung eingestellt, andernfalls, wenn ein tatbestandsmässiges Verhalten nachgewiesen wird, wird Anklage erhoben, falls das Verfahren nicht direkt mit dem Erlass einer Strafverfügung bzw. einem Strafbefehl abgeschlossen werden kann.

Die vorliegende Arbeit befasst sich ausschliesslich mit Fällen, in denen digitale Beweise bei der Untersuchung, ob ein tatbestandsmässiges Verhalten vorliegt, eine entscheidende Rolle spielen.

Eine entscheidende Rolle wird der digitale Beweis immer dann spielen, wenn es um die Aufklärung eines Computerdelikts im engeren Sinne geht. Dazu gehören die unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die Datenbeschädigung (Art. 144 ^{bis} StGB), der betrügerischen Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) und das Erschleichen von Computer-Leistungen (Art. 150 StGB).

Die Computertatbestände, welche nachfolgend kurz dargestellt wurden, wurden einzelnen Tatbeständen des bestehenden Strafrechts nachgebildet, nämlich die unbefugte Datenbeschaffung dem gemeinen Diebstahl im Sinne von Art. 139 StGB, das unbefugte Eindringen in ein Datenverarbeitungssystem dem Hausfriedensbruch im Sinne von Art. 186 StGB und die Datenbeschädigung der Sachbeschädigung im Sinne von Art. 144 StGB. Die Erschleichung einer Computer-Leistung wurde einfach als Tatbestandsvariante in den allgemeinen Straftatbestand des Erschleichens einer Leistung im Sinne von Art. 150 StGB aufgenommen.

1.2.1 Art. 143 StGB Unbefugte Datenbeschaffung

Unbefugte Datenbeschaffung im Sinne von Art. 143 StGB begeht, wer in Bereicherungsabsicht sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind. Im Rahmen der Strafuntersuchung ist dem mutmasslichen Täter demnach nachzuweisen, dass er über Daten verfügt, die nicht für ihn bestimmt sind und die er durch Überwinden von besonderen Sicherungsmassnahmen erlangt hat, beispielsweise durch Überwinden einer physischen Sicherung (Abschliessen etc.) oder einer logischen Sicherung (Passwort etc.). Wie weit die Daten gegen den unbefugten Zugriff des Täters geschützt sein müssen, ist nicht klar definiert. Gemäss Lehre genügen verkehrsüblichen Sicherungsmassnahmen.[1] Nebst dem Nachweis der objektiven Tatbestandsmerkmale ist dem mutmasslichen Täter weiter nachzuweisen, dass er sich die Daten mit Bereicherungsabsicht beschafft hat.

Bei der unbefugten Datenbeschaffung wird dem Inhalt der beschafften Daten keine Rechnung getragen. Dies hat zur Folge, dass ein Täter - je nach Inhalt der Daten - zusätzlich zur unbefugten Datenbeschaffung noch weitere Straftatbestände aus dem Schweizerischen Strafgesetzbuch oder aus Nebengesetzen erfüllt. Beispielsweise können zusammen mit Art. 143 StGB das Fabrikations- und Geschäftsgeheimnis gemäss Art. 162 StGB verletzt sein oder es kann eine Verletzung des wirtschaftlichen Nachrichtendienstes gemäss Art. 273 StGB vorliegen. Nebst Art. 143 StGB kann zudem eine Verletzung des Bankgeheimnis (Art. 47 BankG) gegeben sein oder es können wettbewerbsrechtliche (Art. 23 UWG) oder urheberrechtliche Bestimmungen (Art. 67 URG) verletzt worden sein.

Gemäss Art. 67 URG wird unter anderem auf Antrag bestraft, wer vorsätzlich und unrechtmässig ein Werk unter einer falschen Bezeichnung verwendet (lit. a), ein Werk veröffentlicht (lit. b), ändert (lit. c), zur Schaffung eines Werks aus zweiter Hand verwendet (lit. d), auf irgendeine Weise Werkexemplare herstellt (lit. e), solche anbietet, veräussert oder verbreitet (lit. f), ein Werk direkt oder indirekt vorträgt (lit. g), ein solches über Radio/TV oder sonst wie sendet (lit. h), ein gesendetes Werk wahrnehmbar macht (lit. i), sich weigert, der zuständigen Behörde die Herkunft der in seinem Besitz befindlichen, rechtswidrig hergestellten oder in Verkehr gebrachten Werkexemplare anzugeben (lit. k) oder ein Computerprogramm vermietet (lit. l). Art. 2 Abs. 1 URG definiert als Werke, unabhängig von Wert oder Zweck, geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben. Als Werke gelten gemäss Art. 2 Abs. 3 URG auch Computerprogramme.

Art. 23 UWG bestraft, wer vorsätzlich unlauteren Wettbewerb nach den Artikeln 3, 4, 5 oder 6 UWG begeht. Nach Art. 5 UWG handelt unlauter, wer ein ihm anvertrautes Arbeitsergebnis wie Offerten, Berechnungen oder Pläne unbefugt verwertet, ein Arbeitsergebnis eines Dritten, wie Offerten, Berechnungen oder Pläne, verwertet, obwohl er weiss oder annehmen muss, dass es ihm unbefugterweise überlassen oder zugänglich gemacht worden ist, oder das marktreife Arbeitsergebnis eines anderen ohne angemessenen eigenen Aufwand durch technische Reproduktionsverfahren übernimmt und verwertet. Unlauter handelt nach Art. 6 UWG insbesondere, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie unrechtmässig erfahren hat, verwertet oder anderen mitteilt. Geschäfts- und Fabrikationsgeheimnisse sind im Übrigen auch durch die Straftatbestände Art. 162 StGB (Verletzung des Geschäfts- und Fabrikationsgeheimnisses) und Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) geschützt.

[1] Niggli Marcel/Riklin F.

1.2.2 Art. 143 bis StGB Unbefugtes Eindringen in ein Datenverwaltungssystem

Wie bereits erwähnt ist beim „Datendiebstahl“ erforderlich, dass der Täter mit Bereicherungsabsicht handelt. Handelt der Täter ohne Bereicherungsabsicht, macht er sich nach Art. 143bis StGB strafbar. Bei Art. 143bis StGB handelt es sich um den so genannten „Hackertatbestand“. Nach Art. 143bis StGB ist zu bestrafen, wer ohne Bereicherungsabsicht auf dem Weg von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt. Eine Bestrafung gemäss Art. 143bis StGB setzt demzufolge voraus, dass dem mutmasslichen Täter im Rahmen der Strafuntersuchung nachgewiesen wird, dass er durch Überwinden einer Zugangssicherung (üblicherweise ein Code oder Passwort) in eine fremde Datenverarbeitungsanlage eingedrungen ist. Die Tathandlung besteht im Eindringen auf dem Weg von Datenübertragungseinrichtungen, das physische Eindringen beispielsweise in einen speziell gesicherten Raum ist von Art. 143bis StGB nicht erfasst.[2]

1.2.3 Art. 144 bis StGB Datenbeschädigung

Der Datenbeschädigung im Sinne von Art. 144 ^{bis} Ziff. 1 StGB macht sich strafbar, wer unbefugt elektronische oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht. Zudem macht sich nach Art. 144 ^{bis} Ziff. 2 StGB strafbar, wer Programme, von denen er weiss, dass sie elektronische oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändern, löschen oder unbrauchbar machen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt. Bei einer Datenbeschädigung im Sinne von Art. 144 ^{bis} Ziff. 1 StGB ist dem mutmasslichen Täter im Rahmen einer Strafuntersuchung nachzuweisen, dass er gegen den ausdrücklichen oder vermutlichen Willen des Datenberechtigten Daten unbefugt verändert hat (z. B. Abändern des Inhaltes oder der Form), dass er Daten gelöscht hat (z. B. vollständiges Vernichten von Daten) oder dass er Daten unbrauchbar gemacht hat (z. B. indem er Daten durch ein Passwort abgesperrt hat). Bei Ziff. 2 von Art. 144 ^{bis} StGB besteht die Tathandlung in der Vorbereitung einer Datenbeschädigung gemäss Art. 144 ^{bis} Ziff. 1 StGB. Gemäss Art. 144 ^{bis} Ziff. 2 StGB ist das Herstellen, Einführen, Inverkehrbringen, Anpreisen, Anbieten und Zugänglichmachen der fraglichen Programme strafbar, nicht jedoch der Besitz oder Erwerb von solchen.[3]

1.2.4 Art. 147 StGB Betrügerischer Missbrauch einer Datenverarbeitungsanlage

Ein betrügerischer Missbrauch einer Datenverarbeitungsanlage im Sinne von Art. 147 StGB liegt vor, wenn jemand in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar danach verdeckt. Täter eines betrügerischen Missbrauchs einer Datenverarbeitungsanlage kann jedermann sein. Täter kann insbesondere auch jener sein, der berechtigt ist, Informationen in eine Datenverarbeitungsanlage einzugeben. Erfahrungsgemäss sind nämlich bei betrügerischen Datenmanipulationen die meisten Täter Angehörige des von der Manipulation betroffenen Unternehmens.[4] Anstelle einer arglistigen Täuschung, wie sie der Betrug gemäss Art. 146 StGB voraussetzt, besteht bei Art. 147 StGB die Tathandlung in der Einwirkung auf einen Vor-

[2] Niggli Marcel/Riklin F.
[3] Niggli Marcel/Riklin F.
[4] Schmid Niklaus, S. 224, N 21.

gang der Datenverarbeitungsanlage bzw. Datenübermittlung. Dem Täter ist einerseits nachzuweisen, dass er unrichtige oder unvollständige Daten verwendet hat. Unrichtige Daten liegen dann vor, wenn im Rahmen von Datenverarbeitungsvorgängen Daten verwendet werden, die in ihrem Informationsgehalt im Widerspruch zur objektiven Sach- oder Rechtslage im Zeitpunkt des Datenverarbeitungsvorgangs stehen. Unter diese Handlungsvariante fällt auch die Verwendung unrichtiger Programme, sei es, dass manipulierte Programme in die Datenverarbeitung eingeführt werden, sei es, dass dort bereits eingespiesene Programme unerlaubt verändert werden.[5] Bei der Verwendung von unvollständigen Daten handelt es sich im Grunde genommen um eine Variante von unrichtigen Daten, denn unvollständige Daten sind per se unrichtige Daten.[6] Dem Täter ist andererseits nachzuweisen, dass er unbefugt Daten verwendet hat, das heisst, dass er zwar „richtige" Daten verwendet bzw. einen „richtigen" Datenverarbeitungsvorgang initiiert hat, dies aber unrechtmässig ist, weil er subjektiv zur Verwendung nicht befugt ist.[7] Das Einwirken auf den Datenverarbeitungs- oder -übermittlungsvorgang muss einerseits ein unrichtiges Ergebnis des Datenverarbeitungs- bzw. -übermittlungsvorgangs zur Folge haben und andererseits eine Vermögensverschiebung bewirkt haben. Eine Vermögensverschiebung ist gegeben, wenn das Vermögen des Betroffenen durch die widerrechtliche Einwirkung des Täters auf den Datenverarbeitungs- oder -übermittlungsvorgang unmittelbar im Wert vermindert und das Vermögen des Täters (oder eines Dritten) entsprechend vermehrt wurde. Schliesslich muss durch die Tathandlung – wie beim Betrug – ein Vermögensschaden bewirkt worden sein. Auf der subjektiven Seite ist dem Täter nachzuweisen, dass er mit Bereicherungsabsicht gehandelt hat.

1.2.5 Art. 150 StGB Erschleichung einer Leistung

Nach Art. 150 StGB macht sich unter anderem strafbar, wer ohne zu zahlen eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, indem er eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht. Einem mutmasslichen Täter ist demzufolge nachzuweisen, dass er durch Überwindung von technischen oder menschlichen Kontrollen Leistungen in Anspruch genommen hat, die normalerweise nur gegen Entgelt erbracht wird.

1.2.6 Art. 110 Abs. 4 StGB Definition Urkunde

In Art. 110 Abs. 4 StGB stellt das Strafgesetzbuch die digitale Urkunde auf die Ebene der Schrifturkunde. Digitale Urkunden sind Aufzeichnungen auf Datenträger, die eine menschliche Gedankenäusserung enthalten und die dazu bestimmt und geeignet sind, rechtlich relevante Tatsachen zu beweisen. Dies hat zur Folge, dass das Fälschen von digitalen Urkunden (Art. 251 StGB i. V. m. Art. 110 Abs. 4 StGB und für Beamte bzw. Personen des öffentlichen Glaubens Art. 317 StGB i. V. m. Art. 110 Abs. 4 StGB) und Unterdrücken von digitalen Urkunden (Art. 254 StGB i. V. m. Art. 110 Abs. 4 StGB) tatbestandsmässige Handlungen im Sinne des Schweizerischen Strafgesetzbuches sind. Insbesondere beim Fälschen von digitalen Urkunden spielen digitale Beweise eine zentrale Rolle.

1.2.7 Rechtliche Schlussfolgerung

Da in der heutigen Geschäftswelt beinahe sämtliche Geschäfts- und teilweise auch Lebensvorgänge elektronisch erfasst werden, spielen digitale Beweise nicht nur bei der Aufklärung von Computerdelikten oder Urkundendelikten eine wichtige Rolle. Ganz allgemein kann

[5] Schmid Niklaus, S. 231, N 45 und 46.
[6] Schmid Niklaus, S. 233, N 54.
[7] Schmid Niklaus, S. 236, N 61.

festgestellt werden, dass der Kreis der Straftatbestände, bei welchen zur Aufklärung der Delikte digitale Beweise herangezogen werden können, aufgrund des Umstandes, dass wir in einer „digitalen“ Welt leben, beliebig weit gezogen werden kann. Der Vollständigkeit halber sei darauf hingewiesen, dass insbesondere bei der Aufklärung von Verstössen gegen den Pornografieartikel (Art. 197 StGB) digitale Beweise *das* zentrale Beweismittel sind. Wie Andreas Ochsenbein so schön sagt:“ Digitale Beweise fallen laufend an. Der Verzicht auf die Erhebung digitaler Beweise ist deshalb auch bei „normalen Delikten“ ein grosser Fehler“.[8]

1.3 Momentane Situation im polizeilichen Ermittlungsverfahren

1.3.1 Stand der IT-Ermittlungen bei der Polizei

Der Umstand, dass wir in einer „digitalen“ Welt leben, hat dazu geführt, dass in den polizeilichen Kriminalstatistiken seit Jahren eine stetige Zunahme von Delikten der Computerkriminalität im engeren Sinne verzeichnet wird. Eine vergleichbare, wenn nicht gar stärkere Tendenz, ist bei den Computerdelikten im weiteren Sinne feststellbar. Diese Entwicklung hat zu einer markanten Zunahme von Strafuntersuchungen mit IT-Bezug geführt und eine stetige Weiterentwicklung der IT-Forensik erforderliche gemacht. Die Polizeicorps der Kantone haben auf die Zunahme der Strafuntersuchungen mit IT-Bezug reagiert. Sie haben entweder aus ihren eigenen Reihen Polizisten im Bereich der IT-Forensik ausbilden lassen oder IT-Spezialisten für die Sicherstellung und Auswertung von digitalen Spuren eingestellt. Bei Bedarf greifen sie auf externe Spezialisten aus dem Bereich der Computerforensik zurück.

Die speziellen Probleme, welche es im Zusammenhang mit der Sicherung von digitalen Spuren gibt, sind der Polizei heutzutage bekannt. Weniger bekannt ist, wie die Polizei in den verschiedenen Kantonen ihre IT-Ermittlung organisiert, wie sie bei der Sicherstellung und Auswertung von Daten vorgeht und wie sie mit der Untersuchungsbehörde bzw. Staatsanwaltschaft zusammen arbeitet. Um dies herauszufinden, wurde im Rahmen der vorliegenden Arbeit eine Umfrage bei sieben verschiedenen kantonalen Polizeidienststellen gemacht.

Aufgrund dieser Umfrage können folgende allgemeine Aussagen über die polizeilichen IT-Ermittlungen gemacht werden:

- alle angefragten Kantone stellen für IT-Ermittlungen personelle Ressourcen zur Verfügung;
- die meisten angefragten Kantone verfügen über eine gute technische Infrastruktur;
- für die IT-Ermittlungen gelten die allgemeinen Grundsätze der Verfahrens- und Polizeitaktik;
- in den meisten angefragten Kantonen wird im Rahmen von IT-Ermittlungen nach internen Weisungen und Checklisten gearbeitet;
- bei den Untersuchungsbehörden und Gerichten kann IT-Knowhow (aufgrund von Berührungsängsten) nicht vorausgesetzt werden;
- die angefragten Kantone greifen nur selten auf externe IT-Spezialisten zurück;
- in den angefragten Kantonen bestimmt die Polizei die Einsatztaktik und nimmt allfällige Umfeldabklärungen vor Ort vor.

[8] Ochsenbein Andreas.

Unterschiede zwischen den Kantonen zeigten sich insbesondere bei der personellen Ausgestaltung der IT-Ermittlungen, dem Vorgehen bei der Spurensicherung und -auswertung sowie bei der Zusammenarbeit mit den Untersuchungsbehörden.
Nachfolgend wird die aktuelle Situation im Bereich der IT-Ermittlung in den angefragten Kantonen aufgezeigt. Anschliessend werden die Anstrengungen des Kantons St. Gallen zu einer Optimierung der Zusammenarbeit zwischen der Polizei und der Staatsanwaltschaft aufgezeigt.

1.3.2 Kantonspolizei 1

Die Kantonspolizei 1 beschäftigt zur Zeit fünf IT-Spezialisten (zwei weitere Stellen sind bewilligt), welche in erster Linie für die Datensicherung und -auswerten zuständig sind. Diese fünf IT-Spezialisten nehmen nur in Spezialfällen (zum Beispiel bei Hausdurchsuchungen in Firmen) und nur auf ausdrückliches Aufgebot hin an Hausdurchsuchungen teil. Hausdurchsuchungen und Beschlagnahmungen werden im Kanton 1 durch speziell ausgebildete Polizisten (so genannte Sicherstellungsverantwortliche) vorgenommen.

Die Sicherstellungsverantwortlichen erstellen nach Durchführung einer Hausdurchsuchung einen Sicherstellungsbericht. In diesem Bericht wird festgehalten, welche Situation vor Ort angetroffen wurde (meistens mit Fotodokumentation), welche Massnahmen ergriffen wurden, was gesucht wurde und welche Sicherstellungen (unter anderem Beschlagnahme von elektronischen Geräten) erfolgten. Es ist anschliessend Aufgabe der IT-Spezialisten, vor dem Hintergrund des Sicherstellungsberichts die auf den beschlagnahmten Geräten befindlichen Daten zu sichern, aufzubereiten, zu sichten und auszuwerten. In komplexen Fällen, wo Fallkenntnisse benötigt werden, werden die Daten so aufbereitet, dass eine Sichtung durch den zuständigen polizeilichen Sachbearbeiter erfolgen kann. Nach der Auswertung erstellen die IT-Spezialisten einen Auswertungsbericht mit den relevanten Daten, welcher zusammen mit dem sichergestellten Material dem zuständigen polizeilichen Sachbearbeiter übergeben wird.

Im Kanton 1 haben die IT-Spezialisten anfänglich noch mit einer Checkliste gearbeitet. Diese Checkliste wurde aber nicht mehr aktualisiert (stetiger Wandel) und ist mittlerweile veraltet. Der Kanton 1 hat bis heute noch keine Aufträge an externe Spezialisten erteilt.

1.3.3 Kantonspolizei 2

Die Kantonspolizei 2 verfügt über Spezialisten, welche für die Aufbereitung (forensische Sicherung, Suchläufe etc.) und die Auswertung von Daten zuständig sind. Hausdurchsuchungen und Beschlagnahmungen erfolgen aus personellen Gründen nicht durch einen IT-Spezialisten, sondern durch den zuständigen polizeilichen Sachbearbeiter selber. In schwierigen Fällen unterstützen die IT-Spezialisten jedoch den polizeilichen Sachbearbeiter mittels telefonischen Auskünften oder gehen ausnahmsweise mit vor Ort.

Die IT-Spezialisten erhalten vom polizeilichen Sachbearbeiter oder vom Untersuchungsbeamten einen Auftrag, in welchem steht, nach was die Daten zu durchsuchen sind. Eine präzise Anleitung, wie eine forensische Beweissicherung zu erfolgen hat, kann durch den Auftraggeber infolge mangelnder Fachkenntnisse nicht gegeben werden. Die Datenbestände werden von den IT-Spezialisten zuhanden der Verfahrensakten ausgewertet und dokumentiert. Danach stehen die IT-Spezialisten den polizeilichen Sachbearbeitern und den Untersuchungsbeamten bei Unklarheiten oder Rückfragen unterstützend zur Seite.

1.3.4 Kantonspolizei 3

Bei der Kantonspolizei 3 sind acht IT-Ermittler im Einsatz. Aufgrund knapper personeller Ressourcen wird die Sicherstellung von Computern und/oder Datenträgern anlässlich von Hausdurchsuchungen nicht durch die IT-Ermittler vorgenommen. Die mit der Sicherstellung von Computern und/oder Datenträgern beauftragten Polizisten verfügen über ein Mindestmass an IT-Kenntnissen, mit welchen sie eine "normale", unproblematische Sicherstellung vornehmen können. Mit diesem Vorgehen werden rund 80 % der Hausdurchsuchungen abgedeckt. Tauchen bei einer Hausdurchsuchung unerwartet Komplikationen auf, stehen die Informatikspezialisten jederzeit für telefonische Auskünfte zur Verfügung. Falls sich eine Situation telefonisch nicht klären lässt, begibt sich ein Informatikspezialist nachträglich noch vor Ort. Bestehen vor Durchführung der Hausdurchsuchung Hinweise auf eine komplexere Situation, nehmen ein bis zwei Informatikspezialisten direkt an der Hausdurchsuchung teil, oder stehen mindestens auf Abruf bereit. Beim Umgang mit Netzwerken oder bei der Sicherung von Daten vor Ort nehmen die IT-Ermittler zwingend an Hausdurchsuchungen teil.

Bei der Kantonspolizei 3 entscheiden die IT-Ermittler, was vor Ort untersucht und allenfalls beschlagnahmt und gesichert wird. Ihre Auswertungen halten sie in einem schriftlichen Bericht zuhanden der Staatsanwaltschaft fest. Nebst den Auswertungen enthält der schriftliche Bericht die Vorgehensweise der IT-Ermittler und auffällige von ihnen festgestellte Unregelmässigkeiten. Die IT-Ermittler der Kantonspolizei 3 erachten ihren schriftlichen Bericht daher als „beweissicher“. Nach Abgabe des Berichts an die Staatsanwaltschaft stehen die IT-Ermittler der Staatsanwaltschaft zur Verfügung, um allfällige Unklarheiten zu bereinigen.

1.3.5 Kantonspolizei 4

Bei der Kantonspolizei 4 gibt es eine rudimentäre Checkliste für das Vorgehen bei der Sicherung von Systemen und Datenträgern sowie einige Dienstbefehle. Es bestehen keine Vorgaben, wie die Datensicherung zu erfolgen hat. Die Sicherung richtet sich aber grundsätzlich nach den Kriterien Verhältnismässigkeit, Nachvollziehbarkeit, Integrität und Authentizität.

Die Kantonspolizei 4 vertritt die Ansicht, dass vor Aktionsbeginn zwingend eine Sitzung zwischen dem Untersuchungsrichter und der IT-Spezialist erfolgen muss. In dieser Sitzung werden die gegenseitigen Bedürfnisse erhoben. Die Untersuchungsrichter geben dem IT-Ermittler (gemäss Strafprozessordnung) keine Anweisungen in Bezug auf die Einsatztaktik. Diese ist Sache der Polizei. Die Polizei ist bestrebt, dem Untersuchungsrichter einen optimalen Service zu bieten. Es werden aus Zeitgründen nicht immer umfassende Umfeldabklärungen gemacht. Es kommt primär auf den Auftrag an und auf den Ausgang der Besprechung zwischen dem Untersuchungsrichter und IT-Spezialisten. Die gesicherten Daten werden gemäss Auftrag des Untersuchungsrichters detailliert durch die IT-Ermittler ausgewertet. Anschliessend wird ein schriftlicher Analysebericht erstellt, in welchem die vom Untersuchungsrichter gestellten Fragen beantwortet werden.

1.3.6 Kantonspolizei 5

Der IT-Ermittler der Kantonspolizei 5 hat an der HSW in Luzern alle drei Module der Ausbildung zum Cyber-Cop absolviert. Bei der Kantonspolizei 5 wird nach der Checkliste gearbeitet, die der IT-Ermittler an der HSW in Luzern anlässlich der Ausbildung zum Cyber-Cop erhalten hat. Eine Umfeldabklärung wird meistens gemacht. Die sichergestellten Datenträger werden je nach Situation gespiegelt und durch den IT-Ermittler ausgewertet. Die Rapportierung mit den Resultaten erfolgt an das Verhöramt. Die Datenträger werden bis zum Entscheid, was der Richter anordnet (Löschung der entsprechenden Dateien oder Löschung des kompletten Datenträgers, Vernichtung etc.), bei der Polizei gelagert. Nur wenn der IT-Ermittler mit Hilfe der eigenen Mitteln (spezielle Software) nicht mehr weiter kommt, werden Aufträge an externe Experten erteilt.

1.3.7 Kantonspolizei 6

Aufgrund der steigenden Anzahl von Kriminalfällen mit IT-Bezug wurde ein Mitarbeiter der Kantonspolizei 6 speziell mit der Erhebung von Daten beauftragt. Es handelt sich um eine jüngere, informatikversierte Fachkraft, die jedoch nicht über eine Ausbildung in der Informatik verfügt.

1.3.8 Kantonspolizei 7

Seit dem Jahr 2003 werden bei der Kantonspolizei 7 die IT-Spuren (deliktische Spuren in Computer, Handys und sonstigen elektronischen Geräten) polizeilich gesichert und ausgewertet. Da für die Abwicklung dieser Aufgaben kein zusätzliches Personal eingestellt werden durfte, werden diese zusätzlichen Aufgaben durch das bestehende Personal wahrgenommen; in der Zwischenzeit wurde eine Personaleinheit für diesen speziellen Bereich ausgeschieden. Diese Personaleinheit ist lediglich in der Lage, die allerwichtigsten Aufträge zu erledigen. Umfangreiche Sicherungsarbeiten werden an externe Sachverständige weitergeben.

1.3.9 Schlussfolgerung Polizei

Die Fälle, bei denen die Sicherstellung und Auswertung von digitalen Informationen eine zentrale Rolle spielen, wurden bis anhin von den einzelnen Polizeicorps unterschiedlich bearbeitet. Es gibt zudem Unterschiede bei der Auftragserteilung sowie bei den Erwartungen der Auftraggeber in Bezug auf die Rapportierung. Da die Ressourcen der technischen Spezialisten und der Spezialdienste der Polizeicorps begrenzt sind, sind Engpässe in der Auftragsabwicklung unausweichlich. Die Bearbeitung von Fällen mit IT-Bezug bedarf auch bei den Untersuchungsbehörden Fachwissen und technisches Verständnis, insbesondere bei der Formulierung der Aufträge und bei der Auseinandersetzung mit den Ergebnissen der Auswertungen.

1.4 Optimierung der Ablaufprozesse: Fallmuster Kantonspolizei St.Gallen

Einzelne Kantone haben die Schwierigkeit bei der Erhebung und der Analyse von IT-Daten erkannt. Die Kantonspolizei St.Gallen zum Beispiel befasst sich derzeit mit der Entwicklung verschiedener Leitfäden (siehe Anhang A-H der Kantonspolizei St.Gallen) für die Zusammenarbeit mit den Justizbehörden. Sie ist der Auffassung, dass sich die Strafverfolgungsbe-

hörden, Rechtsanwälte und Richter mit diesen neuen Hilfsmitteln vertraut machen und sich zu diesem Zweck die entsprechenden Kenntnisse aneignen müssen.

Um diesen Ziel zu erreichen, setzten der Polizeikommandant der Kantonspolizei St. Gallen und der Erste Staatsanwalt der Staatsanwaltschaft St. Gallen die Arbeitsgruppe „Anforderungen an die IT-Analyse“ ein und erteilten ihr den Auftrag, die elektronische Beweisführung zu untersuchen und Vorschläge zur Optimierung der Verfahrensabläufe und des Einsatzes der technischen und personellen Ressourcen zu erarbeiten. Die Arbeit an den Schnittstellen zwischen der Kantonspolizei und der Staatsanwaltschaft sollte effizienter, einheitlicher und qualitativ besser werden.

1.4.1 Aufgaben der Arbeitsgruppe

Die Arbeitsgruppe führte eine Analyse der Beweisführung mit modernen Mitteln der Informationstechnologie durch und prüfte hierbei die nachfolgenden Themenfelder:

- Konzepte der Beweisführung (Beweisführungsstrategie, Beweisziele, Beweisfelder, Mittel);
- Beleuchtung der Rahmenbedingungen: rechtlich, technisch, organisatorisch, finanziell, kriminaltaktisch, personell;
- Bedürfniserhebung (z.B. fallbezogene Zusammenarbeit und Auftragsstellung, Zuständigkeiten zur Bewertung von Beweisen, Umfang der Auswertungen und Dokumentation);
- Betrachtung der Spannungsfelder: Verhältnismässigkeit, Effizienz, Qualität;
- Ausführungen zu technischen Untersuchungsmethoden und Hilfsmitteln, sowie Aufwandbetrachtung.

Zunächst wurden folgende Problemfelder erkannt:

- Vielfalt der Kriminalitätsbereiche;
- Instruktion / Schulung / Weiterbildung (Staatsanwaltschaft / Polizei);
- Rechtliche Anforderungen / fehlende Richtlinien / Verhältnismässigkeit;
- Einheitlichkeit bei Untersuchungsämtern / Untersuchungsrichtern;
- Form der Zusammenarbeit (Team / Auftragsverhältnis);
- Auftragsformulierungen / Klassifizierung der Fälle;
- Form der Auswertungen;
- Form der Rapporterstellungen.

Aufgrund der Vielfältigkeit dieser Problembereiche war ein schrittweise Vorgehen und eine Fokussierung auf nachfolgende Themen notwendig. Um die fehlenden Richtlinien mit Rahmenbedingungen festzulegen, wurde ein Fallmuster (Anhang A Musterfall. Beschreibung der Charakteristik eines Kriminalitätsbereiches) und Auftragsformulare (Anhang B) sowie Vorlagen für die Rapportierung (Anhang C-E) bezogen auf dieses Fallmuster erstellt. Ausserdem wurde eine Weisung zur Verwendung dieser Vorlagen entworfen.

1.4.2 Empfehlungen der Arbeitsgruppe

Zusätzlich wurden Empfehlungen abgegeben, die, wie in vielen Geschäftprozessen, bei der Ermittlung neben rechtlichen Aspekten auch technische und insbesondere organisatorische Aspekte berücksichtigen:

1.4.2.1 Zweistufiges Verfahren (Anhang F)

Eine erste Klassifizierung und Priorisierung, nach Verfahrenseröffnung, gilt für die ersten Ermittlungstätigkeiten. Sobald Resultate vorliegen, soll aufgrund der neuen Erkenntnisse eine zweite Beurteilung vorgenommen werden, welche auch das Tatvorgehen sowie das Verhalten des Angeschuldigten berücksichtigt. Die Priorisierung steuert hierbei die zeitliche Abarbeitung von Fällen (Priorität 1 = unmittelbare Aufnahme der Ermittlungstätigkeit notwendig) und die Klassifizierung den erwarteten Ermittlungsaufwand bzw. die zu treffenden Massnahmen.

Die fallbezogene Priorisierung/Klassifizierung erfolgt im Team zwischen Staatsanwaltschaft und polizeilichem Sachbearbeiter aufgrund der Fakten des Falls, der technischen Möglichkeiten und der personellen Ressourcen der Kantonspolizei. Entsteht dadurch (z.B. Häufung der Fälle) eine Überlastung bei der Kantonspolizei, wird dies der Staatsanwaltschaft gemeldet, welche sodann die übergeordnete Priorisierung vornimmt.

1.4.2.2 Befragungsschema für Erstbefragung (Anhänge G+H)

Das Befragungsschema unterstützt die optimale Vorbereitung auf Einvernahmen und kann zur Vorbereitung der Erstbefragung dienen. Damit wird auch sichergestellt, dass wichtige Aspekte nicht vergessen werden. Im Zweifelsfall oder bei der Klassifizierung „schwer“ ist der Beizug von Spezialisten empfohlen.

1.4.2.3 Vorlage Rapportierung (Anhang C-E)

Während der Ermittlungsbeamte das Sicherstellungsverzeichnis der Hausdurchsuchung erstellt, schreibt die Dienststelle Informationstechnologie der Kantonspolizei einen „Sicherstellungsbericht“, welcher das Untersuchungsgut auflistet und Angaben zur technischen Konservierung der darauf enthaltenen Datenbestände macht.

Der polizeiliche Sachbearbeiter sichtet die sichergestellten Daten und dokumentiert die Erkenntnisse im Schlussbericht. Nur bei Fällen der Klassifizierung „schwer“ wird er ohne speziellen Auftrag eine Auswertung des gesamten Datenbestandes vornehmen. Ergeben sich aus den Ermittlungsresultaten weitere Fragen, wird die Dienststelle IT mit einer vertieften Auswertung beauftragt. Daraus resultiert ein Auswertungsbericht, welcher die Fragen des Ermittlers beziehungsweise der Staatsanwaltschaft beantwortet und eine Einschätzung über das Tatvorgehen beinhaltet. Über sämtliche Ermittlungsergebnisse wird ein Schlussbericht zuhanden der Staatsanwaltschaft erstellt. Dieser enthält eine Bewertung sämtlicher Erkenntnisse sowie der vorliegenden Datenbestände.

1.4.2.4 Checkliste Auftragsbearbeitung (Anhang B)

Damit der Auftrag der Staatsanwaltschaft an die Kantonspolizei die notwendigen Informationen für die Ermittlungstätigkeit enthält, wurde eine Checkliste erarbeitet. Mit deren Hilfe kann der Auftraggeber prüfen, ob alle notwendigen Angaben weitergereicht werden. Dies betrifft insbesondere die Klassifizierung/Priorisierung und die Form der Zusammenarbeit und setzt voraus, dass vorgängig die Zielsetzung der Fallbearbeitung im Team besprochen wurde. Ein schriftlicher Ermittlungsauftrag (vorbesprochen mit dem polizeilichen Sachbearbeiter respektive dem technischen Sachverständigen) wird nach der zweiten Priorisirung/Klassifizierung abgegeben. Gestützt darauf wird der Auswertungsbericht bzw. Schlussbericht erarbeitet.

Für den Vollzug der Sicherstellung genügt der Hausdurchsuchungs-Befehl respektive die Beschlagnahmeverfügung. Als Rückmeldung erhält der verfügende Untersuchungsrichter vom polizeilichen Sachbearbeiter ein Hausdurchsuchung-Protokoll, ein Sicherstellungsverzeichnis sowie einen Sicherstellungsbericht der Dienststelle IT.

1.4.2.5 Ausbildung aller Fallbeteiligten

Staatsanwaltschaft und Kantonspolizei sollen bezüglich technischem sowie juristischem Verständnis und grundlegender Zusammenarbeit (z.B. Dialog mit Experten, saubere Beweisführung) ausgebildet werden.

1.4.3 Fazit des St.Galler Ansatzes

Die Ermittlung bei Computerkriminalität und Fällen mit IT-Bezug verlangt spezielle Kenntnisse und Techniken. Leicht können digitale Beweismittel manipuliert oder durch unbefugtes Handeln verändert werden. Nachträglich sind solche Manipulationen nur schwer nachzuvollziehen beziehungsweise zu beweisen. Analog zu anderen Bereichen der Kriminalistik gilt auch hier, alle relevanten Beweise zu sammeln, zu analysieren, zu rekonstruieren und neutral, nachvollziehbar und gerichtsverwertbar sicher zu stellen.

Fehler bei der Leitung von Polizeieinsätzen können unter Umständen zu fehlerhaftem Umgang mit den verfügbaren digitalen Beweismitteln führen. Durch Verkennung des Wertes von digitalen Beweisen können auch die Entscheidungen von Gerichten fehlgeleitet werden. Das heisst, alle Beteiligte brauchen eine angemessene Schulung.

Der Ansatzpunkt für eine verbesserte Zusammenarbeit zwischen der Polizei und der Staatsanwaltschaft ist mit der Initiative der St. Galler Strafverfolgungsbehörden gegeben. Die IT-Spezialisten müssen mit Richtern, Staatsanwälten und Ermittlungsbeamten zusammenarbeiten, damit diese digitale Beweise und deren Qualität erkennen.

1.5 Momentane Situation im Untersuchungsverfahren

Der Untersuchungsrichter unter Einhaltung der Regeln des Strafprozessrechts zu untersuchen, ob das Verhalten einer angeschuldigten Person unter einen Tatbestand des Schweizerischen Strafgesetzbuches subsumiert werden kann. Im Rahmen der Strafuntersuchung hat er sowohl belastende als auch entlastende Beweise zu sammeln.

Bei Straffällen mit IT-Bezug überlegt sich der Untersuchungsrichter zuerst, wo im konkreten Fall überall IT-Spuren erhoben werden können. Beispielsweise fallen Spuren an bei der Datenspeicherung, bei der Kommunikation oder auf Applikationen. In heiklen Fällen wird bereits zu diesem Zeitpunkt eine Fachperson kontaktiert, um Informationen darüber zu sammeln, wo überall IT-Spuren vorhanden sein könnten.

Der Untersuchungsrichter hat dann dafür besorgt zu sein, dass die elektronisch gespeicherten Daten sichergestellt werden. Er muss zu diesem Zweck prüfen, ob die Voraussetzungen für die Durchführung einer Hausdurchsuchung und der Beschlagname von elektronisch gespeicherten Daten als Beweismittel gegeben sind.

Die Beschlagnahme von elektronisch gespeicherten Daten ist ein Eingriff in die Eigentumsgarantie gemäss Art. 26 BV. Sie kann daher nur durchgeführt werden, wenn eine gesetzliche

Grundlage und ein öffentliches Interesse gegeben und die Beschlagnahme der elektronisch gespeicherten Daten verhältnismässig ist. Zudem ist ein dringender tatbezogener Tatverdacht erforderlich.[9]

Die gesetzliche Grundlage für die Beschlagnahme findet sich in der Strafprozessordnung. Das öffentliche Interesse ist in diesem Zusammenhang das Interesse der Allgemeinheit an der Ahndung von Straftaten und der Wahrheitsfindung im Rahmen des Strafprozesses. Eine Beweismittelbeschlagnahme zur ausschliesslichen Abklärung und Durchsetzung von adhäsionsweise geltend gemachten Zivilansprüchen erfüllt das Erfordernis des öffentlichen Interesses nicht.[10] Die Beschlagnahme von elektronisch gespeicherten Daten ist verhältnismässig, wenn diese Massnahme zum Herausfinden der materiellen Wahrheit notwendig ist, und keine mildere, geeignete Massnahme (z. B. freiwillige Herausgabe der Daten) zur Verfügung steht. Notwendig ist die Beschlagnahme von elektronisch gespeicherten Daten immer dann, wenn das Strafverfahren ohne die zu beschlagnahmenden Gegenstände voraussichtlich nicht ordentlich zu Ende geführt werden kann. Von einer Beschlagnahme ist abzusehen, falls andere, hinreichende Beweisgegenstände zur Verfügung stehen. Die Erforderlichkeit führt dazu, dass die Untersuchungsbehörde, bevor sie zur Beschlagnahme schreitet, grundsätzlich mildere Massnahmen ergreifen muss, falls diese ebenfalls zum Ziel führen.[11]

Als nächstes stellt sich der Untersuchungsrichter die Frage, wen er mit der Sicherung der digitalen Beweismittel beauftragen soll. In erster Linie werden dies behördliche Sachverständige sein (EDV-Spezialisten bei der Polizei) oder private Sachverständige, die unter Hinweis auf Art. 307 StGB mit der Sicherstellung der elektronisch gespeicherten Daten beauftragt werden. Bei der Wahl des Sachverständigen ist darauf zu achten, dass dieser ein Experte der Computerforensik ist und mit allgemein anerkannten Mitteln und nach allgemein anerkannten Methoden arbeitet. Andernfalls besteht später ein Problem der Verwertbarkeit der erhobenen Beweise.

Die Sicherstellung der elektronisch gespeicherten Daten hat mit dem Ziel der Verwertbarkeit der Beweise vor Gericht zu erfolgen. Die Beweise sind rechtmässig zu beschaffen. Zudem muss die Integrität und Authentizität der Daten gewährleistet und die Beweismittelerhebung dokumentiert sein. Die anlässlich der Hausdurchsuchung beschlagnahmten Gegenstände sind weiter einzeln im Hausdurchsuchungsprotokoll aufzuführen.

Nach der Sicherstellung der elektronisch gespeicherten Daten werden diese durch einen EDV-Spezialisten bei der Polizei oder einen externen Sachverständigen – falls nicht zuerst ein Entsiegelungsverfahren durchgeführt werden muss – durchsucht, analysiert und interpretiert.

Der EDV-Sachverständige wird nach Abschluss seiner Analyse einen schriftlichen Bericht verfassen. In diesem schriftlichen Bericht übermittelt der Sachverständige dem Untersuchungsrichter auf verständliche Weise Fachwissen, hält von ihm festgestellte Tatsachen fest und beurteilt aus der Optik eines Spezialisten einen bestimmten Sachverhalt.

Das Sachverständigengutachten bildet zusammen mit den übrigen vom Untersuchungsrichter im Rahmen der Strafuntersuchung gesammelten Beweise (Urkunden, Zeugeneinvernahmen, Augeschein). Basis zur Erhebung der Anklage bzw. zum Erlass eines Strafbefehls.

---

[9] Aepli Michael, S. 40 und 41.
[10] Aepli Michael, S. 62.
[11] Aepli Michael, S. 72.

Ohne Hilfe von Computerforensik-Spezialisten wären heutzutage sowohl die Untersuchungsrichter als auch die Richter überfordert, ein sachgemässes Urteil zu fällen. Die Möglichkeiten dieser Experten erscheinen fast unbegrenzt, denn zum einen können sie sehr genaue Informationen über bestimmte Daten liefern, und zum andern können sie schon längst vergessene oder bewusst gelöschte, überschriebene oder formatierte Dateien wiederherstellen und so dem Beweis zugänglich machen.[12]

Grundsätzlich unterliegt auch das Sachverständigengutachten eines Computerforensik-Spezialisten der freien richterlichen Beweiswürdigung. Unter der freien richterlichen Beweiswürdigung versteht man, dass der Richter alleine aufgrund seiner Überzeugung über die Aussagekraft der eingebrachten Beweismittel entscheidet. Im Falle von Sachverständigengutachten betreffend die Computerforensik wird es im Normalfall so sein, dass sich die Richter an die gewonnenen Erkenntnisse des Spezialisten halten.[13] Der Richter wird es jedoch nicht unterlassen, in einem ersten Schritt das dem Sachverständigen als Basis seiner Expertise zur Verfügung stehende Beweismaterial zu würdigen und zu prüfen, ob der Sachverständige vertrauenswürdig ist.[14]

1.6 Notwendigkeit von Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug

Die heutige Technik bringt es mit sich, dass die Untersuchungsbehörden im Rahmen der Untersuchung von Straffällen mit IT-Bezug einen EDV-Spezialisten als Sachverständigen oder Polizeibeamte, die auf EDV spezialisiert sind, beiziehen. Wie bereits erwähnt, sind faktisch sowohl der Untersuchungsrichter oder Staatsanwalt als auch der Richter darauf angewiesen, dass ihm ein Spezialist sein Fachwissen auf eine verständliche und nachvollziehbare Art und Weise vermittelt und bestimmte Sachverhalte vor dem Hintergrund seines Fachwissens beurteilt. Der Sachverständige fungiert praktisch als Entscheidungshilfe. Er sichert die digitalen Beweise, analysiert und interpretiert sie. Aufgrund der Komplexität dieses Fachgebietes ist davon auszugehen, dass kaum ein Untersuchungsrichter oder Richter im Rahmen der Beweiswürdigung vom Ergebnis des Sachverständigengutachtens abweichen wird. Da der Richter mit grosser Wahrscheinlichkeit auf das Gutachten der Computerspezialisten abstellt, ist es umso wichtiger, die Parameter, welche das Zustandekommen des IT-Gutachtens beeinflussen, im Auge zu behalten.

Die Literatur und Rechtsprechung befassen sich vorwiegend mit der strafprozessualen Sicherstellung von elektronisch gespeicherten Daten. Dem IT-Gutachten, dem Umgang mit IT-Gutachten und der richterliche Beweiswürdigung von Gutachten in Straffällen mit IT-Bezug wird eher wenig Aufmerksamkeit geschenkt. Diese Lücke ist zu schliessen.

In Straffällen mit IT-Bezug können mit gezielten Umfeldabklärungen die Ergebnisse eines IT-Gutachtens sowie die Beweise, auf die sich das Gutachten stützt, hinterfragt werden. Weiter dienen gezielte Umfeldabklärungen bei Sachverhalten mit IT-Bezug dazu, die Zurechnung eines tatbestandsmässigen Verhaltens zu einer bestimmten Person zu erleichtern, breit abgestützte Argumente für die Anklageerhebung zu finden oder zusätzliche Indizien und Beweise zu sammeln, welche die Ergebnisse des IT-Gutachtens stützen.

[12] Ryser Dominic, S. 585.
[13] Ryser Dominic, S. 590.
[14] Ryser Dominic, S. 585.

2. Teil: Der Ratgeber

2.1 Konzept und Grundlage für einen Ratgeber

2.1.1 Konzept der Datenintegrität

Heute sind viele Unternehmen von modernen Informations- und Kommunikationstechniken abhängig. Die IT dient als Basis für die einzelnen Geschäftsprozesse wie Einkauf, Produktion und die gesamte Verwaltung. Neben einem Geschäftsarbeitsplatz haben immer mehr Mitarbeiter auch einen Heimarbeitsplatz, einen portablen PC für den mobilen Einsatz oder sie habe generell extern über Modem oder Netzwerkanschluss Zugriff zu Daten der Firma.

Gemäss dem Statistischen Bundesamt in Deutschland nutzten im Jahr 2005 84% aller Unternehmen einen Computer, der Trend wird weiter zunehmen.[15] Diese grossflächige Nutzung bedeutet aber auch eine Abhängigkeit von IT-Systemen, was wiederum ein gut funktionierendes IT-Risikomanagement erfordert. Die Risiken können nicht alle eliminiert werden. Sie sollten aber auf einem geringen Niveau gehalten werden und wirtschaftlich noch tragbar sein. Die Grundlage für ein erfolgreiches IT-Risikomanagement sind die folgenden vier IT- Grundziele.[16]

- Vertraulichkeit: Es ist sichergestellt, dass sensible Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können. Nicht für die Öffentlichkeit bestimmte Daten oder Informationen sollen mit Diskretion behandelt werden.
- Verfügbarkeit: Die Funktionalität von Systemen kann nicht auf unbefugte Weise beeinträchtigt werden. Daten stehen dann zu Verfügung, wenn sie benötigt werden.
- Verbindlichkeit: Alle Aktionen einer Instanz werden eindeutig zugeordnet und können nicht geleugnet werden;
- Integrität: Die Daten und Systeme können nicht unautorisiert manipuliert werden, Ziel ist die Makellosigkeit und Unversehrtheit der Daten.

Überträgt man diese vier Grundziele auf die vorliegende Arbeit, kristallisiert sich die Datenintegrität als wichtigstes Ziel heraus. Kann die Strafverfolgungsbehörde aus den vorliegenden Informationen Rückschlüsse auf den Urheber oder Manipulator der Daten ziehen? Ist sichergestellt, dass sich kein Dritter Zugriff verschafft und dabei die Daten verändert hat? Mit diesen und weiteren Fragen befasst sich diese Arbeit. Sie versucht dabei, Massnahmen und Risiken bei Strafffällen mit IT-Bezug aufzuzeigen, damit mit gezielten Umfeldabklärungen die Integrität der Daten aus Beweisen und IT-Gutachten vertieft abgeklärt werden kann.

2.1.2 Vollständigkeit aufgrund von anerkannten Frameworks

Um die Vollständigkeit der Abklärungen für Strafffällen mit IT-Umfeld zu gewährleisten, wurde nach einem umfassenden Framework gesucht. Die verschiedenen und gut verfügbaren Frameworks wurden als Basis untersucht und weisen nachfolgende Eigenschaften auf.

[15] BITKOM, Seite 7.
[16] Rieder Carlos.

2.1.3 IT-Grundschutzkatalog des BSI

Der IT-Grundschutzkatalog wird vom Deutsche Bundesamt für Sicherheit (BSI) herausgegeben und besteht unter anderem aus einem Massnahmenkatalog für die folgenden Bereiche: Infrastruktur, Organisation, Personal, Hard und Software, Kommunikation und Notfallvorsorge. Der Aufbau ist gemäss einem Baukastensystem konzipiert mit einer Vielzahl von Bausteinen. Jeder Baustein enthält eine standarisierte Gefährdungslage und entsprechende Massnahmen dazu.

Der IT-Grundschutzkatalog ist ein Handbuch mit Empfehlungen für Sicherheitsmassnahmen, er enthält Umsetzungshinweise und Hilfsmittel für typische IT-Systeme. Ziel ist es, durch gezielte Anwendungen von organisatorischen, personellen, technischen und infrastrukturellen Standards ein geschütztes IT-System aufzubauen. Der Massnahmenkatalog beinhaltet Verantwortlichkeiten, Massnahmen und Kontrollfragen. Das Handbuch ist auch in Englisch verfügbar und hat somit internationalen Charakter.

Aufgrund des freien Verfügbarkeit im Internet, ist es jedem kostenlos zugänglich. Es besteht aus Gefährdungs- und Massnahmenkatalog und zeigt somit eine klare Richtlinie. Da es auch noch mehrsprachig ist, erfüllte es am Besten die Anforderungen für eine Checkliste, wie sie diese Arbeit darstellen will.

2.1.4 COBIT

Das Modell von COBIT (Control Objectives for Information and Related Technology) stellt ein Konzept von generell anwendbaren und international akzeptierten Kontrollzielen für IT-Security, IT-Audit & IT-Governance dar, die für eine sichere und ordnungsgemässe IT notwendig sind.

COBIT ist ein international anerkannter Standard für die IT-Revision. Das Modell wurde von Revisoren aus der Industrie und dem Berufsstand "ISACA" (Information System Audit and Control Association) auf Basis von Revisionsrichtlinien, Kontrollemodellen und branchenspezifischen Richtlinien gebildet. COBIT soll einem IT-spezifischen Kontrollsystem gerecht werden und soll dabei die Integration von Kontrollzielen für Geschäftsprozesse, Organisation & Kommunikation und Informationstechnologie sicherstellen.

Ziel von COBIT ist es, die Geschäftsziele und -prozesse optimal durch die fünf verfügbaren IT-Ressourcen (Daten, Applikationen, Technologien, Anlagen und Personal) zu unterstützen. Dabei werden für vier so genannte Domänen (Planung & Organisation, Akquisition & Implementierung, Auslieferung & Unterstützung und Überwachung) 34 zentrale IT-Prozesse und 215 Kontrollziele definiert.[17] Jedes Kontrollziel enthält eine Reihe von Fragen, deren Beantwortung, Beurteilung und Umsetzung eine verlässliche Anwendung der IT gewährt. Es verbessert die Abstimmung zwischen den Geschäftseinheiten und der IT.

COBIT ist ein sehr umfassendes und weitreichendes Framework, das aber sehr allgemein bleibt und nicht auf detaillierte, anschauliche Massnahmen eingeht.

2.1.5 ISO 17799

Der ISO 17799 Standard (Code of Practice for Information Security Management) ist ein internationaler Standard, der aus elf Bereichen besteht. Diesen Bereichen werden 134 Massnahen zugeordnet. Die Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis

[17] Dummer, Stefan; Seite 87

bildet die Grundlage für diese Standardisierung. Eine Zertifizierung nach ISO 27001 ist möglich, wobei aber auf ISO 17799 abgestützt wird. Der Ursprung der ISO Standard ist BS 7799-1 (Britisch Standard BS 7799-1).

2.1.6 Warum BSI ?

Bei der Wahl der Grundlage für den "Ratgeber für Strafverfoglungsbehörden bei Abklärungen im IT-Umfeld" wurden diese verschiedenen Frameworks analysiert. Das IT-Grundschutzkatalog vom BSI wurde als die am besten geeignete Grundlage angesehen, da die Massnahmen umfassend und sehr konkret dargestellt werden. Das Handbuch ist international anerkannt und neben Deutsch auch in Englisch verfügbar. Durch die einfache Zugänglichkeit übers Internet ist es jederzeit und allen frei verfügbar.

2.2 Vorgehen bei der Erstellung des Ratgebers

Es gibt zahlreiche Möglichkeiten, einen Ratgeber für Strafverfolgungsbehörden bei Abklärungen im IT-Umfeld zu erstellen. Im Nachfolgenden wird beschrieben, welches konkrete Vorgehen im Rahmen dieser Arbeit gewählt wurde, um schliesslich das im Anhang aufgeführte Ergebnis zu erhalten.

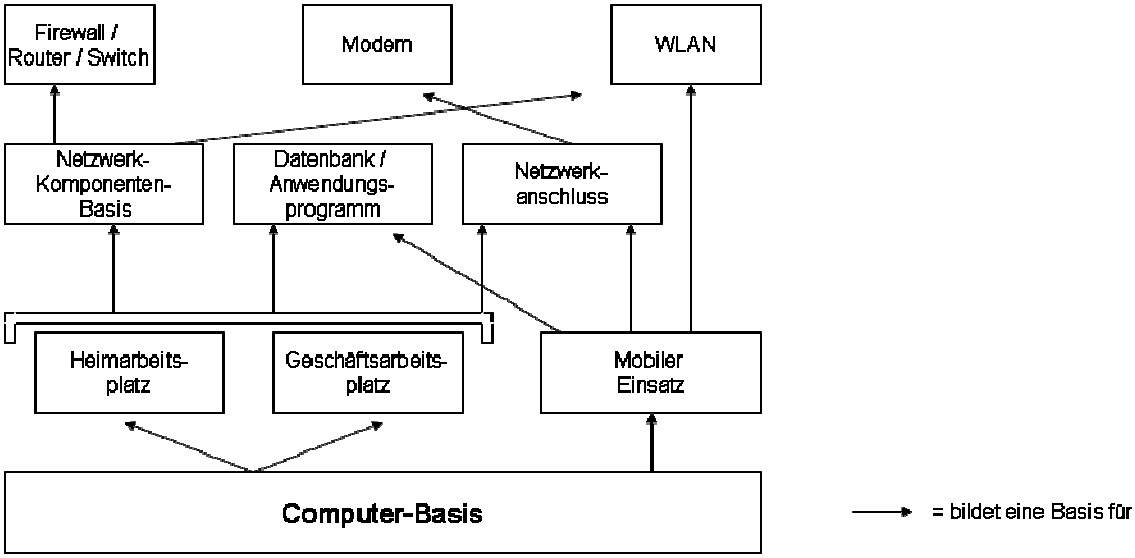
2.2.1 Modularer Ansatz

In vielen alltäglichen Abläufen werden IT-Systeme verwendet. Als Nebenerscheinung nimmt dadurch die Bedeutung von IT-Systemen auch bei kriminellen Handlungen und schliesslich bei der Computerforensik zu. Bei der IT-Spurensuche sind die IT-Systeme entweder das Ziel, das Werkzeug oder ein zufälliges Hilfsmittel einer verbotenen, verdächtigen oder ungewöhnlichen Aktivität.[18]

Aufgrund der Komplexität und zahlreichen Anwendungsbereiche der IT wird klar, dass bei der Erstellung eines Ratgebers zwingend eine konsequente Systematik zur Abgrenzung der verschiedenen Themenbereiche zu verfolgen ist. So unterteilt Marfurt[19] die Spuren grundsätzlich nach „Datenspeicherung“, „Kommunikation“ und „Applikation“. Das BSI[20] strukturiert das Thema „IT“ mittels so genannten Bausteinen in die Hauptkapitel „übergeordnete Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“, wobei die jeweiligen Unterkapitel anschliessend detailliert auf die jeweiligen Bausteine eingehen.

Bei der Erstellung des Ratgebers wurde unter Berücksichtigung der Unterteilung gemäss Marfurt und BSI ein modularer Ansatz gewählt:

[18] Tuccillo Maurizio, Seite 5.
[19] Marfurt Konrad, Seite 3.
[20] BSI.



Aufeinander aufbauende Module zur Abgrenzung der IT-Themen und Eingrenzung des IT-Umfelds

Die Module bauen aufeinander auf und sind folgendermassen charakterisiert:

- Computer-Basis: Dieses Modul beinhaltet grundlegende Aspekte, welche in der Regel bei jedem Computer zu beachten sind.
- Heimarbeitsplatz oder Geschäftsarbeitsplatz: Diese Module beinhalten Aspekte, welche zusätzlich zur Computer-Basis zu berücksichtigen sind, abhängig vom Standort des Computers.
- Mobiler Einsatz: Hier werden spezifische Aspekte im Zusammenhang mit tragbaren Computersystemen erwähnt.
- Netzwerkanschluss und Modem: Kommunikationsspezifische Aspekte aus Sicht eines Client-Computers werden hier behandelt. Als Spezialthema ist zudem noch der Einsatz eines Modems aufgeführt.
- Netzwerkkomponenten-Basis: Im Gegensatz zum Modul „Netzwerkanschluss“ werden hier grundlegende Aspekte aus Sicht von Servern und anderen zentralen Netzwerkgeräten erwähnt.
- Firewall / Router / Switch und WLAN: Diese Module beinhalten spezifische Aspekte, welche neben den darunter liegenden Modulen zusätzlich zu beachten sind, sofern die entsprechenden Geräte für die Untersuchungen relevant sind.
- Datenbank / Anwendungsprogramm: Hier werden spezifische Aspekte aufgeführt, welche bei Datenbanken und Anwendungsprogrammen zu berücksichtigen sind.

Folgende Vorgehensweise wird nun bei der Arbeit mit dem „Ratgeber“ vorgeschlagen: Der Benutzer des Ratgebers wählt die für den jeweiligen Untersuchungsfall relevanten Module aus und erhält dadurch sämtliche zu berücksichtigende Aspekte, welche im Ratgeber für die ausgewählten Module sowie den darunter liegenden Modulen beschrieben sind.

2.2.2 Form

Im Rahmen der Spuren-Sicherung, Untersuchung und Interpretation werden häufig Checklisten verwendet.[21] Der Vorteil dieser Darstellungsform liegt darin, dass wesentliche Punkte nicht vergessen werden. Zudem können Checklisten verwendet werden, um die durchge-

[21] zum Beispiel Pfefferli Peter W. (2005).

führten Tätigkeiten zu dokumentieren und in einem möglichen Strafprozess für Dritte nachvollziehbar zu machen.

Aus diesen Gründen wurde entschieden, den „Ratgeber“ in Form einer Checkliste mit geschlossenen Fragen zu erstellen.

2.2.3 Inhalt

In den IT-Grundschutz-Katalogen des BSIs werden 421 Gefährdungen und 954 Massnahmen bezüglich der Informationssicherheit diskutiert. In der Regel bildet eine Analyse der Gefährdungen den Ausgangspunkt einer Beurteilung der Informationssicherheit.[22] Folgende Überlegungen sprechen jedoch dafür, dass bei der Erstellung einer Checkliste auf Massnahmen anstelle der Gefährdungen fokussiert wird:

- Die Massnahmen sind sehr konkret beschrieben und einfach zu messen. Demgegenüber sind die Gefährdungen gemäss den IT-Grundschutz-Katalogen relativ abstrakt.[23]
- Es handelt sich bei den BSI-Katalogen um einen Grundschutz, das heisst, viele der genannten Gefährdungen sind weit verbreitet und die abgeleiteten Massnahmen sollten dadurch in jedem Fall ergriffen werden.

Konkret wurde die Checkliste in folgenden Schritten erstellt:

1. Sämtliche Titel der Massnahmen gemäss IT-Grundschutz wurden in die Checkliste kopiert. Daneben wurde jeweils eine eindeutige Referenz auf die Quelle[24] beigefügt, so dass der Leser im Bedarfsfall an der betreffenden Stelle zusätzliche Informationen abrufen kann.
2. Massnahmen betreffend „Verfügbarkeit“ sowie „technischen Details“ wurden anschliessend wieder aus der Checkliste entfernt.
3. Die Massnahmen wurden anschliessend hinsichtlich Wichtigkeit für jedes Modul bewertet. Unwichtige Massnahmen wurden daraufhin aus der Checkliste entfernt und besonders wichtige wurden mit einem Stern (*) markiert.
4. Bei jeder Massnahme wurde der Titel mit einer geschlossenen Fragestellung ergänzt. Wo hilfreich, wurden zudem Beispiele, Risiko-Beschreibungen und Referenzen auf weitere BSI-Massnahmen beigefügt.

Da die Schritte 1 bis 4 relativ viel Entscheidungs- und Interpretationsspielraum offen lassen, wurden die Schritte von den verschiedenen Autoren gegenseitig überprüft. Dabei wurde darauf geachtet, dass die Checkliste die Aspekte der IT-Sicherheit genügend berücksichtigt und zugleich die Zweckmässigkeit und die Verständlichkeit für die Strafverfolgungsbehörden gegeben ist.

Von den ursprünglich 954 Massnahmen gemäss BSI sind schliesslich 61 Punkte in die Checkliste übernommen worden.

2.2.4 Einschränkungen und Grenzen

Einige Punkte sind absichtlich ausgeklammert worden. Beim Lesen und Gebrauch der Checkliste in der Praxis wird empfohlen, folgende Einschränkungen und Grenzen speziell zu beachten:

---

[22] Zum Beispiel Harris Shon, Seite 78.

[23] BSI, G 4.30, erwähnt zum Beispiel sehr allgemein die Gefährdung „Verlust der Datenbankintegrität/-konsistenz“.

[24] Bei der Quelle handelt es sich stets um Massnahmen gemäss BSI (2006).

- Technische Details: In den IT-Grundschutz-Katalogen sind einige Massnahmen enthalten, welche auf technische Details eingehen. Diese ausgewählten Massnahmen sind in der Checkliste nicht enthalten, da solche Massnahmen für allgemeine Abklärungen wohl zu ausführlich und für einen Nicht-IT-Experten kaum zu beantworten sind.[25]
- Verfügbarkeit: Einige Massnahmen des BSIs zielen ausschliesslich auf die System- und Datenverfügbarkeit ab, wobei die Integrität und Vertraulichkeit keine (oder eine stark untergeordnete) Rolle spielt. So ist beispielsweise zur Beurteilung der Integrität von sichergestellten Daten unerheblich, ob im fraglichen Gebäude Handfeuerlöscher zur Verfügung gestanden haben oder Massnahmen gegen Denial-of-Service-Attacken ergriffen wurden. Deshalb sind Massnahmen in der Checkliste nicht aufgeführt, welche ausschliesslich auf die Verfügbarkeit abzielen.
- Weitere Module: Mobiltelefone, PDAs, Telekommunikationsanlagen, Kopierer und Datenarchive wurden aus Zeitgründen nicht speziell behandelt und sind nicht explizit im Ratgeber als Module berücksichtigt. Einige Massnahmen aus der Checkliste treffen zwar für diese möglichen Module zu, es existieren jedoch auch weitere Massnahmen gemäss BSI, welche bei diesen Modulen zu beachten wären.
- Gefährdungen: Zu jeder Massnahme lassen sich via den BSI-Bausteinen die Gefährdungen ablesen. Auf eine explizite Referenzierung wurde in der Checkliste verzichtet; der Leser des Ratgebers kann somit die Gefährdungen nicht direkt beim BSI nachschlagen. Allerdings wurden in der Checkliste die wichtigsten Risiken hinsichtlich Datenintegrität zusammengefasst und bei jeder Massnahme erwähnt.
- Sprache: Aus Zeitgründen wurde die Checkliste ausschliesslich in Deutsch verfasst. Da die IT-Grundschutzkataloge sowohl in Deutsch als auch in Englisch gratis und einfach online abrufbar sind, würde einer Übersetzung der Checkliste ins Englische nichts im Wege stehen und den potentiellen Benutzerkreis über Sprachgrenzen hinaus vergrössern.
- Automatisierte Checkliste: Momentan liegt die Checkliste ausschliesslich als eine Aufzählung vor, welche von Hand sequentiell abzuarbeiten ist. Aus Zeitgründen wurde auf eine Tool-unterstützte Lösung verzichtet. So könnte die Checkliste automatisch generiert werden, indem der Benutzer in einer ersten Phase die relevanten Module auswählt, sprich anklickt, und daraufhin eine Liste erstellt wird, welche nur noch die relevanten Aspekte präsentiert.

2.3 Anwendung

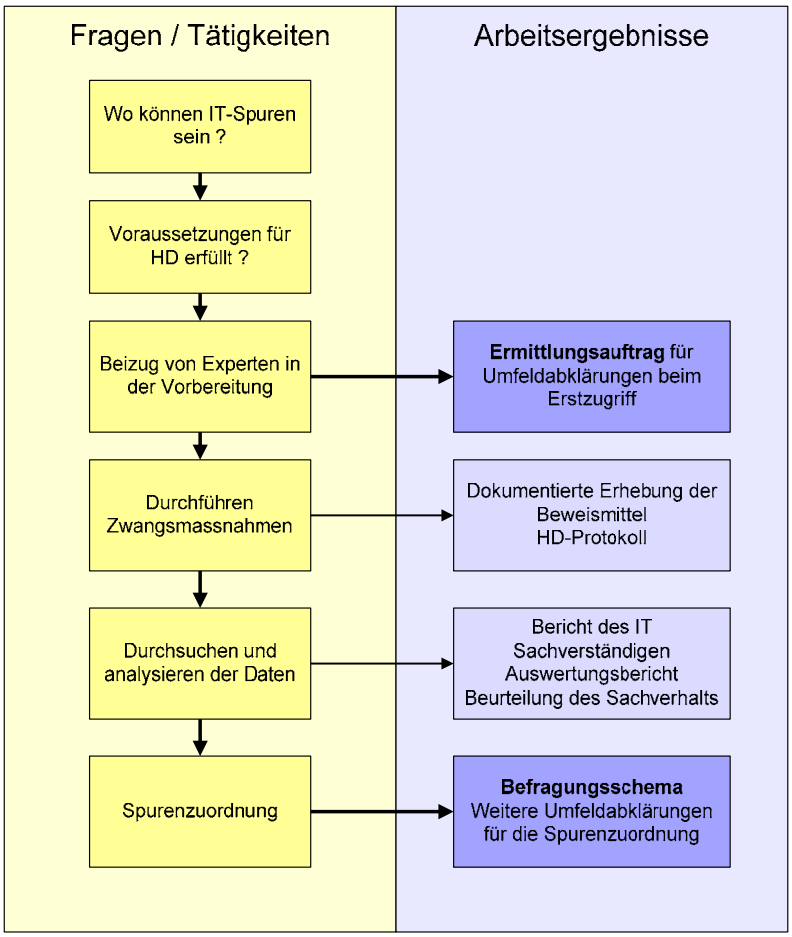
Die in die Checkliste aufgenommenen Massnahmen – respektive die dazu formulierten Fragen – dienen der gezielten Umfeldabklärung. Der in den vorliegenden Polizeirapporten und Auswertungsberichten dargestellte Sachverhalt soll als tatbestandsmässiges Verhalten bestimmten Personen zugeordnet werden. Dabei gilt die Annahme, dass Beweise im technischen Sinne bereits korrekt gesichert worden sind.

Die Checkliste ist ein Hilfsmittel mit einer einfachen Zielsetzung: sie unterstützt systematisch das Stellen von möglicherweise relevanten Fragen und gibt Hinwese auf Konstellationen, die im jeweiligen Sachverhalt ausgeschlossen werden können und auf Probleme, die berücksichtigt werden müssen.

[25] Zum Beispiel Empfehlungen zu UNIX-Systemeinstellungen betreffend dem Setzen von s- und t-Bits in der Massnahme M 4.19 des BSIs.

2.3.1 Einordnung in den Arbeitsablauf

Die folgende Abbildung zeigt in einer vereinfachten Darstellung den typischen Arbeitsablauf bei der Vorbereitung und Durchführung von Zwangsmassnahmen um IT-Spuren sicherzustellen:



Die Checkliste kann den Untersuchungsrichter in zwei Tätigkeiten unterstützen

- bei der Formulierung des Ermittlungsauftrags
- beim Aufstellen des Befragungsschemas

Die Formulierung eines **Ermittlungsauftrags** am Beispiel einer Checkliste sieht unter anderem folgende Punkte vor

- Abgrenzung der Zuständigkeit UR / Polizei.
- Klare Definition von Zwangsmassnahmen.
- Klare Vorgaben zu Form und Umfang von Auswertungen.[26]

Bei der Ausgestaltung des **Befragungsschemas** kann die Checkliste sowohl für Erstbefragungen als auch für spätere Befragungen und Einvernahmen beigezogen werden.[27]

Schliesslich kann die Checkliste bei der gezielten Formulierung von Aufträgen für ergänzende Auswertungen und für die ergänzende Beweissicherung beigezogen werden.[28]

---

[26] vgl. Anhang B: Checkliste Ermittlungsauftrag in Pornographiefällen gemäss Musterfall, Kantonspolizei St.Gallen, Punkte 5, 6 und 10

[27] vgl. Anhang H: Befragungsschema für Erstbefragung, Kantonspolizei St.Gallen

[28] vgl. Anhang A: Checkliste Ermittlungsauftrag in Pornographiefällen gemäss Musterfall, Kantonspolizei St.Gallen, Punkte 14 a, b und c sowie Punkt 16

2.3.2 Typologie der Spur

Die Sicherstellung und Auswertung der IT-Mittel liefert Indizien und Beweise, die als Spur zu verstehen sind. Diese Spuren können sein:

- eine Datei;
- eine logisch zusammengehörende Menge von Datensätzen in einer Datenbank;
- eine Log-Information;
- Metadaten der drei vorstehenden.

Eine Datei kann unterschiedliche Formate und Inhalte haben

- Word-Datei und weitere Textdateien;
- Excel-Datei auch mit mehreren Reitern;
- Bilder, Zeichnungen, Pläne;
- Multimedia (Mindestens bezüglich der Datenspeicherung wird auch ein Film oder eine Tonspur von einem IT-System als Datei behandelt, gleich wie ein Brief).

Auf ausgedruckte Dokumente und die damit verbundenen spezifischen Fragestellungen wird hier nicht eingegangen.

2.3.3 Bedeutung der Spur

Die IT-Auswertung im engeren Sinn liefert die Aussage, dass eine Spur auf einem IT-Mittel gefunden wurde. Zudem hat die Auswertung die Spur sichtbar gemacht. Die Auffindung der Spur ist verknüpft mit:

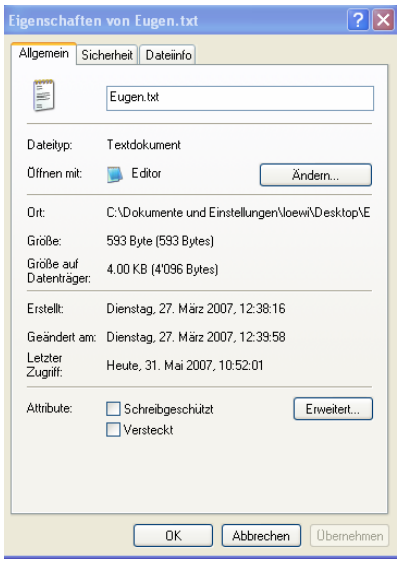
- der Speicherung von Dateien oder von Daten auf einem der sichergestellten IT-Mittel oder
- dem Nachweis der Übertragung von Dateien von oder zu einem sichergestellten IT-Mittel.

Die IT-Auswertung kann auch eine Aussage machen, ob die IT-Spur im technischen Sinne identisch ist mit einer anderen IT-Spur. Dies geschieht mit dem sogenannten Hash-Wert Vergleich. Damit ist das Vorhandensein einer Spur belegt, die Spur ist lesbar, sie kann ausserdem einer Vergleichsspur zugeordnet sein.

In der Zuordnung der Spur zum jeweiligen Lebenssachverhalt sind jedoch – je nach Fragestellung – weitere Angaben relevant:

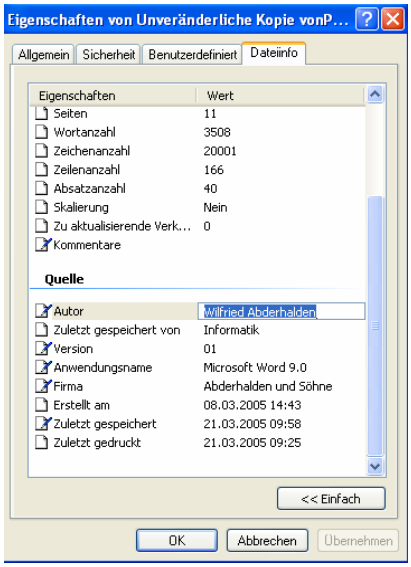
- Wer hat die Daten erstellt?
- Von wem sind die Daten nach der Erstellung noch verändert worden?
- Vom wem oder an wen sind die Daten vermittelt worden?
- Wer hat die Daten eingesehen?

Diese Angaben kommen entweder aus der Datei selber, aus den Metadaten der Datei oder aus Log-Daten, die die Zugriffe auf die Daten aufzeichnen.



Beispiel: Metadaten einer Textdatei

Aus diesen Angaben ist ersichtlich, wann die Datei erstellt und verändert wurde, die Autoren sind jedoch nicht aufgezeichnet. Die Angabe über den letzten Zugriff ist nicht eindeutig. Entweder wurde die Datei zu diesem Zeitpunkt geöffnet oder die Eigenschaften zu dieser Datei wurden zu diesem Zeitpunkt letztmals betrachtet.



Beispiel: Metadaten einer Worddatei

Aus diesen Angaben ist unter anderem ersichtlich, wer der Autor ist. Die Angabe ist aber überschreibbar, das heisst: über die Eigenschaften der Datei kann ein Autor eingetragen werden, ohne dass die Datei selber geöffnet werden muss.

2.3.4 Zuordnung der Spur

Als Daten im Sinne der Legaldefinition kommen alle Informationen über einen Sachverhalt in Form von Buchstaben, Zahlen, Zeichen, Zeichnungen und ähnliches in Frage, die zur weiteren Verwendung vermittelt, verarbeitet oder aufbewahrt werden.[29]

[29] Trechsel Stefan., Urkundenfälschung 11c.

Die Basis ist also eine lesbare Spur in Form von Daten in Verbindung mit einer oder mehreren weiteren Tatsachen. Die Tatsachen besagen, wann und von wem die Daten erstellt wurden, ob und von wem sie verändert worden sind, an wen sie übermittelt wurden und wer die Daten gesehen hat. Die IT-Ermittlung sollte diese Angaben immer liefern.

In einer ersten Bewertung kann so unter Ausschluss aller organisatorischen Einflüsse beurteilt werden, ob die Spur im Sinne des konkreten Sachverhalts eindeutig zugeordnet werden kann.

An diesem Punkt setzt die Checkliste an. Mit Hilfe dieses Arbeitsmittels kann hinterfragt werden, ob die technischen Ergebnisse der IT-Ermittlung eindeutig dem Lebenssachverhalt zugeordnet werden können. Diese Zuordnung kann aus verschiedenen Gründen fehlschlagen. Einige mögliche Problemstellungen bei der Zuordnung der Spuren werden nachfolgend kurz dargestellt:

Für die Zuordnung des Autors (für die Erstellung oder die Veränderung von Daten):
- Die Angabe über den Autor kann bei der Erstellung der Daten oder nachträglich gefälscht worden sein.
- Die Angabe über den Autor ist abgeleitet aus dem Login und es ist einem Dritten möglich, mit diesem Login zu arbeiten. Dadurch ist die Angabe über den Autor nicht eindeutig oder irreführend.

Für den Zeitpunkt der Erstellung oder der Veränderung von Daten:
- Die Angabe über den Zeitpunkt der Erstellung oder der Veränderung der Daten kann nachträglich gefälscht worden sein.
- Die Angaben über den Zeitpunkt sind aus der Systemzeit abgeleitet und es ist einem Dritten möglich, diese Systemeinstellungen zu verändern.

Für die Übermittlung von Daten:
- Die Angaben zur Übermittlung von Daten (Sender, Empfänger, Zeitpunkt) sind im Moment der Übertragung oder nachträglich verfälscht worden.
- Es war auch einem Dritten möglich, die selben Daten zu empfangen oder zu versenden.

Für das Lesen von Daten:
- Die Log-Angaben zum Lesen von Daten wurden nachträglich verändert.
- Die Leseprozesse werden nicht lückenlos dokumentiert (beispielsweise das Kopieren einer Datei und das Drucken wird nicht protokolliert).
- Der Zugriff auf die Daten und der Versand werden nicht lückenlos dokumentiert. In den letzten beiden Fällen ist es so möglich, dass unbekannte Dritte die Daten auf einem weiteren Arbeitsplatz, möglicherweise auch ausserhalb der untersuchten IT-Umgebung lesen konnten.

Zusammengefasst sind die folgenden Handlungen des Verdächtigen oder von Dritten in die Frage der Spurzuordnung einzubeziehen:
- Erzeugen von verfälschten Hinweisen in Metadaten oder Log-Dateien,
- Erzeugen von „echten“ Hinweisen in Metadaten oder Log-Dateien durch das Nutzen von fremden Accounts (Logins) oder durch Systemmanipulationen (zum Beispiel Systemzeit verstellen),
- Löschen von Metadaten und Log-Dateien,
- Umgehung von Sicherheitsmassnahmen durch Nutzung von Privilegien (Administrator-Rechten),

- Umgehung von Sicherheitsmassnahmen durch Datenmanipulation via Bordmittel des Betriebssystems und der Datenbanken (beispielsweise direkter Zugriff auf SQL-Tabellen mit Hilfe eines Administrations-Programms).

2.3.5 Allgemeine Vorgehensweise

Zur Tätigung von Umfeldabklärungen bei Straffällen mit IT-Bezug stehen folgende Arbeitshilfen zur Verfügung:
- drei Leporellos (Checklisten in Kurzform);
- eine Detail-Checkliste;
- in der elektronischen Form hat die Checkliste einen Hyperlink auf die IT-Grundschutz-Kataloge des BSI.

Auf dem Leporello sind die Nummern aus dem IT-Grundschutz-Katalog und eine zusammenfassende Frage abgebildet. Mit einem Stern sind die besonders wichtigen Prüfpunkte gekennzeichnet.

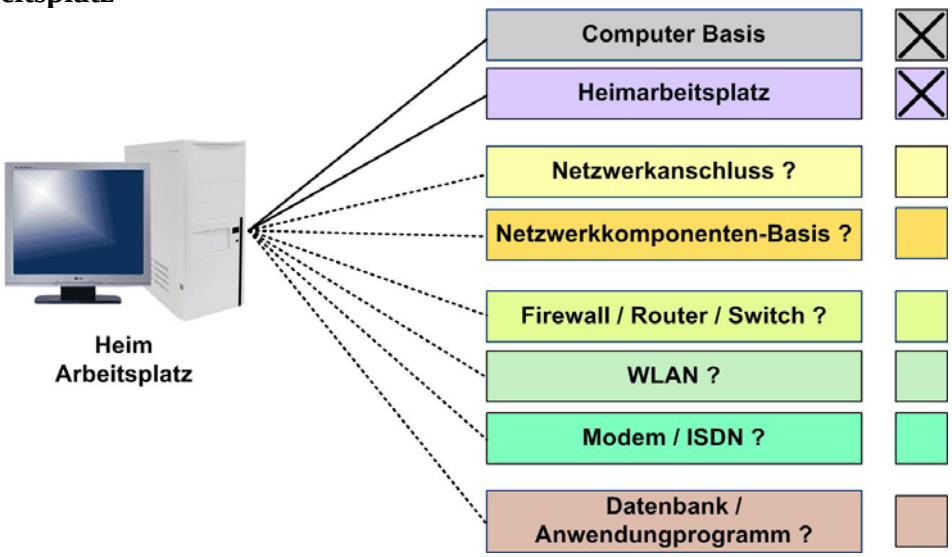
In der Detail-Checkliste sind zusätzliche Erläuterungen meist in Form von Beispielen enthalten. Zudem wird beschrieben, welche Risiken bestehen, wenn die Frage mit „Nein“ zu beantworten ist. Schliesslich sind Querverweise zu weiteren relevanten Prüfpunkten aufgeführt. Der Hyperlink auf den IT-Grundschutz-Katalog zeigt die gesamte Beschreibung zum jeweiligen Prüfpunkt.

Die Checkliste ist so aufgebaut, dass sie nach einem einfachen Muster bearbeitet werden kann:
a) Auswahl des Leporellos;
b) Festlegen der anwendbaren Module;
c) Abarbeiten der Prüfpunkte von oben nach unten;
d) Prüfen, ob ein Mangel für den konkreten Sachverhalt relevant ist (bei Nein-Antworten).

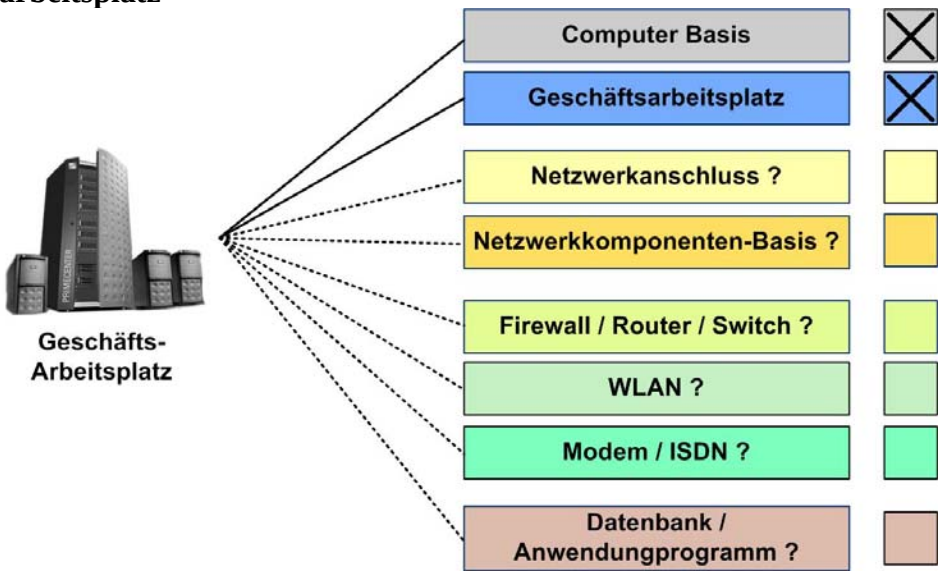
a) Auswahl der Leporellos
Es gibt für die unterschiedlichen Verwendungen von Geräten drei verschiedene Checklisten:
- Heimarbeitsplatz;
- Geschäftsarbeitsplatz;
- Mobiler Einsatz.

Mit dieser Grundauswahl sind zwei Prüfbereiche festgelegt: „Computer-Basis“ und das für das jeweilige Gerät typische Modul. Ausserdem werden die auf dieses Gerät anwendbaren Module aufgelistet.

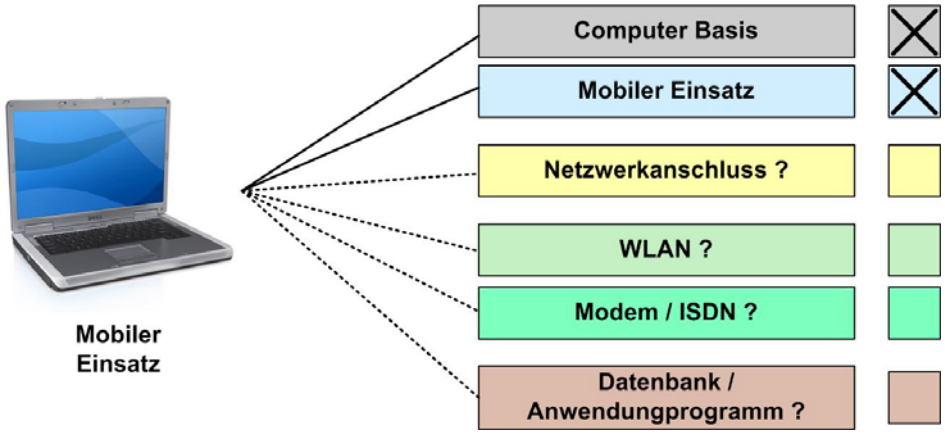
Heimarbeitsplatz



Geschäftsarbeitsplatz



Mobiler Einsatz



So wie die Checkliste heute aufgebaut ist, muss pro gleichartiges Gerät (bezüglich der technischen Voraussetzungen und der Verwendung) eine Checkliste geführt werden.

b) Festlegen der anwendbaren Module
Beim Festlegen der anwendbaren Module sind nur minimale technische Kenntnisse notwendig. Im Anhang 1 (IT-Checkliste) sind für alle drei Checklisten Entscheiddiagramme beigelegt.
Die einfachen Faustregeln:

- ohne Netzwerkanschluss muss nur noch festgelegt werden, ob das Modul „Datenbank / Anwendungsprogramm“ geprüft werden muss;
- das Modul Netzwerkkomponenten-Basis ist bei Heimarbeitsplätzen nur anwendbar, wenn im privaten Umfeld eine professionelle Netzwerk-Infrastruktur aufgebaut wurde.

c) Abarbeiten der Prüfpunkte von oben nach unten.
Die Checkliste ist so aufgebaut, dass die Fragen innerhalb der Module aufeinander aufbauen. Deshalb können die Fragen von oben nach unten abgearbeitet werden. Sobald eine Frage innerhalb eines Bereichs mit „Nein“ beantworten wird, ist die Beantwortung der folgenden Fragen möglicherweise nicht mehr notwendig, zumindest werden sie durch die Nein-Antwort auf eine zuvor gestellte Frage relativiert. Auch die Wirksamkeit der vorher mit „Ja“ beantworteten Prüfpunkte sind allenfalls wieder in Frage zu stellen.

Beispiel: Computer-Basis, Massnahmen Organisation

Prüfpunkt	Antwort	Bedeutung
M 2.5 Aufgabenverteilung und Funktionstrennung	**JA**	Voraussetzungen für eine weitere organisatorische Umsetzung sind gegeben
M 2.7 Vergabe von Zugangsberechtigungen	**JA**	Funktionstrennung wird durch die persönliche Zuteilung von Benutzerkonti umgesetzt.
M 2.11 Regelung des Passwortgebrauchs	**NEIN**	Für den Prüfpunkt 2.7: Die persönlichen Benutzerkonti können von verschiedenen Personen genutzt werden. Auf die folgenden Prüfpunkte M 2.23 und M 2.38 wirkt sich dieser Mangel ebenfalls aus.

d) Prüfen, ob ein Mangel für den konkreten Sachverhalt relevant ist (bei Nein-Antworten)
Ein Prüfpunkt wurde mit „Nein“ beantwortet. Das bedeutet aber nicht, dass damit automatisch ein Problem verbunden ist. Es kann sein dass die Frage nicht relevant ist:

- weil es sich aus dem konkreten Sachverhalt so ergibt;
- weil die Frage aus technischen Gründen nicht anwendbar ist;
- weil es zur konkreten Problemstellung eine Umgehungslösung gibt.

Dieser Arbeitsschritt kann eigentlich nur dann zufriedenstellend ausgeführt werden, wenn die Kenntnis des Sachverhalts sowie die Vertrautheit mit der Technik und dem IT-Grundschutz-Katalog in einer Person, oder in einem Team vereint sind. Im Rahmen dieser Arbeit können höchstens einige Anhaltspunkte aufgeführt werden.

Zum Schluss noch ein Hinweis für weniger Geübte und Ungeübte: es kann sein, dass mit Hilfe dieser Checkliste Fragen gestellt werden, die für einen mit der IT besser vertrauten Befragten im konkreten Fall offensichtlich nicht anwendbar sind. Man sollte sich von solchen

Erlebnissen nicht entmutigen lassen. In diesen Fällen kann der Fachmann dem Laien in der Regel auch plausibel erklären, warum die Frage nicht anwendbar ist.

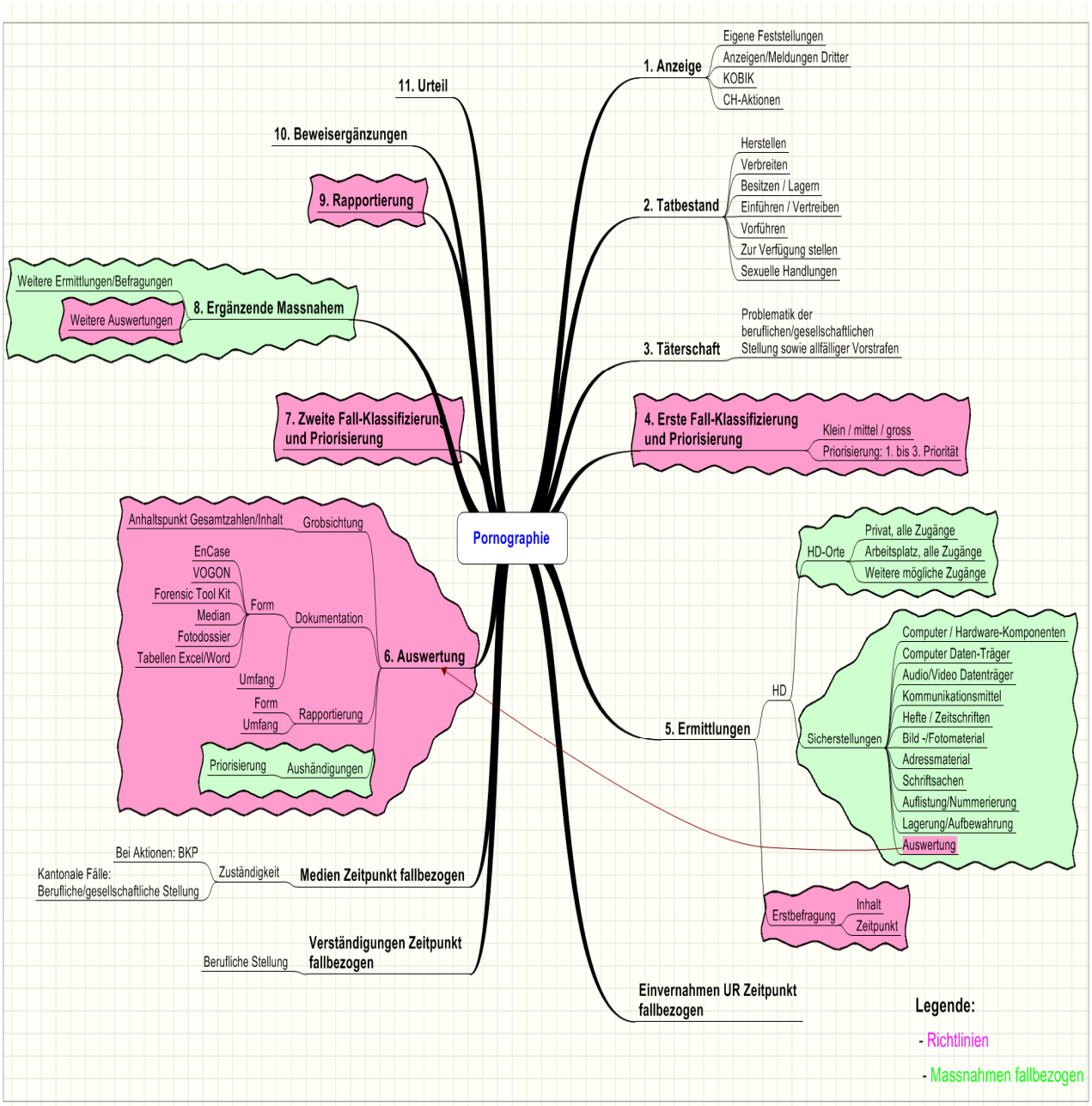
2.4 Fazit

Die vorliegende Arbeit zeigt auf, dass die Strafverfolgungsbehörden mit einer neuen Herausforderung namens IT konfrontiert sind. IT ist für viele Untersuchungsrichter, Staatsanwälte und Richter ein Schreckgespenst. Dieses Gespenst – so schrecklich es auch sein mag – lässt sich jedoch nicht vertreiben.

Wie bereits in der Kurzzusammenfassung erwähnt wurde, handelt es sich bei der Checkliste, welche im Rahmen der vorliegenden Arbeit zusammengestellt wurde, nicht um ein ausgefeiltes Expertensystem, das dem Untersuchungsrichter oder dem Staatsanwalt nach Abarbeiten der Fragen den Täter auf dem goldigen Tablett serviert. Es ermöglicht den Strafverfolgungsbehörden lediglich, die richtigen Fragen zu stellen.

Die Checkliste leistet einen Beitrag, um die Lücke zwischen den Strafverfolgungsbehörden und den IT-Sachverständigen zu schliessen.

Anhang A
St.Gallen: Musterfall



Anhang B
ST. Gallen: Checkliste Auftragsformulierung

Kantonspolizei St.Gallen
Kriminalpolizei
Klosterhof 12, 9001 St.Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kaposg.ch

Checkliste Ermittlungsauftrag in Pornographie-Fällen gemäss Musterfall

1. Prüfung der Anzeige gemäss Punkt 2 und 3 (Musterfall)
   a. Tatbestands-Qualifizierung
   b. Täterschaft
2. Fall-Klassifizierung (kleiner/mittlerer/schwerer Fall)
3. Fall-Priorisierung (1. bis 3. Priorität)
4. Ermittlungsmassnahmen und Ermittlungsziel gemäss Punkt 5
5. Abgrenzung der Zuständigkeit UR / Polizei gemäss Punkt 5 und folgende (Grundlagen der Zusammenarbeit: Auftragsverhältnis/Teamarbeit)
6. Klare Definition von Zwangsmassnahmen gemäss Punkt 5
   a. Vorladung/Zuführung/Festnahme
   b. KT-Behandlung
   c. Hausdurchsuchungen
   d. Sicherstellungen/Beschlagnahmungen/Editionen
   e. Randdatenerhebungen/Überwachungsmassnahmen
7. Einvernahmen/Befragungen
   Absprache und Abgrenzung der Durchführung UR / Polizei
8. Verständigungen
   Absprache und Abgrenzung der Durchführung UR / Polizei
9. Medienorientierung
   Absprache und Abgrenzung der Zuständigkeit UR / Polizei
10. Klare Vorgaben zu Form und Umfang von Auswertungen gemäss Punkt 6 (Grobsichtung / Vollauswertung)
11. Priorisierung der Auswertungen
12. Klare Vorgaben zu Form und Umfang von Berichten/Rapporten gemäss Punkt 9, sofern sie von der Standardform abweichen
13. Zweite Fall-Klassifizierung
14. Klare Definition von ergänzenden Massnahmen gemäss Punkt 8
    a. Ergänzende Abklärungen/Befragungen
    b. Weitere Zwangsmassnahmen
    c. Ergänzende Auswertungen
    d. Aushändigungen/Beschlagnahmungen von Sicherstellungen
15. Klare Vorgaben zu Form und Umfang von Berichten/Rapporten gemäss Punkt 9, sofern sie von der Standardform abweichen
16. Klare Formulierungen von Aufträgen für ergänzende Beweissicherungen gemäss Punkt 10

Anhang C
ST. Gallen: Auswertungsbericht

Kantonspolizei St. Gallen
Kriminalpolizei
Klosterhof 12, 9001 St. Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kapo.sg.ch

Proz.Nr.
Zuständig
Direktwahl
St. Gallen,

Auswertungsbericht Digitale Forensik

Im Strafverfahren gegen

Muster	Peter (vollständige Personalien) wegen des Verdachts der Pornografie
Proz. No. ST.	des UA xxx - Zuständig UR lic.iur. Peter Richter Polizeilicher Sachbearbeiter: Wm Walter Nase, Kantonspolizei Spezialdienst

1. **Untersuchungsauftrag** (**Auftrag des polizeilichen Sachbearbeiters)**

2. **Untersuchungsgut**
   (tabellarische Auflistung aller untersuchten PC-Geräte, Festplatten und Datenträger. gemäss Untersuchungsauftrag)

3. **Untersuchungsmethode**
   Kurze Ausführung und Verweis auf Anhang für weitergehende Erklärungen. Im Anhang sollen auch technische Ausdrücke und Bezeichnungen erklärt werden.

4. **Untersuchungsergebnisse**

   a) Antworten auf Fragen im Ermittlungsauftrag:
   b) Beurteilung der techn. Hilfsmittel und deren Anwendung (Tatvorgehen):
   Welche technischen Hilfsmittel und Vorgehen wurden durch die Täterschaft benutzt.
   Vorläufige Qualifizierung des Vorgehens (z.B. Hinweise bei Verdacht auf Gewerbsmässigkeit, Methode der Weiterverbreitung oder Beschaffung, Eigenverschulden oder technische Fehler/Automatismus, etc.)
   c) Besondere Feststellungen: (z.B. Hinweise auf technische Eigenarten wie Systemfehler, Automatismen oder spezielle Systemmanipulationen resp. -einstellungen etc.)

5. **Schlussbemerkungen**
   Empfohlene Einziehungen:

Beilagen:
- Anhang mit technischen Erläuterungen
- Y Datenträger mit den angeforderten Dokumenten (im Original für Akten und als Arbeitskopie für polizeilichen Sachbearbeiter)

Anhang D
ST. Gallen: Sicherstellungsbericht

Kantonspolizei St. Gallen
Kriminalpolizei
Klosterhof 12, 9001 St. Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kapo.sg.ch

Vorlage Rapportierung

Proz.Nr.
Zuständig
Direktwahl
St. Gallen,

Sicherstellungsbericht Digitale Forensik

Im Strafverfahren gegen

Muster	Peter (vollständige Personalien) wegen des Verdachts der Pornografie
Proz. No. ST.	des UA xxx - Zuständig UR lic.iur. Peter Richter Polizeilicher Sachbearbeiter: Wm Walter Nase, Kantonspolizei Spezialdienst

1. **Einleitung**
   Kurze Einleitung (z.B. Der Angeschuldigte steht unter dem Verdacht, sich gegen Bezahlung mit seiner Kreditkarte Zugang zu strafbaren Internet-Dateien verschafft zu haben.

2. **Untersuchungsgut**
   (tabellarische Auflistung aller sichergestellten und zu untersuchenden PC-Geräte, Festplatten, Datenträger)

3. **Sicherstellungsmethode**
   Kurze Ausführung und Verweis auf Anhang für weitergehende Erklärungen. Im Anhang sollen auch technische Ausdrücke und Bezeichnungen erklärt werden.

4. **Untersuchungsergebnisse der Grobsichtung des Untersuchungsgutes**

   Datenträger xxx enthält insgesamt ohne Qualifizierung des Inhaltes:

Anzahl Bilder:	☐ <10’000	☐ <100'000	☐ <1’000'000	☐ >1’000'000
Anzahl Filme:	☐ <1’000	☐ <10'000	☐ <100'000	☐ >100’000

   Anzahl Bilder/Filme insgesamt: ca. _____

   Auf dem Untersuchungsgut installiert sind folgende Programme:

   Filesharing-Programme:
   Im Shared Folder vorhanden sind: ca. .... Filme und ca. ..... Bilder

   Weitere Programme:
   - z.B. Verschlüsselungsprogramme

Mailkonten:

Benutzerkonten:

Die Grobsichtung der Daten ergab, dass sich darunter Bild- oder Filmmaterial befindet, welche für die Ermittlungen von Relevanz sein könnten. Vorwiegend handelt es sich dabei um: (Wenn Feststellungen gemacht wurden, dann mit Stichwörtern analog Schlussbericht)

5. Bemerkungen/Besondere Feststellungen

Beilagen:
- Datensicherungsbänder
- Checkliste technische Datensicherung
- Anhang mit technischen Erläuterungen

Anhang E
ST. Gallen: Schlussbericht

Kantonspolizei St. Gallen
Kriminalpolizei
Klosterhof 12, 9001 St. Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kapo.sg.ch

Proz.Nr.
Zuständig
Direktwahl

St. Gallen,

Schlussbericht über die kriminalpolizeilichen Ermittlungen

Im Strafverfahren gegen

Muster	Peter (vollständige Personalien) wegen des Verdachts der Pornografie
Proz. No. ST.	des UA xxx - Zuständig UR lic.iur. Peter Richter Polizeilicher Sachbearbeiter: Wm Walter Nase, Kantonspolizei Spezialdienst

1. Einleitung

2. Sachverhalt

Kurze Schilderung der Verdachtsmomente, z.B. Der Angeschuldigte steht unter dem Verdacht, sich gegen Bezahlung mit seiner Kreditkarte Zugang zu strafbaren Internet Dateien verschafft zu haben.

3. Zwangsmassnahmen

4. Auswertung

a) Total verdächtiger Dateien
Gemäss Sicherstellungsbericht der Dienststelle IT enthielten die Datenträger insgesamt folgende Dateien (Uebernahme von Ziff. 4 des IT-Berichts):

b) Gemäss Auftrag vom .....wurden die verdächtigen Datenträger

☐ gesamthaft ausgewertet

☐ teilweise ausgewertet; Von den insgesamt sichergestellten Dateien wurden ..... Bild und .....Filmdateien einer Detailauswertung unterzogen.

Die Ergebnisse der Auswertung lauten wie folgt:
Bilddateien: 35 % Kinderpornografie
10 % Tierpornografie
5 % Sexuelle Gewalt
5 % Ausscheidungspornografie

35 % weiche Pornografie
10 % Andere

Filmdateien: 35 % Kinderpornografie
10 % Tierpornografie
5 % Sexuelle Gewalt
5 % Ausscheidungspornografie
35 % weiche Pornografie
10 % Andere

Davon sind Temporäre Internet-Dateien(automatische Downloads):

Manuell heruntergeladene Dateien:

Pornografische Dateien im Shared Folder:

davon sind

☐harte Pornografie .....%

☐ weiche Pornografie ..... %

selbst hergestellte oder manipulierte/veränderte Dateien:
..... (Kurzbeschreibung)

E-mail Verkehr: ☐ keine Hinweise auf strafbare Inhalte
☐ Verdacht auf strafbare Inhalte
---------- (Kurzbeschreibung)

5. Weitere Erkenntnisse

6. Rechtshilfeersuchen

7. Untersuchungshaft

8. Schlussbemerkungen
Empfohlene Einziehung:

Auflistung sämtlicher „verseuchter“ Datenträger

Beilagen:

- X Datensicherungsbänder
- Y Datenträger mit den angeforderten Dokumenten
- Ausdrucke in Papierform

Anhang F
ST. Gallen: Priorisierung und Klassifizierung

Klassifizierung nach Tathandlungen

Schwer

- Herstellung unter physischem Missbrauch von Drittpersonen, insbesondere Kindern (Beschuldigter steht im Verdacht direkt beteiligt zu sein)
- Herstellung mittels Foto-/ Filmmontagen unter Verwendung von privaten Fotos oder Filmen
- gewerbsmässige Handlungen

Mittel

- Verbreiten über das Internet (z.B. Filesharing oder Mails)
- Zur Verfügung stellen an Kinder und Jugendliche
- Herstellen durch Verändern, Vergrössern oder neu Zusammensetzen von fremden Darstellungen, d.h. ohne persönlichen Bezug zu den Modellen/ohne direkte physische Beteiligung des Beschuldigten

Gering

- Herstellen im Sinne von Herunterladen (Eigengebrauch)
- Beschaffen über das Internet (Abonnement in Memberbereichen)

Priorisierung

Priorität 1

Immer vordringlich an die Hand zu nehmen sind

a) sensitive Personen-Gruppen; Verdächtige, die in Beruf oder Freizeit mit Kindern arbeiten, z.B. Ärzte, Pädagogen, Sportlehrer, Bademeister, Musiklehrer etc.
b) Verdächtige, die vorbestraft sind wegen sexueller Handlungen mit Kind
c) einschlägig Vorbestrafte
d) Haftbegründung: Die Erkenntnisse aus der Auswertung sind für die Haftbegründung entscheidend
e) Fälle mit Klassifikation “schwer“
f) Gefährdung Dritter und wenn grosses öffentliches Interesse

Priorität 2

a) Nicht sensitive Personen-Gruppen
b) Ermittlungsfortgang: Die Erkenntnisse aus der Auswertung sind für den Fortgang der Ermittlungen und/oder die Haftverlängerung entscheidend
c) Rasche Aushändigung: Eine rasche Aushändigung der Sicherstellungen ist aus speziellen Gründen anzustreben (z.B. Computer und Datenträger von Drittpersonen, werden für die Berufsausübung zwingend benötigt).
d) Fälle mit Klassifikation “mittel“

Priorität 3

a) Standardfälle: Die Auswertung der Sicherstellungen dient "lediglich" der Beweissicherung und hat in zeitlicher Hinsicht keinen direkten Einfluss auf den Fortgang des Ermittlungsverfahrens
b) Fälle mit Klassifikation “gering“

Für Zweitklassifizierung gilt:

1 Ist der Angeschuldigte geständig, dann wird in der Regel die Klassifizierung „gering“ angewendet. Ausnahmen bilden Fälle mit Klassifizierung “schwer“.
2 Liegt ein qualifiziertes Tatvorgehen vor (mit Fachwissen, besondere Vorkehrungen) so wird die Klassifizierung „schwer“ angewandt.

Anhang G
ST. Gallen: Frageschema

Kantonspolizei St. Gallen
Kriminalpolizei
Klosterhof 12, 9001 St. Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kapo.sg.ch

Befragungsschema für Erstbefragung
(am Beispiel Verdacht Kinderpornografie über das Internet)

Einvernahme als Angeschuldigter

Vorhalt:
Sie werden als Angeschuldigter wegen Delikt einvernommen. Das Untersuchungsamt hat deshalb gegen Sie eine Strafuntersuchung eröffnet.

Sie werden darauf aufmerksam gemacht, dass Sie nicht zur Aussage verpflichtet sind und das Recht haben, einen Verteidiger beizuziehen. Haben Sie das verstanden?

Aufgrund Lebenssachverhalt kurz wiedergeben besteht der Verdacht, dass Sie sich des/der rechtl. Tatvorwurf (z.B. der Pornografie) schuldig gemacht haben. Sie haben jetzt Gelegenheit, sich umfassend dazu zu äussern[30] Was sagen Sie zu diesem Vorwurf der/des Tatvorwurf[31]?

Was verstehen Sie unter Bsp. Pornografie?

(Falls entsprechende Zwangsmassnahmen bereits erfolgt sind:) An Ihrem Wohnort wurde soeben eine Hausdurchsuchung durchgeführt und Beweisgegenstände sichergestellt. Haben Sie Bemerkungen dazu?

Wohnt ausser Ihnen sonst noch jemand in Ihrer Wohnung an genaue Adresse

Kreditkarten:
Benutzen oder benützten Sie je Kreditkarten?

(Wenn ja) Auf wessen Namen lauten diese?

Bei welcher Kreditkartenfirma und seit wann?

Führen Sie diese Karten im Moment auf sich?

(Wenn ja: Protokollnotiz) Kreditkartenfirma.... Karten-Nr. .... lt.auf ....

Werden diese ausser Ihnen sonst noch von jemandem benutzt? (Falls ja: Möglichst genaue Angaben der betreffenden Person(en).)

---

[30] Bericht des Angeschuldigten, sollte dem Verhör stets vorausgehen, siehe Art. 76 Abs. 1 StP

[31] im Zweifelsfall immer zuvor UR fragen

Erhalten Sie für Ihre Kreditkartenbezüge eine Rechnung oder erfolgt eine direkte Belastung auf Ihrem Konto?

Wo bewahren Sie Ihre Kreditkartenunterlagen auf?

Wie kontrollieren Sie die Richtigkeit der Kreditkartenbelastung?

Ist es bezüglich der Belastung jemals zu Unregelmässigkeiten gekommen?

Wurde Ihre Kreditkarte jemals entwendet oder wurden Sie jemals Opfer eines Kreditkartenmissbrauchs?

Computernutzung:
Von wem wird Ihr Computer benutzt? (Gegebenenfalls: Möglichst genaue Angaben über weitere Benutzer, Intensität und Zweck der Dritt-Benutzung, Eingerichtete Benutzerkonten.)

Nennen Sie mir die Passwörter, die allenfalls nötig sind, um Ihren Computer und die installierten Programme in Betrieb zu nehmen (für alle Benutzerkonten)?

Haben Sie einzelne passwortgeschützte Dateien/Dokumente/Tabellen? (wenn ja: verwendete Passwörter?)

Verwenden Sie Verschlüsselungsprogramme und Dateien/Dokumente/Tabellen zu schützen?

Verfügen Sie an Ihrem Arbeitsplatz über einen Computer?

Falls Ja: Allein oder haben andere Personen Zugriff dazu?

Mit oder ohne Internetanschluss?

Internet:
Verfügen Sie über einen Internet-Anschluss?

Wenn ja, seit wann und bei welchem Provider?

Wie lautet Ihre aktuelle E-Mail Adresse?

Haben Sie weitere E-Mail Adressen? wie lauten diese?

Haben Sie jemals pornografisches Material (Bilder, Filme, Texte), insbesondere kinderpornografisches Material, im Internet gesucht?

Als "Pornografie" im Sinne von Art. 197 StGB gelten Schriften, Ton- oder Bildaufnahmen und Abbildungen oder andere Gegenstände solcher Art die sexuelle Handlungen mit Kindern, Tieren, menschlichen Ausscheidungen oder Gewalttätigkeiten zum Inhalt haben.
Besitzen oder besassen Sie in irgend einer Form solches Material?

Haben Sie jemals solches Material heruntergeladen?
(Wenn ja: wann, wie oft, was genau...)

Sind auf Ihrem Computer und/oder in Ihrem Besitz befindlichen Datenträgern kinderpornografische oder andere hartpornografische Daten der genannten Art gespeichert?

Haben Sie sich bei irgendwelchen Anbietern pornografischer Inhalte eine kostenpflichtige Mitgliedschaft errichtet oder sich im Zusammenhang mit einem Gratiszugang registrieren lassen?

Wenn ja, bei welchen Anbietern und zu welchen Konditionen?

Gemäss uns zugegangener Unterlagen wurde Ihre Kreditkarte als Zahlungsmittel für einen oder mehrere Zugriffe auf Websites mit kinderpornografischen Angeboten verwendet. Was sagen Sie dazu?

Wer hat sich bei diesen Websites registrieren lassen?

Was für Passwörter wurden dabei verwendet?

Wann und von welchem Computer aus wurde die Registrierung vorgenommen bzw. wurde auf die fraglichen Websites Zugriff genommen?

Was wurde auf diesen Websites konkret angeboten?

Gemäss den uns vorliegenden Informationen haben die abonnierten Websites Kinderpornografie enthalten. Ihre Stellungnahme?

Was verstehen Sie unter Kinderpornografie?

Wie viele Websites haben Sie abonniert und für wie lange?

Haben Sie ab abonnierten Websites hartpornografische Bilder, Filme oder Texte heruntergeladen? (Falls ja: auf welchen PC - privat oder Arbeitsplatz?)

Wenn ja, was geschah mit diesen Daten?

Bewahren Sie pornografisches, insbesondere kinderpornografisches Material auf?

Wenn ja, wo?

Hatten oder haben Sie Kontakte zu Personen, welche an kinderpornografischem oder anderem hartpornographischem Material interessiert sind?

Wenn ja, was für Kontakte und zu wem?

Haben Sie jemals hartpornografisches Material hergestellt, getauscht, angeboten, vorgezeigt oder jemandem zugänglich gemacht?

Nutzen Sie Filesharing Programme? (Wenn ja, welche? - z.B. Kazaa, eMule, Beashare, e-Donkey usw.)

(Falls ja) Sind mit diesem Programm hartpornographische Darstellungen in Ihren Besitz gelangt?

Sind Sie in diesem Filesharingprogramm als Anbieter aufgetreten?

(Falls Ja) Was für Dateien?

(Falls Nein) Welche Vorkehren haben Sie getroffen, um den weiteren Zugriff auf die Darstellungen zu verhindern, welche aus diesen Programmen stammen?

Sind Sie im Umgang mit dem Filesharingprogramm vertraut? -> Beschreiben Sie die Funktionsweise dieses Programms.

Haben Sie hart pornographische Darstellungen kopiert? (Falls ja: Wann, wie, wo?)

Was für ein Programm verwenden Sie für den Mail-Verkehr?

Verfügen Sie bei einer externen Stelle über zusätzlichen Speicherplatz?

Welche Bereiche des Internet nutzen Sie?

Haben Sie Zugang zu Newsgruppen? (Wenn ja: Zugangsprovider)

Chatten Sie? (Wenn ja: Wo? Unter welchen Pseudonymen?)

Benutzen Sie ICQ, NetMeeting oder mlRC? (Pseudonyme?)

Fühlen Sie sich sexuell zu Kindern hingezogen?

Hatten Sie jemals sexuelle Kontakte zu Kindern?

Fragen zur Person:
Wie sind Ihre finanziellen Verhältnisse? (Einkommen, Vermögen, Schulden etc.)

Sind sie vorbestraft?

(Wenn ja) Weswegen? durch wen, wo und wann?

Schluss:
Haben Sie alles verstanden?

(Nach Vorhalt/Durchsicht des Protokolls) Haben Sie Ergänzungen oder Berichtigungen zum Protokoll anzubringen?

Wurden Sie korrekt behandelt?

Anhang H
ST. Gallen: Anhang zum Befragungsschema

Kantonspolizei St. Gallen
Kriminalpolizei
Klosterhof 12, 9001 St. Gallen

Telefon 071 229 49 49
Telefax 071 223 26 60
Internet www.kapo.sg.ch

Anhang zum Befragungsschema:

Auszug aus dem Strafprozessgesetz vom 1. Juli 1999

Protokoll
a) Protokollierungspflicht
Art. 69.
1 Die Beweiserhebung wird protokolliert.

b) Inhalt
1. allgemein
Art. 70.
1 Aus dem Protokoll sind ersichtlich:
a) Ort, Beginn und Ende der Verhandlung;
b) die an der Verhandlung mitwirkenden Personen;
c) der Gang der Verhandlung;
d) die Einhaltung der gesetzlichen Formvorschriften;
e) die getroffenen Feststellungen;
f) die wesentlichen Aussagen der befragten Personen.

2. Protokollierung von Einvernahmen
Art. 71.
1 Bei Einvernahmen werden Fragen und Antworten gesondert protokolliert. Die Aussagen werden genau zu Protokoll genommen, wenn möglich mit den Worten des Einvernommenen und in Mundart, wenn dies für das Verständnis notwendig ist.
2 Sie können zusätzlich auf einen Ton- oder Bildträger aufgenommen werden, der Bestandteil der Akten bildet. Der Einzuvernehmende wird über die Aufnahme orientiert. Er kann die Aufnahme auf einen Tonträger verlangen.

c) Bestätigung der Richtigkeit
Art. 72.
1 Am Schluss der Verhandlung wird das Protokoll den Beteiligten vorgelesen oder zur Einsicht gegeben. Der Einvernommene wird darauf hingewiesen, dass er Ergänzungen oder Berichtigungen verlangen kann.
2 Die Beteiligten unterzeichnen das Protokoll mit der Bestätigung der korrekten Wiedergabe der Aussagen. Eingefügte Berichtigungen und Nachträge werden kenntlich gemacht und gesondert unterzeichnet.
3 Wird die Unterzeichnung verweigert, werden die Weigerung und deren allfällige Begründung angemerkt.

Einvernahme des Angeschuldigten
Pflicht
Art. 75.
1 Der Angeschuldigte darf nur verurteilt werden, wenn er wenigstens einmal untersuchungsrichterlich einvernommen worden ist. Vorbehalten bleibt Art. 170 dieses Gesetzes.

2 Bei Übertretungen sowie zur Abklärung von Nebenumständen eines Verbrechens oder Vergehens genügt die polizeiliche Einvernahme.

Einvernahme zur Sache
a) Durchführung
Art. 76.
1 Der Angeschuldigte wird aufgefordert, sich zur Anschuldigung zu äussern und eine zusammenhängende Darstellung des Sachverhalts zu geben.
2 Im Verlauf der Einvernahme wird ihm von der ihm zur Last gelegten Handlung Kenntnis gegeben. Er erhält Gelegenheit, zu den Aussagen von Mitangeschuldigten, Zeugen und Auskunftspersonen sowie zu den Ergebnissen anderer Beweiserhebungen Stellung zu nehmen.

b) Geständnis und Bestreitung
Art. 77.
1 Gesteht der Angeschuldigte die Straftat, wird die Glaubwürdigkeit des Geständnisses geprüft sowie der Angeschuldigte einlässlich über den Tathergang und die Beweggründe befragt.
2 Bestreitet er die ihm zur Last gelegte Straftat, werden ihm die belastenden Tatsachen vorgehalten. Er erhält Gelegenheit, sie zu entkräften sowie die zu seiner Entlastung dienenden Tatsachen und Beweismittel anzuführen.

Einvernahme zur Person
Art. 78.
3 Der Angeschuldigte wird zu seinen persönlichen Verhältnissen und zu seinem Vorleben befragt. Er erhält Gelegenheit, zu den eingeholten Berichten und Auskünften Stellung zu nehmen.

Einvernahmegrundsätze
a) allgemein
Art. 79.
1 Der Angeschuldigte wird vor der ersten Einvernahme belehrt, dass er nicht zur Aussage verpflichtet ist und einen Verteidiger beiziehen kann.
2 Die Fragen müssen klar und deutlich sein. Fragen, in denen eine nicht feststehende Tatsache als erwiesen angenommen wird, sind nicht zulässig.

b) unzulässige Methoden
Art. 81.
1 Bei der Einvernahme dürfen weder Versprechungen oder Vorspiegelungen noch Drohungen oder andere Zwangsmittel eingesetzt werden, um den Angeschuldigten zu einer Aussage oder zu einem Geständnis zu bewegen.
2 Mittel zur Erlangung von Aussagen, welche die Freiheit der Willensbildung oder der Willensbetätigung beeinträchtigen, sind nicht zulässig, auch wenn der Angeschuldigte der Anwendung zustimmt.
3 Aussagen, die durch eine Einwirkung nach Abs. 1 und 2 dieser Bestimmung erlangt worden sind, werden nicht verwertet.

Anhang I
IT-Checkliste

IT-Checkliste

„Datenintegrität“

Spuren sind vorhanden und sichergestellt!

… aber wer kommt als Täter in Frage ?

1.1 Inhaltsverzeichnis

1.2 Überblick zur Checkliste

Hintergrund: IT-Systeme unterstützen uns in zahlreichen Lebensbereichen und bilden einen integralen Bestandteil unserer Gesellschaft. Mit der zunehmenden Verbreitung spielen IT-Systeme jedoch immer häufiger auch eine zentrale Rolle im Zusammenhang mit kriminellen Handlungen, wodurch die Bedeutung von elektronischen Spuren und Beweisen zunimmt. Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug sind (neben der ordnungsgemässen Sicherstellung von digitalen Beweismitteln) eine wesentliche Voraussetzung für eine bessere Einschätzung und erhöhte Aussagekraft vor Gericht.

Zweck: Wenn Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug durchgeführt werden, soll die vorliegende Checkliste helfen, die folgende Frage zu beantworten: „Haben unberechtigte Personen die Möglichkeit gehabt, auf das IT-System zuzugreifen und Daten zu manipulieren?“ Dadurch soll besser eingeschätzt und eingegrenzt werden können, wer welche Eingaben / Transaktionen am IT-System durchgeführt hat und welcher Person der digitale Beweis zuzuordnen ist.

Zielpublikum: Strafverfolgungsbehörden und Verteidiger – Die Checkliste ist so aufgebaut, dass für eine erste Beurteilung keine vertieften Informatik-Kenntnisse notwendig sind.

Theorie und Grundlage: IT-Sicherheit wird häufig unterteilt nach den Zielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Zur Beantwortung der Frage nach dem eigentlichen Urheber einer Transaktion im IT-System wird primär die „Datenintegrität“ angesprochen, sekundär auch die „Vertraulichkeit“. So gefährden öffentliche Passwörter nämlich indirekt die Datenintegrität. Die Checkliste basiert auf den IT-Grundschutzkatalogen des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI; Kataloge im Internet gratis abrufbar unter „http://www.bsi.de“). Aus den über 900 detailliert beschriebenen Massnahmen wurden 61 Massnahmen ausgewählt, wobei die Auswahl aufgrund des Zwecks der Checkliste sowie des Zielpublikums erfolgte. Die Titel wurden übernommen und mit eigenen Fragen, Beispielen und Risikobeschreibungen der Autoren ergänzt. Zudem sind Referenzen zu den konkreten Massnahmen gemäss IT-Grundschutzkatalogen angegeben. (Tipp: Im elektronischen Dokument sind die Hyperlinks aktiviert.)

Benutzeranleitung: Die Checkliste sollte verwendet werden, wenn der Ermittlungsauftrag formuliert wird. Ebenso kann die Liste auch im Anschluss an die Sicherstellung von digitalen Beweisen benutzt werden, um weitere Umfeldabklärungen zu machen. Dabei sind die für den konkreten Fall relevanten Module (wie beispielsweise Computer-Basis, mobiler Einsatz, Netzwerkanschluss) gemäss der im nächsten Kapitel aufgeführten Beschreibung auszuwählen. Fragen, welche mit „Nein“ beantwortet werden, geben Hinweise auf Schwachstellen und Risiken. Zudem können sich durch ein „Nein“ einige der nachfolgenden Fragen erübrigen. Mit Stern (★) gekennzeichnete Themen sind besonders wichtig und daher speziell zu beachten.

Annahme: Die digitalen Beweise sind ordnungsgemäss erhoben worden.

Autoren: Christian de Raemy, Nicole Jerjen, Andreas Löwinger, Daniel Russenberger,
Anita Tschopp

1.3 Leporello und Ablauf-Schema

Als Arbeitshilfe stehen zur Verfügung:
- drei Leporellos (Checklisten in Kurzform);
- drei Ablauf-Schemata;
- eine Detail-Checkliste;
- ein Glossar.

Die Vorgehensweise:
a) Auswahl des Leporellos;
b) Festlegen der anwendbaren Module mit Hilfe des dazugehörenden Ablauf-Schemas;
c) Abarbeiten der Prüfpunkte von oben nach unten;
d) Prüfen, ob ein Mangel für den konkreten Sachverhalt relevant ist (bei Nein-Antworten).

Der Leporello dient der Übersicht in Form einer Checkliste. Für die unterschiedlichen Verwendungen von Geräten gibt es drei verschiedene Leporellos:
- Heimarbeitsplatz;
- Geschäftsarbeitsplatz;
- Mobiler Einsatz.

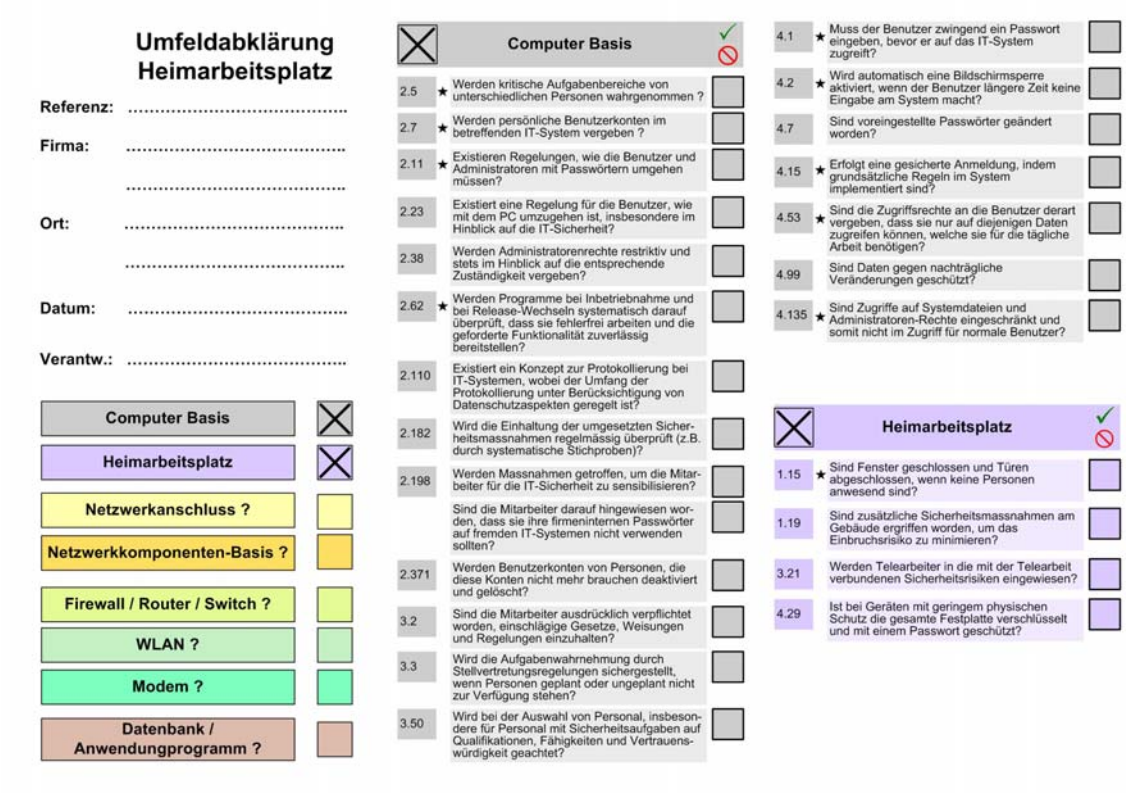
Mit Hilfe des Ablaufschemas kann für den jeweiligen Leporello festgelegt werden, welche Module anwendbar sind.

In der Detail-Checkliste sind zusätzliche Erläuterungen meist in Form von Beispielen enthalten. Zudem wird beschrieben, welche Risiken bestehen, wenn die Frage mit „Nein“ beantwortet wird. Schliesslich wird auf weitere hilfreiche Informationen in den IT-Grundschutz-Katalogen verwiesen. Die Hyperlinks zeigen auf die vollständige Beschreibung der Massnahmen gemäss IT-Grundschutz-Katalogen.

Im Glossar sind die in der Checkliste verwendeten IT-Fachausdrücke kurz erläutert.

Heimarbeitsplatz

Leporello Vorderseite



Umfeldabklärung Heimarbeitsplatz

Referenz: .....

Firma: .....

.....

Ort: .....

.....

Datum: .....

Verantw.: .....

- Computer Basis
- Heimarbeitsplatz
- Netzwerkanschluss ?
- Netzwerkkomponenten-Basis ?
- Firewall / Router / Switch ?
- WLAN ?
- Modem ?
- Datenbank / Anwendungprogramm ?

Computer Basis

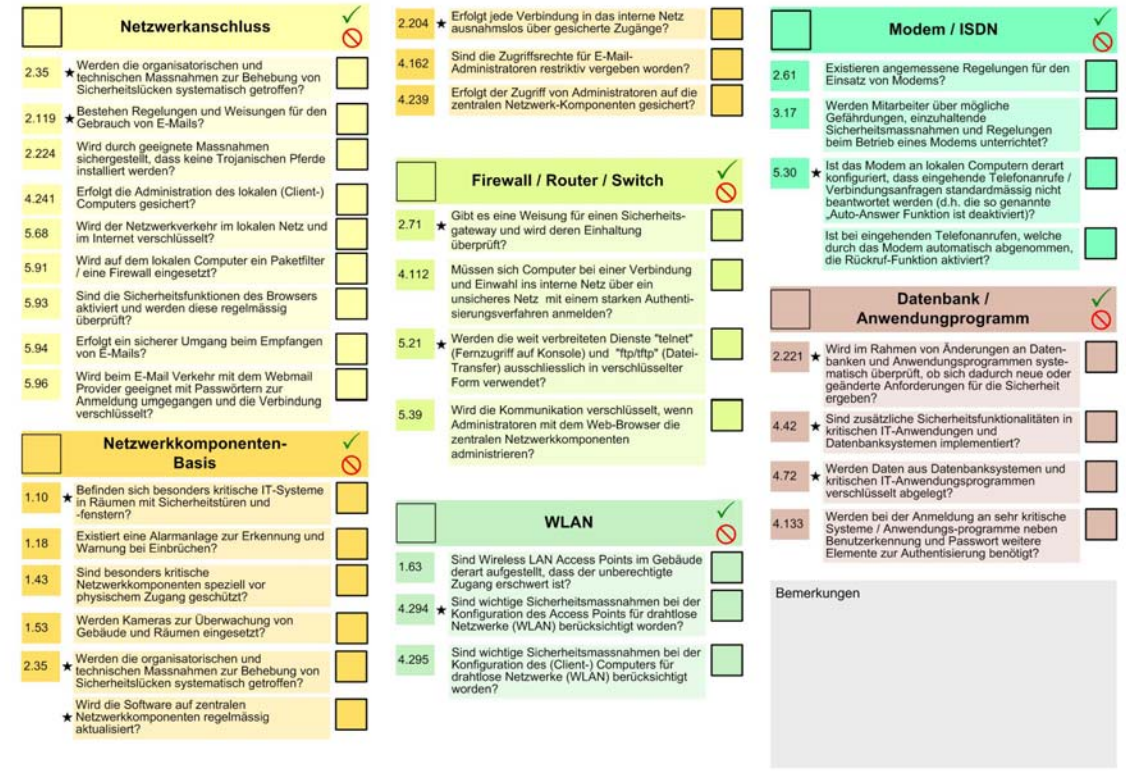
- 2.5 ★ Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen ?
- 2.7 ★ Werden persönliche Benutzerkonten im betreffenden IT-System vergeben ?
- 2.11 ★ Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen?
- 2.23 Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit?
- 2.38 Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben?
- 2.62 ★ Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen?
- 2.110 Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist?
- 2.182 Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)?
- 2.198 Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren?
- Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten?
- 2.371 Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen deaktiviert und gelöscht?
- 3.2 Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten?
- 3.3 Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen?
- 3.50 Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben auf Qualifikationen, Fähigkeiten und Vertrauenswürdigkeit geachtet?

- 4.1 ★ Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift?
- 4.2 ★ Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht?
- 4.7 Sind voreingestellte Passwörter geändert worden?
- 4.15 ★ Erfolgt eine gesicherte Anmeldung, indem grundsätzliche Regeln im System implementiert sind?
- 4.53 ★ Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen?
- 4.99 Sind Daten gegen nachträgliche Veränderungen geschützt?
- 4.135 ★ Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer?

Heimarbeitsplatz

- 1.15 ★ Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind?
- 1.19 Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren?
- 3.21 Werden Telearbeiter in die mit der Telearbeit verbundenen Sicherheitsrisiken eingewiesen?
- 4.29 Ist bei Geräten mit geringem physischen Schutz die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt?

Leporello Rückseite



Netzwerkanschluss

- 2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?
- 2.119 ★ Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails?
- 2.224 Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden?
- 4.241 Erfolgt die Administration des lokalen (Client-) Computers gesichert?
- 5.68 Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt?
- 5.91 Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt?
- 5.93 Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft?
- 5.94 Erfolgt ein sicherer Umgang beim Empfangen von E-Mails?
- 5.96 Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt?

Netzwerkkomponenten-Basis

- 1.10 ★ Befinden sich besonders kritische IT-Systeme in Räumen mit Sicherheitstüren und -fenstern?
- 1.18 Existiert eine Alarmanlage zur Erkennung und Warnung bei Einbrüchen?
- 1.43 Sind besonders kritische Netzwerkkomponenten speziell vor physischem Zugang geschützt?
- 1.53 Werden Kameras zur Überwachung von Gebäude und Räumen eingesetzt?
- 2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?
- ★ Wird die Software auf zentralen Netzwerkkomponenten regelmässig aktualisiert?

- 2.204 ★ Erfolgt jede Verbindung in das interne Netz ausnahmslos über gesicherte Zugänge?
- 4.162 Sind die Zugriffsrechte für E-Mail-Administratoren restriktiv vergeben worden?
- 4.239 Erfolgt der Zugriff von Administratoren auf die zentralen Netzwerk-Komponenten gesichert?

Firewall / Router / Switch

- 2.71 ★ Gibt es eine Weisung für einen Sicherheits-gateway und wird deren Einhaltung überprüft?
- 4.112 Müssen sich Computer bei einer Verbindung und Einwahl ins interne Netz über ein unsicheres Netz mit einem starken Authentisierungsverfahren anmelden?
- 5.21 ★ Werden die weit verbreiteten Dienste "telnet" (Fernzugriff auf Konsole) und "ftp/tftp" (Datei-Transfer) ausschliesslich in verschlüsselter Form verwendet?
- 5.39 Wird die Kommunikation verschlüsselt, wenn Administratoren mit dem Web-Browser die zentralen Netzwerkkomponenten administrieren?

WLAN

- 1.63 Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist?
- 4.294 ★ Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden?
- 4.295 Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden?

Modem / ISDN

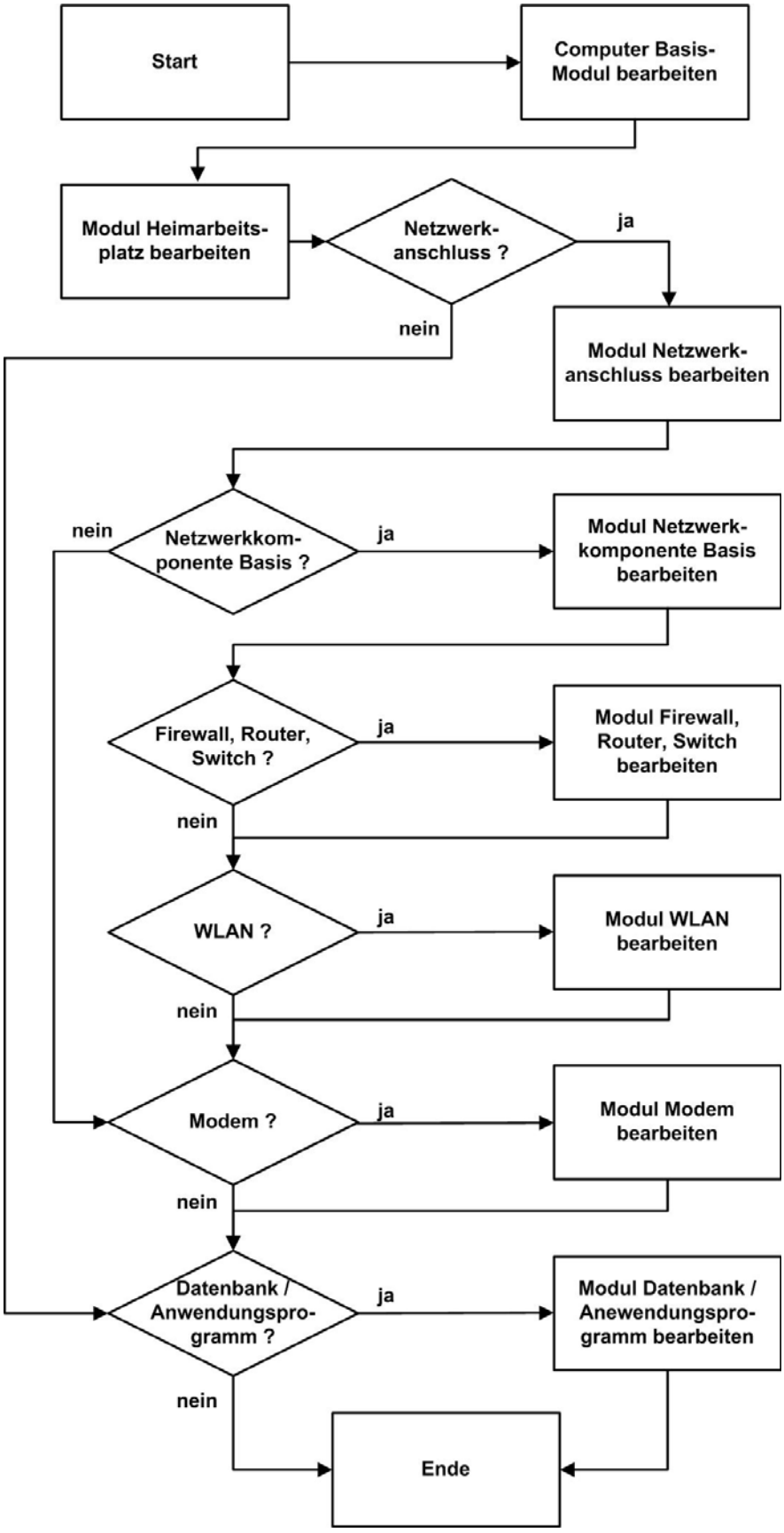
- 2.61 Existieren angemessene Regelungen für den Einsatz von Modems?
- 3.17 Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet?
- 5.30 ★ Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)?
- Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen, die Rückruf-Funktion aktiviert?

Datenbank / Anwendungprogramm

- 2.221 ★ Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?
- 4.42 ★ Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?
- 4.72 ★ Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?
- 4.133 Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

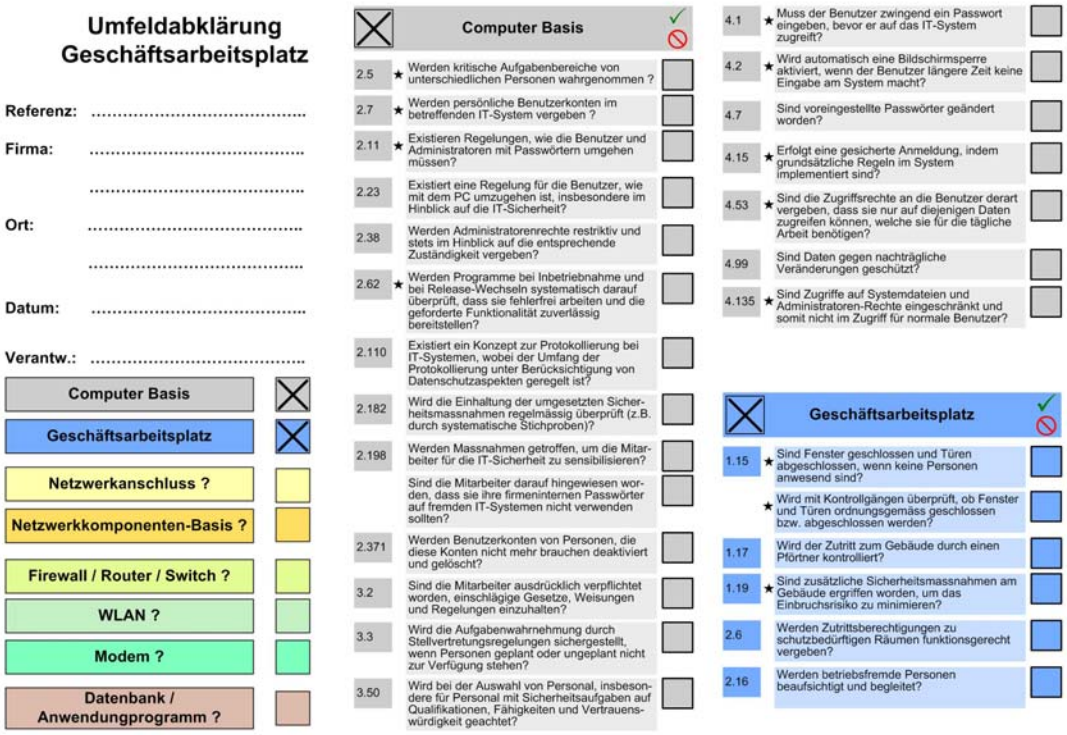
Bemerkungen

Heimarbeitsplatz - Ablaufschema

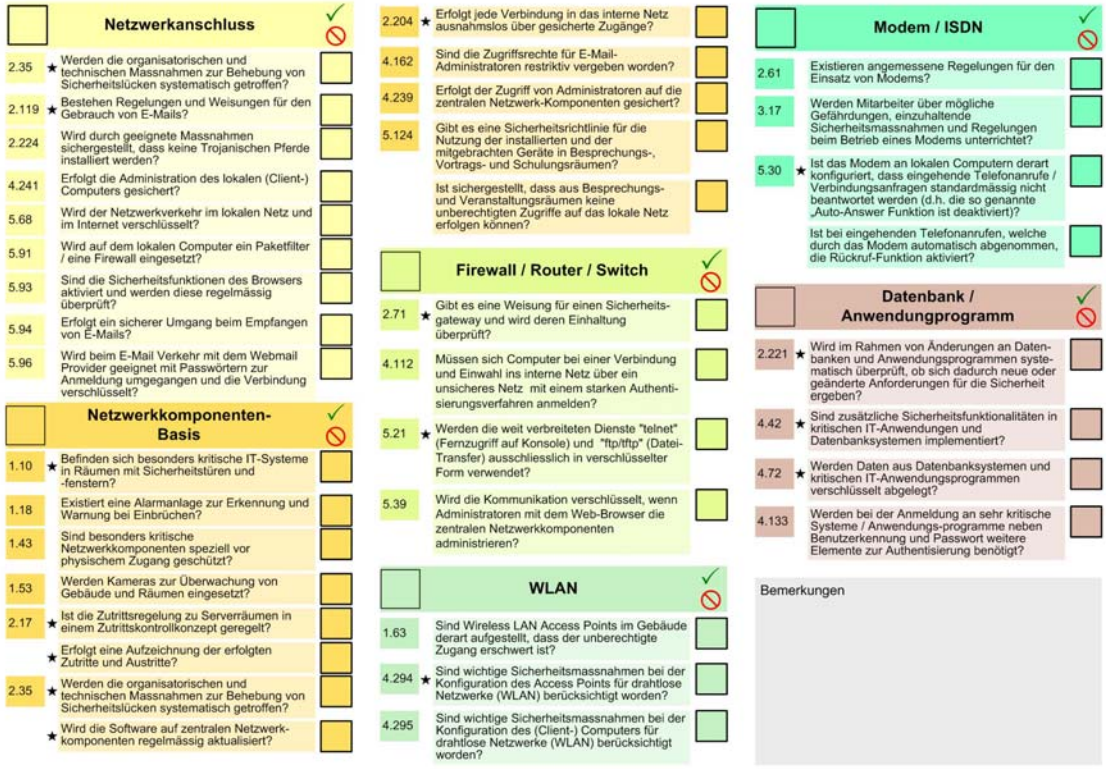


Geschäftsarbeitsplatz

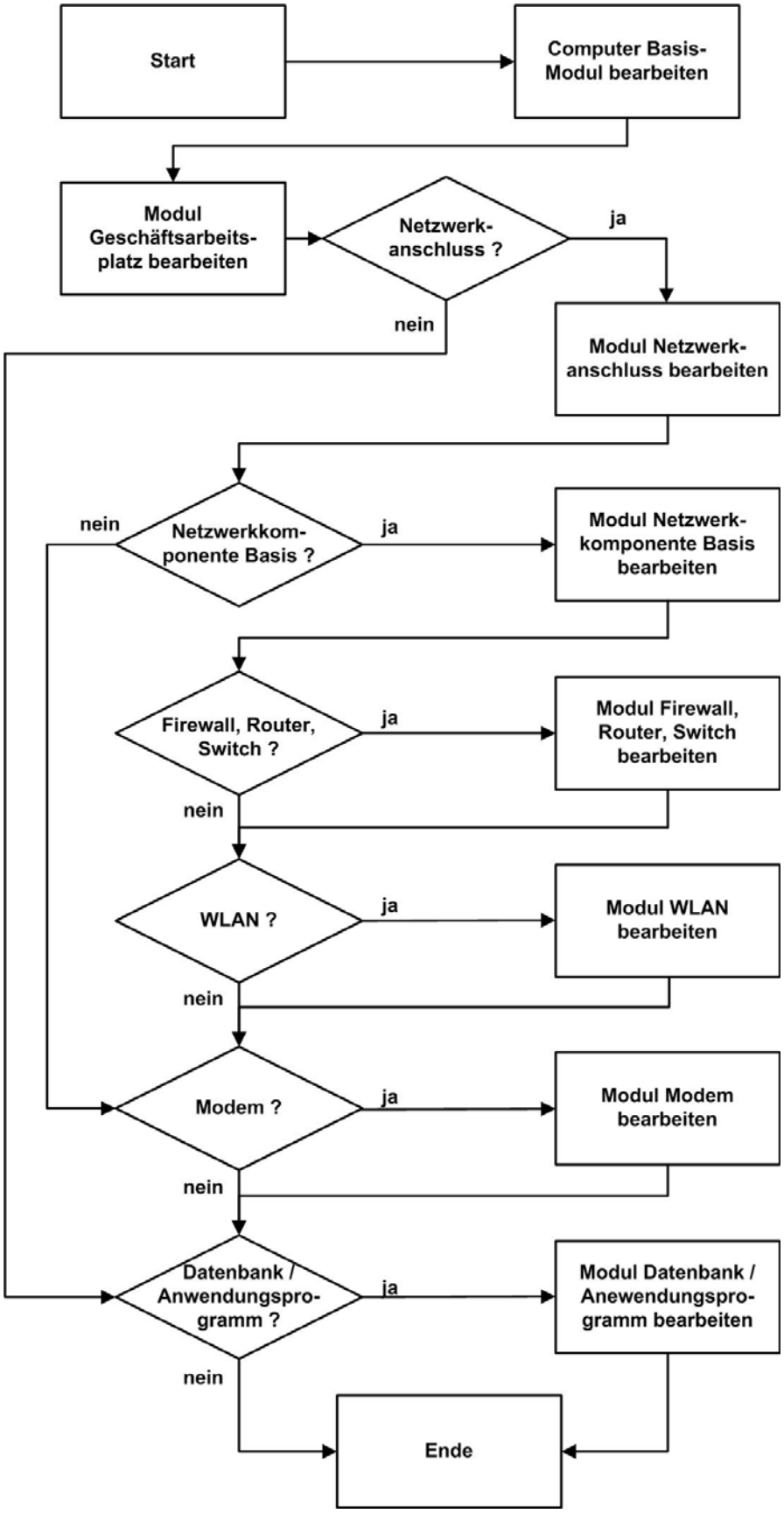
Leporello Vorderseite



Leporello Rückseite

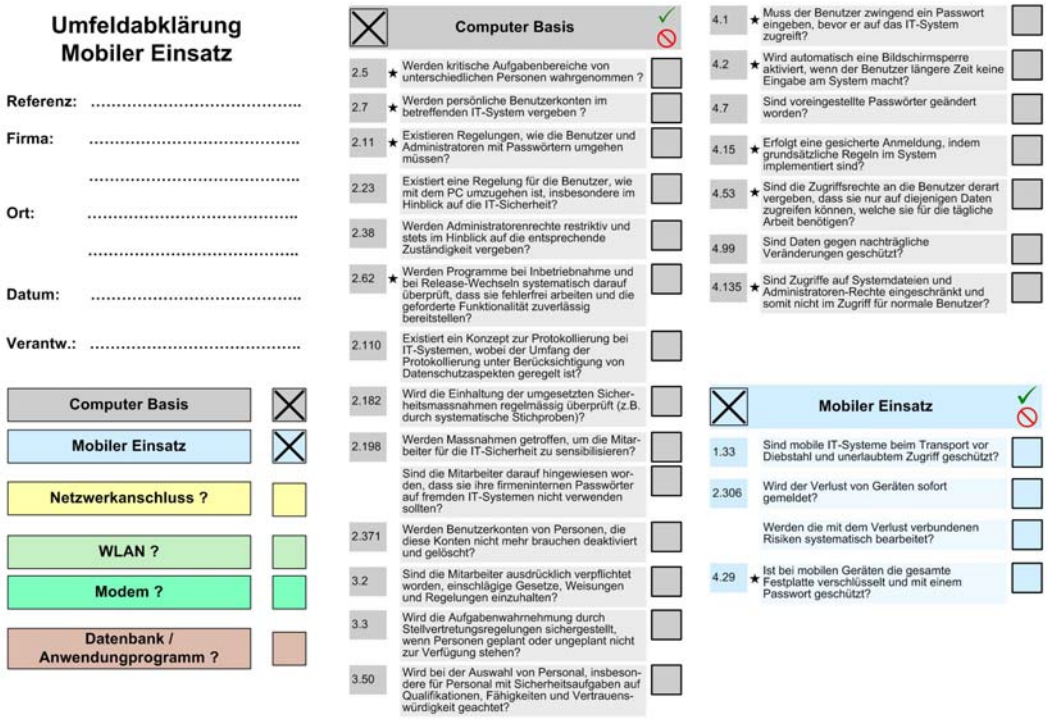


Geschäftsarbeitsplatz - Ablaufschema



Mobiler Einsatz

Leporello Vorderseite



Umfeldabklärung Mobiler Einsatz

Referenz: .....

Firma: .....

.....

Ort: .....

.....

Datum: .....

Verantw.: .....

Computer Basis

Mobiler Einsatz

Netzwerkanschluss ?

WLAN ?

Modem ?

Datenbank / Anwendungsprogramm ?

Computer Basis

2.5 ★ Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen ?

2.7 ★ Werden persönliche Benutzerkonten im betreffenden IT-System vergeben ?

2.11 ★ Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen?

2.23 Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit?

2.38 Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben?

2.62 ★ Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen?

2.110 Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist?

2.182 Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)?

2.198 Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren?

Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten?

2.371 Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen deaktiviert und gelöscht?

3.2 Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten?

3.3 Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen?

3.50 Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben auf Qualifikationen, Fähigkeiten und Vertrauenswürdigkeit geachtet?

4.1 ★ Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift?

4.2 ★ Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht?

4.7 Sind voreingestellte Passwörter geändert worden?

4.15 ★ Erfolgt eine gesicherte Anmeldung, indem grundsätzliche Regeln im System implementiert sind?

4.53 ★ Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen?

4.99 Sind Daten gegen nachträgliche Veränderungen geschützt?

4.135 ★ Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer?

Mobiler Einsatz

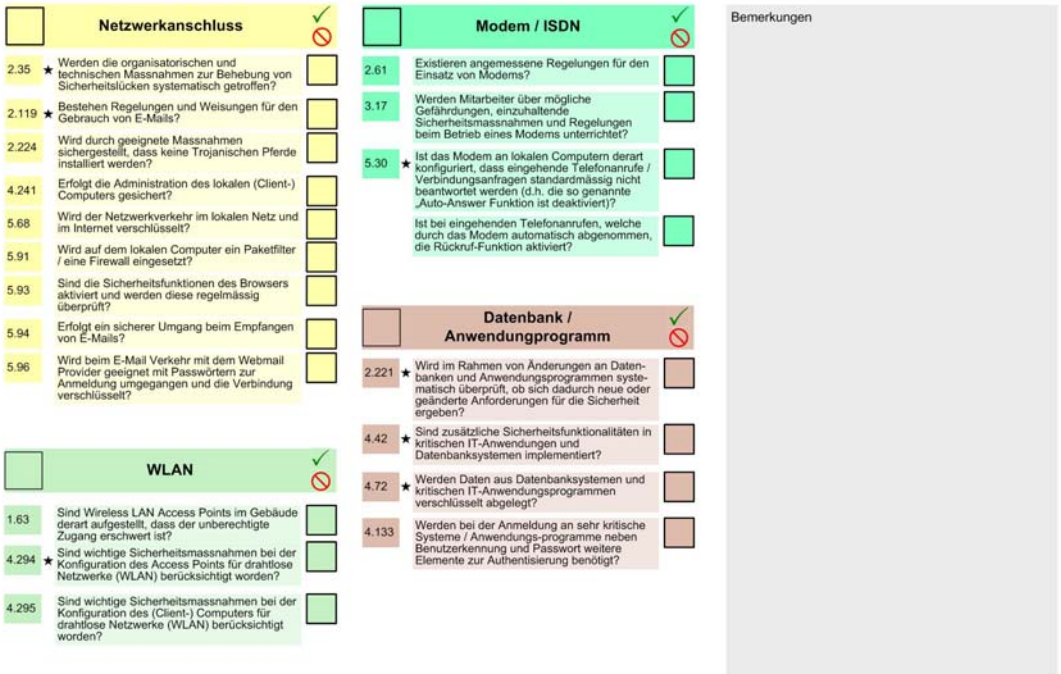
1.33 Sind mobile IT-Systeme beim Transport vor Diebstahl und unerlaubtem Zugriff geschützt?

2.306 Wird der Verlust von Geräten sofort gemeldet?

Werden die mit dem Verlust verbundenen Risiken systematisch bearbeitet?

4.29 ★ Ist bei mobilen Geräten die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt?

Leporello Rückseite



Netzwerkanschluss

2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?

2.119 ★ Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails?

2.224 Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden?

4.241 Erfolgt die Administration des lokalen (Client-) Computers gesichert?

5.68 Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt?

5.91 Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt?

5.93 Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft?

5.94 Erfolgt ein sicherer Umgang beim Empfangen von E-Mails?

5.96 Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt?

WLAN

1.63 Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist?

4.294 ★ Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden?

4.295 Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden?

Modem / ISDN

2.61 Existieren angemessene Regelungen für den Einsatz von Modems?

3.17 Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet?

5.30 ★ Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)?

Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen, die Rückruf-Funktion aktiviert?

Datenbank / Anwendungsprogramm

2.221 ★ Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?

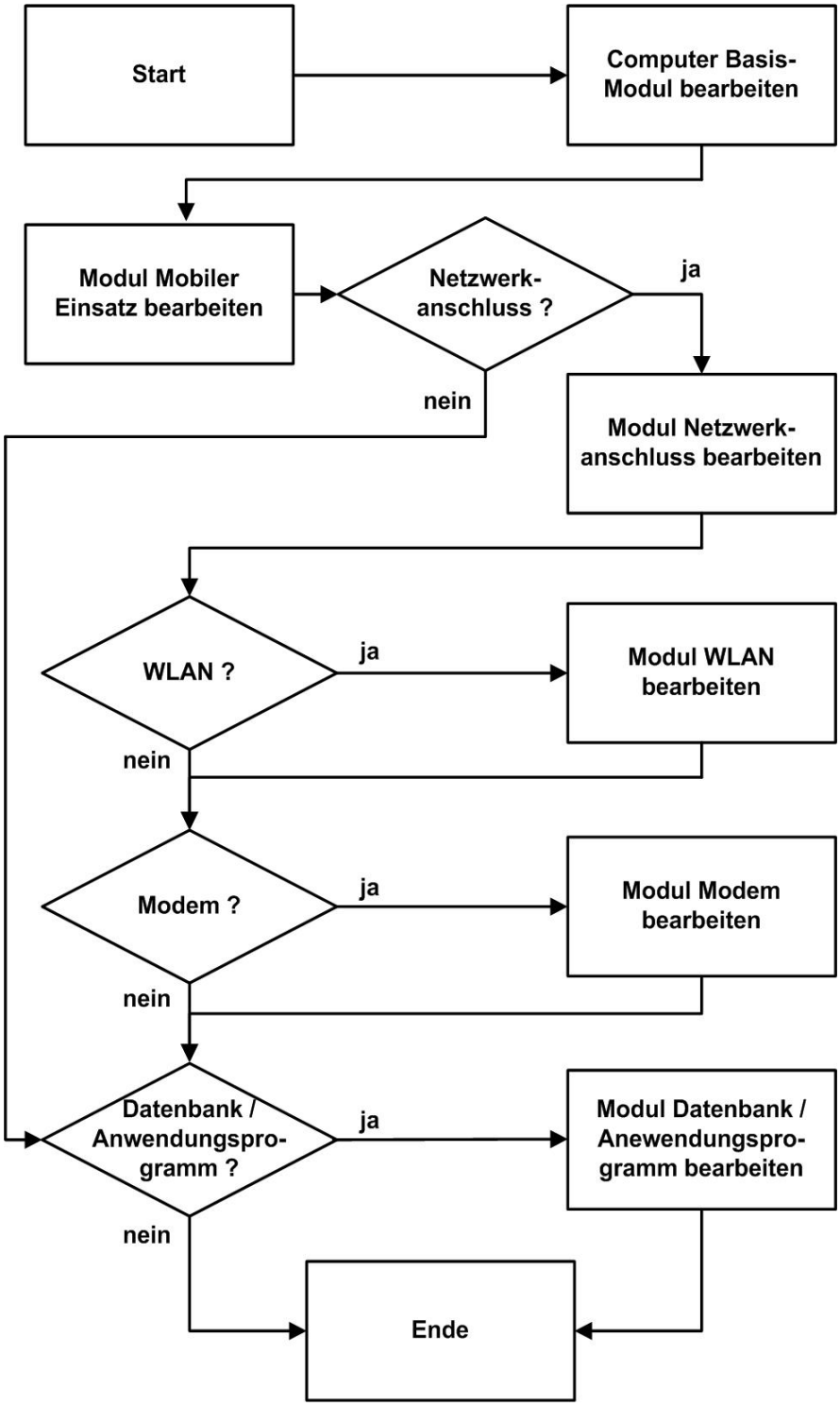
4.42 ★ Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?

4.72 ★ Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?

4.133 Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

Bemerkungen

Mobiler Einsatz - Ablaufschema



1.4 Detail-Checkliste

Computer-Basis

Modul: Computer-Basis

★ M 2.5 – Aufgabenverteilung und Funktionstrennung

Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen? ○ ja ○ nein

Beispiele kritischer Aufgabenbereiche: Programmierung und Überführung der Programme in die Produktion, Arbeit in der IT und im Fachbereich, Zahlungserfassung und Zahlungsfreigabe

Wenn keine angemessene Funktionstrennung stattfindet (d.h. eine Person übernimmt mehrere kritische Aufgaben und Funktionen gleichzeitig), besteht das Risiko, dass bestehende Kontrollen umgangen werden und unerlaubte Handlungen von Schlüsselpersonen unentdeckt bleiben. Es besteht das erhöhte Risiko, dass Schlüsselpersonen andere Login-Daten kennen (z.B. Passwort) und generell zu weitreichende Zugriffsrechte (beispielsweise Administrator-Rechte) besitzen.

★ M 2.7 – Vergabe von Zugangsberechtigungen

Werden persönliche Benutzerkonten im betreffenden IT-System vergeben? ○ ja ○ nein

Beispiele: Jeder Benutzer erhält ein persönliches Benutzerkonto, und es werden keine Benutzerkonten von mehreren Personen geteilt.

Wenn Zugangsberechtigungen nicht oder unvollständig verwaltet werden, besteht das Risiko, dass unerlaubte Handlungen keiner Person oder keinem eingegrenzten Personenkreis zugeordnet werden können.

Weitere Informationen sind beim BSI zu finden unter M 2.8 , M 2.30, M 2.31, M 2.63, M 2.94, M 4.53, M 4.135.

★ M 2.11 – Regelung des Passwortgebrauchs

Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen? ○ ja ○ nein

Beispiele: Passwörter nicht auf Zettel schreiben, dem Stellvertreter nicht weitergeben, regelmässig wechseln, Mindestlänge wählen etc.

Es besteht das Risiko, dass die Benutzer das Passwort nicht vertraulich behandeln und dadurch eine andere Person in den Besitz des Passworts kommt. Dadurch kann diese Person unter einer anderen Benutzerkennung arbeiten.

M 2.23 – Herausgabe einer PC-Richtlinie

Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit? ○ ja ○ nein

Beispielsweise wird geregelt: Installation von fremden Programmen, Bildschirmsperre beim Verlassen des Arbeitsplatzes etc.

Es besteht das Risiko, dass aufgrund von Mängeln in der Handhabung von IT-Systemen unberechtigte Personen auf Daten zugreifen und diese verändern können (entweder direkt über ein fremdes Benutzerkonto oder indirekt über das Erlangen eines fremden Passworts).

M 2.38 – Aufteilung der Administrationstätigkeiten

Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben? ○ ja ○ nein

Beispielsweise wird zwischen Netzwerkadministrator und Datenbankadministrator unterschieden. Zudem erhalten normale Benutzer keine Administratorenrechte.

Administratoren besitzen in der Regel weitreichende Zugriffsrechte. Wenn solche Zugriffsrechte nicht restriktiv vergeben werden, besteht das erhöhte Risiko, dass die Administratoren auf vertrauliche Daten (wie Hinweise zu Passwörtern) zugreifen. Zudem besteht stets das Risiko von Fehlmanipulationen, die sich bei Administratoren besonders gravierend auswirken können und dadurch die Datensicherheit generell gefährdet wird.

Weitere Informationen sind beim BSI zu finden unter M 2.26.

★ M 2.62 – Software-Abnahme- und Freigabe-Verfahren

Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen? ○ ja ○ nein

Beispiele: Programme werden mit Testfällen systematisch überprüft, und es existiert ein dokumentiertes Freigabeverfahren unter Einbezug der Fachstellen.

Wenn die systematische Prüfung des fehlerfreien und zuverlässigen Funktionierens der Programme nicht durchgeführt wird, besteht das Risiko, dass die neuen Programme Sicherheitslücken beinhalten und diese nicht erkannt werden. Dadurch wird die Systemsicherheit generell gefährdet.

Weitere Informationen sind beim BSI zu finden unter M 2.86, M 2.221.

M 2.110 – Datenschutzaspekte bei der Protokollierung

Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist? ○ ja ○ nein

Beispielsweise wird protokolliert: An- und Abmeldungen am System, Lese- und Schreibzugriffe auf sehr vertrauliche Daten, Einrichten von Benutzern durch Administratoren, Datensicherungen.

Wenn die Protokollierung nicht, nicht regelmässig oder nicht umfassend erfolgt, ist jede davon betroffene Massnahme nicht nachvollziehbar und damit in Frage gestellt.

Weitere Informationen sind beim BSI zu finden unter M 2.340.

M 2.182 – Regelmässige Kontrollen der IT-Sicherheitsmassnahmen

Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)? ○ ja ○ nein

Wenn die Einhaltung der Sicherheitsmassnahmen nicht regelmässig überprüft wird, besteht das Risiko, dass der durch die Massnahme gewährte Schutz der Vertraulichkeit und der Integrität der Daten nicht mehr wirksam ist.

M 2.198 – Sensibilisierung der Mitarbeiter für IT-Sicherheit

Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren? ○ ja ○ nein

z.B. regelmässige Informationen, interne Weiterbildungen

Wenn die Mitarbeiter nicht auf die IT-Sicherheit sensibilisiert sind, besteht das Risiko, dass vertrauliche Daten durch unsachgemässe Handhabung Unbefugten zugänglich gemacht werden.

Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten? ○ ja ○ nein

z.B. kein Gebrauch im Internet-Cafe, beim Mailprovider, beim Arbeitskollegen etc.

Es besteht das Risiko, dass die fremden IT-Systeme Sicherheitslücken aufweisen oder dass bereits Abhörprogramme (Sniffer) installiert sind. Bei der Verwendung von firmeninternen Passwörtern (bzw. Wahl des gleichen Passworts auf verschiedenen Systemen) auf fremden Systemen kann das Passwort somit gestohlen werden.

Weitere Informationen sind beim BSI zu finden unter M 3.26, M 3.5, M 4.251.

M 2.371 – Geregelte Deaktivierung und Löschung ungenutzter Konten

Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen, deaktiviert und gelöscht? ○ ja ○ nein

Beispiele: regelmässige Überprüfung der Zugriffsrechte; standardisierte Austrittsmeldungen durch die Personalabteilung. Ebenso können beispielsweise Benutzerkonten, welche längere Zeit nicht verwendet wurden, automatisch vom System deaktiviert werden.

Wenn die Konten nicht deaktiviert und gelöscht werden, besteht das Risiko, dass mit Hilfe dieser Konten unerkannt Daten eingesehen und manipuliert werden.

Weitere Informationen sind beim BSI zu finden unter M 4.17.

M 3.2 – Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten? ○ ja ○ nein

z.B. mittels schriftlicher Bestätigung bei der Neueinstellung von Mitarbeitern

Es besteht das Risiko, dass Mitarbeiter sich ihrer Verantwortung zur Einhaltung von Gesetzen, Weisungen und Regelungen nicht (bzw. zuwenig) bewusst sind. Dadurch wird unter anderem die Datensicherheit gefährdet, wie beispielsweise die Vertraulichkeit von Passwörtern oder die Datenintegrität generell.

M 3.3 – Vertretungsregelungen

Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen? ○ ja ○ nein

Beispielsweise besitzt der Stellvertreter die notwenigen Zugriffsrechte, so dass die Weitergabe von persönlichen Passwörtern nicht notwendig ist.

Wenn Stellvertretungsregelungen fehlen, besteht das Risiko, dass die Aufgaben nicht in der gleichen Zuverlässigkeit (bezüglich der Sicherheitsmassnahmen) wahrgenommen werden. Bei der Weitergabe von Passwörtern an Stellvertreter besteht das Risiko, dass Datenabfragen und -manipulationen später nicht zugeordnet werden können.

M 3.50 – Auswahl von Personal

Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben, auf Qualifikationen, Fähigkeiten und Vertrau- ○ ja ○ nein

enswürdigkeit geachtet?

Es besteht das Risiko, dass Mitarbeiter die Anforderungen für eine ordnungsgemässe Umsetzung der Sicherheitsmassnahmen nicht erfüllen können und sich dadurch generell erhöhte Sicherheitsrisiken ergeben. Bei fehlender oder unklarer Vertrauenswürdigkeit besteht ein erhöhtes Risiko von unerlaubten Handlungen.

Weitere Informationen sind beim BSI zu finden unter M 3.10, M 3.33.

★ M 4.1 – Passwortschutz für IT-Systeme

Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift? ○ ja ○ nein

z.B. Anmeldung am Betriebssystem, Anmeldung bei einem Anwendungsprogramm

Ohne Passwortschutz besteht das Risiko, dass sich Benutzer unter einer anderen Benutzerkennung anmelden und dadurch nicht mehr nachvollziehbar ist, welcher Benutzer effektiv am System gearbeitet hat.

★ M 4.2 – Bildschirmsperre

Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht? ○ ja ○ nein

z.B. Aktivierung des Bildschirmschoners und Wiedereinstieg durch erneute Passworteingabe

Ohne automatische Bildschirmsperre besteht das Risiko, dass Benutzer beim Verlassen des Arbeitsplatzes (z.B. in der Mittagspause oder nach Büroschluss) den Computer nicht sperren und dadurch unberechtigte Personen unter der fremden Benutzerkennung auf das System zugreifen. Zudem besitzen die Personen in einem solchen Fall möglicherweise mehr Zugriffsrechte als im Normalfall.

Weitere Informationen sind beim BSI zu finden unter M 4.16.

M 4.7 – Änderung voreingestellter Passwörter

Sind voreingestellte Passwörter geändert worden? ○ ja ○ nein

Viele Betriebssysteme, Datenbanken, Netzwerk-Geräte etc. werden mit allgemein bekannten Standard-Passwörtern ausgeliefert oder verwenden überhaupt keine Passwörter.

Es besteht das Risiko, dass durch die Benutzung eines voreingestellten Passworts, welches allgemein bekannt ist, Zugriff aufs System möglich wird. Weil es sich dabei oft um Administratoren-Konten handelt, sind damit weitreichende Zugriffsrechte verbunden. Unter anonymer Benutzerkennung können unberechtigte Transaktionen durchgeführt und gegebenenfalls kann auf vertrauliche Daten zugegriffen werden.

★ M 4.15 – Gesichertes Login

Erfolgt eine gesicherte Anmeldung, indem mindestens die folgenden Regeln im System implementiert sind? ○ ja ○ nein

1) Jeder Benutzer besitzt ein eigenes Benutzerkonto;
2) Jeder Benutzer besitzt ein eigenes Passwort, welches frei wählbar ist;
3) Passwörter besitzen eine Mindestlänge von 8 Zeichen und können nicht aus trivialen Wörtern bestehen;
4) Passwörter müssen regelmässig geändert werden (mindestens alle 90 Tage);
5) Mehrere erfolglose Anmeldeversuche werden verhindert (z.B.

durch Sperren des betreffenden Benutzerkontos oder zeitlicher Verzögerung bei Fehlversuchen).

Es besteht das Risiko, dass Benutzer ein Benutzerkonto oder Passwort gemeinsam verwenden, wodurch die Nachvollziehbarkeit der Transaktionen nicht mehr gegeben ist. Bei kurzen oder trivialen Passwörtern und der Möglichkeit von zahlreichen Anmeldeversuchen besteht das Risiko, dass eine andere Person das Passwort errät (durch systematisches Ausprobieren, manuell oder automatisiert). Wenn das System die Benutzer nicht regelmässig zur Passwortänderung zwingt, kann sich eine unberechtigte Person, die über ein fremdes Passwort verfügt, über einen längeren Zeitraum unter einer falschen Benutzerkennung anmelden.

★ M 4.53 – Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse

Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen? ○ ja ○ nein

Beispielsweise besitzen Benutzer keine Zugriffe auf die persönlichen Verzeichnisse ihrer Kollegen, Mitarbeiter der Zahlungsabteilung besitzen keine Zugriffe zu den Personaldaten und umgekehrt.

Es besteht das Risiko, dass Benutzer bei zu vielen Berechtigungen Zugang zu vertraulichen Daten erhalten (unter anderem Hinweise zu Passwörtern).

Weitere Informationen sind beim BSI zu finden unter M 2.7, M 2.8, M 2.30, M 2.31, M 2.63, M 2.94, M 4.135, M 5.10.

M 4.99 – Schutz gegen nachträgliche Veränderungen von Informationen

Sind Daten gegen nachträgliche Veränderungen geschützt? ○ ja ○ nein

Beispielsweise bieten digitale Signaturen einen hohen Schutz gegen nachträgliche Veränderungen. In abgeschwächter Form kann mittels Read-only Medien und Dateiformaten wie PDF gegen nachträgliche Veränderung geschützt werden.

Wenn Daten nicht mittels digitalen Signaturen geschützt werden, besteht das Risiko, dass diese Daten nachträglich von unberechtigten Personen geändert werden und dies nicht erkannt wird - insbesondere bei Schwachstellen im physischen und logischen Zugriffsschutz. Der Einsatz von digitalen Signaturen kann in einem solchen Umfeld teilweise Abhilfe schaffen. Es besteht aber auch hier ein Rest-Risiko, dass digitale Schlüssel und dazugehörende Passwörter gestohlen werden (z.B. Kopie des Schlüssels und Diebstahl/Ausprobieren des Passworts).

★ M 4.135 – Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer? ○ ja ○ nein

Bei weitreichenden Zugriffsrechten für normale Benutzer besteht das Risiko, dass Sicherheitseinstellungen geändert und Schutzmassnahmen dadurch abgebaut werden. Zudem können Administratoren auf Dateien mit verschlüsselten Passwörtern zugreifen, welche in einem zweiten Schritt bei einfachen Passwörtern relativ einfach geknackt werden können. Weiter besitzen Administratoren häufig Schreib-Zugriffe auf Log-Files, wodurch die Protokolleinträge manipuliert werden können.

M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.

★ M 1.15 – Geschlossene Fenster und Türen

Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind? ○ ja ○ nein

Es besteht das Risiko, dass unberechtigte Personen über offene Fenster oder Türen physischen Zutritt zum IT-System erlangen. Dadurch können beispielsweise gewisse Sicherheitsmechanismen des Betriebssystems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.23.

M 1.19 – Einbruchsschutz

Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren? ○ ja ○ nein

Beispiele: Schliesszylinder, Sicherung von Kellerlichtschächten, Verschluss von nicht benutzten Nebeneingängen.

Es besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt ins Gebäude und zu IT-Systemen erlangen. Bei physischem Zugriff auf ein IT-System können anschliessend gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.40.

M 3.21 – Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters

Werden Telearbeiter in die mit der Telearbeit verbundenen Sicherheitsrisiken eingewiesen? ○ ja ○ nein

z.B. Schulung über IT-Sicherheitsmassnahmen

Es besteht das Risiko, dass Mitarbeiter sich der Sicherheitsrisiken nicht (bzw. zuwenig) bewusst sind und notwendige Massnahmen nicht ergriffen werden. Dies kann unter anderem zu einem Verlust der Datenintegrität und Datenvertraulichkeit führen.

Weitere Informationen sind beim BSI zu finden unter M 2.113.

★ M 4.29 – Einsatz eines Verschlüsselungsproduktes für tragbare PCs

Ist bei Geräten mit geringem physischen Schutz die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt? ○ ja ○ nein

z.B. mit eingebautem BIOS-Festplattenschutz oder gängigen Verschlüsselungsprogrammen

Der physische Schutz ist bei IT-Systemen am Heimarbeitsplatz häufig gering. Es besteht somit ein erhöhtes Risiko, dass das Gerät gestohlen wird und dass der Dieb Zugang zu vertraulichen Daten (wie beispielsweise Passwörtern) erlangt. Im Extremfall können Anmeldungen unter fremder Benutzerkennung und Datenänderungen erfolgen.

M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.

★ M 1.15 – Geschlossene Fenster und Türen

Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind? ○ ja ○ nein

Wird mit Kontrollgängen überprüft, ob Fenster und Türen ordnungsgemäss geschlossen bzw. abgeschlossen werden? ○ ja ○ nein

Es besteht das Risiko, dass unberechtigte Personen über offene Fenster oder Türen physischen Zutritt zum IT-System erlangen. Dadurch können beispielsweise gewisse Sicherheitsmechanismen des Betriebssystems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.23, M 2.18.

M 1.17 – Pförtnerdienst

Wird der Zutritt zum Gebäude durch einen Pförtner kontrolliert? ○ ja ○ nein

Ohne einen Pförtnerdienst besteht das Risiko, dass unberechtigte Personen einfach physischen Zugang zu IT-Systemen erlangen.

★ M 1.19 – Einbruchsschutz

Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren? ○ ja ○ nein

Beispiele: Schliesszylinder, Sicherung von Kellerlichtschächten, Verschluss von nicht benutzten Nebeneingängen, Zaunanlage, Mauerwerk, Zufahrtssperren.

Es besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt ins Gebäude und zu IT-Systemen erlangen. Bei physischem Zugriff auf ein IT-System können anschliessend gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.10, M 1.12, M 1.16, M 1.40, M 1.53, M 1.55.

M 2.6 – Vergabe von Zutrittsberechtigungen

Werden Zutrittsberechtigungen zu schutzbedürftigen Räumen funktionsgerecht vergeben? ○ ja ○ nein

z.B. Serverraum nur mit Badge, Datensicherungsraum nur mit Pin-Code

Wenn unbestimmte Personenkreise Zutritt zu schutzbedürftigen Räumen haben, besteht das Risiko, dass unerlaubte Handlungen keinem bestimmten Personenkreis zugeordnet werden können. Es besteht das erhöhte Risiko, dass Personen Zugang zu Daten erhalten, die nicht ihrer Aufgabenstellung entsprechen (z.B. Administrator-Passwort) oder dass Personen Manipulationsmöglichkeiten erhalten, die sie an ihrem Arbeitsplatz nicht haben.

Weitere Informationen sind beim BSI zu finden unter M 2.14, M 2.17, M 2.97.

M 2.16 – Beaufsichtigung oder Begleitung von Fremdpersonen

Werden betriebsfremde Personen beaufsichtigt und begleitet? ○ ja ○ nein

z.B. Besucher, Handwerker, Servicetechniker, Reinigungspersonal

Wenn sich Personen unbeaufsichtigt oder unbegleitet bewegen können, besteht das Risiko, dass sie unberechtigten Zugang zu vertraulichen Daten erhalten. In Kombination mit anderen organisatorischen Mängeln (z.B. kein geregelter Passwortgebrauch) können betriebsfremde Personen zudem Manipulationen an Systemen und an Daten vornehmen.

Weitere Informationen sind beim BSI zu finden unter M 2.4.

Mobiler Einsatz

M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.

M 1.33 – Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

Sind mobile IT-Systeme beim Transport vor Diebstahl und unerlaubtem Zugriff geschützt? ○ ja ○ nein

Ohne angemessenen Schutz mobiler IT-Systeme besteht das Risiko, dass unberechtigte Personen Zugriff aufs IT-System erhalten (siehe M 1). Kompensierende Kontrollen wie beispielsweise Festplattenverschlüsselung und Bildschirmsperre können das Risiko minimieren.

Weitere Informationen sind beim BSI zu finden unter M 1.61.

M 2.306 – Verlustmeldung

Wird der Verlust von Geräten sofort gemeldet? ○ ja ○ nein

Werden die mit dem Verlust verbundenen Risiken systematisch bearbeitet? ○ ja ○ nein

z.B. Ändern aller Passwörter

Wenn der Verlust nicht gemeldet oder nicht systematisch bearbeitet wird, besteht das Risiko, dass unberechtigte Dritte sich mit Hilfe von Informationen aus dem mobilen Gerät Zugang zum IT-System verschaffen.

★ M 4.29 – Einsatz eines Verschlüsselungsproduktes für tragbare PCs

Ist bei mobilen Geräten die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt? ○ ja ○ nein

z.B. mit eingebautem BIOS-Festplattenschutz oder gängigen Verschlüsselungsprogrammen

Der physische Schutz ist bei IT-Systemen am Heimarbeitsplatz häufig gering. Es besteht somit ein erhöhtes Risiko, dass das Gerät gestohlen wird und dass der Dieb Zugang zu vertraulichen Daten (wie beispielsweise Passwörtern) erlangt. Im Extremfall können Anmeldungen unter fremder Benutzerkennung und Datenänderungen erfolgen.

Weitere Informationen sind beim BSI zu finden unter M 4.27.

Netzwerkanschluss

Modul: Netzwerkanschluss

★ M 2.35 – Informationsbeschaffung über Sicherheitslücken des Systems

Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen? ○ ja ○ nein

Beispiele: regelmässige Informationsbeschaffung über bekannte Sicherheitslücken, schnellstmögliches Einspielen von verfügbaren Patches und Updates.

Wird die Software auf den IT-Systemen regelmässig aktualisiert? ○ ja ○ nein

z.B. mittels neuen Software-Releases, Updates bei Tools etc.

Regelmässig werden Schwachstellen in Betriebssystemen, Datenbanken, Tools und Anwendungsprogrammen gefunden und im Internet veröffentlicht und sind dadurch einschlägig bekannt. Wenn die Schwachstellen durch das Einspielen neuer Software/Patches nicht geschlossen werden, besteht das Risiko, dass unberechtigte Personen diese Schwachstelle ausnützen und auf das IT-System zugreifen. Dadurch kann auf vertrauliche Daten zugegriffen, Netzwerk-Verkehr abgehört und Daten sowie Konfigurationen verändert werden. In einem fortgeschrittenen Stadium kann unter falscher Benutzerkennung oder als Administrator auf das System zugegriffen werden. Sehr ausgeprägt ist das Risiko bei Systemen, welche direkt im Zugriff des Internets stehen.

Weitere Informationen sind beim BSI zu finden unter M 2.273, M 4.152.

★ M 2.119 – Regelung für den Einsatz von E-Mail

Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails? ○ ja ○ nein

z.B. Verschlüsselung von Mail-Anlagen, Regeln zur Adressierung, Archivierung von E-Mails, Stellvertreter-Regelung etc.

Wenn das Mail-System ohne begleitende Regelungen genutzt wird, besteht das Risiko, dass unberechtigte Personen auf vertrauliche E-Mails zugreifen können. So kann beispielsweise der Stellvertreter Kenntnis von Passwörtern nehmen, die via E-Mail übermittelt werden, und sich anschliessend unter fremder Benutzerkennung anmelden.

Weitere Informationen sind beim BSI zu finden unter M. 2.118, M 2.274.

M 2.224 – Vorbeugung gegen Trojanische Pferde

Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden? ○ ja ○ nein

Beispiele von geeigneten Massnahmen sind: Unterbinden der Installationsmöglichkeit für die Benutzer, Führen einer Liste von freigegebenen Programmen, Sensibilisierung der Benutzer, Installation von Firewalls auf lokalen Computern der Benutzer, Installation von Software zum Erkennen von schadhaften Programmen etc.

Über Trojanische Pferde können Passwörter ermittelt werden. Ebenso besteht das Risiko, dass über das Trojanische Pferd direkt unter fremder Benutzerkennung auf das System zugegriffen wird.

Weitere Informationen sind beim BSI zu finden unter M 2.235, M 4.253.

M 4.241 – Sicherer Betrieb von Clients

Erfolgt die Administration des lokalen (Client-) Computers gesichert? ○ ja ○ nein

Beispiel: Administration erfolgt mittels Fernzugriff über eine verschlüsselte Verbindung, über ein zentrales Netzwerkmanagement-System oder lokal, wobei die Administratoren-Passwörter nur einer

kleinen Anzahl von Personen zur Verfügung stehen und regelmässig gewechselt werden.

Ohne sichere Administration des lokalen Computers besteht das Risiko, dass sich unberechtigte Personen als Administrator anmelden und dadurch Zugriff auf vertrauliche Daten erlangen (Abhören von Passwörtern, Missbrauch von Administrationsrechten aufgrund einer zu hohen Anzahl an berechtigten Administratoren etc.). Bei Zugriff auf vertrauliche Daten kann unter anderem auch das Passwort von "normalen" Benutzern ermittelt und anschliessend unter der entsprechenden Benutzerkennung gearbeitet werden.

M 5.68 – Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt? ○ ja ○ nein

z.B. erfolgt eine Verschlüsselung bei Client-Server-Anwendungen im LAN, beim Transport von Firmendaten zwischen zwei Standorten der Firma über das Internet (mit VPN), bei Abruf von Maildaten beim öffentlichen Provider etc.

Betriebssysteme senden die Passwörter üblicherweise in verschlüsselter Form über das Netz, so dass sie bei einem Lauschangriff nur geknackt werden können, wenn Sicherheitslücken im Produkt bestehen oder schwache Passwörter (Mindestlänge, Komplexität) gewählt werden; von solchen Schwachstellen ist jedoch auszugehen. Bei Anwendungsprogrammen ohne Passwort-Verschlüsselung (beispielsweise beim Webmail Provider im Internet) besteht ebenfalls das Risiko, dass das Passwort im LAN oder Internet abgehört und für unberechtigte Anmeldungen unter falscher Benutzerkennung verwendet wird. Wenn nicht der gesamte Netzwerkverkehr verschlüsselt wird, besteht das oben genannte Risiko bezüglich Passwörter. Vertrauliche Daten sollten mindestens bei Kommunikation im/durch das Internet verschlüsselt werden.

Weitere Informationen sind beim BSI zu finden unter M 5.66.

★ M 5.91 – Einsatz von Personal Firewalls für Internet-PCs

Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt? ○ ja ○ nein

Es kann zum Beispiel eine lokale Firewall verwendet werden, welche den Netzwerkverkehr vom und zum Computer analysiert - neben beispielsweise einer zentralen Firewall im Firmennetz oder einer Firewall beim Internetprovider im privaten Umfeld.

Falls der Computer weder von einer lokalen noch von einer zentralen Firewall geschützt ist, besteht das sehr hohe Risiko, dass der Computer vom Internet angegriffen wird und die Datensicherheit generell nicht gegeben ist. Falls der Computer zwar von einer zentralen Firewall geschützt ist, aber keine lokale Firewall vorhanden ist, besteht das Risiko von Angriffen aus dem lokalen Netz (was jedoch gewisse IT-Kenntnisse für einen erfolgreichen Angriff voraussetzt). Zudem besteht das Risiko, dass ohne Einsatz von lokalen Firewalls ausgehende Verbindungen nicht kontrolliert werden und deshalb beispielsweise Trojanische Pferde unentdeckt bleiben können.

Weitere Informationen sind beim BSI zu finden unter M 4.238.

★ M 5.93 – Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft? ○ ja ○ nein

Beispielsweise sind in den Browsereinstellungen die folgenden Optionen zu deaktivieren: aktive Inhalte (ActiveX, Java-Skripts), Plug-Ins und automatische Passwortspeicherung bei Formularen.

Es besteht das Risiko, dass ein Angreifer aus dem Internet die Schwäche in der Browser-Konfiguration ausnutzt und Zugriff auf das lokale System erlangt. Dadurch kann der Angreifer unter der lokalen Benutzerkennung Transaktionen durchführen. Weiter besteht das Risiko, dass automatisch abgespeicherte Formulardaten von einer unberechtigten Person erlangt werden (mit Software-Tools unterstützt, insbesondere bei direktem physischen Zugriff).

Weitere Informationen sind beim BSI zu finden unter M 5.69.

M 5.94 – Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs

Erfolgt ein sicherer Umgang beim Empfangen von E-Mails? ○ ja ○ nein

Beispiele für einen sicheren Umgang beim Empfang von E-Mails sind: E-Mail Anhänge werden gefiltert (.exe Dateien blockiert), Passwörter werden nicht via E-Mails an die Benutzer verschickt oder als Alternative werden die E-Mails verschlüsselt.

Wenn gefährliche E-Mail Anhänge (wie .exe) von eingehenden E-Mails nicht gefiltert werden, besteht das erhöhte Risiko, dass Trojanische Pferde installiert werden, welche beispielsweise Passwörter abhören. Alternativ oder zusätzlich können Mitarbeiter im Umgang mit E-Mail-Anhängen geschult werden, so dass sich das Risiko verringert. Beim Versand von Passwörtern in unverschlüsselten E-Mails besteht das Risiko, dass Administratoren, E-Mail-Stellvertreter etc. in den Besitz von Passwörtern von fremden Benutzern kommen und anschliessend unberechtigt die entsprechende Benutzerkennung annehmen.

M 5.96 – Sichere Nutzung von Webmail

Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt? ○ ja ○ nein

Beispiel für eine sichere Nutzung von Webmail: Das E-Mail Passwort für die Anmeldung zum Webmail-Provider wird regelmässig gewechselt, ist mindestens 8 Zeichen lang und wird bei keiner anderen Webseite verwendet. Zudem erfolgt der Zugriff auf die E-Mails beim Webmail-Provider über eine verschlüsselte Verbindung (SSL, https).

Beim unsicheren Umgang mit Webmail besteht das Risiko, dass die Passwörter abgehört oder durch Ausprobieren gefunden werden. Dadurch können E-Mails unter einer falschen Benutzerkennung über Webmail verschickt werden.

Weitere Informationen sind beim BSI zu finden unter M 5.66.

M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.

★ M 1.10 – Verwendung von Sicherheitstüren und -fenstern

Befinden sich besonders kritische IT-Systeme in Räumen mit Sicherheitstüren und -fenstern? ○ ja ○ nein

Beispiele solcher kritischen IT-Systeme sind Netzwerk-Server mit zentraler Ablage von vertraulichen Daten.

Ohne Sicherheitstüren und -fenster besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt zu IT-Systemen mit erhöhtem Schutzbedarf erlangen. Dadurch können gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1). Es kann möglicherweise auf wichtige, zentrale Daten zugegriffen werden (z.B. verschlüsselte Passwörter sämtlicher Netzwerkbenutzer, wobei mehrere Passwörter auf dieser Stufe häufig relativ leicht geknackt werden können).

Weitere Informationen sind beim BSI zu finden unter M 1.49, M 1.58, M 2.18.

M 1.18 – Gefahrenmeldeanlage

Existiert eine Alarmanlage zur Erkennung und Warnung bei Einbrüchen? ○ ja ○ nein

Ohne Alarmanlage besteht das Risiko, dass Einbrüche nicht erkannt werden und unentdeckt bleiben.

M 1.43 – Gesicherte Aufstellung aktiver Netzkomponenten

Sind besonders kritische Netzwerkkomponenten speziell vor physischem Zugang geschützt? ○ ja ○ nein

Beispielsweise werden Netzwerk-Server, Firewall-Systeme und Router in Serverräumen aufbewahrt, teilweise sogar in abschliessbaren Racks/Schränken.

Bei Zugang zu kritischen Netzwerkkomponenten besteht das Risiko, dass gewisse Sicherheitsmechanismen des Systems umgangen werden können (siehe M 1). Insbesondere ist an dieser Stelle ein einfacherer Zugang zu Passwörtern (Abhören und Manipulation des Netzverkehrs, Erlangen und Knacken von verschlüsselten Passwörtern) möglich.

M 1.53 – Videoüberwachung

Werden Kameras zur Überwachung von Gebäude und Räumen eingesetzt? ○ ja ○ nein

Es besteht das Risiko, dass Einbrüche nicht erkannt und Abläufe nicht nachvollzogen werden können. Zusammen mit weiteren Schwachstellen beim Zutrittsschutz kann dies dazu führen, dass unberechtigte Personen relativ einfach physischen Zugang zu IT-Systemen erlangen.

★ M 2.17 – Zutrittsregelung und -kontrolle

Ist die Zutrittsregelung zu Serverräumen in einem Zutrittskontroll- ○ ○

konzept geregelt? ja nein

z.B. Verantwortlichkeit für die Kontrolle, Listen von Zutrittsberechtigten, sichtbares Tragen von Zutrittsausweisen

Erfolgt eine Aufzeichnung der erfolgten Zutritte und Austritte? ○ ja ○ nein

z.B. Aufzeichnung der durch Badge gesicherten Zutritte, Besucherliste mit Ausweisnummer und Visum für Zutritt und Austritt

Wenn Zutrittsregelungen nicht kontrolliert und dokumentiert werden, besteht das Risiko, dass Personen oder Personenkreise Daten unentdeckt einsehen oder manipulieren.

★ M 2.35 – Informationsbeschaffung über Sicherheitslücken des Systems

Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen? ○ ja ○ nein

z.B. regelmässige Informationsbeschaffung über bekannte Sicherheitslücken, schnellstmögliches Einspielen von verfügbaren Patches und Updates

Wird die Software auf zentralen Netzwerkkomponenten regelmässig aktualisiert? ○ ja ○ nein

z.B. mittels neuen Software-Releases, Updates bei Tools etc.

Regelmässig werden Schwachstellen in Betriebssystemen, Datenbanken, Tools und Anwendungsprogrammen gefunden und im Internet veröffentlicht und sind somit einschlägig bekannt. Wenn die Schwachstellen durch das Einspielen neuer Software/Patches nicht geschlossen werden, besteht das Risiko, dass unberechtigte Personen diese Schwachstelle ausnützen und auf das IT-System zugreifen. Dadurch kann auf vertrauliche Daten zugegriffen, kann Netzwerk-Verkehr abgehört und können Daten sowie Konfigurationen verändert werden. In einem fortgeschrittenen Stadium kann unter falscher Benutzerkennung oder als Administrator auf das System zugegriffen werden. Dieses Risiko besteht insbesondere bei zentralen Netzwerk-Komponenten. Sehr ausgeprägt ist das Risiko bei Systemen, welche direkt im Zugriff des Internets stehen.

Weitere Informationen sind beim BSI zu finden unter M 2.273, M 4.152.

★ M 2.204 – Verhinderung ungesicherter Netzzugänge

Erfolgt jede Verbindung in das interne Netz ausnahmslos über gesicherte Zugänge? ○ ja ○ nein

Beispiel: zentrale Firewall, ohne die Möglichkeit, diese Firewall mit WLAN oder Modem zu umgehen.

Wenn Verbindungen über ungesicherte Zugänge möglich sind, besteht das Risiko, dass Unbefugte von aussen einfacher und unbemerkt ins Netz eindringen können.

M 4.162 – Sichere Konfiguration von Exchange 2000 Servern

Sind die Zugriffsrechte für E-Mail-Administratoren restriktiv vergeben worden? ○ ja ○ nein

Die Administrations-Rechte für das E-Mail System sollten restriktiv vergeben werden an Personen, welche die Berechtigungen für ihre tägliche Arbeit benötigen.

Es besteht das Risiko, dass vertrauliche Daten (wie Passwörter) über E-Mail verschickt werden und die E-Mail-Administratoren davon Kenntnis erlangen. Dieses Risiko erhöht sich, je mehr Personen diese Administrationsrechte besitzen.

M 4.239 – Sicherer Betrieb eines Servers

Erfolgt der Zugriff von Administratoren auf die zentralen Netzwerk-Komponenten gesichert? ○ ja ○ nein

Beispiele:
1) Administrationszugang zu zentralen Netzwerk-Komponenten ist ausschliesslich über die lokale Konsole am Server möglich (technisch so eingeschränkt) oder
2) Administrationszugang zu zentralen Netzwerk-Komponenten erfolgt mittels Fernzugriff über eine verschlüsselte Verbindung.

Bei ungesichertem Zugriff auf zentrale Netzwerk-Komponenten ist die Datenintegrität im lokalen Netz generell gefährdet, z.B. durch unberechtigten Administrationszugang und anschliessendem Ermitteln von Benutzerpasswörtern.

Weitere Informationen sind beim BSI zu finden unter M 4.80.

M 5.124 – Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

Gibt es eine Sicherheitsrichtlinie für die Nutzung der installierten und der mitgebrachten Geräte in Besprechungs-, Vortrags- und Schulungsräumen? ○ ja ○ nein

Ist sichergestellt, dass aus Besprechungs- und Veranstaltungsräumen keine unberechtigten Zugriffe auf das lokale Netz erfolgen können? ○ ja ○ nein

Beispiele von angemessenen Sicherheitsmassnahmen sind: Installation von firmeneigenen Computern in Besprechungs- und Veranstaltungsräumen mit sehr eingeschränkten Zugriffsberechtigungen im lokalen Netz sowie Verbot zum Anschliessen von fremden Computern; Installation eines Firewall-Rechners zur Trennung und Kontrolle des lokalen Teilnetzes bei Besprechungs- und Veranstaltungsräumen; technische Einschränkungen für den Anschluss von Computern ans Netz (z.B. Authentisierung über die so genannte MAC-Adresse oder Deaktivierung der automatischen Adress-Zuweisung an fremde Computer (kein DHCP)).

Es besteht das Risiko, dass aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf das lokale Netz unberechtigt zugegriffen wird und somit Besucher auf vertrauliche Daten zugreifen beziehungsweise sich im Extremfall sogar mit den ermittelten Passwörtern unter einer fremden Benutzerkennung einwählen. Kompensierende Sicherheitsmassnahme kann eine ständige Begleitung und Überwachung von Besuchern sein.

Weitere Informationen sind beim BSI zu finden unter M 2.333.

★ M 2.71 – Festlegung einer Policy für ein Sicherheitsgateway

Gibt es eine Weisung für einen Sicherheitsgateway und wird deren Einhaltung überprüft? ○ ja ○ nein

Beispielsweise regelt die Weisung für einen Sicherheitsgateway, welche technischen Kommunikationsprotokolle zwischen dem sicheren und dem unsicheren Netz zugelassen sind. So könnte beispielsweise ausgehender Web-Verkehr zugelassen werden. Weiter kann der Umfang der Protokollierung auf einem solchen System geregelt werden.

Wenn es keine Weisung für einen Sicherheitsgateway gibt, besteht das Risiko, dass der Gateway falsch konfiguriert und ungewollter Netzwerkverkehr zugelassen wird. Dadurch wird die Sicherheit im Netz generell gefährdet. Zudem besteht das Risiko, dass auf dem Sicherheitsgateway wichtige Informationen nicht protokolliert werden, wodurch die Nachvollziehbarkeit von Verbindungen und Transaktionen nicht gegeben ist.

Weitere Informationen sind beim BSI zu finden unter M 2.279, M 2.299, M 4.225.

M 4.112 – Sicherer Betrieb des RAS-Systems

Müssen sich Computer bei einer Verbindung und Einwahl ins interne Netz über ein unsicheres Netz (z.B. über Telefonlinie mittels Modem oder übers Internet) mit einem starken Authentisierungsverfahren anmelden? ○ ja ○ nein

Starke Authentisierungsverfahren beruhen auf mindestens 2 der folgenden 3 Faktoren: Authentisierung mit 1) etwas, das man weiss (z.B. Passwort); 2) etwas, das man hat (z.B. Streichliste); 3) etwas, das man ist (z.B. Fingerabdruck).

Zugriffe aus unsicheren Netzen ins interne Netz sind den Angriffen von (externen) Hackern ausgesetzt. Wenn ein schwaches Authentisierungsverfahren angewendet wird, besteht das Risiko, dass sich eine unberechtigte Person unter einer falschen Benutzerkennung ins interne Netz einwählt (z.B. durch vorgängiges Herausfinden von Passwörtern auf dem Computersystem des berechtigten Benutzers mit Fernzugriff). Durch die Authentisierung mit mehreren Faktoren kann dieses Risiko verringert werden. Alternativ können Schulungen der Benutzer zum sicheren Umgang mit Passwörtern, verschlüsselte Kommunikationsverbindungen und sicher konfigurierte Client-Systeme das Risiko ebenfalls verringern.

★ M 5.21 – Sicherer Einsatz von telnet, ftp, tftp und rexec

Werden die weit verbreiteten Dienste "telnet" (Fernzugriff auf Konsole) und "ftp/tftp" (Datei-Transfer) ausschliesslich in verschlüsselter Form verwendet? ○ ja ○ nein

z.B. durch Einsatz des sicheren Kommunikationsprotokolls SSH (Secure Shell)

Der Einsatz von telnet, ftp und tftp ohne zusätzliche Sicherheitsmassnahmen erhöht das Risiko, dass die Kommunikation der betreffenden Systeme sehr einfach abgehört werden kann. Dadurch können unberechtigte Personen beispielsweise in den Besitz von Administrationspasswörtern gelangen, wodurch generell die Datensicherheit sämtlicher Systeme im lokalen Netz gefährdet wird.

M 5.39 – Sicherer Einsatz der Protokolle und Dienste

Wird die Kommunikation verschlüsselt, wenn Administratoren mit dem Web-Browser die zentralen Netzwerkkomponenten administrieren? ○ ja ○ nein

Es sollten so genannte https-Verbindungen (SSL; Sicherheitsschloss im Browser angezeigt) für die Administration von Firewalls, Router, Switches etc. verwendet werden.

Wenn zentrale Netzwerkkomponenten über unverschlüsselte Verbindungen administriert werden, besteht das Risiko, dass die Passwörter der Administratoren abgehört werden. Dadurch können unberechtigte Personen die Netzwerk-Konfiguration ändern, wodurch die Sicherheit und Datenintegrität im lokalen Netz gefährdet ist. Um eine entsprechende Schwachstelle auszunutzen, ist ein gewisses Informatik-Wissen notwendig. Als alternative Massnahme zu verschlüsselten Verbindungen ist beispielsweise der Einsatz von Einmal-Passwörtern denkbar.

M 1.63 – Geeignete Aufstellung von Access Points

Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist? ○ ja ○ nein

z.B. in Doppelböden, in Metallgehäuse bei Wandhalterung etc.

Es besteht das Risiko, dass die Konfiguration des Wireless LAN Access Points unberechtigt geändert wird (z.B. mittels Reset-Knopf). Dadurch können Sicherheitsmechanismen ausgeschaltet werden, wie beispielsweise verschlüsselter Netzwerkverkehr oder Einschränkung der erlaubten Kommunikationspartner. Somit können Passwörter abgehört werden und die Nachvollziehbarkeit von Internet-Transaktionen ist nicht mehr gegeben (Surfen unter einer falschen IP-Adresse).

★ M 4.294 – Sichere Konfiguration der Access Points

Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden? ○ ja ○ nein

Beispiele von wichtigen Sicherheitsmechanismen sind:
1) Aktivierung der Kommunikations-Verschlüsselung (es sollte mindestens das so genannte WPA Sicherheitsprotokoll verwendet werden; das WEP Protokoll bietet keine ausreichende Sicherheit);
2) Der Zugriff auf den Access Point bzw. die WLAN Kommunikation ist auf ausgewählte Computer eingeschränkt (Aktivierung des so genannten MAC-Filters und zusätzliche Authentisierung mittels Schlüssel/Passwörter)?
3) Die Passwörter/Schlüssel für den Zugriff auf den Access Point bzw. die WLAN Kommunikation sind nicht trivial (d.h. Mindestlänge von 8 Zeichen und kein Wort aus einem Wörterbuch);
4) Der Access Point wird abgeschaltet, wenn er längere Zeit nicht benötigt wird.

Risiken:
1) Wenn die Kommunikation über drahtlose Netzwerke nicht verschlüsselt wird, können vertrauliche Daten von Personen in der näheren Umgebung (ca. 200 m) abgehört werden. Anschliessend können beispielsweise die so erlangte Benutzerkennungen und Passwörter von der unberechtigten Person im Internet verwendet werden (Internetzugriff über eine fremde Benutzerkennung beim Provider; Webmail-Zugriff und E-Mail-Versand unter falscher Benutzerkennung etc.).
2 und 3) Wenn der Zugriff auf den Access Point und die WLAN Kommunikation nicht auf ausgewählte Computer eingeschränkt wird, besteht das erhöhte Risiko, dass unberechtigte Personen über das drahtlose Netz kommunizieren. Dadurch kann auf andere Computer des Netzwerks zugegriffen oder es kann unter einer fremden Benutzerkennung auf das Internet zugegriffen werden. Ein analoges Risiko besteht, wenn Passwörter und Schlüssel für die WLAN Kommunikation trivial gewählt werden.
4) Wenn der Access Point nicht benötigt und trotzdem nicht abgeschaltet wird, ist die WLAN Kommunikation unnötig gefährdet (durch beispielsweise Risiken wie oben genannt).

Weitere Informationen sind beim BSI zu finden unter M 4.293, M 5.139, M 5.141.

M 4.295 – Sichere Konfiguration der WLAN-Clients

Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden? ○ ja ○ nein

Beispiele von wichtigen Sicherheitsmassnahmen sind:
1) Der Computer ist so konfiguriert, dass er selbst nicht WLAN Verbindungsanfragen von anderen WLAN Comutern direkt entgegen nimmt (d.h. der so genannte "Ad-hoc" Modus ist deaktiviert, so dass keine Client-Client Kommunikation stattfinden kann und der WLAN Verkehr stets über die Access Points führt).
2) Der Computer ist so konfiguriert, dass es nicht möglich ist, das WLAN zu nutzen, wenn der Computer gleichzeitig an ein "traditionelles" Kabelnetz angeschlossen ist.

Risiken:
1) Wenn Computer uneingeschränkt WLAN Verbindungsanfragen zulassen, besteht das Risiko, dass über diesen Weg unberechtigte Personen auf den lokalen Computer zugreifen. Alternativ können Verbindungsanfragen zugelassen werden, wenn zusätzliche Sicherheitsmassnahmen ergriffen

werden (insbesondere die Massnahmen "Restriktiver Zugriff auf Verzeichnisse und Dateien", "Sichere Access Point Konfiguration" und "Persönliche Firewalls" (BSI M 4.53, 4.294, 5.91)).
2) Wenn ein Computer gleichzeitig ans lokale (Kabel-) Netz und ans drahtlose Netz angeschlossen ist, besteht das Risiko, dass eine unberechtigte Person vom drahtlosen Netz über den lokalen Computer auf weitere Computersysteme im lokalen Netz zugreift. In diesem Szenario kann ein Angreifer über die drahtlose Verbindung auf das lokale Kabelnetz zugreifen und so die Kontrollen einer zentralen Firewall umgehen, welche eigentlich zum Schutz des lokalen (Kabel-) Netzes vorgesehen war.
Ohne wichtige Sicherheitsmassnahmen bei der Konfiguration des Client-Computers für drahtlose Netzwerke besteht somit das Risiko, dass über einen zusätzlichen Kanal auf den Client Computer zugegriffen werden kann (vorausgesetzt, es existieren keine kompensierenden Sicherheitsmassnahmen).

Weitere Informationen sind beim BSI zu finden unter M 4.297.

Modem / ISDN

Modul: Modem / ISDN

M 2.61 – Regelung des Modem-Einsatzes

Existieren angemessene Regelungen für den Einsatz von Modems? ○ ja ○ nein

Beispiele von Regelungen: Festlegung der berechtigten Benutzer, Protokollierung der Modem-Nutzung, Einschränkungen beim Versand von sehr vertraulichen Daten etc.

Es besteht das Risiko, dass Modemleitungen abgehört werden oder dass über Modems unberechtigt auf dahinter liegende Systeme zugegriffen wird.

M 3.17 – Einweisung des Personals in die Modem-Benutzung

Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet? ○ ja ○ nein

Es besteht das Risiko, dass Mitarbeiter durch unsachgemässe Handhabung der Modem-Nutzung einem Unberechtigten den Zugang zu Daten aktiv oder passiv verschaffen.

★ M 5.30 – Aktivierung einer vorhandenen Callback-Option

Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)? ○ ja ○ nein

Wenn das Modem eingehende Telefonanrufe / Verbindungsanfragen automatisch entgegen nimmt, besteht das Risiko, dass sich unberechtigte Personen über diese Verbindung Zugang zu dahinter liegenden Systemen verschaffen.

Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen werden, die Rückruf-Funktion aktiviert? ○ ja ○ nein

Beispiel: Die Einwahl ins Firmennetz über ein Modem ist nur von ausgewählten Rufnummern möglich. Deshalb trennt das Modem eingehende Verbindungsanfragen umgehend und ruft automatisch zurück, wenn die Rufnummer in der Liste der autorisierten Anrufer ist.

Ohne die Aktivierung der Rückruf-Funktion bei Modems besteht das Risiko, dass eine unberechtigte Person von einem beliebigen Telefonanschluss über das Modem auf das dahinter liegende Computersystem (Einzelplatz-Rechner oder lokales Netz) zugreift. Mit der Aktivierung der Rückruf-Funktion kann das Risiko reduziert werden, da nur noch von ausgewählten Rufnummern über das Modem auf das Computersystem zugegriffen werden kann. Auf die Aktivierung der Rückruf-Funktion kann verzichtet werden, wenn alternativ andere Massnahmen zur Authentisierung eingesetzt werden, üblicherweise mit Benutzerkennung, Passwort UND Streichlisten/Nummerngeneratoren (Einmal-Passwörter) (d.h. Authentisierung mit etwas, was man weiss, und zusätzlich mit etwas, was man hat/ist).

Weitere Informationen sind beim BSI zu finden unter M 5.31.

Datenbank / Anwendungsprogramm

★ M 2.221 – Änderungsmanagement

Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?

○ ja ○ nein

Wenn die systematische Überprüfung der Sicherheitsanforderungen nicht erfolgt, besteht das Risiko, dass die getroffenen Massnahmen nicht mehr wirksam sind. Es besteht das erhöhte Risiko, dass man sich in einer falschen Sicherheit wähnt.

Weitere Informationen sind beim BSI zu finden unter M 2.62.

★ M 4.42 – Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?

○ ja ○ nein

Beispielsweise können bei IT-Anwendungen mit wichtigen Daten folgende Zusatz-Massnahmen ergriffen werden:
1) Vergabe von angemessen abgestuften Zugriffsrechten innerhalb des Anwendungsprogramms
2) Protokollierung der Transaktionen von Benutzer und Administratoren

Wenn Benutzer innerhalb des Anwendungsprogramms Zugriff auf sämtliche Daten haben, besteht das Risiko, dass auf vertrauliche Daten zugegriffen wird. Zudem kann bei fehlender Protokollierung und grossem Benutzerkreis nicht mehr nachvollzogen werden, wer welche Transaktionen durchgeführt hat.
Ohne Protokollierung ist nicht nachvollziehbar, wer welche Transaktionen durchgeführt hat (ausser ein einziger Benutzer besitzt die entsprechenden Zugriffsrechte).

Weitere Informationen sind beim BSI zu finden unter M 2.129, M 2.132.

★ M 4.72 – Datenbank-Verschlüsselung

Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?

○ ja ○ nein

Die in Datenbanken und Anwendungsprogrammen bearbeiteten Daten werden in Form von Dateien vom Betriebssystem gespeichert. Wenn diese Dateien unverschlüsselt abgespeichert werden, besteht das Risiko, dass Benutzer direkt vom Betriebssystem auf die Dateien zugreifen und die Daten abändern. In einem solchen Szenario ist nicht mehr nachvollziehbar, welcher Benutzer die Daten eingegeben bzw. geändert hat. Die Zugriffskontrollen der Anwendungsprogramme und Datenbanksysteme sind in einem solchen Fall wirkungslos und werden umgangen.

M 4.133 – Geeignete Auswahl von Authentikations-Mechanismen

Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

○ ja ○ nein

Beispielsweise werden bei der Anmeldung zusätzlich benötigt: Eingabe eines Einmal-Passworts aus einer Liste, Biometrische Eingabe mittels Scan des Fingerabdrucks, Eingabe eines Pins aus einem Nummern-Generator etc.

Es besteht das Risiko, dass eine Benutzeranmeldung am System unter einer falschen Benutzerkennung erfolgen kann. Bei absoluter Verlässlichkeit auf kompensierende Sicherheitsmechanismen (Verschlüsselung, sicherer Passwortumgang etc.) kann auf zusätzliche Elemente zur Authentisierung verzichtet werden. Aufgrund der generellen Fehleranfälligkeit besteht insbesondere bei kritischen Systemen das Risiko, dass der Schutz ohne diese zusätzlichen Authentikations-Mechanismen nicht angemessen ist.

1.5 Glossar

Einige der Begriffe stammen aus www.wikipedia.de; eine weitere hilfreiche Quelle ist www.whatis.com.

Access Point	Bezeichnung für eine aktive Verbindung zum Internet bzw. zu einem Online-Dienst. Ein Wireless Access Point ist ein elektronisches Gerät, das als Schnittstelle zwischen einem Funknetz und einem kabelgebundenen Rechnernetz fungiert.
ActiveX	ActiveX ist eine Entwicklung von Microsoft, welche die Freigabe von Informationen zwischen Anwendungen erleichtert und die Einbettung beliebiger Objekte (Video, Sound,...) in fremden Dokumenten wie z.B. Web-Seiten erlaubt. Damit lassen sich also "aktive Inhalte" in Web-Seiten realisieren: Programme werden vom Server auf den Rechner des "Surfers" übertragen und dort ausgeführt.
Administrator	Als Administrator wird der Systemverwalter zum Beispiel eines Netzwerks, eines Computers oder eines ganzen Computer-Systems bezeichnet. Er besitzt weit reichende Zugriffsrechte, kann oft zahlreiche oder alle Einstellungen am System vornehmen, Benutzernamen und Kennwörter verwalten und ist für die Aufrechterhaltung des IT-Systems zuständig.
Authentisierung	Die Begriffe Authentisierung und Authentifizierung werden hier synonym verwendet für den Vorgang des Nachweises der eigenen Identität bzw. den Vorgang der Überprüfung (Verifikation) der behaupteten Identität eines Gegenübers, beispielsweise einer Person oder eines Computersystems.
Backup	Unter Backup (auch Datensicherung genannt) versteht man das Kopieren der in einem Computersystem vorhandenen Daten auf ein alternatives (häufig transportables) Speichermedium. Dort werden diese mit dem Ziel aufbewahrt, den Datenverlust bei Systemausfällen zu begrenzen.
Betriebssystem	Ein Betriebssystem ist die Software, welche die Verwendung (den Betrieb) eines Computers ermöglicht. Es verwaltet Betriebsmittel wie Speicher, Ein- und Ausgabegeräte und steuert die Ausführung von Programmen.
BIOS	Basic Input Output System: BIOS ist der hardwaregebundene Kern eines Betriebssystems, der beim Ausschalten nicht gelöscht wird. Dieser Chip wird einmalig mit Daten beschrieben, die vom Computer nur gelesen und nachträglich lediglich mit Hilfe von Spezialprogrammen verändert werden können. Nach jedem Einschalten des Rechners führt das BIOS zunächst einen Selbsttest durch. Dann benutzt der Computer das BIOS, um das Betriebssystem zu starten und die Daten zwischen der Festplatte, Grafik-Karte, Keyboard, Maus und Drucker zu kontrollieren, bis ihm diese Aufgabe von einem anderen System - z.B. dem Betriebssystem - abgenommen wird.
BSI	Bundesamtes für Sicherheit in der Informationstechnik (Deutschland)

Callback-Option	Rückruf-Funktion
Client	Programm oder ein Computer, der in direkter Verbindung mit einem Server Informationen abruft.
Datenbank	Die Datenbank gleicht einem elektronischen Karteikasten. Hier findet man eine Sammlung von Daten, die miteinander in Beziehung stehen und stets aktualisiert werden. Übersichtliches Suchen, Korrigieren, Sortieren und Bearbeiten von vielen unterschiedlichen Daten wird hier ermöglicht.
DHCP	Dynamic Host Configuration Protocol: Das DHCP weist den angeschlossenen Clients aus einem festgelegten Bereich von IP-Adressen automatisch eine IP-Adresse zu und spart so viel Konfigurationsarbeit bei grösseren Netzen.
Email	Elektronische Post. Einer der wichtigsten Internet-Dienste, der das schnelle Übermitteln von Nachrichten ermöglicht. Im Anhang (Attachment) von E-Mails können auch Bild- und Textdateien sowie Softwareprogramme mit verschickt werden.
Exchange	Der Exchange Server ist ein Groupware- und Messaging-System der Firma Microsoft. Er kann für umfangreiche und vielfältige Aufgaben in von Microsoft-Produkten geprägten Infrastrukturen eingesetzt werden und eignet sich sowohl für kleine als auch grosse Netzwerke: so können beispielsweise E-Mails verwaltet und gefiltert, Zeitpläne erstellt, Termine vereinbart und Diskussionen geführt werden.
Firewall	Eine Firewall auch Sicherheitsgateway, Netzwerk-, oder Hardware-Firewall genannt, ist eine Netzwerk-Sicherheitskomponente in der Computertechnik, die Netzwerkverkehr anhand eines definierten Firewall-Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauens-Stufen abzusichern. Ein typischer Einsatzzweck ist es, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren.
FTP	File Transfer Protocol: wichtiger Dienst, der es ermöglicht, Dateien von externen Servern auf den eigenen Computer herunterzuladen (Download) und lokal erstellte Dateien (z.B. Aktualisierungen der eigenen Webseite) auf den Server zu kopieren.
Gateway	Computer/Gerät am Übergang zwischen zwei Netzwerken
Hacker	Ein IT-Spezialist, der mit seinem Fachwissen Sicherheitslücken sucht und ausnutzt.
HTTPS	HTTPS steht für Hyper Text Transfer Protocol Secure. Das Protokoll dient zur Verschlüsselung und zur Authentisierung der Kommunikation zwischen Webserver und Browser im World Wide Web.
Internet	Weltweiter Verbund von Computernetzwerken auf der Grundlage des einheitlichen Übertragungsprotokolls TCP/IP, in dem Kommunikation und Datenaustausch mit Hilfe verschiedener Internet-Dienste möglich

	sind. Zugang zum Internet verschaffen ISP (Internet Service Provider) und Online-Dienste.
Internetprovider	Zugangsvermittler zum Internet.
Intranet	Firmeninternes Netzwerk auf Grundlage der Internet-Dienste und Technologien (TCP/IP). Über ein Intranet kann (muss aber nicht) ein Zugang zum Internet und Extranet hergestellt werden.
IP-Adresse	Adresse eines einzelnen Computers im Internet. Die IP-Adresse besteht aus vier Zahlen von 0 bis 255, jeweils durch Punkte getrennt (Beispiel: 193.7.250.19).
ISDN	ISDN steht für "integrated services digital network". Die Leitidee des ISDN ist die Integration verschiedener Informationsformen (Sprache, Text, Bild, Daten), für die früher aufgrund ihrer unterschiedlichen physikalischen Struktur auch unterschiedliche Kommunikationsnetze bereitgestellt werden mussten.
Java-Skripts	Scriptsprache von Netscape, die im lokalen Browser interpretiert und ausgeführt wird, ohne dass dabei der Webserver involviert ist.
Konfiguration	Mit einer Konfiguration bezeichnet man eine bestimmte Einstellung von Programmen oder Hardwarebestandteilen eines Computers.
Konsole	Fenster, in dem Befehle per Kommandozeile eingegeben werden können.
LAN	Lokales Netzwerk, das Arbeitsplatzrechner (Clients) untereinander und (zumeist) mit einem oder mehreren Servern verbindet. Grundvoraussetzung für den internen Datenaustausch und die Realisierung eines Intranets.
MAC-Adresse	Media Access Control: Ein Zugangsverfahren zum eigentlichen Medium (Kabel) eines Netzes, das im Netzwerkcontroller implementiert ist - also beispielsweise in der Netzwerkkarte. Diese verfügt über eine so genannte MAC-Adresse (oder Hardware-Adresse), durch die eine Station eindeutig im Netz identifiziert ist. Es handelt sich sozusagen um die unverwechselbare Seriennummer eines Netzwerkgerätes.
Mailprovider	Zugangsvermittler zum Mail.
Modem	Modem ist ein Gerät zur Datenfernübertragung, welches eine Verbindung zu einer Gegenstation aufbaut, Signale, die vom Computer kommen, in Töne umsetzt und diese zur Gegenstation sendet und - auf der anderen Seite der Leitung eingesetzt - die empfangenen Töne wieder in maschinenverständliche Signale zurückübersetzt (moduliert).
Netzwerk	Verbund von Rechnern, die untereinander Daten austauschen. Netzwerk-Rechner können als Host beziehungsweise Server Daten zur Verfügung stellen oder als Client auf diese zugreifen. In manchen Netzwerken üben die verbundenen Rechner auch beide Funktionen gleichzeitig aus.

Patch	Kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt.
PC	Personal Computer
PDA	Persönlicher Digitaler Assistent: Ein PDA ist ein Computer im Westentaschenformat. Die Geräte verfügen über Büro-Funktionen wie Kalender, Adress- oder Notizbuch und erlauben die digitale Kommunikation (z.B. für E-Mail per Handy-Modem).
PDF	PDF steht für Portable Document Format und ist ein plattformunabhängiges weit verbreitetes Dateiformat. PDF-Dokumente können zwischen Rechnern unterschiedlicher Betriebssysteme ausgetauscht und auch in Browsern mit dem entsprechenden PlugIn (PDF-Viewer) dargestellt werden.
Pin	Verfahren zur Authentisierung. Hierbei sind für den Zugang zum Konto neben der Konto- oder Kundennummer die geheime PIN (Personal Identification Number) anzugeben.
Plug-In	Hilfsprogramm, das sich in ein anderes Programm "einklinkt" und dessen Funktionalitäten erweitert.
Protokollierung	Dokumentieren in Protokollen (oder Protokolldateien, Log-Files), welche Transaktionen ausgeführt wurden oder welche Fehler aufgetreten sind.
Rexec	Um Befehle auf einem Nicht-Windows-Remotecomputer auszuführen, können von Computern unter Betriebssystemen der Windows Server 2003-Produktfamilie, Windows XP und Windows 2000 mit dem Tool Rexec eine Verbindung zu Nicht-Windows-Computern hergestellt werden. Der Befehl rexec authentisiert den Benutzernamen auf dem Remotecomputer, bevor der angegebene Befehl ausgeführt wird.
Router	Ein Router ist eine Netzwerkkomponente, die mehrere Rechnernetze koppelt.
RAS	Remote Access Service: Online-Anwendung, mit dessen Hilfe sich externe Nutzer (z.B. Aussendienstmitarbeiter) über Telekommunikationsleitungen in ein internes Firmennetz (LAN, Intranet) einwählen können und Zugriff auf alle dort verfügbaren Programme und Dateien haben.
Server	Computer, der im Dauerbetrieb arbeitet, Programme und Dateien (Datenbanken, Textdateien) zentral speichert und diese zum Abruf durch Client-Rechner bereithält. Server sind einerseits Knotenpunkte in firmeninternen Netzen (LAN, Intranet) und halten dort gemeinsam genutzte Programme und Dateien vor. Mailserver dienen zur Verwaltung und Weiterleitung von E-Mails. Webserver speichern Webseiten und machen sie im Internet verfügbar.
SSH	Secure Shell: Programm und Netzwerkprotokoll gleichen Namens, um sich übers Internet auf einen entfernten Computer einzuloggen und Daten auszutauschen oder dort Programme auszuführen. Im Gegen-

	satz zu z.B. TELNET geschieht die Kommunikation über ein ungesichertes Netzwerk, aber verschlüsselt und mit Authentisierung.
SSL	Secure Socket Layer: Möglichkeit zur Verschlüsselung der Datenübertragung. SSL ist zwar grundsätzlich für verschiedene Anwendungen nutzbar, wird aber relativ häufig bei Web-Zugriffen im Bereich des E-Commerce, Online-Banking oder E-Governments eingesetzt.
Switch	Ein Switch (engl. Schalter, auch Weiche) ist eine Netzwerk-Komponente zur Verbindung mehrerer Computer beziehungsweise Netz-Segmente in einem lokalen Netz (LAN).
TELNET	Dienst im Internet, der es erlaubt sich auf entfernten Rechnern einzuloggen und zu arbeiten.
TFTP	Das Trivial File Transfer Protocol (TFTP) ist ein sehr einfaches Dateiübertragungsprotokoll. TFTP unterstützt lediglich das Lesen oder Schreiben von Dateien.
Tools	Dienstprogramm, das für den Benutzer beziehungsweise Systemverwalter eines Computers allgemeine, oft systemnahe Aufgaben ausführt. Üblicherweise gehört eine Reihe von Dienstprogrammen zum Lieferumfang eines Betriebssystems, wobei jedes Dienstprogramm meistens auf eine ganz bestimmte Aufgabe spezialisiert ist.
Trojanisches Pferd	Programm, das neben einer offiziellen Funktion eine zweite Funktion (in der Regel eine Schadfunktion) hat. Sinn eines Trojanischen Pferds kann es beispielsweise sein, Zugangskennungen mitzuprotokollieren.
Update	Eine Aktualisierung, oft auch als (engl.) Update bezeichnet, beschreibt den Vorgang, etwas bereits Vorhandenes auf den neuesten Stand zu bringen. Eine Aktualisierung beziehungsweise ein Update kann also nur durchgeführt werden, wenn eine bestehende Version existiert.
Verschlüsselung	Übersetzung von sinnvollen Daten in scheinbar sinnlose Daten mit Hilfe eines (elektronischen) Schlüssels. Eine Rückübersetzung ist nur mit Hilfe eines geeigneten Schlüssels möglich. Sind die Schlüssel für Ver- und Entschlüsselung identisch, handelt es sich um symmetrische Verschlüsselung. Wird zum Entschlüsseln ein anderer (privater) Schlüssel als zum Verschlüsseln (öffentlicher) benötigt, spricht man von asymmetrischer Verschlüsselung.
VPN	VPN steht für Virtual Privat Network. Mit VPN lässt sich der Zugriff auf einen Rechner oder ein Firmennetzwerk über das Internet aufbauen.
Webmail	Nach Überprüfung der Zugangsberechtigung stellt dieses Interface dem Benutzer die Funktionalität eines E-Mail-Clients über das Internet zur Verfügung. E-Mails können so online über die Web-Oberfläche gelesen oder verschickt werden.
WEP	Wired Equivalent Privacy: Bezeichnet ein Verschlüsselungsverfahren, das für Wireless LANs verwendetet wird.

WLAN	Wireless-LAN, auch W-LAN genannt, bezeichnet ein Netzwerk, das nicht wie bekannt über Kabel, erstellt ist, sondern kabellos (Englisch: wireless) funktioniert.
WPA	WPA steht für Wi-Fi Protected Access: Nachdem sich die WLAN-Verschlüsselung WEP als unsicher erwiesen hat, wurde der WPA-Standard zur Absicherung von Funknetzen entwickelt. Er bietet zusätzlichen Schutz durch dynamische Schlüssel.
WWW	Das World Wide Web (kurz Web, WWW oder deutsch: Weltweites Netzwerk; wörtlich: web „Gewebe, Netz“) ist ein über das Internet abrufbares Hypertext-System. Hierzu benötigt man einen Webbrowser, um die Daten vom Webserver zu holen und z.B. auf dem Bildschirm anzuzeigen.
WWW-Browser	Programm zum Abruf und zur Anzeige von Dokumenten im World Wide Web; notwendige Voraussetzung zur Informationssuche im Netz und zum Besuch von Webseiten. Die am weitesten verbreiteten Browser sind Netscape Navigator und Microsoft Internet Explorer.