



FAKULTÄT FÜR **INFORMATIK**

Erstellung und Umsetzung eines didaktischen Konzeptes zur Steigerung des Sicherheitsbewusstseins im IT-Bereich

DIPLOMARBEIT

zur Erlangung des akademischen Grades

**Magister der Sozial- und
Wirtschaftswissenschaften**

im Rahmen des Studiums

Informatikmanagement

eingereicht von

Andreas Weiner
Matrikelnummer 9625212

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer/Betreuerin: Univ.Prof. Dipl.-Ing Dr.techn. Werner Purgathofer

Wien, 13.01.2010

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Ich möchte diese Masterarbeit all jenen widmen, die mir während meines Studiums in irgendeiner Art und Weise beigetragen sind. Auch möchte ich sie den Leuten widmen, die gemeint haben, ich würde nie so weit kommen und ewiger Student bleiben.

Das Spiel ist die höchste Form der Forschung.

(Albert Einstein)

INHALTSVERZEICHNIS

Inhaltsverzeichnis.....	6
Disclaimer.....	8
Vorwort.....	9
Sicherheit und Sicherheitsverständnis.....	10
Allgemein.....	10
IT.....	11
Didaktische Verfahren.....	14
Frontalunterricht.....	14
Diskussionsrunden.....	15
Lernen durch Lehren / Selbststudium / Studienzirkel.....	15
eLearning / Programmierter Unterricht.....	16
Learning by Doing.....	17
Simulativer Unterricht / Spielerisches Lernen.....	19
Wer ist die Zielgruppe?.....	21
Was soll vermittelt werden?.....	21
Maßnahmenkatalog des BSI.....	23
Einführung.....	23
M 1 Maßnahmenkatalog Infrastruktur.....	26
M 2 Maßnahmenkatalog Organisation.....	47
M 3 Maßnahmenkatalog Personal.....	83
M 4 Maßnahmenkatalog Hardware und Software.....	96
M 5 Maßnahmenkatalog Kommunikation.....	140
M 6 Maßnahmenkatalog Notfallvorsorge.....	157
Zusammenfassung.....	195
Wie soll das Wissen vermittelt werden.....	196
Bestandsaufnahme.....	196
Das Spiel und die Spielmechanik.....	198
Überlegte Spielvarianten.....	198
Spielvariante 1 – Das Kartenspiel.....	199
Spielvariante 2 – Ein Brettspiel mit Karten und Würfeln.....	200

Spielvariante 3 – Die Brettspielvariante mit einem flexibel gestaltbarem Spielbrett, Miniaturen, Würfeln und Karten	202
Spielvariante 4 – Das Quizspiel	204
Spielvariante 5 – Das Kartenspiel ergänzt durch Würfel	205
Die von uns gewählte Spielvariante im Detail	207
Beschreibung des Spieles „Damn IT! – Die verrückte Welt der IT“	209
Worum geht es bei dem Spiel?	209
Empfohlenes Alter	209
Spiellänge	209
Mögliche Spieleranzahl	209
Inhalt des Spiels.....	209
Das Spielbrett	210
Die Punkteleiste	211
Spelaufbau.....	211
Spielablauf	212
Ein Spielzug folgt folgendem Schema	212
Es gibt folgende Möglichkeiten an Punkte zu kommen:	212
Die Spielfelder und darauf mögliche Aktionen:	213
Ein Feld auf dem bereits andere Mitspieler stehen	216
Die Angriffsaktion	216
Die Verteidigungsaktion	216
Aktionskarten im Spiel.....	217
10 Angriffskarten (jeweils 2 mal – insgesamt 20 Karten)	218
17 Verteidigungskarten (2 Sets: Einmal in Stärke 1 und einmal in Stärke 2) insgesamt 34 Karten.....	221
Ereigniskarten im Spiel	226
14 negative Ereignisse: (insgesamt 14 Karten).....	226
10 positive Ereignisse: (insgesamt 10 Karten).....	230
10 Zufallsereignisse (insgesamt 10 Karten)	233
Arbeitsaufteilung.....	236
Resümee.....	238
Literaturverzeichnis.....	239
Appendix	242
Anleitung	242

DISCLAIMER

Die Inhalte dieser Arbeit sprechen Frauen wie Männer gleichermaßen an. Zur besseren Lesbarkeit wird nur die männliche Sprachform verwendet. Bezeichnungen wie "der Durchschnittsbenutzer", „der User“, usw. sind daher als geschlechtsneutral anzusehen.

VORWORT

Sicherheit im IT-Bereich ist ein Thema, welches durch das stetige Wachstum dieses Bereichs immer aktueller wird. Immer wieder ist in verschiedensten Medien von Computerkriminalität zu hören, durch die viele Leute teilweise nicht unbeträchtlichen Schaden, vor allem monetärer Art, erleiden.

Aber auch IT-Probleme, die nicht von Kriminellen verursacht werden, können ihren Weg in die Schlagzeilen finden, z.B. wenn irgendwelche sensitiven Daten verloren gegangen sind.

Manchmal hat man dabei den Eindruck, dass Sicherheitsmaßnahmen gegen diese Gefahren nur von Experten gesetzt werden könnten. Aber das ist so nicht richtig, denn gegen sehr viele Gefahren im IT-Bereich kann sich ein Benutzer relativ leicht selbst schützen. Aber dazu bedarf es des Wissens um mögliche Gefahren und des Wissens darum mit welchen Maßnahmen man sich gegen diese schützen kann.

Wir haben uns in dieser Arbeit folgenden Fragen gewidmet:

„Welche Gefahren sind im IT-Bereich sehr verbreitet und was sind geeignete Maßnahmen dagegen?“

„Wie steigern wir bei einem Durchschnittsbenutzer das Sicherheitsbewusstsein im IT-Bereich?“

„Wie kann man Durchschnittsbenutzern das Wissen um Gefahren im IT-Bereich bzw. die Maßnahmen dagegen relativ leicht vermitteln?“

Und wir glauben eine Möglichkeit gefunden zu haben, wie dies realisierbar ist.

SICHERHEIT UND SICHERHEITSVERSTÄNDNIS

ALLGEMEIN

Sicherheit im Alltag ist heutzutage nicht mehr wegzudenken. Nicht nur im privaten Bereich ist ein gewisses Grundmaß an Sicherheit unumgänglich, vielmehr ist Sicherheit auch am Arbeitsplatz ein großes Thema. Viele potentielle Gefahrenquellen müssen bedacht werden um schließlich ein hohes Maß an Sicherheit gewährleisten zu können. Die Quellen für mögliche Schäden sind dabei sehr weit gestreut; angefangen bei Bränden und Blitzschäden bis hin zu Angriffen auf Leben und Besitz lässt sich die Liste beliebig lange fortsetzen. Auch Diebstähle liegen heutzutage schon beinahe an der Tagesordnung und sind nur eine weitere von vielen Gefahren.

Natürlich muss auch angesprochen werden, dass sich ein beträchtlicher Anteil der Bedrohungen im Alltag durch „menschliches Versagen“ wie z.B. Unachtsamkeit einschleichen. Sehr oft werden drohende Gefahren nicht als solche erkannt und können dadurch fatale Folgen nach sich ziehen.

Glücklicherweise wird jeder Mensch auf mannigfaltige Art und Weise über die Mehrheit der Gefahren seiner Umwelt aufgeklärt. Schon Kinder lernen, dass Feuer gefährlich sein kann, später lernen Jugendliche auf verschiedenen Wegen über die Gefahren im Straßenverkehr. Zeitungen berichten über Einbrüche und Diebstähle und nicht selten liest man im selben Artikel, dass ein Einbruch mit einer Sicherheitstür verhindert werden könnte. Genauso wird man regelmäßig über die Vorteile einer Versicherung informiert, die Gefahren nicht verhindern aber immerhin den Schaden einschränken können.

Zusammenfassend kann man sagen, dass man im Alltag selten mit neuen Gefahren konfrontiert wird, und in der Regel Gegenmaßnahmen kennt, deren Umsetzung in der jeweils eigenen Verantwortung liegt.

IT

Im IT-Bereich steht die Menge von Bedrohungen der im Alltag um nichts nach. Neben den genauso gültigen Gefahren wie Feuer, Blitzschlag oder Diebstahl stellen beispielsweise Viren, Trojaner, Malware und Phishing für den IT-Bereich zusätzliche weit verbreitete Gefahrenquellen dar.

Das Problem dieser IT-spezifischen Risiken im Gegensatz zu den alltäglichen ist aber, dass man nur in Ausnahmefällen darüber informiert wird. An den meisten Schulen werden inzwischen Notebook-Klassen eingeführt, aber es gibt keine Aufklärungsarbeit über die Risiken und Gefahrenquellen. Dasselbe gilt für PCs daheim. Internetanschlüsse finden sich in immer mehr Haushalten, die Benutzer machen sich aber keine Gedanken darüber, welche Informationen sie über sich in Foren und Chats verbreiten oder woher sie Software herunterladen und was sie sich unter Umständen damit an Spyware ins Haus holen.

Um seine Güter am PC-Arbeitsplatz, ob elektronischer (Emails, Fotos, Software) oder physischer (CDs, Hardware) Art, zu schützen, ist es die Aufgabe jedes einzelnen, sich passende Notfallstrategien zurechtzulegen um Angriffe jeglicher Art abwehren zu können und Schäden zu verhindern. Der größte Problempunkt hierbei ist das Erkennen von Gefahren als solche. Wenn mögliche Gefahren als solche erkannt und eingeschätzt werden können, ist bereits ein wichtiges Fundament für ein gesteigertes Sicherheitsniveau gelegt, auf das schlussendlich aufgebaut werden kann.

Nachdem nun ein guter Ansatzpunkt gefunden wurde, der der Schlüssel zu einem erfolgreichen Sicherheitssystem ist, wollen wir die sogenannte „Awareness-Bildung“ in den Mittelpunkt unseres Projektes Stellen. Bewusstsein schaffen um mehr Sicherheit gewähren zu können ist der beste Weg um Schäden verhindern zu können.

Die drei Schlagwörter die mit der Bewusstseinsbildung gekoppelt sind lauten demnach

Wahrnehmen-Erkennen-Bewältigen

Der User soll lernen Gefahren wahrnehmen zu können, sie im Falle des Falles auch zu erkennen, und schließlich auch zu bewältigen. Mit dieser Strategie befindet sich der IT-Benutzer auf dem besten Weg mehr Sicherheit für sein Hab und Gut zu gewährleisten. Wenn jeder Benutzer optimal für den ihm zugeteilten Arbeitsbereich (d.h. entweder sein PC daheim oder sein Arbeitsplatz mit allem was dazugehört) sorgt und wachsam bleibt, profitiert das gesamte Umfeld. Natürlich ist hierbei jeder Teil des Ganzen wichtig, um ein hohes Sicherheitsniveau zu garantieren.

Exemplarisch sollen im Folgenden einige Beispiele für Gefahren und deren Gegenmaßnahmen genannt werden:

<i>Gefahr</i>	<i>mögliche Auswirkung</i>	<i>Gegenmaßnahmen</i>
Feuer / Wasser	Zerstörung von Eigentum, Dokumenten, uvm. Neben dem finanziellen Schaden fließt enorm viel Zeit und Energie in Wiederbeschaffung über Versicherungen. Durch Löscharbeiten kann es zu weiteren Schäden durch Wasser kommen.	Vorsicht, Sicherungen für elektronische Geräte, feuerfester Tresor, evtl. Sprinkleranlage, Versicherung
Einbruch	Diebstahl von Eigentum, Dokumenten, uvm. Abgesehen vom finanziellen Schaden kostet die Wiederbeschaffung durch Polizei und Versicherung viel Zeit und Energie.	Sicherheitstüren, Alarmanlage, Gebäudeschutzfirma
Überschreitung des Lebensalters von Speichermedien	Verlust von Daten, Musik, Fotos u.a. Wiederbeschaffung eventuell gegen enormen Kosten- und Zeitaufwand	Lebensdauer der Speichermedien im Auge behalten, Backups an einer zweiten Stelle ablegen

<i>Gefahr</i>	<i>mögliche Auswirkung</i>	<i>Gegenmaßnahmen</i>
Viren, Trojaner	Datenverlust bzw. Zugriff auf Daten für Unberechtigte, Finanzielle Schädigung	Virens Scanner, Updates, geeignete Wahl der Software
Hacker	Zugriff auf alle Daten am System für Personen ohne Zugangsberechtigung, Finanzielle Schädigung	Firewall, unnötige Services abschalten
Phishing	Datenübertragung an Dritte ohne Berechtigung, Finanzielle Schädigung	Browserplugins die vor solchen Attacken warnen, gesundes Misstrauen

DIDAKTISCHE VERFAHREN

Generell kann man davon ausgehen, dass Wissen um Gefahrenquellen und mögliche Reaktionen auf diese Gefahren die Voraussetzung für Sicherheitsbewusstsein ist. Daraus ergibt sich das Problem, wie dieses Wissen einer möglichst großen Zielgruppe dargebracht werden kann. Bekanntermaßen gibt es verschiedene Lehrstile und Methoden, von denen für den Bereich IT-Sicherheit manche besser und manche schlechter geeignet wären. Daher wird es nötig sein, eine gut geeignete Lehr-Methode zu bestimmen um darauf aufbauen zu können. Eine Analyse einiger dieser Lehrtechniken hinsichtlich relevanter Kriterien wie z.B. „Zielgruppe“, „Zeit“, „Ort“, „Voraussetzungen“, „Kosten“ oder „Motivationssteigerung“ ist daher die Voraussetzung für die Planung von bewusstseinsbildenden Maßnahmen.

FRONTALUNTERRICHT

Der Frontalunterricht wird immer durch den Lehrer dominiert. Der Lehrstoff wird im Rahmen eines Vortrags bzw. Lehr-Gesprächs vermittelt. Es wird vorausgesetzt, dass alle Lernenden alles zur gleichen Zeit aufnehmen, lernen, verstehen und begreifen. Im klassischen Sinne des Frontalunterrichts finden sich verschiedene Lehrformen: Vortragen, Vorlesen, Erzählen, Berichten, Vormachen, Vorführen, Demonstrieren, sowie Erklären durch Veranschaulichen und auch das Lehrgespräch. Außerdem werden immer öfter auch moderne Medien (Videoprojektoren, Filme) eingebaut. Weiters wird auch das Unterrichtsgespräch – d.h. Wissensvermittlung durch geschicktes Fragen stellen - dieser Unterrichtsform zugeordnet.

Ein wichtiger Vorteil des Frontalunterrichtes ist die Führung durch den Unterrichtenden. Die Themengebiete werden professionell aufbereitet und verständlich vorgetragen. Der Vortragende kann auf aktuelle Themen eingehen und dient gleichzeitig als Ansprechpartner wenn Fragen aufkommen. Leider können im schlechtesten Fall genau diese positiven Aspekte zu großen Stolpersteinen werden, denn wenn der Experte es nicht schafft sich auf seine Zielgruppe einzustellen und vergisst auf Grundlagen einzugehen, welche bei Anfängern nicht vorausgesetzt werden können, hilft den Anfängern auch der beste Vortrag nichts.

Ein nicht zu vernachlässigender Punkt bei diesem Vortragsstil ist einerseits, dass ein Experte

zu einem Thema notwendig ist, welcher unter Umständen nur gegen eine entsprechende Entlohnung bereit ist, sein Wissen weiter zu geben. Andererseits ist es nötig die Zielgruppe zu einer bestimmten Zeit an einem bestimmten Ort zu versammeln. In der Schule oder bei Weiterbildungen ist das ein selbstverständlicher Bestandteil. Einer kleineren Gruppe von Wissbegierigen, die sich über ein Thema informieren will, kann dieser Organisationsaufwand aber bereits große Probleme bereiten.

DISKUSSIONSRUNDEN

Bei Diskussionsrunden tritt die Lehrperson in den Hintergrund. Alle Beteiligten an der Diskussionsrunde sind gleichberechtigt und zu gleichen Teilen verantwortlich für den Ablauf der Diskussion. Solche Diskussionsrunden sind ein mächtiges Instrument, wenn es darum geht Wissen zu vertiefen oder andere Standpunkte kennen zu lernen – für die Vermittlung von Grundlagen ist eine Diskussionsrunde aber wohl nur geeignet, wenn zumindest ein Anteil der Teilnehmer bereits Erfahrung mit einem Thema hat. Der Vorteil bzw. der Unterschied gegenüber dem Frontalunterricht wäre dabei aber, dass besser auf einzelne Teilnehmer eingegangen werden kann. Fragen können detaillierter beantwortet und Missverständnisse schneller aufgeklärt werden.

Auch für Diskussionsrunden ist ein Mindestmaß an organisatorischer Vorarbeit notwendig. Alle Teilnehmer müssen sich auf einen Termin einigen. Eine Räumlichkeit muss gefunden werden und bei großen Gruppen ist eventuell sogar Tontechnik nötig, damit auch alle Anwesenden hören können was gerade von den anderen Beteiligten gesprochen wird.

LERNEN DURCH LEHREN / SELBSTSTUDIUM / STUDIENZIRKEL

Der Studienzirkel ist keine klassische Unterrichtsform. Am ehesten realisierbar ist ein Studienzirkel mit Erwachsenen oder älteren Jugendlichen. Es handelt sich um eine demokratische Lernform und ist beispielsweise in Schweden sehr beliebt. Es trifft sich dabei eine überschaubare Gruppe für einen gewissen Zeitraum, etwa einige Stunden, um sich zu einem selbstgewählten Thema Wissen zu erarbeiten. Die inhaltlichen Schwerpunkte werden dabei von der Gruppe selbst gewählt, wobei meist eine bestimmte Problemstellung

die Personen zusammenführt. Alle Mitglieder sind gleichberechtigt, alle Teilnehmer sind Experten.

Alternativ dazu besteht die Möglichkeit, dass sich diese Gruppen weiter aufteilen und sich auf einzelne Teile eines Themenbereiches konzentrieren und zu einem späteren Zeitpunkt für die restlichen Teilnehmer aufbereiten. Auch wäre vorstellbar, dass die Ausarbeitung und Aufbereitung eines Themenbereiches durch Einzelpersonen abseits des Studienzirkels stattfindet, wodurch sich der Studienzirkel wiederum in Frontalunterricht mit abwechselnden Lehrpersonen oder eine Diskussionsrunde entwickeln.

Da es sich bei Studienzirkeln per Definition um Klein- und Kleinstgruppen handelt, ist der organisatorische Aufwand vernachlässigbar. Dennoch bleibt zu berücksichtigen, dass die Teilnehmer sich auf jeden Fall selbst um passende Materialien kümmern müssen und insbesondere im Rahmen des Selbststudiums nur auf sich gestellt sind.

Außerdem ist ein grundlegendes Interesse an dem Thema sowie Disziplin vorausgesetzt, um aus einem Studienzirkel bzw. Selbststudium Profit zu ziehen.

ELEARNING / PROGRAMMIERTER UNTERRICHT

Unter den Begriff eLearning fallen alle Formen des Lernens, bei denen digitale Medien für die Präsentation und Distribution von Lernmaterialien, sowie zur Unterstützung zwischenmenschlicher Kommunikation zum Einsatz kommen.

Es gibt verschiedene Formen des eLearning¹, die eine unterschiedliche Einsatzweise mit sich bringen.

Beim Virtual Classroom beispielsweise ersetzt das Internet als Kommunikationsmedium das herkömmliche Klassenzimmer und ermöglicht somit synchrones Lernen für geographisch getrennte Schüler und Lehrer.

Blended Learning vermischt die Vorteile von klassischen Lehrmethoden mit anwesenden Schülern mit den Vorteilen von eLearning. So wird beispielsweise theoretisch Erlerntes

¹ http://de.wikipedia.org/wiki/E-Learning#Formen_des_E-Learning, 23.4.09

mittels Simulationen und Computertests unmittelbar angewandt bzw. überprüft.

Beim Mikrolernen werden viele Lerneinheiten in möglichst kurzen Schritten, häufig über das Internet oder Mobiltelefon, vermittelt.

Zunehmend gewinnen auch 3D-Infrastrukturplattformen wie Second Life^{2 3} an Bedeutung für eLearning-Anwendungen. Durch den Erlebnis-Charakter dieser virtuellen Welten und die starke Identifikation mit dem Avatar, wird ein sehr hoher Immersionsgrad erreicht. Davon verspricht man sich eine höhere Lerneffizienz, da Spielen & Lernen zusammenwächst. Durch simulierte Erlebniswelten kann man nun in Situationen eintauchen und diese erleben.

Die Stärken des eLearnings liegen in der Interaktivität der Kurse. Abstrakte Vorgänge können simuliert und so leichter verständlich gemacht werden. Schüler können synchron und asynchron gemeinsam an einem Thema arbeiten, wodurch Zeit und Ort das Lernen nicht mehr beeinflussen.

Das eLearning wird am stärksten dafür kritisiert, dass die Lernenden erst den Umgang mit den verschiedenen Publikationsformen erlernen müssen. Außerdem beeinflusst die zur Verfügung stehende Technik die Inhalte von eLearningkursen. Außerdem befürchten Kritiker eine soziale Isolation wenn Kommunikation nur noch über das Internet stattfindet.

LEARNING BY DOING

Das Konzept „Learning by Doing“ besagt, dass Lernerfolge nur möglich sind, wenn Dinge ausprobiert und anschließend reflektiert werden. Es handelt sich dabei um eine handlungsorientierte Form⁴ des Lernens. Ziel ist es einerseits durch Experimente Wissen zu vertiefen und andererseits Erkenntnisse aus dem Beobachteten abzuleiten.

Tatsächlich unterstützt dieses Konzept beispielsweise im Chemie- oder Physikunterricht die Lernerfolge der Schüler seit etlichen Jahren. Das eigenständige Erleben und Erforschen von chemischen oder physikalischen Vorgängen ist dabei wesentlich einprägsamer als die

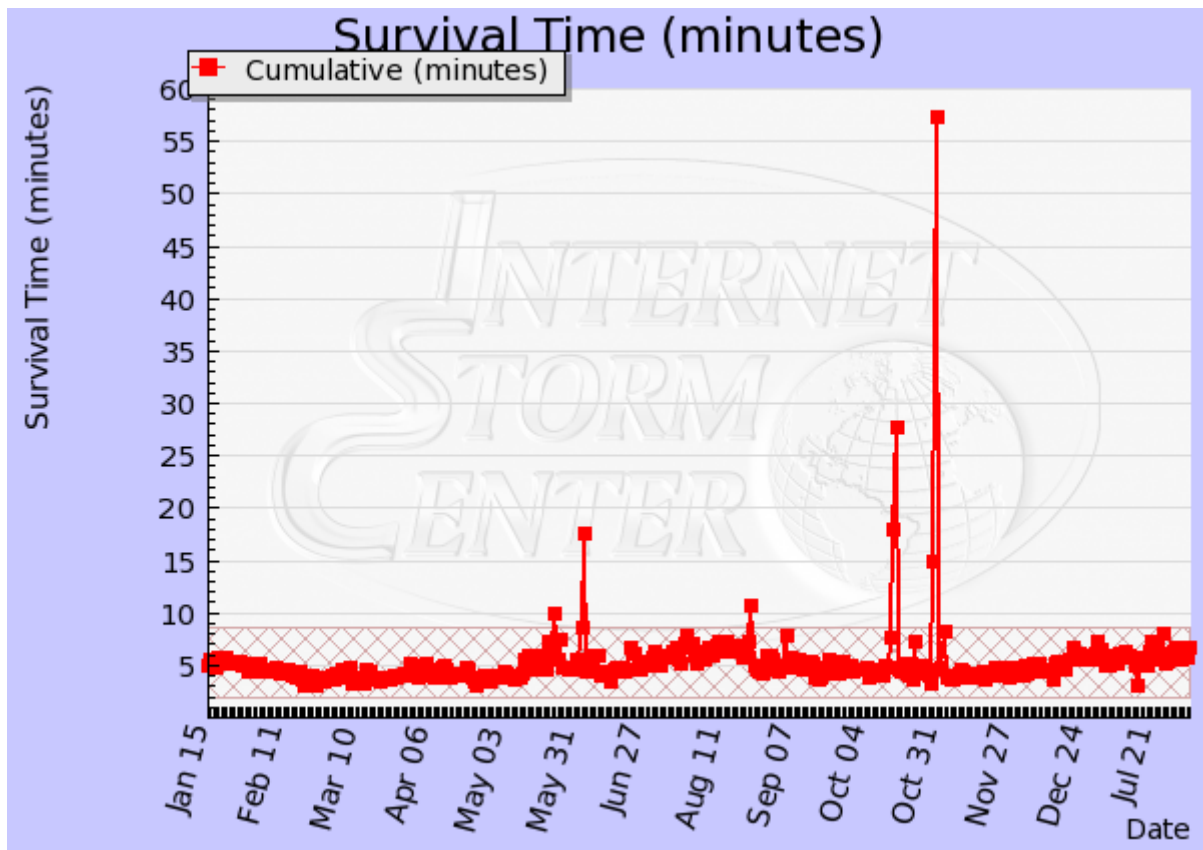
² <http://secondlife.com>

³ <http://www.e-learning3d.de/>

⁴ http://de.wikipedia.org/wiki/Handlungsorientierter_Unterricht , 23.4.09

theoretische Erklärung derselben Vorgänge.

Auch im Bereich IT-Sicherheit würde dieser Ansatz funktionieren, allerdings besteht hierbei die Gefahr, dass man gewisse Lektionen mit einem hohen Preis bezahlen muss. So beträgt etwa die durchschnittliche Zeit⁵ zwischen einer Neuinstallation von Windows XP ohne Sicherheitsupdates bis zur Infektion mit einem Wurm 5 Minuten.



Der Vorteil wäre jedoch, dass der Lernende Schritt für Schritt von Grund auf alles Wichtige erlernen und dabei seine eigene Geschwindigkeit einhalten kann. Es gibt auch keine zeitlichen Grenzen, das Lernen kann zu jeder beliebigen Zeit erfolgen und auch die - zumindest unter Verwendung eines Notebooks - geographische Unabhängigkeit ist ein Vorteil bei dieser Art des Lernens.

⁵ <http://isc.sans.org/survivaltime.HTML>

SIMULATIVER UNTERRICHT / SPIELERISCHES LERNEN

Alle Spiele, darin sind sich Spielpädagogen einig, haben einen Lern- oder Übungseffekt beim Anwender, egal ob es sich um Erwachsene oder Kinder handelt. Daher sind Lernspiele schwer vom allgemeinen Spielbegriff zu unterscheiden, da Spiele in der Regel einen Lernprozess initiieren. Es ist daher naheliegend, Spiele zur Unterstützung oder Einleitung von Lernprozessen einzusetzen. Wissen kann dadurch sowohl neu erworben als auch vervollkommnet und gefestigt werden. Aus historischer Sicht sind die Spiele Fröbels⁶ zur Vermittlung von Rechentechniken und zur Unterstützung des Lesenlernens bemerkenswert.

Mit der steigenden Verbreitung von PCs und Spielkonsolen nahm auch die Bedeutung von Computerspielen zu. Schulbuchverlage begannen gemeinsam mit der Spieleindustrie vermehrt digitale Lernspiele auf den Markt zu bringen. Auch diese digitalen Lernspiele richten sich an Kinder sowie Jugendliche und Erwachsene und versuchen insbesondere über motivationales Design Bildungsprozesse anzuregen. Man findet also häufig Belohnungssysteme (Ranglisten etc.) welche eine Wiederholung des Lernstoffes anregen.

Natürlich werden Lernspiele auch häufig von Pädagogen im Unterricht eingesetzt. Die einfachsten Beispiele dafür wären das Buchstabenspiel Galgenmännchen im Lese- bzw. Fremdsprachenunterricht, Stadt – Land – Fluss als Lernspiel für Sach- bzw. Deutschunterricht, sowie Schiffe versenken im Mathematikunterricht zur Festigung des Koordinatensystems. Lernspiele die etwas mehr Vorbereitung und Einsatzmittel benötigen sind in der Regel kommerzieller Natur. Beispiele dafür wären „Sagrada“ / Parland Spiele / Ulrich Paulus⁷, „Graffiti“ / Huch & friends / Jacques Zeimet⁸ oder „BallCube“ / Herz Spiele / Claudia Herz⁹.

Bei den meisten Lernspielen ist es nötig, dass mindestens 2 Personen am Spiel teilnehmen. Dadurch ergibt sich bei dieser Lernform eine zeitliche und geographische Abhängigkeit, allerdings hält sich der organisatorische Aufwand in Grenzen, da kaum mehr als 6 Personen gleichzeitig an einem Spiel teilnehmen. Als unterstützendes Medium im Schulunterricht fällt

⁶ <http://www.amazon.de/>, ASIN (=eindeutige Produktbezeichnung): B000R9UVHQ

⁷ <http://www.parland.de/spiele.HTML>

⁸ <http://www.huchandfriends.de/page/de/Die-Spiele/Spiele-Detail.php?oid=65>

⁹ <http://www.herz-spiele.de/25.HTML>

der organisatorische Mehraufwand gänzlich aus, da ja die Spieler schon in der Klasse versammelt sind.

Zum besseren Überblick fassen wir, insbesondere unter Berücksichtigung des IT-Bereichs, die in unseren Augen essentiellen Kriterien dieser Lerntechniken nochmals tabellarisch zusammen.

	Zielgruppe	zeitlich abhängig von anderen	geogr. abhängig von anderen	Voraussetzungen	Kosten
Frontalunterricht	Interessierte, Alter: 10-	Ja	Ja	Je nach Art des Vortrags evtl. Vorkenntnisse	Evtl. Kosten für Vortragenden und Räumlichkeiten, Schulgeld, Mitgliedsbeiträge
Diskussionsrunden	Interessierte Alter: 10-	ja	ja	Diskussionsbereitschaft, evtl. Vorkenntnisse, Interesse	Evtl. Kosten für Diskussionsleiter und Räumlichkeiten
Lernen durch Lehren / Selbststudium / Studienzirkel	Interessierte Alter: 10-	Selbststudium: nein, sonst ja	Selbststudium: nein, sonst ja	Interesse, Motivation, Disziplin	Kosten für Lernmaterialien (Bücher)
eLearning / programmierter Unterricht	Interessierte Alter: 10-	nein	nein	Disziplin, Interesse	Kosten für eLearning Module, Kosten für Hardware um Module auszuführen
Learning by Doing	Interessierte Alter: 10-	nein	nein	Interesse	Lernmaterialien (Hardware, evtl. Bücher)
Simulativer Unterricht / Spielerisches Lernen	Interessierte Alter: 10-	ja	ja	Interesse,	evtl. Kosten für Spiel

Aufgrund der Vorteile des spielerischen Lernens erachten wir diese Form der Wissensvermittlung als geeignet um einer breiten Bevölkerungsschicht einschlägiges Wissen zu vermitteln. Daher wollen wir nun ein Spiel konstruieren, welches sicherheitsrelevante Themen der Zielgruppe ohne Druck näher bringen kann.

WER IST DIE ZIELGRUPPE?

Zuerst wollen wir die Zielgruppe abstecken und eruieren welche Sicherheitsbereiche besonders berücksichtigt werden sollen. Ob für Kinder und Jugendliche, welche ihre ersten Schritte im Internet machen oder ältere Leute, die mit Computern allgemein noch nicht viele oder keine Erfahrungen gemacht haben oder aber für bereits fortgeschrittene Internetbenutzer, alles wäre machbar. Die von uns anvisierte Zielgruppe für die Steigerung des Bewusstseins für IT-Sicherheit sind die durchschnittlichen Computerbenutzer. Das können Jugendliche, die das Internet zur Kommunikation mit Freunden sowie für Onlinespiele nutzen oder Büroangestellte, welche Dokumente via Email versenden, oder einfach Neueinsteiger in die IT-Welt sein. Der gemeinsame Nenner ist aber auf jeden Fall ein fehlendes oder minimal ausgeprägtes Interesse für Themen wie Datenschutz, Datensicherheit oder Privatsphäre.

Die Thematik des Spiels kann sich natürlich auf weit mehr als nur auf Computer und das Internet beziehen. Es kann auch auf beliebige andere, jedoch sicherheitsrelevante, Bereiche ausgedehnt werden, aber besonders in dem Bereich Computer/Internet besteht sehr viel Aufklärungsbedarf. Hierbei soll auch einfließen, was die Ursache vieler Sicherheitsprobleme ist.

WAS SOLL VERMITTELT WERDEN?

Nun stellt sich die Frage, welche Bereiche des Sicherheitsbewusstseins mit einem spielerischen Ansatz angesprochen werden sollen? Da das Spiel keine klassische Zielgruppe, wie Kinder von 6 – 14 oder ähnliche, und damit eigentlich Jedermann – also insbesondere

auch Personen ohne IT oder Security-Vorbildung – ansprechen soll, ist es unser Ziel einen breiten Überblick über das Thema Sicherheit zu vermitteln und damit einen Grundstock an Sicherheitsbewusstsein zu schaffen, auf den später, wenn man es so will, aufgebaut werden kann.

Was nützt beispielsweise das Wissen, welche Firewalldistribution den bestmöglichen Schutz bietet, wenn man einfachere Dinge wie „Ist mein Passwort sicher?“, „Darf ich meine TAN-Codes auf dieser Homepage eingeben?“, „Ist das Mail in dem ich aufgefordert werde meine Paypal-Daten bekannt zu geben authentisch?“ nicht beachtet?

Dementsprechend ist das Ziel, einem Durchschnittsbenutzer genügend grundlegende Information zu vermitteln, um sich selbst vor Gefahren im Internet schützen zu können. Es sollen daher keine detaillierten Methoden für konkrete Gefahren vermittelt werden – die Information, dass ein bestimmter Virus mit einem bestimmten Programm auf eine einzige Art entfernt werden kann ist zwar nützlich, trägt aber sicher nicht zur Steigerung des Sicherheitsbewusstseins bei. Eine Art von Metawissen – ein aktualisierter Virens Scanner, hilft Viren zu erkennen und zu bekämpfen – ist hingegen wesentlich hilfreicher. Der Vorteil dabei ist, dass der Benutzer zum Denken angeregt wird und versteht, dass bestimmte Maßnahmen einer bestimmten Art von Bedrohung entgegenwirken können und die Möglichkeit bekommt, zur jeweiligen Zeit das geeignete Werkzeug auszuwählen.

MAßNAHMENKATALOG DES BSI

EINFÜHRUNG

Zu allererst werden wir uns mit den potentiellen Gefahren im IT-Bereich befassen und den Maßnahmen, die gesetzt werden können um diese Gefahren zu beseitigen oder zumindest zu minimieren.

Wir wollen in weiterer Folge herausfinden auf welche Gefahren IT-Anfänger und IT-Durchschnittsbenutzer besonders häufig stoßen werden und mit welchen geeigneten Maßnahmen man diesen begegnen kann.

Außerdem wollen wir evaluieren, wie schwer oder einfach man den Benutzern das Wissen um diese Gefahren/Maßnahmen vermitteln kann und mit welchem finanziellen und zeitlichen Aufwand das Setzen dieser Maßnahmen verbunden wäre.

Unter einem Durchschnittsbenutzer verstehen wir in dieser Arbeit eine Person, welche gerade angefangen hat mit Computern zu arbeiten oder aber jemanden der einen Computern auf Anwendungsseite bedienen kann, aber keinen Einblick in die darunterliegenden Abläufe des Systems hat.

Desweiteren gehen wir bei unserer Definition des Durchschnittsbenutzers davon aus, dass er in einer Organisation oder Firma keine höhere leitende Funktion hat.

Als Ausgangsbasis für unsere Evaluierung haben wir den Maßnahmenkatalog aus den IT Grundschutz-Katalogen¹⁰ des BSI¹¹ (Bundesamt für Sicherheit in der Informationstechnik (Bundesrepublik Deutschland)) herangezogen.

In den IT-Grundschutzkatalogen des BSI, bis 2005 unter dem Namen "IT-Grundschutzhandbuch" zu finden, wird schon seit vielen Jahren versucht zu vermitteln, wie man die Sicherheit in der IT in allen Aspekten verbessern und ein gewisser Sicherheitsstandard gewährleistet werden kann. Die IT-Grundschutzkataloge sind extrem umfangreich, die von uns als Basis verwendete Version umfasst in der pdf-Version 3914 Seiten (IT-Grundschutz-Kataloge 10.Ergänzungslieferung – Oktober 2008) und ist in die drei großen Kapitel „Bausteine“, „Gefahren“ und „Maßnahmen“ aufgegliedert.

Während das Kapitel "Bausteine" auf grundlegende Konzepte des IT-Grundschutz eingeht und die Gefahren mit Stichworten umschreibt, wird im Kapitel "Gefahren" detailliert auf die einzelnen Gefahrenquellen eingegangen.

¹⁰

https://www.bsi.bund.de/cln_136/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/inhalt_node.HT ML

¹¹ <https://www.bsi.bund.de>

Für uns interessant war jedoch das Kapitel "Maßnahmen"¹², in welchem konkrete Maßnahmen für bestimmte Gefahren beschrieben werden, denn im Endeffekt ist es ja genau unser Ziel viele dieser Maßnahmen an IT-Benutzer zu vermitteln. Deshalb haben wir den Maßnahmenkatalog herangezogen und sind ihn Punkt für Punkt durchgegangen um jede dieser Maßnahmen auf folgende Aspekte zu überprüfen:

Welche Relevanz hat die Maßnahme für den IT-Anfänger bzw. den IT-Durchschnittsbenutzer? Wird der Durchschnittsbenutzer in der Realität jemals mit der Gefahr konfrontiert werden?

Sollte die Maßnahme für den Durchschnittsbenutzer nicht weiter relevant sein wird auf diese nicht näher eingegangen. Diese Maßnahmen findet man dann im Appendix dieser Arbeit.

Desweiteren sollen folgende Fragen beantwortet werden:

Welche Szenarien können sich ergeben wenn man die Maßnahme nicht setzt? Wie hoch ist der Schaden, der im Extremfall entstehen kann und wie wahrscheinlich ist es, dass so ein Schadensfall eintritt? Die Erklärung soll anhand von fiktiven, aber greifbaren Beispielen geschehen. Wie schwer ist es die Maßnahme umzusetzen, wie leicht kann sie einem Durchschnittsbenutzer vermittelt werden und ist sie mit hohen Kosten oder hohem Zeitaufwand verbunden?

Nach der Evaluierung des Maßnahmenkataloges werden dann die Maßnahmen herausgesucht, bei denen es besonders wichtig wäre sie an einen Durchschnittsbenutzer zu vermitteln.

Wir haben die Nummerierung der Maßnahmen aus dem IT-Grundschutzkatalog des BSI bei dieser Evaluierung beibehalten. Maßnahmen, welche wir als nicht wichtig für den Durchschnittsbenutzer eingestuft haben, sind mit einer kurzen Begründung, warum wir sie für nicht relevant für den Durchschnittsbenutzer halten im Appendix dieser Arbeit zu finden.

Die Evaluierung der Maßnahmen geschieht dabei nach folgendem Schema:

Relevanz für den Durchschnittsbenutzer: <keine/gering/mittel/hoch

¹²

https://www.bsi.bund.de/cln_136/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/massnahmenkataloge_node.HTML

Hier soll eine kurze Einschätzung getroffen werden, inwieweit diese Maßnahme wichtig und relevant für einen Durchschnittsbenutzer ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Anhand eines einfachen und greifbaren Beispiels soll verdeutlicht werden, was passieren kann wenn man auf diese Maßnahme verzichtet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Hier soll die Frage beantwortet werden, ob es schwer ist einem Durchschnittsbenutzer die Maßnahme zu vermitteln bzw. ob sie schwer umzusetzen ist. Sollte sie das sein, wird kurz erklärt wo die Probleme liegen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Hier wird die Frage beantwortet ob, die Implementierung bzw. das Durchführen dieser Maßnahme eventuell mit hohen Kosten oder hohem Zeitaufwand verbunden ist und wenn ja, wo und wie genau.

M 1 MAßNAHMENKATALOG INFRASTRUKTUR

Der Maßnahmenkatalog 1 behandelt alle Themen die Infrastruktur und IT-Sicherheit betreffen.

Darunter fallen z.B. der physische Schutz vor wetterbedingten Phänomenen, der Schutz vor Einbrechern, die geeignete Wahl eines Ortes um elektronische Geräten aufzustellen und diverse Verhaltensregeln, die man in Bezug auf Gebäude und Infrastruktur in Bezug auf die IT beachten sollte.

M 1.4 BLITZSCHUTZEINRICHTUNGEN

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft in erster Linie die Haustechnik. Trotzdem sollte ein Durchschnittsbenutzer wissen, ob das Gebäude in dem er sich befindet durch eine Blitzschutzeinrichtung gesichert ist bzw. ob zumindest der lokale Stromkreis an dem der Computer hängt, durch einen ausreichenden Überspannungsschutz geschützt ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Katrin hat morgen eine Deadline für ein wichtiges Projekt und muss zu diesem Zweck viel am Computer tippen. Während sie arbeitet zieht ein Gewitter auf. Sie weiß, dass das alte Gebäude über keine ausreichende Blitzschutzeinrichtung verfügt. Trotzdem arbeitet sie weiter und reagiert darauf nicht und denkt sich: „Wird schon nichts passieren.“. Plötzlich schlägt ein Blitz in die nahegelegene Stromleitung ein und gelangt in Folge auch zu Katrins Computer. Das Resultat: Der Computer und einige elektrische Geräte die am Stromkreis gehangen sind, sind jetzt kaputt und Katrin hat alle Projektdaten verloren. Danach ist Katrin verzweifelt und denkt sich: „Hätte ich doch nur den Stromstecker abgezogen als das Gewitter aufgezogen ist oder mir zumindest einen Überspannungsschutz besorgt!“

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, die Maßnahme ist weder schwer zu vermitteln noch schwer zu erlernen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Eine Blitzschutzeinrichtung für ein Gebäude ist sicher mit höheren Kosten verbunden aber z.B. ein einfacher Überspannungsschutz für eine Steckdose kostet nur wenige Euro und kann innerhalb von kürzester Zeit montiert bzw. angesteckt werden.

M 1.6 EINHALTUNG VON BRANDSCHUTZVORSCHRIFTEN

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft in erster Linie die Haustechnik und/oder den Brandschutzbeauftragten. Aber auch ein Durchschnittsbenutzer sollte sich zu diesem Thema etwas informieren, ansonsten könnte das unangenehme Folgen haben.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Jens ist Angestellter in einer IT-Firma. Als er wieder einmal seiner Arbeit nachgeht wird der Feueralarm ausgelöst. Jens glaubt es ist ein Probealarm und bleibt fürs erste sitzen bis er dann doch Rauch riecht. Jetzt ist auch ihm klar, dass es sich um keinen Probealarm handelt. Schnell versucht er nach draußen zu gelangen, aber oh weh, er hat sich nicht über die Fluchtwege informiert und den Aufzug den er üblicherweise nimmt, soll er in so einer Situation ja nicht benutzen, wie er selbst weiß. Jens versucht einen Ausweg zu finden aber weiß nicht wo er jetzt hin soll, er ist ja neu in dieser Firma. Zum Glück kommt eine Arbeitskollegin vorbei welche die Fluchtwege kennt. Sie kommen rechtzeitig aus dem Gebäude aber das hätte böse ins Auge gehen können.

Beispiel 2: Otto ist nicht der ordentlichste Mensch. Seine Dokumente und Notizzettel häuft er am liebsten irgendwo auf, statt sie irgendwo einzuordnen. Das wäre an sich nicht so schlimm, wäre sein Lieblingsablageort nicht sein PC. Dokumente sind unter, über und neben diesem zu finden und gerade einmal der Schalter zum Ein- und Ausschalten des Computers ist noch zu sehen. Eines Tages verfängt sich eines dieser Dokumente im Lüfter des Netzteils des Computers und da der Computer durch die vielen Dokumente auf ihm kaum Wärme abgeben kann ist dieser schon sehr heiß. Schlussendlich bilden sich einige Funken im Netzteil und das darin verklemmte Papier wird in Brand gesetzt. Otto war während dies passiert ist auf der Toilette und als er zurückkommt brennt der gesamte Dokumentenstapel. Otto kann das Feuer noch löschen, aber die Dokumente sind verbrannt und auch sein Computer ist jetzt kaputt. Er hätte sich wohl doch überlegen sollen, dass man nicht so leichtfertig elektronische Geräte als Ablagestapel verwenden soll, immerhin spricht so ein Verhalten auch mit Sicherheit gegen die Brandschutzvorschriften.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, diese Maßnahme ist leicht zu vermitteln und auch die Umsetzung ist einfach. Der normale Hausverstand reicht in der Regel aus um Schlimmeres zu verhindern.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Nein, ein wenig nachdenken und sich über das Thema informieren reicht meistens aus.

M 1.7 HANDFEUERLÖSCHER

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft in erster Linie die Haustechnik und oder den Brandschutzbeauftragten. Aber auch den Durchschnittsbenutzer kann dieser Punkt betreffen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Birgit arbeitet in einer kleinen Firma als Sekretärin. Sie bemerkt plötzlich, dass jemand unerlaubterweise geraucht hat und offenbar den glühenden Zigarettenstummel in einen Mistkübel voller Papier geworfen hat. Dieser brennt jetzt natürlich. Birgit hat nur leider keine Ahnung wo der Handfeuerlöscher ist und beginnt verzweifelt danach zu suchen. Mittlerweile hat das Feuer leider auch schon auf weitere Teile des Büros übergegriffen. Die Feuerwehr muss schlussendlich das Feuer löschen und es ist ein großer Sachschaden entstanden. Hätte Birgit gewusst wo der Handfeuerlöscher ist und hätte sie ihn schnell zur Hand gehabt, hätte sie das Feuer schnell selbst löschen können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, es ist einfach jemandem zu zeigen wo ein Handfeuerlöscher ist. Der Durchschnittsbenutzer sollte aber auch darauf hingewiesen werden, dass nicht jeder Handfeuerlöscher für jede Art von Brand geeignet ist.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme ist gering und die Kosten für einen Handfeuerlöscher trägt der Durchschnittsbenutzer eher selten.

M 1.10 VERWENDUNG VON SICHERHEITSTÜREN UND -FENSTERN

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft in erster Linie die Haustechnik. Aber auch ein Durchschnittsbenutzer sollte sich Gedanken machen wann es sinnvoll ist etwas in einem Raum mit Sicherheitstüren und -fenstern zu lagern.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Karl arbeitet in einer Marketing-Abteilung und hat einige sensible Daten zur neuen Marketing-Kampagne auf einer externen Festplatte gespeichert, an welche die Konkurrenz schon die ganze Zeit gelangen will. Da das Wetter schön ist hat Karl beschlossen daheim in seinem kleinen gemütlichen hölzernen Gartenhäuschen zu arbeiten und lässt sein Notebook und die Festplatte nach vollbrachter Arbeit dort drin liegen. Natürlich hat er sich vorher

versichert, dass beim Gartenhäuschen alle Fenster verschlossen sind und die Türe abgesperrt ist.

Als er am nächsten Tag zurückkommt sind jedoch sowohl das Notebook als auch die externe Festplatte weg. Eines der dünnen Holzfenster ist offenbar ohne Mühe aufgebrochen worden und dadurch konnte jemand in das Häuschen gelangen. Die sensiblen Daten sind in jedem Fall weg und Karl muss sich den Vorwurf machen: "Wieso war ich nur so dumm und habe das Notebook und die Festplatte im gut einsehbaren Gartenhäuschen gelagert, statt sie ins Haupthaus zu tragen wo ich Sicherheitstüren und Fenster gehabt hätte?"

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, die Maßnahme ist einfach an den Durchschnittsbenutzer zu vermitteln, sofern schon Räume mit Sicherheitstüren und -fenstern vorhanden sind.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Dem Durchschnittsbenutzer verlangt diese Maßnahme in der Regel kaum Zeit ab und meistens auch keine Kosten, außer der Benutzer lässt sich extra Sicherheitstüren und -fenster einbauen und nutzt nicht bereits existierende. Dann wird die Sache in der Regel schnell teuer.

M 1.12 VERMEIDUNG VON LAGEHINWEISEN AUF SCHÜTZENSWERTE GEBÄUDETEILE

Relevanz für den Durchschnittsbenutzer: gering/mittel

Ein Durchschnittsbenutzer sollte wissen, dass man die Lage von potentiell schützenswerten Gebäudeteilen nicht einfach an Außenstehende weitergibt. Die folgenden Beispiele sollen zeigen wieso.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiele: Bert ist Praktikant in einer Firma und etwas übermotiviert. Er soll eigentlich nur die Beschilderung der Büros neu machen aber er beschließt mehr zu machen und stellt auch gleich Wegweiser zu allen möglichen Orten auf unter anderem zum Serverraum und zum Archiv.

Helmut ist von einer Konkurrenzfirma zu Besuch und würde nur allzu gerne etwas über diese Firma herausfinden. Leider will ihm aber niemand in der Firma Auskunft über das geben was er eigentlich wissen will. Aber da sind ja zum Glück diese Wegweiser und als er unbeobachtet ist begibt sich Helmut ins Archiv und findet dort auch tatsächlich die Informationen die er gesucht hat.

Diese Informationen wird er aber sicher nicht zum Wohle der Firma nutzen.

Und alles nur weil man den übermotivierten Praktikanten nicht zurückgehalten hat, Helmut hätte den Weg zum Archiv sonst nicht so leicht gefunden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer an den Durchschnittsbenutzer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist maximal mit etwas Zeitaufwand verbunden nicht aber mit Kosten.

M 1.15 GESCHLOSSENE FENSTER UND TÜREN**Relevanz für den Durchschnittsbenutzer: hoch**

Das Türen und Fenster in gewissen Situationen geschlossen sein müssen ist auch für einen Durchschnittsbenutzer wichtig zu wissen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Heinz hat sich neuerdings Sicherheitstüren und Fenster in seine Wohnung einbauen lassen, nachdem in seine Wohnung schon einmal eingebrochen worden ist, da seine Wohnungstür und das Türschloss alt und wenig stabil gewesen waren. In der Wohnung bewahrt Heinz wichtige Daten seiner Firma auf einem Memory-Stick auf. Eines Tages wird er von seiner Liebsten angerufen und sie wollen zusammen Mittagessen gehen. Voller Freude verlässt er eiligst das Haus, wirft die Türe zu und verlässt das Haus. Leider hat die Wohnungstüre aber nicht richtig geschlossen. Mr. X, ein Spion der Konkurrenzfirma hat dies zufällig mitbekommen und kann jetzt trotz der stabilen Sicherheitstür mit dem hervorragendem Türschloss problemlos in die Wohnung und ungestört und unbeobachtet den Memory-Stick mitnehmen. Heinz wird nicht erfreut sein wenn er zurück kommt und seine Firma genauso wenig.

Beispiel 2: Bettina arbeitet in ihrem Büro im 5. Stock. Es ist heiß und die Klimaanlage ist ausgefallen. Also hat Bettina das Fenster aufgemacht. Als sie am Abend das Büro verlässt lässt sie die Fenster offen, damit es morgen in der Früh nicht stickig in diesem ist. Einbrechen wird im 5. Stock bei einem schwer zugänglichen Fenster ja eh niemand.

Womit Bettina aber nicht gerechnet hat: Ein starker Sturm zieht in der Nacht auf und da das Fenster offen war richtet dieser Sturm massiven Schaden im Büro an und das Fenster ist zudem auch noch kaputt. Hätte sie doch nur das Fenster beim Weggehen zu gemacht.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme kann ganz leicht an einen Durchschnittsbenutzer vermittelt werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist nicht mit Kosten sondern maximal mit etwas Zeitaufwand verbunden.

M 1.18 GEFAHREMELDEANLAGE

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft in erster Linie die Haustechnik, den Brandschutzbeauftragten und z.B. das IT-Sicherheitsmanagement. Aber auch der Durchschnittsbenutzer sollte von vorhandenen Gefahrenmeldeanlagen wissen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Stefan ist Mitarbeiter in einem IT-Helpdesk und ein leidenschaftlicher Raucher. Üblicherweise raucht er im Hof aber da es heute ein besonders stressiger Tag ist, raucht er heute ausnahmsweise am Gang.

Leider weiß er nicht, dass hier überall Rauchmelder installiert sind. Der Alarm wird ausgelöst und das Gebäude wie in solchen Fällen vorgesehen evakuiert. Bis klar ist, dass es doch nicht brennt wurde schon die Feuerwehr informiert und die Mitarbeitern aus dem Gebäude geschafft. Das wird wohl ein böses Nachspiel für Stefan haben.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahmen sollten in der Regel in einer Schulung leicht einem Durchschnittsbenutzer zu vermitteln sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Wenn der Benutzer solche Maßnahmen selbst einbauen lässt fallen nicht unerheblichen Kosten an und es wird auch ausreichend Zeit für die Installation der Maßnahmen benötigt.

Wenn der Benutzer nur über diese informiert werden muss ist das nur mit etwas Zeitaufwand verbunden.

M 1.19 EINBRUCHSSCHUTZ

Relevanz für den Durchschnittsbenutzer: mittel

Einbruchschutz ist auch für einen Durchschnittsbenutzer ein wichtiger Punkt.

In einer Firma werden damit in der Regel die Haustechnik und eigene Sicherheitsbeauftragte beauftragt. Aber auch eine Privat-Wohnung sollte gegen Einbrüche zumindest mit vertretbarem Aufwand geschützt sein, sei es durch den Einbau einer Alarmanlage, von Sicherheitstüren und Fenster, sicheren Türschlössern, etc.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Peter ist in eine Altbauwohnung eingezogen. Er stellt fest, dass sowohl das Türschloss als auch die Tür alt und wenig stabil sind. Aber Peter will kein Geld für ein neues Türschloss oder sogar eine neue Tür ausgeben und verlässt sich darauf, dass hier eh nichts passieren wird.

Eine Woche später hat jemand in seiner Abwesenheit offenbar ohne Probleme die Tür aufgebrochen und alle Wertgegenstände und sämtliche Datenträger aus der Wohnung gestohlen. Ein Einbrecher hätte so eine Tat bei einer besseren Tür bzw. einem besseren Schloss vielleicht nicht gewagt, da es zu viel Zeit und Aufwand erfordert hätte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht sehr schwer diese Maßnahmen an Durchschnittsbenutzer zu vermitteln aber um die Maßnahmen umzusetzen werden oft Spezialisten benötigt.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahmen können unter Umständen mit hohen Kosten verbunden sein und auch der Zeitaufwand um diese umzusetzen kann, je nach Art des Einbruchschutzes, grösser sein.

M 1.22 MATERIELLE SICHERUNG VON LEITUNGEN UND VERTEILERN

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft zwar in erster Linie die Haustechnik eines Gebäudes. Aber auch für einen Durchschnittsbenutzer kann dies durchaus einmal ein Thema sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Dagmar hat unlängst einen Internetanschluss bekommen und auch gleich auch ein langes Kabel zu ihrem Bett gelegt, damit sie auch vom Bett aus in Ruhe im Internet surfen kann. Leider hat sie auch einen sehr verspielten und neugierigen Kater. Als sie eines Tages nicht zu Hause ist, spielt sich der Kater intensiv mit dem Kabel und reißt an diesem an als plötzlich Modem und Router, die an das Kabel angeschlossen sind, vom Tisch auf dem sie stehen heruntergezogen werden und dann auf den harten Steinboden fallen. Beide Geräte

sind kaputt, das war es vorerst mit dem Surfen im Internet. Hätte man das Kabel etwas geschickter verlegt wäre das nicht passiert.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einem Durchschnittsbenutzer leicht zu vermitteln und in einfacher Form auch nicht allzu schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Manche Maßnahmen sind sicher mit hohem Zeitaufwand und Kosten verbunden aber z.B. einfach ein Kabel schön an einer Wand zu verlegen, sodass man z.B. nicht darüber stolpert, ist etwas das auch für einen Durchschnittsbenutzer Sinn macht und mit geringen Kosten und moderatem Zeitaufwand machbar ist.

M 1.23 ABGESCHLOSSENE TÜREN

siehe Punkt M 1.15.

M 1.24 VERMEIDUNG VON WASSERFÜHRENDEN LEITUNGEN

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft zwar in erster Linie die Haustechnik eines Gebäudes und die IT-Verantwortlichen, aber auch für einen Durchschnittsbenutzer kann das Thema Wasser und IT-Geräte betreffen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Dietmar hat ein Notebook und arbeitet damit gerne überall, auch in der Küche neben der Abwasch.

Einmal vergisst er das Notebook wieder aus der Küche mitzunehmen und beim nächsten mal Geschirr abwaschen spritzt viel Wasser auf das dort stehende Notebook. Dietmar bekommt das nicht mit und schaltet sein Notebook nebenbei ein und ein seltsames Geräusch beim Starten und die Tatsache, dass das Notebook danach nicht mehr starten will ist das Resultat. Deshalb hätte er sein Notebook nicht in die Nähe von Wasser bzw. wasserführenden Leitungen betreiben sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einem Durchschnittsbenutzer leicht zu vermitteln und auch einfach umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Für einen Durchschnittsbenutzer ist diese Maßnahme in der Regel nicht mit Kosten oder Zeitaufwand verbunden. Ein wenig Nachdenken genügt.

M 1.25 ÜBERSPANNUNGSSCHUTZ

siehe Punkt M 1.4.

M 1.26 NOT-AUS-SCHALTER

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft zwar in erster Linie die Haustechnik eines Gebäudes und die IT-Verantwortlichen, aber auch für einen Durchschnittsbenutzer kann dies relevant sein. Zumindest sollte der Benutzer wissen, wo sich im Notfall ein Not-Aus-Schalter befindet falls einer existiert.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: In einem Raum mit elektrischen Geräten gibt es einen gut verdeckten Not-Aus-Schalter um den Strom abzuschalten. Die Sicherungen zu dem Stromkreis des Raumes sind nur im Keller zugänglich. Eines der Geräte fängt aus irgendeinem Grund an zu brennen. Löschen ist nicht so leicht, da die Gefahr von elektrischen Spannungen nach wie vor besteht. Da keiner weiß das es einen Not-Aus-Schalter gibt, muss mühsam nach dem Sicherungskasten gesucht werden um die Stromzufuhr zu unterbrechen. Dabei geht Zeit verloren und das Feuer kann so erst später gelöscht werden als wenn der Not-Aus-Schalter betätigt worden wäre. Der angerichtet Schaden ist dadurch deutlich größer.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme einem Durchschnittsbenutzer zu zeigen wo ein Not-Aus-Schalter ist und wann dieser einzusetzen ist, ist an sich einfach zu vermitteln und auch umzusetzen. In einem Privathaushalt wäre es z.B. auch eine gute Sache wenn der Benutzer zumindest wüsste, wo der Sicherungskasten ist und wie er dort schnell den Stromkreis abstellen kann wenn schon kein Not-Aus-Schalter vorhanden ist.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Für einen Durchschnittsbenutzer ist diese Maßnahme in der Regel nicht mit Kosten oder größerem Zeitaufwand verbunden. Kosten fallen nur an wenn so ein Not-Aus-Schalter extra installiert werden muß.

M 1.27 KLIMATISIERUNG

Relevanz für den Durchschnittsbenutzer: gering

Dieser Punkt betrifft zwar in erster Linie die Haustechnik eines Gebäudes und die IT-Verantwortlichen, aber auch für einen Durchschnittsbenutzer kann dies relevant sein, schließlich werden IT-Geräte auch in einer Privatwohnung vom Raumklima beeinflusst.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Heinrich sitzt ihm Sommer daheim vor dem Computer weil er noch etwas für die Arbeit erledigen muss. Es ist sehr heiß und Heinrich ärgert sich heute schon zum dritten Mal, dass sein Computer abgestürzt ist und danach dann einige Zeit lang nicht mehr hochfahren will.

Offenbar wird der Computer zu heiß. Liegt wohl auch daran, dass der Computer in einem mit Schaumstoff ausgepolstertem Fach unter seinem Schreibtisch steht.

Mit einer entsprechenden Klimatisierung für den Computer würde so etwas nicht passieren.

Wahrscheinlich würde es schon viel helfen, wenn Heinrich den Computer aus dem Fach herausziehen und irgendwo hinstellen würde, wo die Wärmedämmung nicht so intensiv ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Manchen Benutzern muss erst beigebracht werden, dass z.B. Hitze oder andere klimatische Bedingungen einem IT-Gerät sehr schaden oder zumindest dessen Betrieb stark beeinträchtigen können. Die Maßnahmen zu vermitteln sollte aber nicht sehr schwer sein.

In manchen Fällen können die Maßnahmen dagegen aber schwerer umzusetzen sein (z.B. bei einer Wohnung mit schlechter Isolierung).

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann, muss aber nicht, durch höhere Kosten (z.B. durch eine Klimaanlage) oder größerem Zeitaufwand (Einbau einer Klimaanlage, neue Wärmedämmung der Wohnung, etc.) verbunden sein.

M 1.28 LOKALE UNTERBRECHUNGSFREIE STROMVERSORGUNG

Relevanz für den Durchschnittsbenutzer: gering

Diese Maßnahme ist sicher kein Muss für einen Durchschnittsbenutzer, kann aber in manchen Situationen hilfreich sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Dianna arbeitet schon den ganzen Nachmittag an ihrer Diplomarbeit und schreibt intensiv daran. Sie will speichern als plötzlich der Strom in ihrer Wohnung weg ist, offenbar ein Stromausfall.

Der Strom ist bald wieder da aber wie Susanne bemerken muss ist ihre Arbeit vom Nachmittag offenbar nicht rechtzeitig gespeichert worden. Mit einer lokalen unterbrechungsfreien Stromversorgung (USV) hätte sie zumindest noch genug Zeit gehabt ihre Arbeit rechtzeitig zu speichern oder aber überhaupt in der Zeit des Stromausfalls, sofern dieser nicht zu lange dauern würde, normal weiter zu machen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch besonders schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in jedem Fall mit Kosten verbunden da so eine unterbrechungsfreie Stromversorgung nicht billig ist. Zudem benötigt sie auch Platz. Ob sich die Anschaffung für einen Durchschnittsbenutzer rentiert, hängt vom Einzelfall ab. Der Zeitaufwand um die Maßnahme umzusetzen ist hingegen eher gering (kaufen, anstecken und einschalten).

M 1.29 GEEIGNETE AUFSTELLUNG EINES IT-SYSTEMS**Relevanz für den Durchschnittsbenutzer: hoch**

Dieser Punkt ist auch für Durchschnittsbenutzer sehr wichtig, denn viele Punkte betreffen diesen direkt. Hervorzuheben wären etwa die Punkte Schutz vor Schmutz, Ergonomie (siehe auch M 3.9 Ergonomischer Arbeitsplatz) oder Schutz vor Manipulation.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Othmar ist leidenschaftlicher Bastler und hat viele Bastelanleitungen auf seinem Computer gespeichert. Den Computer hat er, damit er die Anleitungen immer schnell ansehen kann, direkt in die Werkstatt gestellt. In letzter Zeit arbeitet er viel mit Holz und Sägespäne fliegen bei seinen Arbeiten oft herum. Plötzlich geht der Computer nicht mehr. Als Othmar das Computergehäuse öffnet, liegen darin eine Unmenge an Schmutz von seinen Basteleien. Das dürfte der Computer nicht verkraftet haben.

Beispiel 2: Ludwig arbeitet gerne am Fenster, da er beim Arbeiten am Computer gerne auch etwas Sonne haben will. Er hat auch noch einen sehr großen und guten Monitor gekauft damit er seine Augen schont. Leider hat dies einen Nachteil. Der neugierige Olaf von Gegenüber kann ihn so die ganze Zeit beobachten bei dem was er macht und weiß in kurzer Zeit viel über Ludwig was dieser eigentlich nicht preisgeben wollte. Unter anderem auch Passwörter und Zugangsdaten zu diversen Seiten weil Olaf bei seinen Beobachtungen die Tastatur von Ludwig sehr gut sehen konnte und Ludwig nicht besonders schnell tippen kann. Das hätte Ludwig berücksichtigen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer zu vermitteln und auch die Umsetzung sollte, außer bei massivem Platzmangel, in der Regel kein Problem darstellen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel kaum mit Kosten und nur mit dem Zeitaufwand verbunden um die

IT-Geräte an einem geeigneten Ort aufzustellen.

M 1.32 GEEIGNETE AUFSTELLUNG VON DRUCKERN UND KOPIERERN

Relevanz für den Durchschnittsbenutzer: mittel

Die geeignete Aufstellung von Druckern und Kopierern betrifft in erster Linie die IT-Abteilung einer Firma aber auch ein Durchschnittsbenutzer sollte wissen wo die Drucker stehen auf denen er Dokumente ausdruckt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Henry druckt in seiner Firma ein paar sensible Dokumente mit Firmendaten aus die eigentlich niemand der normalen Belegschaft sehen sollte.

Leider hat Henry nicht bedacht, dass der Drucker, auf dem er die Dokumente ausdruckt am Gang steht, wo alle Mitarbeiter regelmäßig vorbeigehen. Und um die Dokumente abzuholen braucht er auch einige Minuten. In dieser Zeit haben viele Mitarbeiter aber schon die Dokumente gesehen.

Das kann böse Konsequenzen haben.

Beispiel 2: Florian will in der Firma ein paar sensible Dokumente auf einem Netzwerkdrucker ausdrucken, die nur für den Chef bestimmt sind und welche die anderen Mitarbeiter nicht sehen sollten. Der Drucker befindet sich in einem eigenen Raum und diesen hat er vorher abgesperrt, da niemand die ausgedruckten Dokumente sehen soll. Als er dann zum Drucker kommt, sieht er, dass nichts ausgedruckt wurde.

Florian denkt der Drucker sei kaputt und beschließt das Ausdrucken auf den nächsten Tag zu verschieben. Die Tür zum Druckerraum lässt er offen da ja auch andere Mitarbeiter auf diesem Drucker etwas ausdrucken müssen. Er hat dabei jedoch eine Sache nicht bedacht: Der Drucker war nicht kaputt sondern hatte lediglich einen Papierstau der noch am Abend von einem Mitarbeiter beseitigt wird, woraufhin die sensiblen Dokumente doch ausgedruckt werden und für alle Mitarbeiter die in den Raum kommen zugänglich sind. Natürlich sehen sich einige neugierig die Dokumente an. Der Chef wird nicht erfreut sein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht zu vermitteln und umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

In der Regel ist diese Maßnahme weder mit hohem Zeitaufwand noch mit hohen Kosten verbunden.

M 1.33 GEEIGNETE AUFBEWAHRUNG TRAGBARER IT-SYSTEME BEI MOBILEM EINSATZ

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme ist auch für Durchschnittsbenutzer sehr wichtig, da IT-Geräte immer kleiner und portabler werden und auf diesen auch zunehmend mehr gespeichert werden kann. Der Diebstahl oder Verlust so eines Gerätes kann dann sehr ärgerlich sein, vor allem wenn der Verlust bzw. der Diebstahl durch geeignete Aufbewahrung verhindert werden hätte können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Mary hat ihr Notebook in ihrem Auto zurückgelassen da sie noch schnell etwas einkaufen will. Das Notebook, ein neues und teures Modell, liegt für alle sichtbar auf dem Beifahrersitz. Als Mary nach einiger Zeit zurückkommt, ist die Autotür offen und das Notebook verschwunden. Sie hätte es nicht offen sichtbar herumliegen lassen dürfen, das war wohl für einen Dieb zu verlockend.

Beispiel 2: Ulf hat einen PDA, auf dem er alle seinen wichtigen Daten und auch Passwörter abgespeichert. Er hat ein Zimmer in einem Hotel gemietet und will dort übernachten. Bevor er schlafen geht, will er sich noch an der Bar etwas zu trinken genehmigen. Seinen PDA lässt

er dabei neben sich auf der Bar liegen. Als er sich einmal zu lange abgelenkt wird, ist der PDA plötzlich weg. Er hätte ihn wohl besser nicht so sichtbar herumliegen lassen sollen, auch wenn er direkt daneben gestanden ist.

Beispiel 3: Charlotte hat ein neues Handy auf dem sie all ihre Termine speichert. An einem heißen Badetag nimmt sie es in ein Schwimmbad mit und lässt es dort unvorsichtigerweise einfach so liegen. Den ganzen Tag scheint die Sonne sehr heiß auf das Gerät während sie sich im Wasser vergnügt. Als sie zurückkommt und das Handy benutzen will, geht dieses nicht mehr. Die Hitze war zu viel für das Gerät. Da hätte Charlotte etwas mehr Vorsicht an den Tag legen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht an Durchschnittsbenutzer zu vermitteln und auch leicht umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit hohem Zeitaufwand noch mit großen Kosten verbunden.

M 1.34 GEEIGNETE AUFBEWAHRUNG TRAGBARER IT-SYSTEME IM STATIONÄREN EINSATZ

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme ist für einen Durchschnittsbenutzer nicht ganz so relevant wie die Aufbewahrung tragbarer IT-Systeme im mobilen Einsatz, aber dennoch ist sie nicht zu unterschätzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Theodor arbeitet in einer Firma und hat für seine Arbeit ein Notebook bekommen. Er arbeitet nur im Büro damit, aber hier kommen oft externe Leute vorbei.

Einmal ist Theodor alleine und als er für eine Stunde außer Haus beim Mittagessen ist und er zurückkommt ist sein Notebook verschwunden. Offenbar hat das jemand beim Vorbeigehen mitgehen lassen. Wäre das Notebook durch ein Notebook-Schloss am Tisch fixiert gewesen wäre dies vermutlich nicht passiert.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist nicht mit hohem Zeitaufwand verbunden. Kosten können entstehen wenn man extra dafür etwas Zubehör kaufen muss (z.B. ein Notebook-Schloss).

M 1.36 SICHERE AUFBEWAHRUNG DER DATENTRÄGER VOR UND NACH VERSAND**Relevanz für den Durchschnittsbenutzer: mittel**

Diese Maßnahme kann für einen Durchschnittsbenutzer durchaus relevant sein, wenn dieser Datenträger öfter verschickt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Hubert soll eine CD mit sensiblen Daten an einen Freund Harald verschicken. Er will sie am nächsten Tag verschicken. Er lässt sie bei sich am Büro am Tisch liegen, sodass er die CD am nächsten Tag auch sicher sieht und nicht vergisst. Dummerweise ist das Büro offen zugänglich und das nutzt eine unbekannte Person aus schnappt sich die CD, kopiert die darauf gespeicherten Daten auf das mitgebrachte Notebook und legt die CD dann wieder genau an die Stelle wo sie vorher gelegen ist. Hubert verschickt die CD am nächsten Tag, unwissend was inzwischen passiert ist. Harald bekommt das Päckchen mit der CD und öffnet es. Da es schon spät ist, beschließt er sich die Daten erst am nächsten Tag anzusehen und lässt sie im Büro auf der Tischkante liegen, beim Schließen der Bürotür fällt die CD durch die leichte Erschütterung beim Schließen der Türe in den darunter stehenden Mistkübel. Am nächsten Tag ist die CD weg, sie wurde von den Reinigungskräften zusammen mit dem restlichen Mist entsorgt. Da hätten sowohl Hubert als auch Harald mehr Sorgfalt an den Tag legen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit hohen Kosten noch mit hohem Zeitaufwand verbunden.

M 1.37 GEEIGNETE AUFSTELLUNG EINES FAXGERÄTES**Relevanz für den Durchschnittsbenutzer: gering**

Die wenigstens Durchschnittsbenutzer haben ein Faxgerät daheim. Für die, die eines haben ist diese Maßnahme aber zu beachten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn man diese Maßnahme nicht setzt kann es leicht passieren, dass jemand Fax-Nachrichten lesen kann die nicht für diesen bestimmt sind. Die Situation ist sehr ähnlich wie bei Maßnahme M 1.32 (siehe Beispiel davon).

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht zu vermitteln und auch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit hohen Kosten noch mit hohem Zeitaufwand verbunden.

M 1.38 GEEIGNETE AUFSTELLUNG EINES MODEMS

Relevanz für den Durchschnittsbenutzer: gering

In der Regel wird ein Durchschnittsbenutzer kein ein eigenes Modem am Arbeitsplatz haben, sondern im lokalen Firmennetz sein und in einer Privatwohnung das Modem auch nicht besonders gefährdet sein. Dennoch gibt es Fälle wo diese Maßnahme von Interesse ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Gustav lebt in einer Wohngemeinschaft und hat ein neues Modem bekommen. Er zahlt für den Internetzugang alleine und teilt ihn deshalb nicht mit den anderen WG-Bewohnern und lässt sie diesen auch nicht benutzen. Das Modem steht aber frei zugänglich in der Wohnung herum.

Dummerweise wohnt auch Gerlinde in der Wohnung. Sie kennt sich sehr gut mit IT aus und wie Gustav einmal weg ist hängt sie ihr Notebook an das Modem und beginnt wie wild Sachen aus dem Netz herunterzuladen. Gustav hat nur leider ein Downloadlimit bei seinem Internetzugang und durch Gerlindes Tat ist er in diesem Monat deutlich darüber. Er ist ziemlich sauer als er die nächste Rechnung bekommt, weiß aber nicht wie sie zustande gekommen ist.

Da hätte er wohl besser das Modem in seinem Zimmer eingesperrt als es offen herumstehen zu lassen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht zu vermitteln und auch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit Kosten noch mit hohem Zeitaufwand verbunden.

M 1.43 GESICHERTE AUFSTELLUNG AKTIVER NETZKOMPONENTEN**Relevanz für den Durchschnittsbenutzer: gering**

In der Regel wird sich damit wohl eher die Haustechnik bzw. die IT-Abteilung einer Firma beschäftigen. Für einen Durchschnittsbenutzer kann diese Maßnahme nur unter gewissen Umständen auch relevant sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Es kann z.B. ähnliches passieren wie bei Punkt M 1.38 (geeignete Aufstellung eines Modems) nur das dasselbe z.B. auch Switches oder Router betreffen kann.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht zu vermitteln und auch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit Kosten noch mit hohem Zeitaufwand verbunden.

M 1.44 GEEIGNETE EINRICHTUNG EINES HÄUSLICHEN ARBEITSPLATZES**Relevanz für den Durchschnittsbenutzer: mittel**

Dieser Punkt ist dann sehr wichtig für einen Durchschnittsbenutzer, wenn er von zu Hause aus arbeitet.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Frank arbeitet seit neuestem ab und zu daheim da er seine Frau mit den beiden Kleinkindern verstärkt unterstützen will. Er hat sich jedoch nicht die Mühe gemacht einen

eigenen Arbeitsraum dafür einzurichten. Leider war dies ein Fehler. Durch den Lärm der Kinder kann er sich nur schwer konzentrieren. Weiters hat sein kleiner Sohn sein Notebook entdeckt und darauf herum gehämmert und dabei wichtige Daten am Firmenserver gelöscht, da Frank vergessen hatte sich von diesem abzumelden. Außerdem hat er nach kurzer Zeit Probleme mit dem Rücken, da die Couch auf der er daheim arbeitet nicht besonders ergonomisch ist.

Das alles wäre nicht passiert hätte er sich die Zeit genommen sich ein Arbeitszimmer einzurichten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht besonders schwer zu vermitteln kann aber bei Platzmangel schwer umzusetzen sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann mit höherem Zeitaufwand und höheren Kosten verbunden sein.

M 1.45 GEEIGNETE AUFBEWAHRUNG DIENSTLICHER UNTERLAGEN UND DATENTRÄGER

Relevanz für den Durchschnittsbenutzer: hoch

Dieser Punkt ist für einen Durchschnittsbenutzer sehr wichtig, schließlich ist auch er dafür verantwortlich, dass dienstliche Unterlagen und Datenträger nicht in falsche Hände gelangen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Udo hat oft dienstliche Unterlagen und Datenträger daheim. Trotzdem kümmert er sich nicht sehr gewissenhaft um die Aufbewahrung derselben. Eines Tages hat er wieder ein paar wichtige CDs und Dokumente daheim herumliegen. Die CDs liegen am Fensterbrett und die Dokumente am Schreibtisch. Als Ulf kurz weg ist weht ein kleiner Windstoß durch das offene Fenster und die Dokumente vom Tisch fallen in den Altpapierstapel. Währenddessen wird es auch sonnig und sehr heiß und die CDs sind dem prallen Sonnenlicht ausgesetzt. Zudem ist aus irgendeinem Grund auch noch die Heizung eingeschaltet, welche direkt unter dem Fensterbrett montiert ist.

Die CDs verformen sich unter der zu großen Hitze. Ulf bemerkt das alles nicht und als er zurückkommt beschließt er erst einmal den schon viel zu großen Altpapierstapel wegzuschaffen (mit den wichtigen Dokumenten, wovon er aber nichts mitbekommt).

Am nächsten Tag will er die Dokumente durchsehen und auch den Inhalt der CDs überprüfen.

Doch wie er feststellen muss sind die CDs nicht mehr lesbar und die Dokumente verschwunden.

Hätte er sich mehr Gedanken um die geeignet Aufbewahrung gemacht, wäre das nicht passiert.

Abgesehen davon hätten die Dokumente bzw. die CDs auch leicht von jemanden gestohlen werden können, da Ulfs Wohnung im Erdgeschoss liegt und das Fenster offen war.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme kann man leicht vermitteln und leicht umsetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme benötigt nicht besonders viel Zeit aber möglicherweise Kosten wenn der Situation angemessene Aufbewahrungseinheiten angeschafft werden müssen.

M 1.46 EINSATZ VON DIEBSTAHL-SICHERUNGEN

Relevanz für den Durchschnittsbenutzer: gering/mittel

Diese Maßnahme kann bis zu einem gewissen Grad auch für einen Durchschnittsbenutzer wichtig sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Hermann ist oft mit seinem Notebook auf Konferenzen unterwegs. Er will es nur nicht immer mit sich herumschleppen z.B. wenn er das stille Örtchen aufsucht. Also lässt er das Notebook auf einem Tisch vor der Toilette stehen, da wird es in der kurzen Zeit ja wohl keiner mitnehmen.

Als er zurückkommt ist es aber doch weg. Mit einem Notebook-Schloss hätte er sein Notebook an den Tisch ketten können und es wäre dann vermutlich nicht verschwunden. Aber später ist man immer klüger.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für die Maßnahme ist nicht sehr hoch aber solche Diebstahl-Sicherungen können durchaus höhere Kosten verursachen, je nachdem welche Diebstahl-Sicherungen man sich zulegen will.

M 1.55 PERIMETERSCHUTZ

Relevanz für den Durchschnittsbenutzer: gering

Diese Maßnahme betrifft im großen Stil eher Behörden- und Unternehmensleitungen, z.B. zur Absicherung eines Gebäudes oder Geländeteils, aber im kleinen Rahmen kann dies auch einen Durchschnittsbenutzer betreffen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Tarik hat einen WLAN-Router bei sich im Wohnzimmer einfach so herumstehen. Auch hat er zwei sehr aktive kleine Kinder. Als Tarik einmal nicht aufpasst sehen die Kinder den Router im Wohnzimmer und beginnen mit diesem herumzuspielen. Als Tarik plötzlich keine WLAN-Verbindung mehr hat, da schwant ihm Übles. Zurück im Wohnzimmer sieht er zwei vergnügte Kinder aber leider auch einen kaputten WLAN-Router. Hätte er den Bereich um den Router irgendwie abgesichert, sodass die Kinder den WLAN-Router nicht hätten erreichen können, wäre das nicht passiert.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, die Maßnahme ist nicht schwer zu vermitteln oder umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit etwas Zeitaufwand verbunden und kann Kosten verursachen, muss es aber nicht.

M 1.59 GEEIGNETE AUFSTELLUNG VON SPEICHER- UND ARCHIVSYSTEMEN

Relevanz für den Durchschnittsbenutzer: mittel

Dieser Punkt ist für den Benutzer durchaus relevant, da auch er seine Daten irgendwo brauchbar archivieren sollte.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Heike fotografiert sehr gerne und viel mit ihrer neuen Digitalkamera. Sie archiviert alle ihre Fotos auf ihrer externen Festplatte. Diese benutzt sie auch um Daten von zu Hause in die Arbeit zu transportieren und umgekehrt. Eines Tages hat sie wieder ein paar Daten auf der externen Festplatte in die Arbeit mitgebracht. Ein Mitarbeiter von ihr braucht die Daten

dringend und steckt die externe Festplatte bei sich an, klickt aber das falsche Verzeichnis an und ist plötzlich in Heikes Fotosammlung. Da sind aber leider auch einige Fotos dabei die Heike ihren Arbeitskollegen mit Sicherheit nicht zeigen wollte, nur jetzt ist es leider zu spät. Heikes Kopf ist hochrot. Das nächstemal verwendet sie sicher nicht dieselbe Platte für das Archivieren ihrer privaten Fotos und für das Speichern von Daten für die Arbeit.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme benötigt nur geringen Zeitaufwand, kann aber mit Kosten verbunden sein (z.B. wie in dem Beispiel durch das Besorgen einer externen Festplatte die dann daheim gut und sicher verwahrt wird).

M 1.60 GEEIGNETE LAGERUNG VON ARCHIVMEDIEN

Relevanz für den Durchschnittsbenutzer: hoch

Wie man Archivmedien richtig lagert ist auch für einen Durchschnittsbenutzer von großer Bedeutung. Denn schließlich will auch ein Durchschnittsbenutzer auf die archivierten Daten noch zugreifen können wenn er sie braucht.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Melissa hat ihre Daten auf beschreibbaren DVDs archiviert. Leider hat sie diese im Keller verwahrt wo es im Winter kalt, im Herbst feucht und im Sommer viel zu heiß ist. Die DVDs sind zudem nicht in einzelnen Hüllen gesteckt sondern einfach zusammen in eine Schuhschachtel gepackt worden. Als Melissa jetzt ein paar alte Daten wieder benötigt muss sie feststellen, dass der Großteil ihrer DVDs nicht mehr lesbar ist und die benötigten Daten so unwiederbringlich verloren sind. Da hätte sie mehr Sorgfalt bei der Lagerung an den Tag legen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme sollte im Normalfall weder mit viel Zeitaufwand noch Kosten verbunden sein.

M 2 MAßNAHMENKATALOG ORGANISATION

Dieser Maßnahmenkatalog behandelt alle Maßnahmen die das Thema IT-Sicherheit in einer Organisation, z.B. einer Firma oder einer Behörde, betreffen. Wenn mehrere Personen miteinander arbeiten und dabei auch sensitive Daten ausgetauscht werden müssen, müssen viele Maßnahmen gesetzt werden, damit es potentiell zu keinen Problemen im Bezug auf die IT-Sicherheit kommt. Diese Maßnahmen reichen von der regelmäßigen Sicherung von wichtigen Daten und deren sicherer Aufbewahrung, der Vergabe von Zutritts- und Zugangsrechten, der Umgang mit mobilen Geräten bzw. der richtige Umgang mit Geräten die von mehreren Personen genutzt werden bis zur Aufstellung ein Einhaltung von diversen Richtlinien etwa um gesetzliche Rahmenbedingungen zu erfüllen.

M 2.2 BETRIEBSMITTELVERWALTUNG

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme ist dann für den Durchschnittsbenutzer interessant wenn er selbst diese beschaffen muss (z.B. als Privatperson) und da kann man einige Fehler machen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel1: Theodor, Wolfgang und Helga wollen sich privat alle einen neuen PC kaufen.

Alle drei haben sehr wenig Ahnung davon, informieren sich aber trotzdem im Vorfeld kaum und kaufen auf einfach irgendwo einen PC.

Theodors PC funktioniert zwar gut aber er hat aber deutlich mehr bezahlt, als der PC eigentlich wert wäre.

Wolfgang's PC war zwar günstig funktioniert aber nicht richtig und er reklamiert ihn. Aber bei dem Händler wo er den PC gekauft hat dauert es ewig bis das Gerät ausgetauscht wird und nachdem endlich der Austausch erfolgt ist, bekommt er wieder ein Gerät das kurze Zeit später dieselben Probleme hat.

Bei Helgas PC fehlt das Betriebssystem und da sie selbst keines installieren kann, ist der PC für sie so nutzlos.

Alle drei hätten diese Probleme bzw. Nachteile vermeiden können hätten sie sich vor der Beschaffung der Computer besser informiert oder noch besser jemanden zu Rate gezogen der sich gut mit der Beschaffung von PCs auskennt. Diese Probleme kann es nämlich auch bei anderen Geräten wie Druckern, Scannern oder anderen Hardware und Software-Komponenten geben.

Beispiel 2: Udo hat sich zu Hause ein kleines Büro eingerichtet. Die Betriebsmittelverwaltung erledigt er selbst. Unter anderem steht auch ein Drucker in seinem Büro der täglich viel im Einsatz ist. Auch archiviert er wichtige Daten auf auf DVDs.

Leider ist Udo nachlässig was die Betriebsmittelverwaltung betrifft und er hat nicht bedacht, dass ihm die DVD-Rohlinge und der Toner seines Druckers ausgehen könnten.

Eines Tages ist es dann soweit, er hat keine DVD-Rohlinge mehr. Das ist noch kein Problem, denn der nahe gelegene Supermarkt hat die auf Lager und Udo kann sie dort schnell einkaufen. Das kostet aber Zeit. Am selben Tag geht ihm auch zufällig der Toner vom Drucker aus. Das ist jetzt ein Problem, denn der Toner für diesen Druckertyp hat ein paar Tage Lieferzeit und Udo kann in der Zeit jetzt nichts ausdrucken, was er für seine Arbeit aber unbedingt tun müsste.

Da hätte Udo die Betriebsmittelverwaltung doch deutlich besser machen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen und in den meisten Fällen auch nicht schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann mit etwas Zeitaufwand und auch mit Kosten verbunden sein, kann aber auch helfen Geld und viel Zeit zu sparen wenn Betriebsmittel durch entsprechende Vorsorge günstiger erworben werden können bzw. die benötigten Betriebsmittel immer da sind wenn man sie braucht.

M 2.3 DATENTRÄGERVERWALTUNG

Relevanz für den Durchschnittsbenutzer: hoch

Die Lagerung, die Kennzeichnung und der Transport von Datenträgern betrifft auch den Durchschnittsbenutzer wie das folgende Beispiel zeigen wird.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel1: Ludwig archiviert seine Daten immer auf selbstgebrannten CDs oder DVDs.

Jedoch ist er etwas nachlässig was die Aufbewahrung und Kennzeichnung derselben betrifft.

Auf die CDs oder DVDs schreibt er lediglich eine Nummer und gelagert werden die CDs/DVDs dann einfach in einer Schuhschachtel.

Eines Tages wird Ludwigs Festplatte kaputt. Ludwig denkt sich, dass das ja kein Problem sei er habe ja ein Backup von alle seinen Daten. Er geht also zur Schuhschachtel und öffnet diese

und muss erst einmal entdecken, dass die Kennzeichnung nicht gut gewählt war. Denn er weiß so nicht auf welcher CD/DVD sich welche Daten befinden und wie aktuell diese sind. Also muss er mühsam alle per Hand durchsehen, wobei ihm dabei auffällt, dass manche CDs/DVDs nicht mehr lesbar sind, da er sie ohne Schutzhülle in die Schuhschachtel gelegt hat und diese jetzt teilweise stark zerkratzt sind.

Manche Daten hat Ludwig dadurch wohl für immer verloren. Ein bessere Lagerungsstrategie und eine bessere Kennzeichnung hätten da doch sehr geholfen.

Beispiel 2: Iris muss ihrer Freundin Doris eine CD mit wichtigen Daten schicken. Sie steckt die CD ohne darüber nachzudenken in ein Briefkuvert welches ausreichend groß ist und verschickt den Brief mit der Post. Als Doris den Brief bekommt muss sie leider eine ungute Entdeckung machen: Der Transport hat der CD nicht gut getan, sie ist jetzt völlig zerkratzt und nicht mehr lesbar.

Das wäre nicht passiert hätte Iris die CD vor dem Versenden in eine Schutzhülle getan und z.B. in einem Luftpolsterkuvert verschickt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die richtige Kennzeichnung bzw. eine Bestandsliste von Datenträgern zu führen kann durchaus Zeit in Anspruch nehmen, verursacht in der Regel aber keine Kosten.

Das richtige Versenden von Datenträgern benötigt nicht viel Zeit, aber ist durch leicht höhere Verpackungskosten etwas teurer als der normale Versand.

M 2.4 REGELUNGEN FÜR WARTUNGS- UND REPARATURARBEITEN

Relevanz für den Durchschnittsbenutzer: mittel

Viele Wartungsarbeiten kann der Durchschnittsbenutzer in der Regel nicht selbst durchführen, aber sehr wohl solche Sachen wie das grobe Reinigen von Geräten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ivan isst und raucht sehr gerne nebenbei während er an seinem Computer arbeitet. Da lässt es sich schwer vermeiden, dass hin und wieder ein paar Krümel in der Tastatur landen.

Auch ist es in seinem Arbeitszimmer eher staubig aber Aufräumen oder Putzen ist nicht die

große Stärke von ihm. Mit der Zeit ist die Tastatur so verdreckt, dass einzelne Tasten nur noch schwer gehen und die Tastatur neben der eingeschränkten Funktionalität nur noch ekelhaft ist.

Dazu kommt, dass der PC dauernd abstürzt weil sich Ablagerungen von Staub und Zigarettenrauch im Gehäuse angesammelt haben durch die der PC jetzt sehr schnell überhitzt.

Das alles hätte Ivan vermeiden können, hätte er nur hin und wieder seinen Computer und seine Tastatur gereinigt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Ein wenig Zeitaufwand ist für diese Maßnahme notwendig, die Kosten sind, sollten überhaupt welche anfallen, aber sehr moderat.

M 2.6 VERGABE VON ZUTRIITTSBERECHTIGUNGEN

Relevanz für den Durchschnittsbenutzer: hoch

Sollte der Durchschnittsbenutzer anderen Zugang zu Räumlichkeiten gewähren können die für die IT-Infrastruktur wichtig sind, sollte sich der Durchschnittsbenutzer genau überlegen wem er das erlaubt und unter welchen Bedingungen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Da Petra immer viel um die Ohren hat, hat sie beschlossen sich eine Reinigungskraft für ihre Wohnung zu leisten, damit sie das mühsame Putzen und Aufräumen nicht mehr selbst machen muss. Die Reinigungskraft bekommt den Schlüssel für die Wohnung, sodass sie auch in Petras Abwesenheit sauber machen kann. Petra bewahrt ja eh nichts wirklich Wertvolles in der Wohnung auf, also macht sie sich keine Sorgen. Sie hat nur nicht bedacht, dass ihr alten Computer auch noch dort steht. Und auf diesem sind hochsensible private Daten gespeichert und die Backups liegen als DVDs einfach daneben.

Diese sensiblen Daten sind so potentiell gefährdet in die Hände von Leuten zu gelangen welche diese nicht bekommen sollten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel weder mit hohem Zeitaufwand oder Kosten verbunden.

M 2.7 VERGABE VON ZUGANGSBERECHTIGUNGEN

Relevanz für den Durchschnittsbenutzer: mittel

In der Regel wird diese Maßnahme von Administratoren oder dem IT-Sicherheitsmanagement gesetzt. Sollte der Durchschnittsbenutzer aber einmal in der Situation kommen selbst Zugangsberechtigungen zu gewissen IT-relevanten Systemen verteilen zu müssen, sollte er sich darüber im Klaren sein, wie er das tut und was er damit tut.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Paul hat einen neuen WLAN-Router zu Hause über den er ins Internet kann und da er öfters Gäste mit Notebooks bei sich hat, hat er beschlossen einfach allen den Zugang zum Internet über seinen WLAN-Router zu gestatten. Dabei hat er nur eines nicht bedacht: Den Zugang können nicht nur seine Gäste benutzen sondern jede Person die in der Reichweite seines Routers ein WLAN benutzen will. Kurze Zeit später bekommt er auch schon ein Schreiben von seinem Internet-Anbieter, seine Internetverbindung massiv belastet wurde, was zu deftigen Nachzahlungen führt.

Da hätte Paul wohl etwas mehr Nachdenken müssen bevor er so leichtfertig allen den Zugang gestattet hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen, doch kann es etwas dauern bis man dem Durchschnittsbenutzer das Gefahrenpotential vermittelt hat.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohem Zeitaufwand noch mit Kosten verbunden.

M 2.8 VERGABE VON ZUGRIFFSRECHTEN

Relevanz für den Durchschnittsbenutzer: mittel

In der Regel wird diese Maßnahme von Administratoren oder dem IT-Sicherheitsmanagement gesetzt. Sollte der Durchschnittsbenutzer aber z.B. in die Situation kommen irgendwelche Daten anderen Leuten zur Verfügung stellen zu wollen, dann muss er sich auch darüber im Klaren sein was und wie er das eigentlich macht.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Gabriel hat ein paar tolle Videos für die Firma erstellt und will die auch seinen Kollegen zeigen. Also gibt er den Ordner auf seinem Notebook in dem die Videos liegen für alle im Netzwerk frei. Die Videos enthalten auch wichtige Informationen die aber innerhalb der Firma bleiben sollen.

Später geht Gabriel dann zu einem Vortrag und nimmt sein Notebook mit.

Er hat nur vergessen, dass der Ordner noch immer für alle im Netz zugänglich ist. Bei dem Vortrag gibt es auch ein WLAN. Sehr fein denkt sich Gabriel und surft dann über dieses im Internet. Leider ist der Ordner damit auch für alle anderen Vortragsteilnehmer offen zu erreichen und die Videos gelangen kurze Zeit später auf ein Videoportal wo sie eigentlich gar nicht hinsollten.

Da hat Gabriel nicht richtig bei der Vergabe der Zugriffsrechte aufgepasst und jetzt wird er deshalb vermutlich Probleme bekommen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen, allerdings kann es etwas dauern bis man einem Durchschnittsbenutzer erklärt hat, wie das System der Zugriffsrechte auf seinem System funktioniert.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann etwas Zeit in Anspruch nehmen ist in der Regel aber nicht mit Kosten verbunden.

M 2.9 NUTZUNGSVERBOT NICHT FREIGEgebENER HARD- UND SOFTWARE**Relevanz für den Durchschnittsbenutzer: gering**

Diese Maßnahme ist in erster Linie für die Unternehmensleitung und das IT-Sicherheitsmanagement interessant. Dem Durchschnittsbenutzer sollte nur zur Kenntnis gebracht werden welche Hard- und Software er selbst nicht in einem Unternehmen einsetzen darf bzw. welche er benutzen darf.

M 2.11 REGELUNG DES PASSWORTGEBRAUCHS

Relevanz für den Durchschnittsbenutzer: mittel

Die Regelungen für den Passwortgebrauch aufzustellen ist in erster Linie Aufgabe der IT-Leitung und der IT-Sicherheitsbeauftragten. Aber auch der Durchschnittsbenutzer sollte ein paar Dinge über den Passwortgebrauch wissen z.B. wie man ein richtiges Passwort wählt und wo man dieses aufbewahrt bzw. wo nicht.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Konrad speichert fast alle wichtigen Daten auf seinem Notebook. Da er sich Passwörter so schwer merkt hat er beschlossen einfach seinen Namen als Passwort zu verwenden.

Auf einer Konferenz lässt er einmal sein Notebook mit einem Notebook-Schloss angekettet auf einem Tisch stehen, sperrt den Bildschirm und geht weg weil er dringend etwas erledigen muss.

Der neugierige Klaus sieht das und setzt sich vor das Notebook wie Konrad weg ist und gibt spaßhalber den Namen „Konrad“ als Passwort ein und siehe da, er hat jetzt vollen Zugriff auf alles und kann in allen wichtigen Daten von Konrad herumstöbern.

Den eigenen Namen als Passwort zu wählen war wohl keine gute Idee von Konrad.

Beispiel 2: Susanne hat ein gutes Passwort von der IT-Abteilung damit sich ja niemand mit Susannes Benutzer an ihrem PC anmelden kann, da man mit diesem Zugriff auf sehr sensible Daten hat. Leider hat Susanne den Sinn und Zweck des Passworts nicht ganz verstanden und da sie es immer vergisst hat sie es einfach auf einen Zettel geschrieben und diesen auf ihren Monitor geklebt.

Kurze Zeit später wird Susannes Benutzer auch von Unbefugten verwendet. Das wird wahrscheinlich Ärger für Susanne bedeuten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohem Zeitaufwand noch mit Kosten verbunden.

M 2.13 ORDNUNGSGEMÄßE ENTSORGUNG VON SCHÜTZENSWERTEN BETRIEBSMITTELN

Relevanz für den Durchschnittsbenutzer: mittel

Auch dieser Punkt betrifft den Durchschnittsbenutzer wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Fritz hat einen neuen PC bekommen und verkauft deshalb seinen alten PC.

Seine Daten hat er sorgsam vorher alle gesichert und auf den neuen PC überspielt und die Festplatte am alten PC hat er formatiert, denn auf diesem waren ja sensible Firmendaten.

Was er nicht bedacht hat: das einfache Formatieren ein Festplatte reicht bei weitem nicht aus um die Daten sicher zu löschen. Der Käufer des PCs arbeitet zufällig beim Konkurrenzunternehmen und kennt sich mit Datenwiederherstellung aus und hat durch den Kauf von Fritz PC jetzt quasi auch all diese sensiblen Firmendaten bekommen.

Da hätte sich Fritz vorher besser informieren sollen wie man Daten verlässlich löscht.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen aber es kann einige Zeit dauern bis der Durchschnittsbenutzer begreift was für Probleme auftreten können.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann zwar einiges an Zeit in Anspruch nehmen sollte aber in der Regel keine Kosten verursachen.

M 2.14 SCHLÜSSELVERWALTUNG

Relevanz für den Durchschnittsbenutzer: mittel

Dieser Punkt betrifft in erster Linie die Haustechnik und ansonsten gilt für den Durchschnittsbenutzer quasi dasselbe wie bei M 2.6.

M 2.16 BEAUFSICHTIGUNG ODER BEGLEITUNG VON FREMDPERSONEN

Relevanz für den Durchschnittsbenutzer: mittel

Die Beaufsichtigung von Fremdpersonen ist auch für einen Durchschnittsbenutzer relevant wie das folgende Beispiel zeigt:

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Lukas will ein Zimmer in seiner Wohnung neu ausmalen lassen. Da er viel zu tun hat schickt er den Maler, als dieser eintrifft, einfach in das entsprechende Zimmer und lässt diesen dort alleine arbeiten. Dummerweise hat Lukas etwas vergessen. In dem Zimmer liegen noch sein Memory-Stick mit sehr wichtigen Daten darauf.

Die hätte der Maler jetzt einfach mitnehmen können. Aber der Maler ist ein ehrlicher Mensch und hat ihn dort gelassen wo er gelegen ist, was leider aber auch nicht gut war, da der Stick ein paar Farbspritzer abbekommen hat und zwar genau so, dass er jetzt kaputt ist.

Da hätte Lukas doch besser den Maler beim Abdecken des Arbeitsbereiches zu beaufsichtigen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch an einen Durchschnittsbenutzer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann zeitintensiv sein aber ist in der Regel nicht mit Kosten verbunden.

M 2.17 ZUTRITTSREGELUNG UND -KONTROLLE

Relevanz für den Durchschnittsbenutzer: mittel

Dieser Punkt betrifft in erster Linie die Haustechnik und ansonsten gilt für den Durchschnittsbenutzer quasi dasselbe wie bei M 2.6.

M 2.21 RAUCHVERBOT

Relevanz für den Durchschnittsbenutzer: mittel

Das Rauchverbot sollte vom Durchschnittsbenutzer in jedem Fall eingehalten werden, denn sonst kann es, neben gesundheitlichen Problemen für die Person, auch zu Problemen führen welche die IT-Sicherheit beeinträchtigen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Wenn man an einem Ort raucht wo Rauchmelder installiert sind, kann dies zu einem Feuersalarm oder im weiteren Fall sogar zu Gegenmaßnahmen wie der Aktivierung der

Sprinkleranlage führen. Das Wasser der Sprinkleranlage kann in weiterer Folge dann IT-Geräte beschädigen.

Beispiel 2: Es wird oft unterschätzt, dass der Rauch von Zigaretten mit der Zeit Ablagerungen auf und in IT-Geräten hinterlassen kann die im schlimmsten Fall dazu führen, dass das IT-Gerät nicht mehr funktioniert.

Beispiel 3: Rauchen ist auch potentiell immer eine Brandgefahr. Oft ist es schon passiert, dass eine unachtsam weggeworfene und schlecht ausgedämpfte Zigarette einen Brand ausgelöst hat. Dass dies dann auch ein Problem für IT-Geräte darstellt sollte klar sein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist leicht zu vermitteln und umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohen Kosten noch mit hohem Zeitaufwand verbunden.

M 2.22 HINTERLEGEN DES PASSWORTES

Relevanz für den Durchschnittsbenutzer: gering/mittel

Diese Maßnahme kann den Durchschnittsbenutzer dann betreffen, wenn er in einem Team arbeitet, wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Jan arbeitet in einem Team und bereitet Daten mit einem Programm so auf, dass seine Kollegen diese dann später weiterbearbeiten können. Jan fährt eines Tages für zwei Wochen auf Urlaub. Er hat auch extra vorgearbeitet, sodass die Daten für seine Kollegen schon vorbereitet sind.

Leider hat er vergessen ihnen das Passwort zu sagen mit dem sie die Daten von seinem System auf ihre PCs transferieren können. Jetzt können Jans Kollegen für zwei Wochen nichts machen, da Jan nicht erreichbar ist und keiner das Passwort kennt.

Da hätte im Vorfeld schon eine Stelle eingerichtet gehört, wo jeder sein Passwort für genau solche Fälle hinterlegen muss.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer zu vermitteln, erfordert aber etwas Zeit um sich für die Umsetzung der ordnungsgemäßen Hinterlegung der Passwörter eine geeignete Strategie einfallen zu lassen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit etwas Zeitaufwand und möglicherweise auch Kosten verbunden (z.B. um einen für die Aufbewahrung geeigneten Schrank zu besorgen).

M 2.37 "DER AUFGERÄUMTE ARBEITSPLATZ"

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme betrifft Durchschnittsbenutzer die den Arbeitsplatz bzw. den Computer mit anderen Personen teilen. Am folgenden Beispiel sieht man recht einfach warum das „Aufräumen“ des Arbeitsplatzes wichtig ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Jens arbeitet in einer Firma im Telefonsupport. Er benutzt regelmäßig andere PCs, je nachdem wann seine Schicht beginnt. Danach wird der PC von Kollegen welche in der nächsten Schicht arbeiten verwendet. Jens ist noch relativ neu, hat aber trotzdem Zugang zu vielen sensiblen Daten über ein Webinterface. Da diese Daten sehr sensibel sind, hat Jens sein eigenes Passwort für dieses Webinterface. Da die Daten aber oft nur sehr langsam am Bildschirm erscheinen und er oft dieselben Daten abfragen muss, beschließt Jens sie einfach lokal am Desktop abzuspeichern, da er so deutlich schneller ist.

Irgendwann endet seine Schicht und da er übermüdet ist verlässt er flott die Arbeit, vergisst aber die Daten vom Desktop zu löschen. Der nächste im Schichtbetrieb kann sich dann also all diese sensiblen Daten ansehen, obwohl er eigentlich keine Berechtigung dafür hat.

Das bekommt auch der Abteilungsleiter mit und Jens bekommt eine Standpauke und er verspricht das nicht mehr zu machen.

Dafür macht er bei der nächsten Schicht den nächsten Fehler. Da er immer sein Passwort eingeben muss wenn er etwas im Webinterface abfragt, beschließt er das Passwort im Browser zu speichern.

Nach seiner Schicht vergisst er das Passwort aus der Passwortliste zu löschen und damit hat der Kollege in der nächsten Schicht sogar Vollzugriff auf alle Daten in dem Webinterface.

Es setzt also die nächste Standpauke für Jens. Er bekommt am nächsten Tag ein neues Passwort, da das alte jetzt bekannt ist. Das neue Passwort ist aber komplizierter und Jens merkt es sich schlecht. Also schreibt er es auf einen Zettel und klebt es auf seinen Monitor und tippt es von dort ab wenn er es braucht. Und auch diesmal vergisst er nach seinem

Schichtende den Zettel zu entfernen, wobei es schon schlimm genug war, dass jeder der vorbeiging sich das Passwort theoretisch hätte notieren können. Jens hat das mit dem „aufgeräumten Arbeitsplatz“ wohl überhaupt nicht verstanden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist in der Regel nicht mit Kosten verbunden und auch der Zeitaufwand einen Arbeitsplatz „aufzuräumen“ hält sich in Grenzen.

M 2.41 VERPFLICHTUNG DER MITARBEITER ZUR DATENSICHERUNG

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme muss zwar in erster Linie von der Unternehmensleitung gesetzt werden, aber für den Durchschnittsbenutzer ist diese, vor allem auch im privaten Bereich, sehr wichtig.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Andreas speichert alle seine wichtigen Daten sowohl die privaten als auch die beruflichen auf seinem Notebook. An eine Datensicherung hat er nie gedacht und auch in seiner Firma gibt es dazu keine Verpflichtung. Eines Tages wird aber die Festplatte im Notebook kaputt. Jetzt ist der Jammer natürlich groß. Andreas hat damit alle Daten verloren, sowohl die beruflichen als auch die privaten und er wird sie auch nirgends mehr herbekommen können.

Deshalb sollte jeder Durchschnittsbenutzer wissen, dass eine regelmäßige Datensicherung extrem wichtig ist, den Datenträger wie Festplatten haben nur eine begrenzte Lebensdauer und können manchmal auch von einem Tag auf den anderen nicht mehr funktionieren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen und auch nicht schwer an einen Durchschnittsbenutzer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Eine Datensicherung kann je nach Datenmenge natürlich sehr zeitintensiv sein und auch mit Kosten verbunden sein (Speichermedien!), aber die Kosten sind es wert, und daher sollte nicht an der falschen Stelle gespart werden.

M 2.44 SICHERE VERPACKUNG DER DATENTRÄGER

Relevanz für den Durchschnittsbenutzer: mittel

Siehe auch M 2.3.

M 2.50 GEEIGNETE ENTSORGUNG VON FAX-VERBRAUCHSGÜTERN UND – ERSATZTEILEN

Relevanz für den Durchschnittsbenutzer: gering

Sollte ein Durchschnittsbenutzer selbst in die Situation kommen, dass er Fax-Verbrauchsgüter oder Ersatzteile entsorgen muss, dann sollte er zumindest ein paar grundlegende Dinge dabei beachten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Das Faxgerät in Irenes Firma macht einige Probleme und die letzten Ausdrucke waren verschmiert und nicht besonders gut. Die hauseigenen Techniker haben in der Zwischenzeit dieses Problem behoben aber es gibt jetzt einen Stapel mit fehlerhaften Ausdrucken die Irene entsorgen soll. Umweltbewusst wie sie ist gibt sie diese ins Altpapier.

Sie hat nur eine Sache nicht dabei bedacht: Auch auf diesen Ausdrucken sind genügend sensible Informationen zu erkennen die nicht jeder erfahren sollte.

Da hätte sie diese Ausdrucke wohl besser vorher durch den Aktenvernichter laufen lassen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann etwas Zeitaufwand und auch Kosten verursachen (z.B. Kosten für einen Aktenvernichter).

M 2.51 FERTIGUNG VON KOPIEN EINGEHENDER FAXSENDUNGEN

Relevanz für den Durchschnittsbenutzer: mittel

Faxsendungen können manchmal wichtige Informationen enthalten und für den Fall, dass das originale Fax verloren geht oder aus irgendwelchen Gründen unleserlich wird, ist es nie schlecht wenn der Durchschnittsbenutzer vorher eine Kopie angefertigt hat.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Nicole arbeitet als Sekretärin in einer Firma und betreut auch das Fax-Gerät. Eines Tages kommt ein wichtiges Fax an ihren Chef herein, welches sie diesem sofort bringt ohne zuerst eine Kopie davon gemacht zu haben, wie sie das eigentlich tun sollte.

Wenige Tage später fragt der Chef Nicole, ob er ihr die Kopie vom Fax aus dem Archiv geben könne, da er das Original nicht mehr finden kann und auf diesem Fax extrem wichtige Informationen stehen die er jetzt ganz dringend benötigt.

Da bemerkt Nicole, dass sie vergessen hat, eine Kopie von dem Fax zu machen. Ihr Chef wird nicht erfreut sein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit ein wenig Zeitaufwand und auch ein paar, zumeist moderaten, Zusatzkosten verbunden.

M 2.52 VERSORGUNG UND KONTROLLE DER VERBRAUCHSGÜTER**Relevanz für den Durchschnittsbenutzer: gering**

Diese Maßnahme betrifft den Durchschnittsbenutzer dann, wenn er sich selbst mit Verbrauchsgütern versorgen muss.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Emil speichert seine Daten zumeist auf beschreibbaren CDs.

Er hat gerade ein furchtbar wichtiges Projekt fertiggestellt und will dies auf eine CD sichern und dann noch auf eine weitere, um diese dann zu versenden, wobei die Zeit drängt.

Nur hat er leider nicht kontrolliert ob er noch beschreibbare CDs hat und wie er feststellen muss, hat er keine mehr hat und zum Einkaufen kommt er auch nicht mehr.

Jetzt wird die CD die er verschicken will nicht rechtzeitig ankommen können.

Das hätte sich Emil ersparen können wenn er vorher kontrolliert hätte, ob er noch genug beschreibbare CDs zur Verfügung hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme benötigt ein wenig Zeit aber sollte keine Zusatzkosten verursachen.

M 2.63 EINRICHTEN DER ZUGRIFFSRECHTE

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme betrifft das IT-Sicherheitsmanagement und den Administrator und in den meisten Fällen nicht den Durchschnittsbenutzer. Sollte der Durchschnittsbenutzer doch damit zu tun haben gilt dasselbe wie bei M 2.8.

M 2.80 ERSTELLUNG EINES ANFORDERUNGSKATALOGS FÜR STANDARDSOFTWARE

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme betrifft in erster Linie die Leitung einer Fachabteilung. Aber auch einen Durchschnittsbenutzer kann dies betreffen wenn sich dieser selbst Standardsoftware anschaffen will.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Klemens will sich eine neues Textverarbeitungs-, eine neue Tabellenkalkulations- sowie ein gutes Bildbearbeitungsprogramm besorgen. Er informiert sich vorab aber nicht sondern kauft sich einfach günstig irgendeine Software die so aussieht als könne sie das was er braucht. Wie er bald feststellen muss, ist diese aber weder Standard-kompatibel, noch kann sie alles das, was er benötigt. Also kauft er nochmal ein, diesmal das Beste was er kriegen kann und er zahlt ziemlich viel dafür. Das funktioniert jetzt auch, aber wie er später entdecken muss, hätte er sich auch ohne Kosten Open Source Software besorgen können, die alles gekonnt hätten was er gebraucht hätte. So hat er jetzt viel Geld ausgegeben für ein Produkt, welches viel mehr kann, als er eigentlich je braucht.

Klemens hätte sich im Vorfeld doch besser überlegen sollen, was er eigentlich benötigt und sich auch darüber informieren, sollen was es an geeigneten Programmen gibt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann durchaus einiges an Zeit in Anspruch nehmen aber Kosten sollten damit in der Regel keine anfallen.

M 2.81 VORAUSWAHL EINES GEEIGNETEN STANDARDSOFTWAREPRODUKTES**Relevanz für den Durchschnittsbenutzer: mittel**

siehe M 2.80.

M 2.94 FREIGABE VON VERZEICHNISSEN UNTER WINDOWS NT**Relevanz für den Durchschnittsbenutzer: mittel**

siehe M 2.7 und M 2.8.

M 2.111 BEREITHALTEN VON HANDBÜCHERN**Relevanz für den Durchschnittsbenutzer: hoch**

Handbücher sind für Durchschnittsbenutzer sehr wichtig, da in diesen doch viele Dinge erklärt werden, die der Durchschnittsbenutzer dann selbstständig erledigen kann, wenn ihm andere Informationsquellen nicht zur Verfügung stehen. Deshalb sollte der Durchschnittsbenutzer Handbücher auch so archivieren, dass er sie im Bedarf schnell findet.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Michael hat daheim ein ADSL-Modem über welches er sich ins Internet einwählt.

Eines Tages blinkt dies ganz seltsam und die Interneteinwahl funktioniert nicht mehr.

Michael hat das Handbuch des Modems aber entsorgt und weiß jetzt nicht was er tun kann.

Es wird wohl einige Zeit dauern bis Michael wieder im Internet surfen kann.

Hätte er das Handbuch noch gehabt, hätte er darin eine Anleitung gefunden wie man das ADSL-Modem in so einem Fall schnell wieder zum Funktionieren bringt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohen Kosten noch mit hohem Zeitaufwand verbunden.

M 2.112 REGELUNG DES AKTEN- UND DATENTRÄGERTRANSPORTS ZWISCHEN HÄUSLICHEM ARBEITSPLATZ UND INSTITUTION

Relevanz für den Durchschnittsbenutzer: keine bis hoch

Die Regelung ist von der IT-Leitung bzw. den IT-Sicherheitsbeauftragten zu erstellen. Wie wichtig die Regelung ist, hängt von der Art der transportierten Akten- bzw. den transportierten Datenträger ab. Die Regelung ist dann vom Durchschnittsbenutzer einzuhalten.

M 2.119 REGELUNG FÜR DEN EINSATZ VON E-MAIL

Relevanz für den Durchschnittsbenutzer: mittel

Die Regelung für den Einsatz von E-Mail muss an sich durch die IT-Leitung bzw. das IT-Sicherheitsmanagement festgesetzt werden. Die Umsetzung dieser Regelungen betrifft dann aber rein den Benutzer. Hier ein paar Beispiele mit Dingen auf die man beim Einsatz von E-Mail achten sollte.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Maria versendet ein E-Mail mit persönlichen Informationen. Versehentlich vertippt sie sich und schickt die E-Mail nicht an Andrea sondern an einen Andreas. Die E-Mail-Adresse gibt es auch zufällig und die E-Mail wird zugestellt. Marias Daten sind nun in den Händen eines wildfremden.

Beispiel 2: August versendet regelmäßig E-Mails an viele seiner Freunde und Bekannten. Er schreibt einfach alle Empfänger-Adressen in das Empfänger-Feld seines Email-Programms. August weiß nicht, dass die Empfänger die Adressen aller anderen Empfänger dann auch

sehen können. Dadurch gelangen etliche E-Mail-Adressen auf die Verteilerlisten von Spammern und die werden die Besitzer der Adressen werden darüber nicht erfreut sein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist ohne zusätzliche Kosten mit wenig Zeitaufwand umzusetzen.

M 2.138 STRUKTURIERTE DATENHALTUNG

Relevanz für den Durchschnittsbenutzer: mittel

Ähnlich wie in anderen Lebensbereichen, hilft es auch im IT-Bereich etwas Ordnung zu bewahren und das gilt auch beim Abspeichern von Daten. Ansonsten kann das zu Problemen führen wie das folgende Beispiel zeigt:

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Kurt ist leicht chaotisch und speichert alle seine Dokumente/Dateien, die er am Computer erstellt, immer in beliebigen Verzeichnissen ab. Dabei macht er keinen Unterschied ob es etwas Privates oder etwas Berufliches ist. Zudem wählt er beim Abspeichern auch noch wenig sprechende Namen für das was er gerade erstellt hat, wie etwa „Dokument1“ oder ähnlich nichtssagende Namen.

Das führt schon mal dazu, dass er wenn er eine Datei sucht, das einige Zeit in Anspruch nehmen kann.

Eines Tages bemerkt er, dass seine Festplatte Probleme macht und er beschließt ein Backup zu machen. Leider weiß er nur überhaupt nicht mehr wo die wichtigen Dateien jetzt liegen und verbringt viel Zeit damit dies erst mal herauszufinden. Er sichert ein paar Daten, aber dann geht die Festplatte schlussendlich kaputt. Viele Dateien wird Kurt jetzt nicht wiederbekommen können.

Das hätte er leicht vermeiden können hätte er die Daten besser strukturiert abgespeichert.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohem Zeitaufwand noch mit Kosten verbunden.

M 2.157 AUSWAHL EINES GEEIGNETEN COMPUTER-VIREN-SUCHPROGRAMMS

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme ist auf gewissen Systemen sehr wichtig. Für den Durchschnittsbenutzer sind dabei vor allem die Faktoren „Wirksamkeit des Virenschutz“, „Einfluss auf die Systemperformance“ und „Benutzerfreundlichkeit“ von dem Programm wichtig.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Anna hat kein Antivirenprogramm auf ihrem Computer installiert. Sie kriegt sehr viel Spam-E-Mails und da sie neugierig ist öffnet sie auch die meisten davon.

Leider sind viele dieser E-Mails mit Viren oder Trojanern verseucht und auf Annas PC sind deshalb sehr bald einige Computerviren zu finden.

Mit einem aktuellen Anti-Virenprogramm wäre das vermutlich nicht passiert.

Beispiel2: Gustav hat sich eine Antivirensoftware installiert, die er gefunden hat. Die Version der Software ist alt und es gibt keine Aktualisierungen mehr dafür. Aber Gustav denkt sich, dass die schon ausreichen wird. Dabei hat er nicht bedacht, dass regelmäßig neue Computerviren erschaffen werden und ohne eine Aktualisierung die Antivirensoftware einfach nichts taugt.

Also wundert sich Gustav wieso auf seinem Computer nach kurzer Zeit trotz der Antivirensoftware viele Viren zu finden sind.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen, wobei sich der Durchschnittsbenutzer bei der Auswahl der Antivirensoftware gut beraten lassen sollte.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert nicht viel Zeitaufwand, kann aber je nach Antivirensoftware mit Kosten verbunden sein.

M 2.159 AKTUALISIERUNG DER EINGESETZTEN COMPUTER-VIREN-SUCHPROGRAMME

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme ist für den Durchschnittsbenutzer deshalb sehr wichtig, da ohne eine Aktualisierung ein Antivirenprogramm kaum, oder nur unzureichend Schutz vor Viren bietet.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Konrad hat ein Antivirenprogramm, welches sich täglich aktualisieren will. Da Konrad die Aktualisierungsaufforderungen lästig findet, setzt er das Aktualisierungsintervall des Antivirenprogramms auf zwei Wochen hoch, sprich das Antivirenprogramm will sich nur noch im Abstand von zwei Wochen aktualisieren. Leider ist gerade ein neuer Computer-Virus im Umlauf und das Antivirenprogramm müsste aktualisiert werden, damit es diesen erkennt.

Die nächste Aktualisierung passiert aber erst in nicht ganz zwei Wochen und in der Zwischenzeit muss Konrad leider feststellen, dass deshalb der Virus seinen Rechner befallen konnte und dabei einige wichtige Daten ruiniert hat.

Da hätte Konrad wohl lieber die tägliche Aktualisierungsaufforderung in Kauf nehmen und täglich das Antivirenprogramm aktualisieren sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit geringem Zeitaufwand verbunden und kann Kosten verursachen (Aktualisierungskosten des Antivirenprogramms).

M 2.167 SICHERES LÖSCHEN VON DATENTRÄGERN**Relevanz für den Durchschnittsbenutzer: mittel**

Einem Durchschnittsbenutzer sollte vermittelt werden, dass das Löschen von Daten nicht immer gleichbedeutend ist mit „die Daten unwiederbringlich löschen“. Wo der Unterschied ist zeigt das folgende Beispiel.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Josef hat einige CDs mit wichtigen Firmendaten in der Sonne liegen lassen. Als er auf die Daten auf den CDs zugreifen will muss er feststellen, dass die CDs nicht mehr auf seinem Computer lesbar sind, da die CDs die viele Sonne offenbar nicht gut vertragen haben.

Josef wirft die kaputten CDs also einfach in den Papierkorb denn zum Glück hat er ja ein Backup der Daten auf seiner Festplatte.

Viktor vom Reinigungspersonal sieht das und nimmt unbeobachtet die CDs aus dem Papierkorb. Diese gibt er einem Freund der bei der Konkurrenzfirma arbeitet.

Dieser Freund kennt sich etwas mit Datenrettung aus und macht mit ein wenig Arbeit die CDs wieder lesbar. Jetzt hat die Konkurrenz sämtliche wichtigen Firmendaten.

Josef hätte die CDs nicht so sorglos wegwerfen dürfen, sondern hätte sie wohl vorher besser noch physisch zerstört (z.B. zerschnitten), dann wäre das nicht mehr gegangen.

Beispiel2: Erika will ihren Computer verkaufen. In dem Computer sind zwei Festplatten. Eine Festplatte funktioniert schon die längste Zeit nicht mehr, die andere funktioniert aber es befinden sich sehr persönliche Daten von Erika auf dieser Festplatte. Also formatiert sie die Festplatte bevor sie den Computer verkauft. Sie verkauft den Computer schließlich an einen alten Bekannten.

Dieser Bekannte kennt sich sehr gut mit Computern aus und da er neugierig ist, versucht er die gelöschten Daten wiederherzustellen, was ihm auch gelingt, da diese einfache Formatierung nicht ausreichend war um die Daten komplett zu löschen. Und es gelingt ihm sogar die kaputte Festplatte durch den Austausch einiger Komponenten wieder zum Laufen zu bekommen und kann dann auch die ganzen Daten von dort lesen. Auch auf dieser finden sich einige ältere, aber durchaus sehr persönliche Daten.

Da hätte Erika sich vorher schlau machen sollen, wie man die Daten richtig löscht, denn sie wird nicht sehr erfreut sein wenn sie erfährt, dass jetzt jemand so einfach ihre Daten hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen, allerdings benötigt es oft einiges an Zeit einem Durchschnittsbenutzer zu vermitteln, dass wenn Daten gelöscht wurden diese nicht zwangsläufig komplett verschwunden sind.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kostet teilweise einiges an Zeit aber ist nicht mit Kosten verbunden.

M 2.176 GEEIGNETE AUSWAHL EINES INTERNET SERVICE PROVIDERS

Relevanz für den Durchschnittsbenutzer: mittel

Wenn ein Durchschnittsbenutzer einen Internetzugang benötigt, sollte er sich im Vorfeld über den Internet Service Provider erkundigen, über den er den Internetzugang beziehen will, denn vor allem Zuverlässigkeit und Support sind bei verschiedenen Providern oft sehr unterschiedlich.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Tim hat sich einen Internetzugang über einen Internet Service Provider besorgt welcher diesen sehr billig angeboten hat. Leider muss Tim jetzt feststellen, dass es keine gute Idee war nur auf den Preis zu schauen. Es hat Wochen gedauert bis der Internetzugang freigeschalten wurde, die versprochene Bandbreite wird nur in absoluten Ausnahmefällen erreicht, es gibt regelmäßig Netzausfälle und der Support ist kaum erreichbar.

Da hätte sich Tim im Vorfeld doch besser informieren sollen und vielleicht eine etwas teurere aber bessere Alternative wählen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme benötigt etwas Zeit für die Recherchen ist aber nicht mit Kosten verbunden.

M 2.177 SICHERHEIT BEI UMZÜGEN**Relevanz für den Durchschnittsbenutzer: mittel**

Umzüge bergen auch für den Durchschnittsbenutzer die eine oder andere Gefahr, wie etwa das Kaputtgehen von Geräten infolge unsachgemäßen Transports oder dem Verlust von Datenträgern in der Hektik. Das folgende Beispiel soll zeigen was man machen bzw. nicht machen sollte.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1: Klaus ist gut aufgelegt, er zieht heute in eine neue Wohnung die ihm viel besser gefällt als seine alte. In der Vorfreude hat Klaus alles rasch, aber nicht besonders sorgfältig zusammengepackt. Seinen Computer hat er z.B. einfach ungeschützt in eine Kiste gestellt.

Als Klaus in seiner neuen Wohnung wieder den Computer anschließt und hochfahren will erlebt er nun eine böse Überraschung: Die teils groben Erschütterungen beim Transport des Computers haben sich nicht gut auf die Festplatte desselbigen ausgewirkt. Diese will nicht mehr hochfahren und da Klaus im Vorfeld kein Backup gemacht hat, hat er damit alle seine Daten verloren.

Jetzt ist Klaus natürlich sehr betrübt und das hätte er sich mit etwas mehr Sorgfalt beim Verpacken ersparen können.

Beispiel 2: Claudia zieht um und hat alle ihre wichtigen Daten, teils sensible Kundendaten, vorher auf DVDs gespeichert und in eine Kiste gepackt. Leider verläuft der Umzug ziemlich hektisch und wenig organisiert und ein Teil der DVDs verschwindet im Zuge dessen durch ein Loch welches in einer der Kisten war. Jetzt sind diese sensiblen Daten irgendwo und können in die falschen Hände geraten. Claudia ist jetzt natürlich sehr besorgt, sie hätte den Umzug wohl doch besser planen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand sollte sich für diese Maßnahme in Grenzen halten und auch die Kosten sollten wenn dann sehr moderat ausfallen.

M 2.189 SPERRUNG DES MOBILTELEFONS BEI VERLUST

Relevanz für den Durchschnittsbenutzer: hoch

Wenn ein Mobiltelefon verloren geht, muss in jedem Fall der Betreiber verständigt werden, damit dieser das Telefon sperren kann. Ansonsten kann das unguete Konsequenzen mit sich bringen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beim Verlust eines Mobiltelefons, muss man davon ausgehen, dass es ein Dritter in Besitz nehmen kann welcher einerseits unberechtigterweise an Daten kommt die darauf gespeichert sind bzw. andererseits mit dem Telefon jetzt irgendwohin telefonieren und so die Telefonrechnung massiv in die höhe treiben kann.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen und zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist einfach und sollte keine Kosten verursachen.

M 2.215 FEHLERBEHANDLUNG

Relevanz für den Durchschnittsbenutzer: gering

Für Durchschnittsbenutzer ist unmittelbar eigentlich nur relevant, dass er Fehler z.B. in einem Softwareprogramm umgehend melden sollte. Je länger Fehler ignoriert werden, desto schwerwiegender können die Auswirkungen für alle Betroffenen sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Daniel arbeitet regelmäßig mit einem Programm in seiner Firma, welches ihm Zugriff auf die firmeninterne Datenbank gewährt. Bei der Benutzung des Programms öffnet sich bei einigen Aktionen immer ein Fenster mit einer Fehlermeldung. Da Daniel aber problemlos weiterarbeiten kann wenn er diese wegeklickt macht er dies auch regelmäßig und meldet den Fehler nicht.

Was er dabei nicht weiß, der Fehler ist zwar für ihn nicht wichtig, aber zeigt an, dass er mit jeder Aktion einen Teil der Datenbank zerstört, auch wenn dieser Teil für ihn nicht wichtig ist.

So hat Daniel unwissentlich viele Daten zerstört.

Einige Kollegen die mit den Daten aber arbeiten müssen wird das gar nicht freuen.

Hätte Daniel den Fehler gleich gemeldet, hätte man das Problem schneller finden und beheben können und das das Schadensausmaß wäre viel geringer gewesen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen und zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist ohne hohen Zeitaufwand und ohne zusätzliche Kosten für den Durchschnittsbenutzer umzusetzen.

M 2.223 SICHERHEITSVORGABEN FÜR DIE NUTZUNG VON STANDARDSOFTWARE

Relevanz für den Durchschnittsbenutzer: gering

Die Sicherheitsvorgaben müssen von der IT-Leitung, dem IT-Sicherheitsmanagement und Administratoren ausgearbeitet werden. Der Durchschnittsbenutzer muss diese dann aber befolgen. Was passieren kann wenn diese nicht eingehalten werden, zeigt das folgende Beispiel.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Uwe muss in seiner Firma häufig Dokumente mittels eines Textverarbeitungsprogramms so zusammenkürzen, dass sensible Teile die nicht für die Öffentlichkeit bestimmt sind, nicht mehr darin sind. Danach muss er die überarbeitete Version an eine Presseagentur weiterschicken. Eine Sicherheitsrichtlinie zur Benutzung des Textverarbeitungsprogramms besagt, dass er das Dokument nicht im eigentlichen Dateiformat der Textverarbeitungssoftware weiterschicken darf, sondern dieses vorher in ein anderes vorbestimmtes Dateiformat umwandeln muss und dann erst weiter verschicken soll.

Da er es eines Abends eilig hat und das Umwandeln in dieses vorbestimmte Dateiformat so lange dauert, kürzt er einfach aus dem originale Dokument die sensiblen Teile heraus und verschickt dann das Dokument im Ursprungsformat an die Presseagentur.

Das war nur leider ein großer Fehler. Denn in diesem Ursprungsformat werden auch vorgenommene Änderungsvorgänge, die am Dokument gemacht wurden gespeichert, sprich die sensiblen Daten sind so immer noch darin enthalten und können leicht extrahiert werden. Jetzt hat er all die sensiblen Daten an die Presseagentur geschickt. Das wird wohl ein Nachspiel haben und alles nur weil er sich nicht an die Sicherheitsrichtlinien für die Nutzung von Standardsoftware gehalten hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer umzusetzen. Allerdings kann es schwierig sein dem Benutzer klar zu machen, wieso ein Abweichen von manchen Sicherheitsvorgaben unguete Folgen haben kann.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht keine zusätzlichen Kosten und erfordert vom Benutzer nur den Zeitaufwand für das Studieren der Sicherheitsvorgaben.

M 2.224 VORBEUGUNG GEGEN TROJANISCHE PFERDE

Relevanz für den Durchschnittsbenutzer: mittel/hoch

Die Vorbeugung gegen trojanische Pferde ist auf technischer Seite die Aufgabe der IT-Leitung, des IT-Sicherheitsmanagement und von Administratoren. Aber auch der Durchschnittsbenutzer muß hier sehr aufpassen und vor allem ein Mindestmaß an Misstrauen gegenüber Unbekanntem ist hier sehr wichtig. Was schief gehen kann, wenn man dieses Misstrauen nicht an den Tag legt, zeigt das folgende Beispiel.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Peter surft viel und gerne im Internet. Einen Virenschanner hat er nicht mehr, da ihm der alte zu lästig war, deshalb hat er ihn deaktiviert.

Eines Tages bekommt er eine E-Mail die von einem Freund zu sein scheint, zumindest ist dessen E-Mail-Adresse als Absender eingetragen.

In der Mail steht etwas von einem tollen Online-Spiel das er sich unbedingt installieren und ausprobieren soll.

Peter lädt also von der Seite das Spiel herunter und installiert es. Und da ist es auch schon passiert. In dem Spiel war ein Trojaner versteckt welches sein System in nächster Zeit massiv beeinträchtigen und beschädigen wird. Denn die E-Mail stammte nicht von seinem Freund, sondern war eine Spam-Mail die als Absender-Adresse zufällig die Adresse des Freundes benutzt hatte. Eigentlich hätte Peter das auffallen müssen, da sein Freund die Mails nie in so einem Stil verfasst. Hier war die Neugier zu groß und das Misstrauen zu klein.

Das wäre vermutlich nicht passiert, hätte er eine aktivierte und aktualisierte Anti-Viren-Software gehabt, da die den Trojaner womöglich erkannt hätte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen und auch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand ist minimal, Kosten entstehen in der Regel auch keine.

M 2.257 ÜBERWACHUNG DER SPEICHERRESSOURCEN VON ARCHIVMEDIEN**Relevanz für den Durchschnittsbenutzer: mittel**

Diese Maßnahme wird vom Sicherheitsmanagement umgesetzt. Für Durchschnittsbenutzer ist die Kernaussage dieser Maßnahme allerdings ebenfalls relevant, wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Sabine sichert die Daten auf der Festplatte ihres Computers immer auf eine externe Festplatte, um für den Notfall ein Backup zu haben. Dazu startet sie ein Backup-Kommando, welches ihr ein guter Freund aufgeschrieben hat. Eines Tages geht die Festplatte kaputt. Aber Sabine denkt sich, sie hat doch eh ein Backup und muss dann die Daten von dort einfach nur auf eine neue Festplatte spielen. Leider hat sie etwas nicht bedacht: Der Speicherplatz auf der externen Platte war schon seit Wochen voll und das

Backup-Kommando gibt keine Rückmeldung wenn die externe Festplatte voll ist und hat einfach die Daten nicht auf diese kopiert. Jetzt ist Sabine natürlich sehr betrübt da sie viele Daten verloren hat. Sie hätte wohl auch hin und wieder überprüfen müssen ob noch genug Platz auf der externen Festplatte vorhanden ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen und zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert wenig Zeit, kann allerdings Kosten für zusätzlich zu besorgende Datenträger verursachen.

M 2.273 ZEITNAHES EINSPIELEN SICHERHEITSRELEVANTER PATCHES UND UPDATES

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme kann auch den Durchschnittsbenutzer betreffen, sofern er nicht in einem Unternehmen arbeitet, in welchem diese Maßnahme durch einen IT-Beauftragten erledigt wird.

Eine Nichtbeachtung dieser Maßnahme kann unter Umständen böse Folgen haben, wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ferdinand schreibt viel und gerne E-Mails, allerdings benutzt er dazu ein Email-Programm, welches offenbar nicht besonders gut programmiert ist. Regelmäßig werden bei diesem Sicherheitsupdates benötigt, da bei diesem sehr oft Sicherheitslücken entdeckt werden.

Ferdinand nervt allerdings das Einspielen der Sicherheits-Updates und als er eine Funktion in dem Programm entdeckt, mit der man das Einspielen der Updates auf unbestimmte Zeit verschieben kann, benutzt er dies und spielt so über einen längeren Zeitraum keine vorhandenen Sicherheitsupdates mehr ein.

Leider haben ein paar böse Menschen sich mittlerweile daran gesetzt die Sicherheitslücken in dem sehr verbreiteten E-Mail-Programm auszunutzen um Spyware und sonstige Bösartigkeiten damit zu verbreiten. Dies machen sie mit Hilfe von MassenEmails. Ein so modifizierte E-Mail wird von dem betroffenen E Mail-Programm automatisch geöffnet und die Schadensroutine ausgeführt, sofern die Sicherheitsupdates nicht eingespielt wurden.

Auch Ferdinand kriegt dann eine dieser E-Mails und siehe da, sein Rechner macht plötzlich Probleme und viel Spyware befindet sich darauf. Das alles hätte sich Ferdinand ersparen können, hätte er die Sicherheitsupdates gleich eingespielt. Schließlich muss auch bedacht

werden, dass Sicherheitsupdates oft auch nicht sofort nach Bekanntwerden einer Sicherheitslücke veröffentlicht werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen. Man muss dem Durchschnittsbenutzer nur die Notwendigkeit des zeitnahen Einspielens von sicherheitsrelevanten Patches und Updates zur Kenntnis bringen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kostet üblicherweise nur etwas Zeit. Kosten sind damit meist keine verbunden.

M 2.306 VERLUSTMELDUNG

Relevanz für den Durchschnittsbenutzer: mittel/hoch

In einer Organisation sollte der Verlust von Dingen, wie etwa einem Notebook oder einem Memory-Stick mit z.B. sensiblen Daten darauf schnell gemeldet werden damit nicht mehr Schaden daraus entstehen kann.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Helmut hat einen USB-Stick des Unternehmens verloren. Da er zufällig privat einen USB-Stick desselben Typs besitzt, beschließt er einfach diesen ins Unternehmen mitzunehmen und sich privat einen neuen zu kaufen. Nur hat Helmut nicht bedacht, dass auf dem USB-Stick einige Passwörter von ihm und anderen Mitarbeitern abgespeichert waren.

Wenige Wochen später hat sich dann auch jemand von außen in die Unternehmenscomputer mit Helmut's Passwort einloggt und wichtige Daten kopiert und die IT-Abteilung hat dies bemerkt.

Jetzt haben sowohl das Unternehmen als auch Helmut ein Problem, welches er sich leicht ersparen hätte können, wenn er den Verlust sofort gemeldet hätte (dann hätte die IT-Abteilung rechtzeitig die Passwörter ändern können).

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kostet vielleicht etwas Zeit, sollte aber für den Durchschnittsbenutzer nicht mit Kosten verbunden sein.

M 2.313 SICHERE ANMELDUNG BEI INTERNET-DIENSTEN

Relevanz für den Durchschnittsbenutzer: gering/mittel

Die Anmeldung bei Internet-Diensten wird oft über einen Benutzernamen und ein Passwort gemacht. Wenn sich der Durchschnittsbenutzer den verwendeten Rechner mit anderen Benutzern teilen muss, ist es besonders wichtig, dass er diese Daten nicht leichtfertig irgendwo abspeichert oder aber Benutzernamen und Passwort schlecht wählt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Viktor meldet sich auf seinem Arbeits-PC täglich bei einem Internet-Dienst an, auf dem sensible Daten von ihm zu finden sind. Da Viktor aber ein sehr bequemer Mensch ist und nicht immer seinen Benutzernamen und sein Passwort eintippen will, hat er den Benutzernamen und das Passwort im Anmeldeprogramm abgespeichert.

Viktor muss sich den Arbeits-PC aber mit anderen Mitarbeitern teilen. Alle Mitarbeiter waren bisher so nett und haben das Anmeldeprogramm von Viktor nicht benutzt aber als ein neuer Mitarbeiter dazukommt, nutzt dieser die gespeicherten Anmeldedaten um sich Viktors Daten genau anzusehen. Wenn Viktor Pech hat, kommen diese Daten jetzt irgendwohin, wo sie nicht sein sollten.

Ein wenig mehr Vorsicht was seine Anmeldedaten betrifft hätte Viktor wohl an den Tag legen sollen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten treten bei dieser Maßnahme kein auf, einzig der Zeitaufwand wird etwas höher (z.B. die Zeit für das Eintippen von Benutzername und Passwort.)

M 2.323 GEREGLTE AUßERBETRIEBNAHME EINES CLIENTS

Relevanz für den Durchschnittsbenutzer: mittel

In erster Linie betrifft das die IT-Leitung und das IT-Sicherheitsmanagement. Aber auch den Durchschnittsbenutzer kann dies betreffen, wenn er z.B. einen alten Rechner ausmustert.

Es geht dabei vor allem um solche Dinge wie Datensicherung und zuverlässige Löschung der alten Daten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Thomas hat einen neuen PC gekauft und verkauft seinen alten. Nur dummerweise hat er dabei einen großen Fehler gemacht. Da das Betriebssystem auf dem alten Rechner nicht mehr hochfährt, hat er sich die noch vorhandenen Daten auf dem alten PC nicht angesehen, welche sich noch immer auf diesem befinden. Dadurch hat Thomas jetzt zwei Probleme: Auf dem alten Rechner waren ein Großteil seiner Passwörter abgespeichert (die der Käufer jetzt möglicherweise hat) und zudem waren auch noch Daten darauf, welche er nicht auf den neuen Rechner kopiert hat und von denen es kein Backup gibt.

Mit etwas mehr Vorsicht im Vorfeld hätte Thomas diesen Datenverlust und die unbeabsichtigte Weitergabe von Passwörtern an eine nicht näher bekannte Person vermeiden können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer zu vermitteln und auch nicht übermäßig schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert doch einiges an Zeit, verursacht aber in der Regel keine größeren Kosten.

M 2.340 BEACHTUNG RECHTLICHER RAHMENBEDINGUNGEN

Relevanz für den Durchschnittsbenutzer: gering/mittel

In einer Organisation bzw. einem Unternehmen sind dafür die Unternehmensleitung bzw. Vorgesetzte zuständig. Sollte der Durchschnittsbenutzer alleine an einem Projekt arbeiten, muss er sich Wohl oder Übel auch mit den rechtlichen Rahmenbedingungen befassen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte ein Durchschnittsbenutzer sich nicht mit den rechtlichen Rahmenbedingungen befassen, kann es passieren, dass er durch Unachtsamkeit rechtliche Probleme bekommt. Das betrifft vor allem die rechtlichen Bereiche Datenschutz und Urheberrecht, die aktuell auch immer wieder ein Thema sind.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Notwendigkeit dieser Maßnahme zu vermitteln dauert nicht lange.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist leider mit hohem Zeitaufwand verbunden, da die Gesetztestexte zu diesen Themen umfangreich sind und sich öfters auch ändern können und das auch tun.

M 2.384 AUSWAHL GEEIGNETER KRYPTOVERFAHREN FÜR WLAN

Relevanz für den Durchschnittsbenutzer: gering/mittel

Sollte sich ein Durchschnittsbenutzer z.B. einen WLAN-Router für daheim besorgen wird diese Maßnahme relevant. WLAN-Router bieten diverse Kryptoverfahren, also Verschlüsselungsverfahren, an um den Datenverkehr zwischen Endgerät und WLAN-Router zu verschlüsseln. Manche dieser Verfahren sind mittlerweile aber nicht mehr sicher und sehr leicht zu knacken. Deshalb sollte sich auch der Durchschnittsbenutzer informieren welches davon er einsetzen kann und von welchem er lieber die Finger lassen sollte.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Herbert hat sich günstig einen gebrauchten WLAN-Router gekauft und will diesen bei sich daheim einsetzen. Der WLAN-Router unterstützt auch einen Kryptoverfahren namens WEP. Toll denkt sich Herbert, so ist jetzt auch sein Datenverkehr sicher verschlüsselt und er kann in Ruhe im Internet surfen. Was Herbert nur nicht weiß: WEP ist äußerst unsicher und kann sehr schnell geknackt werden.

Und das macht auch sein neugieriger und lästiger Nachbar und kann so alles mitverfolgen was Herbert so im Internet macht. Genau sowas wollte Herbert ja eigentlich vermeiden, sehr ärgerlich, hätte aber leicht vermieden werden können, hätte sich Herbert im Vorfeld besser informiert.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht sehr schwer umzusetzen und auch nicht besonders schwer an den Durchschnittsbenutzer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme hält sich in Grenzen, aber sollte für ein sicheres Kryptoverfahren neue Hardware benötigt werden, können da durchaus einige Kosten anfallen.

M 2.389 SICHERE NUTZUNG VON HOTSPOTS

Relevanz für den Durchschnittsbenutzer: mittel

Hotspots sind Orte mit einem offenem WLAN über das man sich schnell und problemlos ins Internet einloggen kann. Hotspots findet man oft an solchen Orten wie Hotels, Flughäfen, Messehallen, Bahnhöfen etc. Wenn ein Durchschnittsbenutzer diese nutzt, dann bedenkt er aber oft eines nicht: Der Datenverkehr von seinem Computer (meist ein Notebook oder ein anderes mobiles Gerät) zu diesem Hotspot ist oft nicht verschlüsselt oder sonst wie geschützt. Dies kann natürlich ungute Konsequenzen mit sich bringen, wenn man darauf keine Rücksicht nimmt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Konrad ist auf Urlaub und hat sich in einem Hotel einquartiert. Praktisch bei diesem Hotel: Es gibt in diesem Hotspots, sodass Konrad mit seinem Notebook leicht ins Internet kann. Woran Konrad dabei aber nicht denkt: Diese Hotspots werden ohne Verschlüsselung oder sonstige Sicherheitsmaßnahmen betrieben. Konrad surft also ohne darauf zu achten vor sich hin, chattet mit Freunden und dabei werden auch sehr private Informationen ausgetauscht. Natürlich ruft Konrad auch seine E-Mails ab und schickt auch welche. Bei vielen seiner Aktionen muss er sein Passwort eintippen. Und das alles wird Konrad zum Verhängnis, da eine nicht sehr freundliche Person den ganzen unverschlüsselten, drahtlosen Datenverkehr mitgehört hat und so jetzt sehr viele Informationen über Konrad hat und z.B. dessen E-Mail-Account dazu benutzen kann Spam zu verschicken. Da hätte Konrad wohl besser nur Dienste im Internet verwenden sollen, die von vorneherein verschlüsselt sind oder aber auf manche Sachen einfach verzichtet, dann hätte das nicht passieren können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme(n) ist/sind nicht schwer umzusetzen aber diese im Detail an einen Durchschnittsbenutzer zu vermitteln kann unter Umständen schwierig werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kostet in der Regel Zeit aber kaum Geld.

M 2.393 REGELUNG DES INFORMATIONSAUSTAUSCHES

Relevanz für den Durchschnittsbenutzer: gering/mittel

Die Regelung des Informationsaustausches wird durch die Organisations-Leitung, die IT-Leitung und das IT-Sicherheitsmanagement festgelegt. Der Durchschnittsbenutzer muss sich dann an diese halten oder es kann unter Umständen böse für ihn ausgehen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Michael arbeitet an einem Projekt und hat die Anweisung über dieses nur mit gewissen Personen zu reden bzw. mit diesen Dokumente auszutauschen. Doch Michael ist diesbezüglich etwas nachlässig. Oft ist er bei Anna im Büro, eine Kollegin die er sehr schätzt, die aber an sich keinen Zugriff auf die besagten Dokumente haben sollte. Doch Michael unterhält sich immer so blendend mit Anna, also erzählt er ihr schon das eine oder andere über das Projekt. Leider vergisst er aber auch regelmäßig Dokumente bei Anna, was nach einiger Zeit auch seine Vorgesetzten mitbekommen. Schlecht für Michael: Anna ist leider eine sehr neugierige und zugleich sehr mitteilsame Person wodurch jetzt Projektinformationen an Leute gelangt sind, die sie nicht haben sollten. Als Konsequenz davon wurde Michael von dem Projekt abgezogen und entlassen. Das hätte er sich leicht ersparen können hätte er mehr auf diese Regelungen geachtet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist für den Durchschnittsbenutzer weder mit hohem Zeitaufwand noch mit hohen Kosten verbunden.

M 2.398 BENUTZERRICHTLINIEN FÜR DEN UMGANG MIT DRUCKERN, KOPIERERN UND MULTIFUNKTIONSGERÄTEN

Relevanz für den Durchschnittsbenutzer: gering/mittel

Für die Ausarbeitung solcher Richtlinien sind die IT-Leitung und das IT-Sicherheitsmanagement zuständig. Für die Umsetzung aber auch der Durchschnittsbenutzer. Das betrifft vor allem die Behandlung nicht abgeholter Dokumente, den Umgang mit sensiblen Dokumenten, die Auswahl eines Standarddruckers oder das Löschen des Kopierspeichers.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel 1:

Josef arbeitet in einem Büro in einer größeren Firma und muss des Öfteren auch sensible Daten wie Krankenakten bearbeiten und ausdrucken. In dieser Firma gibt es viele Drucker und die sind alle im Netzwerk verfügbar. Als Josef einmal nicht aufpasst druckt er sensible Dokumente auf einem anderen Drucker aus und er bemerkt es nicht. Er glaubt einfach es hätte nur nicht funktioniert und probiert es nochmal (diesmal am richtigen Drucker). Dummerweise sind die sensiblen Dokumente mit den Krankenakten beim ersten Mal doch ausgedruckt worden und jetzt liegen die Krankenakten von Herrn Huber offen in einem Drucker am Gang für jeden einsehbar herum. Das kann zu massivem Ärger führen.

Beispiel 2:

Franz arbeitet in einer Firma die auch viel mit sensiblen Kundendaten arbeitet.

Franz hat gerade ein unwichtiges Dokument ausgedruckt und findet im Drucker noch ein paar alte Ausdrücke von Kollegen, die offenbar nicht sauber ausgedruckt wurden (hässliche Streifen auf dem Papier). Gedankenverloren nimmt Franz die alten Ausdrücke und wirft sie ins Altpapier, bevor er seine Ausdrücke nimmt und wieder weggeht. Eines hat Franz nur nicht beachtet: Bei den fehlerhaften Ausdrücken handelte es sich um hochsensible Kundendaten und eigentlich sollten solche Ausdrücke fachgerecht mit dem Aktenvernichter zerkleinert werden. Jetzt wandern diese Daten normal in den Altpapiercontainer der öffentlich zugänglich ist. Und es gibt Leute die suchen genau solche unvorsichtig weggeworfenen Dokumente und dank Franz werden sie diesmal auch fündig werden und die Firma kann wegen der unbeabsichtigten Weitergabe bzw. dem Verlust der Kundendaten einige Probleme bekommen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

In der Regel sollte für diese Maßnahme maximal etwas Zeit notwendig sein (Einweisung) aber keine Kosten.

M 2.400 SICHERE AUßERBETRIEBNAHME VON DRUCKERN, KOPIERERN UND MULTIFUNKTIONSGERÄTEN

Relevanz für den Durchschnittsbenutzer: gering/mittel

Eine Sache die oft übersehen wird wenn man Drucker, Kopierer oder Multifunktionsgeräte außer Betrieb nehmen will: Diese haben oftmals einen internen Speicher und wenn mit den

Geräten sensible Daten ausgedruckt/kopiert wurden können sich diese noch immer auf diesem internen Speicher befinden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Gregor ist Mitglied einer Partei und hat oft Briefverkehr mit anderen Parteimitgliedern.

Viele brisante Themen hat er sich mit seinem tollen Multifunktionsgerät ausgedruckt bzw. kopiert, vor allem sehr viele Dokumente mit vertraulichem parteiinternem Wissen.

Nur jetzt hat er sich ein schnelleres und viel besseres Multifunktionsgerät gekauft und sein altes verkauft. Er hat dabei nur nicht daran gedacht, dass er den Speicher des Multifunktionsgerätes hätte löschen sollen. Und wie der Zufall so will wandert sein altes Gerät in die Hände eines Mitglieds einer konkurrierenden Partei und diese hat jetzt unglaublich detaillierte Einblicke in die Arbeitsweise und auch Geheimnisse von Gregors Partei bekommen. Diese wird nicht erfreut sein!

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer zu vermitteln noch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme benötigt etwas Zeit, sollte aber keine oder kaum Kosten verursachen.

M 2.401 UMGANG MIT MOBILEN DATENTRÄGERN UND GERÄTEN

Relevanz für den Durchschnittsbenutzer: mittel

Die Richtlinien für den richtigen Umgang mit mobilen Datenträger und Geräten müssen von der IT-Leitung und dem IT-Sicherheitsmanagement erstellt werden. Für die Umsetzung ist dann aber auch der Durchschnittsbenutzer zuständig. Dies betrifft solche Punkte wie: Welche Daten dürfen überhaupt auf welchem Gerät gespeichert sein? Welche Geräte dürfen von wem genutzt werden? Mit welchen externen Geräten/Datenträgern dürfen Daten ausgetauscht werden?

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ralf hat von seiner Firma ein Notebook zur Verfügung gestellt bekommen. Auch hat Ralf eine schriftliche Richtlinie vorgelegt bekommen, wie er mit diesem Notebook umzugehen hat. Ralf war nur zu faul sich diese auch durchzulesen. Er hat viele Daten von der Arbeit auf das Notebook kopiert, da er auf diesem deutlich besser arbeiten kann, als auf dem lahmen

Arbeits-PC, an dem er normalerweise sitzen müsste. Er benutzt das Notebook auch privat und speichert darauf auch Videos und Musikstücke die ihm Freunde auf USB-Stick mitbringen. Auf einem dieser USB-Sticks war nur leider ein Virus und den hat Ralf so auf das Notebook geladen und am Ende wurde der Virus von dort unbemerkt auf die Arbeitsrechner übertragen. Als ihm dann das Notebook auch noch gestohlen wird und herauskommt was er alles mit dem Notebook gemacht hat, droht Ralf ziemlich großer Ärger. Das hätte Ralf alles vermeiden können hätte er sich die Richtlinien zum Umgang mit mobilen Datenträgern und Geräten durchgelesen und sich auch daran gehalten hätte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer zu vermitteln und auch nicht schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten sollten in der Regel keine anfallen. Bis der Durchschnittsbenutzer aber für alle Gefahrenbereiche sensibilisiert ist, kann etwas Zeit vergehen.

M 2.430 SICHERHEITSRICHTLINIEN UND REGELUNGEN FÜR DEN INFORMATIONSSCHUTZ UNTERWEGS

Relevanz für den Durchschnittsbenutzer: mittel

Die Regelungen- und Richtlinien aufzustellen ist Sache von IT-Sicherheitsbeauftragten.

Für die Durchführung bzw. Einhaltung dieser Regelungen ist der Durchschnittsbenutzer selbst verantwortlich und wenn man unterwegs ist, besonders bei Reisen ins Ausland, gibt es einige Dinge auf die man aufpassen sollte. Diese Maßnahme ist sehr ähnlich wie die Maßnahmen aus M 2.401 (Umgang mit mobilen Datenträgern und Geräten), sprich welche Daten dürfen wo mitgeführt werden, wie beaufsichtigt man seine Datenträger bzw. wie verwahrt man mobile Datenträger richtig und hinzu kommen die gesetzlichen Rahmenbedingungen im Ausland die sich doch gröber von den gewohnten unterscheiden können (Stichwort: Zensur, etc.)

M 3 MAßNAHMENKATALOG PERSONAL

Dieser Maßnahmenkatalog behandelt alle Sicherheitsmaßnahmen die wichtig sind, wenn verschiedene Leute zusammen arbeiten.

Diese Maßnahmen beginnen bei der Einweisung neuer Mitarbeiter und behandeln wichtige Maßnahmen wie Schulungen der beteiligten Personen sowie das Aufstellen von Verhaltensregeln, bis hin zum richtigen Verhalten beim Ausscheiden von Mitarbeitern.

M 3.1 GEREGELTE EINARBEITUNG/EINWEISUNG NEUER MITARBEITER

Relevanz für den Durchschnittsbenutzer: mittel

Diese Maßnahme ist für Durchschnittsbenutzer in zweierlei Hinsicht interessant, nämlich wenn er selbst einen neuen Mitarbeiter einweisen muss oder aber neu eingewiesen wird. Was passieren kann wenn dies nicht korrekt erfolgt, zeigt das folgende Beispiel.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Jens soll Maria an ihrem neuen Arbeitsplatz einweisen und ihr die Programme erklären, mit denen sie in nächster Zeit arbeiten soll. Jens ist nur nicht besonders motiviert und erklärt nur halbherzig ein paar Dinge und diese auch noch viel zu schnell. Einige wichtige Punkte lässt er dabei ganz aus. In den nächsten Wochen kommt es immer wieder zu Problemen, weil Maria trotz bester Absichten oft etwas falsch macht und dann alles nachkorrigiert werden muss, bzw. Maria einfach manche Sachen viel zu umständlich angeht.

Hätte Jens alles richtig und in Ruhe erklärt, würde es jetzt besser in der Arbeit vorangehen und auch Maria müsste nicht ständig mit solchen Problemen kämpfen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht schwer an einen Durchschnittsbenutzer zu vermitteln. Die Umsetzung braucht aber etwas Planung. Schließlich muss zuerst festgestellt werden, was bei der Einweisung gezeigt werden soll und wie man es erklärt, sodass es das Gegenüber auch versteht.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand kann durchaus höher sein, Kosten sollten jedoch keine großen dabei entstehen.

M 3.2 VERPFLICHTUNG DER MITARBEITER AUF EINHALTUNG EINSCHLÄGIGER GESETZE, VORSCHRIFTEN UND REGELUNGEN

Relevanz für den Durchschnittsbenutzer: mittel

Der Durchschnittsbenutzer sollte die Gesetze, Vorschriften und Regelungen zumindest einmal gehört haben und diese hin und wieder wiederholen, ansonsten kann das unguete Folgen haben, wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Bert ist für die Aufbewahrung von Datenträgern und den Kameras in einer Firma zuständig. Die Vorschriften würden eigentlich vorsehen, dass er alles genau inventarisiert, eine Liste darüber führt, wo was gerade ist und alle Datenträger bzw. Kameras in einem dafür vorgesehenen Kasten versperrt. Bert beschäftigt sich aber lieber mit anderen Sachen und nimmt die Sache eher locker, vernachlässigt die Inventarisierung und lässt viele Datenträger und Kameras auch einfach so herumliegen. Eines Tages wird dann von höherer Stelle überprüft, ob alles in Ordnung ist und da kommt Bert in Bedrängnis, denn die Inventarliste stimmt überhaupt nicht mit dem überein, was vorhanden ist, einige Datenträger mit teils sensitiven Daten fehlen überhaupt ganz und auch zwei Kameras die eigentlich hier sein sollten sind weg.

Bert kriegt deshalb massiv Ärger, welchen er sich ersparen hätte können, wenn er sich an die Vorschriften gehalten hätte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Das hängt ganz vom Umfang der Vorschriften und der für den Durchschnittsbenutzer relevanten Gesetze im konkreten Fall ab. Das Wichtigste sollte aber relativ leicht zu vermitteln sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Je nach Umfang der Vorschriften wird der Durchschnittsbenutzer mehr oder weniger Zeit benötigen um diese zu verstehen. Kosten sollten dabei aber kaum welche anfallen.

M 3.3 VERTRETUNGSREGELUNGEN

Relevanz für den Durchschnittsbenutzer: gering

Diese Maßnahme betrifft in erster Linie Vorgesetzte und zumeist nicht den Durchschnittsbenutzer. Sollte der Durchschnittsbenutzer aber in die Situation kommen, für

sich selbst eine Vertretung organisieren zu müssen, dann könnte dieser Punkt wichtig werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Jürgen fährt auf Urlaub und hat Hans als seine Vertretung bestimmt. Leider hat Jürgen in der ganzen Urlaubseuphorie etwas Entscheidendes vergessen: Hans beherrscht zwar alles um die Aufgaben erledigen zu können, nur dummerweise hat Jürgen ihm nur den Schlüssel für das Büro gegeben, nicht aber die benötigten Passwörter gesagt. Da Jürgen zudem keinen Handy-Empfang im Urlaub hat, wird Hans wohl nicht viel in dessen Abwesenheit machen können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Nein, die Maßnahme ist leicht an einen Durchschnittsbenutzer zu vermitteln und auch nicht besonders schwer umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Suche nach einer geeigneten Vertretung und der Überlegung, was man diese alles machen last, wird etwas Zeit in Anspruch nehmen. Kosten sollten dabei aber meist keine entstehen.

M 3.4 SCHULUNG VOR PROGRAMMNUTZUNG

Relevanz für den Durchschnittsbenutzer: mittel

siehe auch M 3.1

M 3.5 SCHULUNG ZU IT-SICHERHEITSMABNAHMEN

Relevanz für den Durchschnittsbenutzer: hoch

Der Punkt Schulung ist für Durchschnittsbenutzer extrem wichtig, da viele Gefahren vermieden werden können wenn man im Vorfeld schon über diese Bescheid weiß.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Helga ist neu in der Firma und sollte eigentlich vom IT-Sicherheitsbeauftragten eingeschult werden. Dies ist leider aus unerfindlichen Gründen nicht geschehen. In der Folgezeit macht Helga deshalb aus Unwissenheit einige schwerwiegende Fehler. Zum Beispiel deaktiviert sie die installierte Firewall, weil sie, wenn diese läuft, ihr Lieblingschatprogramm

nicht benutzen kann. Auch die Antivirus-Software auf ihrem Computer deaktiviert sie weil ihrer Meinung nach die Textverarbeitungssoftware so langsam wird, wenn die Antivirus-Software aktiviert ist.

Kurze Zeit später hat sie mehrere Viren und Trojaner auf dem Computer mit dem Resultat, dass viele wichtige Daten kaputt sind bzw. der Computer nicht mehr funktioniert und möglicherweise auch wichtige Passwörter an Unbefugte gelangt sind. Und ein Backup von den kaputten Daten hat sie auch keines, da ihr niemand erklärt hat, dass sie regelmäßig ein Backup machen muss und ihr erst recht keiner gezeigt hat, wie man das richtig macht.

Alles das hätte mit einer Schulung im Vorfeld verhindert werden können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es kommt sehr auf die Menge der Maßnahmen an, die vermittelt werden sollen, aber die Notwendigkeit einer Schulung zu IT-Sicherheitsmaßnahmen wird der Durchschnittsbenutzer schnell einsehen. Manche Maßnahmen sind anfangs nicht so leicht zu vermitteln, da dem Benutzer das Problembewusstsein fehlt. Dieses soll mit der Schulung aber ebenfalls aufgebaut werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kostet dem Durchschnittsbenutzer in jedem Fall Zeit und kann unter Umständen auch mit höheren Kosten für die Schulungen verbunden sein, abhängig davon wie viel Wissen vermittelt werden soll.

M 3.6 GEREGELTE VERFAHRENSWEISE BEIM AUSSCHIEDEN VON MITARBEITERN

Relevanz für den Durchschnittsbenutzer: mittel

Dieser Punkt kann unter Umständen für Durchschnittsbenutzer in einer leitenden Funktion wichtig sein. Denn auch wenn man selbst nicht viel Ahnung von IT hat, sollte man sich darüber im Klaren darüber sein, dass bei Nichteinhaltung Probleme entstehen können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Urban ist der Leiter der Finanzabteilung in einer Firma. Er hatte bis vor kurzem einen Kollegen namens Hugo. Dieser wurde jedoch gekündigt aber niemand hat es für nötig befunden eine Verfahrensweise zu erstellen, was passieren soll, wenn ein Mitarbeiter aus dem Unternehmen ausscheidet. Zwei Wochen ist es schon her das Hugo gekündigt worden ist. Urban muss voller Schrecken bemerken, dass plötzlich alle Finanzdaten der letzten Monate am Computer gelöscht worden sind. Man hat Hugo den Zugang nicht gesperrt und dieser hat in seiner Wut über die Entlassung sich dort jetzt am Firmencomputer ausgetobt.

Das wäre nicht passiert wenn es Regeln gegeben hätte, was passieren muss, wenn ein Mitarbeiter aus dem Unternehmen ausscheidet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Warum man das machen muss ist einem Durchschnittsbenutzer durchaus leicht zu vermitteln. Die Umsetzung erfordert aber doch entsprechende Planung.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten sollten für diese Maßnahme keine anfallen, Zeit muss aber durchaus investiert werden.

M 3.8 VERMEIDUNG VON STÖRUNGEN DES BETRIEBSKLIMAS

Relevanz für den Durchschnittsbenutzer: mittel

Wenn man mit anderen Menschen zusammenarbeitet oder von diesen abhängt, ist ein gutes Betriebsklima auch für den Durchschnittsbenutzer sehr relevant. Ein schlechtes Betriebsklima kann auch massiv die Arbeit selbst beeinflussen, wie das folgende Beispiel zeigt:

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Kurt und Heinz arbeiten im selben Büro nur verstehen sich aber in letzter Zeit nicht besonders gut. Kurt nimmt normalerweise Kundenwünsche entgegen und notiert diese und Heinz bearbeitet diese dann. Da die Kundenwünsche oft ausgefallen sind und nicht immer ganz klar ist, wie so mancher Wunsch gemeint war, wenn Kurt etwas notiert hat, haben sich Kurt und Heinz in der Vergangenheit immer zusammengesetzt und darüber geredet wenn etwas unklar war. Da Heinz und Kurt aber jetzt nicht mehr miteinander reden wollen kommt es infolge des schlechten Betriebsklimas dazu, dass manche Aufgaben gar nicht oder falsch bearbeitet werden, sensible Dateien des anderen schlampig/unsachgemäß verwahrt werden und manche Kundenwünsche schlichtweg nicht erledigt werden. Keine gute Situation für die Firma.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Notwendigkeit der Vermeidung von Störungen des Betriebsklimas ist einem Durchschnittsbenutzer sicher leicht zu vermitteln. Die Umsetzung kann entweder sehr leicht, oder auch sehr schwer sein, das hängt von den beteiligten Personen ab.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann abhängig von den beteiligten Personen mit viel Zeitaufwand verbunden sein.

Kosten sollten dabei aber kaum anfallen.

M 3.9 ERGONOMISCHER ARBEITSPLATZ**Relevanz für den Durchschnittsbenutzer: hoch**

Diese Maßnahme betrifft den Durchschnittsbenutzer sehr direkt und soll deshalb keinesfalls vernachlässigt werden. Kurzzeitig mag man sich darüber vielleicht keine Gedanken machen und es als Unsinn abtun, langfristig gesehen ist diese Maßnahme jedoch sehr wichtig.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ulrike ist Sekretärin in einem Büro. Der Arbeitsplatz ist nicht optimal eingerichtet.

Der Sessel ist zu niedrig, die Position des Monitors dafür zu hoch. Zudem ist hinter Ulrikes Sitzplatz ein Fenster wo an sonnigen Tagen die Sonnenstrahlen vom Monitor reflektiert werden und das Arbeiten am Bildschirm erschweren. Ulrike denkt sich aber nichts dabei, denn da darf man doch nicht so zimperlich sein. Das geht auch zwei Jahre gut. Danach hat Ulrike nur plötzlich Probleme mit den Knien, ihr Hals ist ständig verspannt und ihre Augen tun weh.

Das passiert eben, wenn man nicht auf Ergonomie am Arbeitsplatz achtet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Man benötigt üblicherweise etwas Zeit um einem Durchschnittsbenutzer beizubringen, was es mit Ergonomie auf sich hat. Die Maßnahme kann unter Umständen auch nicht so leicht umzusetzen sein wenn z.B. Platzmangel herrscht oder es keine passenden Möbel gibt.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme umzusetzen benötigt etwas Zeit und kann je nach Ausgangssituation auch mit höheren Kosten verbunden sein (z.B. wenn man neue Möbel anschaffen muss).

M 3.10 AUSWAHL EINES VERTRAUENSWÜRDIGEN ADMINISTRATORS UND VERTRETERS**Relevanz für den Durchschnittsbenutzer: hoch**

Ein Durchschnittsbenutzer muss sich in der IT nicht mit allem auskennen, aber wenn man Hilfe von anderen in Anspruch nimmt, dann sollte man sich vergewissern, dass diese Personen sich nicht nur auskennen, sondern dass man ihnen auch vertrauen kann.

Dasselbe gilt auch für die Wahl eines Vertreters wenn man z.B. auf Urlaub fährt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Emil will die Programme auf seinem Rechner aktualisieren. Leider weiß er nicht wie dies geht, also fragt er Hans, der sich damit sehr auskennt. Da Emil noch einen Termin hat, lässt er Hans alleine die Aktualisierung an seinem Computer machen und gibt ihm sein Passwort. Hans ist nur leider sehr neugierig und zudem auch geschwätzig. In Emils Abwesenheit liest er dessen E-Mails und studiert ein paar persönliche Dokumente während er die Aktualisierungen durchführt.

Emil kommt zurück und ist glücklich, dass die Aktualisierung erfolgreich war.

Nur wenige Wochen später fragt er sich, wieso so viele Leute private Dinge von ihm wissen die er niemandem weitererzählt hat. Was er nicht weiß: Hans war sehr geschwätzig in letzter Zeit und wenig vertrauenswürdig.

Da hätte Emil sich wohl doch lieber an jemanden wenden sollen, der vertrauenswürdiger ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist nicht mit hohem Zeitaufwand oder hohen Kosten verbunden. Eine gute Menschenkenntnis schadet hier allerdings sicher nicht.

M 3.12 INFORMATION ALLER MITARBEITER ÜBER MÖGLICHE TKWARNANZEIGEN, -SYMBOLE UND -TÖNE

Relevanz für den Durchschnittsbenutzer: mittel

Für einen Durchschnittsbenutzer kann es wichtig sein zu wissen was die Anzeigen oder Geräusche an einem TK-Gerät bedeuten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ingrid hat eine neues Telefon an ihrem Arbeitsplatz bekommen. Dieses Telefon besitzt eine eingebaute Freisprecheinrichtung, wovon Ingrid aber nichts weiß. Einmal ruft ein Kunde an, der ziemlich unangenehm ist und etwas erfragen will. Ingrid weiß es auf Anhieb

nicht und deckt den Hörer ab damit der Kunde nichts hört und fragt bei Kolleginnen nach und im Zuge des Gesprächs fallen einige wenig schmeichelhafte Bemerkungen über den Kunden, offenbar kennt man den hier schon genauer. Was Ingrid nicht weiß: Sie hat aus Versehen den Knopf für die Aktivierung der Freisprecheinrichtung erwischt, seitdem blinkt ein rotes Licht auf und der Kunde hat dieses Gespräch in vollem Umfang mithören können. Das hat dann natürlich entsprechende unangenehme Konsequenzen.

Das wäre nicht passiert, hätte Ingrid mehr über die Funktionen des neuen Telefons gewusst und hätte sie gewusst, dass das rote Blinken bedeutet, dass die Freisprecheinrichtung aktiviert ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme sollte ihm Regelfall weder mit hohen Kosten noch mit übermäßig hohem Zeitaufwand verbunden sein.

M 3.13 SENSIBILISIERUNG DER MITARBEITER FÜR MÖGLICHE TKGEFÄHRDUNGEN

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 3.5

M 3.14 EINWEISUNG DES PERSONALS IN DEN GEREGLTEN ABLAUF DER INFORMATIONSGEBUNG UND DES DATENTRÄGERAUSTAUSCHES

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 3.5

M 3.15 INFORMATIONEN FÜR ALLE MITARBEITER ÜBER DIE FAXNUTZUNG

Relevanz für den Durchschnittsbenutzer: gering

Sollte ein FAX vorhanden sein und der Durchschnittsbenutzer damit arbeiten müssen, sollte er zumindest über die grundlegenden Probleme informiert werden, die sicherheitstechnisch bei einem FAX vorkommen können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Ulrich will sensible Daten an eine andere Firma faxen. Da das Faxgerät einige Zeit braucht, bis es die vielen Seiten übertragen hat, geht sich Ulrich in der Zwischenzeit einen Kaffee machen. Woran er aber nicht gedacht hat: Das Fax-Gerät steht offen im Sekretariat und jeder der hereinkommt sieht, welche Dokumente darin liegen. Und auch auf der Gegenseite bei der anderen Firma gibt es ein ähnliches Problem: das Fax ist dort ungünstig aufgestellt und auch dort kann jeder, der daran vorbeikommt sehen, was über das Fax geschickt wird und sogar die übertragenen Seiten einfach mitnehmen. Zudem wird nur hin und wieder überprüft, ob eine neue Faxnachricht gekommen ist. So kann es aber sehr leicht passieren, dass diese sensiblen Daten an unbefugte Personen gelangen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme sollte kaum Zeit in Anspruch nehmen und auch keine Kosten verursachen.

M 3.16 EINWEISUNG IN DIE BEDIENUNG DES ANRUFBEANTWORTERS

Relevanz für den Durchschnittsbenutzer: gering

Wenn ein Anrufbeantworter vorhanden ist und der Durchschnittsbenutzer damit arbeiten muss, dann sollte er ähnlich wie bei der Faxnutzung darüber Bescheid wissen, was aus sicherheitstechnischer Sicht passieren kann.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Irene hat einen neuen Anrufbeantworter in ihrem Büro. Da sie oft im Außendienst arbeitet, hat sie sich es zur Angewohnheit gemacht allen Leuten zu sagen, sie sollen ihr alle ihre Wünsche/Beschwerden auf ihren Anrufbeantworter sprechen.

Irene hat dabei leider ein paar Dinge nicht bedacht. Zum einen kann der Anrufbeantworter nur eine limitierte Gesprächszeit aufzeichnen, also können möglicherweise wichtige Informationen so nicht an sie weitergegeben werden wenn die Aufzeichnungskapazität des Anrufbeantworters bereits überschritten ist. Auf der anderen Seite ist ihr Büro nicht speziell gesichert, also hat theoretisch jeder die Möglichkeit ihren Anrufbeantworter abzuhören und die Nachrichten darauf einfach zu löschen. Das kann zu Problemen führen, wenn sensible Daten auf diese Art weitergegeben werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme sollte kaum Zeit in Anspruch nehmen und auch keine Kosten verursachen.

M 3.17 EINWEISUNG DES PERSONALS IN DIE MODEM-BENUTZUNG**Relevanz für den Durchschnittsbenutzer: mittel**

Sollte der Durchschnittsbenutzer mit einem Modem zu tun haben und es bei diesem in Sachen Sicherheit einige Dinge zu klären geben, gilt dasselbe wie bei M 3.5.

M 3.18 VERPFLICHTUNG DER BENUTZER ZUM ABMELDEN NACH AUFGABENERFÜLLUNG**Relevanz für den Durchschnittsbenutzer: hoch**

Dieser Punkt ist für Durchschnittsbenutzer wichtiger als diese oft vermuten. Warum zeigt das folgende Beispiel.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Gustav arbeitet oft mit einem Programm zur Finanzverwaltung des Unternehmens in welchem er arbeitet. Wenn er damit fertig ist, meldet er sich aus dem Programm aber nicht ab, da das An- und Abmelden ja immer einiges an Zeit benötigt. Stattdessen sperrt er einfach nur den PC, oder dreht manchmal einfach nur den Bildschirm ab und lässt den PC weiter laufen.

Ein schwerer Fehler wie sich herausstellen wird. Helge ist gerade furchtbar sauer auf das Unternehmen und plant zu kündigen. Ihm fällt auf das der PC von Gustav noch immer läuft und nur der Bildschirm ausgeschaltet ist. Er schaltet ihn wieder ein und siehe da, das Finanzverwaltungsprogramm des Unternehmens ist da ja noch offen und der Benutzer „Gustav“ ist noch angemeldet. Also beschließt Helge dem Unternehmen noch ein paar „Abschiedsgeschenke“ in der Finanzverwaltung zu hinterlassen.

Einige Tage später werden die Veränderungen bemerkt und Gustav bekommt riesige Probleme, weil das mit seinem Account passiert ist und das Unternehmen bekommt Probleme weil vieles in der Finanzverwaltung jetzt nicht mehr passt.

Alles das nur deshalb, weil sich Gustav bei dem Finanzverwaltungsprogramm nicht abgemeldet hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme sollte kaum Zeit in Anspruch nehmen und auch keine Kosten verursachen.

M 3.21 SICHERHEITSTECHNISCHE EINWEISUNG DER TELEARBEITER

Relevanz für den Durchschnittsbenutzer: hoch

siehe M 3.5.

M 3.26 EINWEISUNG DES PERSONALS IN DEN SICHEREN UMGANG MIT IT

Relevanz für den Durchschnittsbenutzer: hoch

Es gilt dasselbe wie bei M 3.5.

M 3.44 SENSIBILISIERUNG DES MANAGEMENTS FÜR IT-SICHERHEIT

Relevanz für den Durchschnittsbenutzer: hoch

Prinzipiell gilt dasselbe wie bei Punkt M 3.5.

M 3.46 ANSPRECHPARTNER ZU SICHERHEITSFragen

Relevanz für den Durchschnittsbenutzer: mittel

Der Durchschnittsbenutzer sollte wissen, wen er ansprechen kann wenn er Fragen zum Thema Sicherheit hat. Auch sollte er keine Scheu haben bei Fragen den Ansprechpartner zu kontaktieren.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Lydia hat seit kurzem Probleme mit dem Computer. Dieser stürzt hin und wieder ab und auch seltsame Fehlermeldungen erscheinen regelmäßig auf ihrem Bildschirm. Aus Angst sie hätte etwas falsch gemacht, traut sie sich aber nicht an den Ansprechpartner für Sicherheitsfragen zu wenden. Da sie nichts tut, nehmen die Dinge aber ihren Lauf. Sie hat nämlich einen Virus auf ihrem Computer und dieser verbreitet sich dann auf Memory-Sticks

und andere Speichermedien, sowie andere Computer im Netzwerk bis das Problem von einer Kollegin entdeckt wird.

Das alles hätte verhindert werden können wenn sich Lydia gleich am Anfang getraut hätte den Ansprechpartner für Sicherheitsfragen zu konsultieren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist weder schwer umzusetzen noch schwer zu vermitteln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist weder mit hohem Zeitaufwand noch mit hohen Kosten verbunden.

M 3.47 DURCHFÜHRUNG VON PLANSPIELEN ZUR IT-SICHERHEIT

Relevanz für den Durchschnittsbenutzer: mittel

siehe M 3.5

M 3.58 EINFÜHRUNG IN WLAN-GRUNDBEGRIFFE

Relevanz für den Durchschnittsbenutzer: hoch

WLAN wird immer wichtiger und ist immer weiter verbreitet. Also sollte auch ein Durchschnittsbenutzer zumindest grundlegend wissen wann ihre Verbindung zum WLAN besser gesichert ist und wann weniger. Siehe auch M 3.5.

M 3.59 SCHULUNG ZUM SICHEREN WLAN-EINSATZ

Relevanz für den Durchschnittsbenutzer: hoch

Siehe auch M 3.5.

M 3.60 SENSIBILISIERUNG DER MITARBEITER ZUM SICHEREN UMGANG MIT MOBILEN DATENTRÄGERN UND GERÄTEN

Relevanz für den Durchschnittsbenutzer: hoch

Mobile Datenträger und Geräte werden immer verbreiteter und wichtiger in unserer Welt. Das ist in vielen Bereichen äußerst praktisch, aber es ergeben sich dadurch auch neue Probleme, wie das folgende Beispiel zeigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Beispiel: Peter hat einen neuen MP3-Player mit viel Speicherplatz darauf. Eines Tages will er in der Arbeit sensible Daten auf den dafür vorgesehenen Memory-Stick überspielen um sie dann mit nach Hause zu nehmen. Leider hat er den Memory-Stick vergessen also beschließt er die Daten inzwischen einfach auf seinen MP3-Player zu überspielen, schließlich ist auf diesem noch genug Speicherplatz über. Zu Hause angekommen überspielt er dann die Daten auf seinen privaten PC, vergisst aber die Daten auf dem MP3-Player zu löschen.

Einige Wochen später wird Peter von Julia gefragt ob sie sich seinen MP3-Player für ein paar Tage ausleihen darf und Peter stimmt zu. Als Julia den MP3-Player daheim hat und an ihren PC ansteckt findet sie neben den vielen Musikstücken die darauf sind auch die sensiblen Daten und da sie neugierig ist kopiert sie diese auf ihren PC und studiert sie intensiv. Da sie eine ziemliche Klatschtante ist wird es wohl nicht lange dauern bis mehr Leute davon wissen. Alles nur deshalb weil Peter nicht aufgepasst hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Notwendigkeit der Maßnahme ist leicht zu vermitteln und auch umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten fallen zwar keine an, aber der Zeitaufwand bis ein Durchschnittsbenutzer alle Probleme verstanden hat, die beim Einsatz mit mobilen Datenträgern/Geräten auftreten können, kann höher sein.

M 3.63 SCHULUNG DER BENUTZER ZUR AUTHENTISIERUNG MIT HILFE VON VERZEICHNISDIENSTEN

Relevanz für den Durchschnittsbenutzer: mittel

Sofern Verzeichnisdienste eingesetzt werden ist dies auch für den Durchschnittsbenutzer relevant und es gilt dasselbe wie bei M 3.1, M 3.4 und M 3.5.

M 4 MAßNAHMENKATALOG HARDWARE UND SOFTWARE

Der Maßnahmenkatalog 4 befasst sich mit Sicherheitsaspekten unter besonderer Berücksichtigung bestimmter Hard- und Softwarekomponenten. Insbesondere werden hier Betriebssysteme, einzelne Serverdienste (Web, Mail, Directory) hinsichtlich bekannter Gefahrenquellen analysiert, um gezielt Sicherheitslücken zu schließen.

M 4.1 PASSWORTSCHUTZ FÜR IT-SYSTEME

Relevanz für den Durchschnittsbenutzer: hoch

Ein Passwort ist eine gute Methode zumindest für eine gewisse Zeit unbefugte vom Zugriff auf sensible Daten abzuhalten. Es ist dabei insbesondere auf die Stärke des Passwortes zu achten. Als Grundregel gilt es sowohl Klein-, als auch Großbuchstaben, Sonderzeichen und Ziffern in einem Passwort zu verwenden. Keinesfalls dürfen Wörter aus einem Wörterbuch, (abgewandelte) Benutzernamen, Geburtsdaten oder die Namen von Kindern oder Haustieren als Passwort verwendet werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne ein (ausreichende komplexes) Passwort ist es für Unberechtigte einfach Zugriff auf Daten zu bekommen. Dabei kann es sich um Diebe, Hacker oder Viren gleichermaßen handeln. Hier ein Beispiel:

Beispiel 1: In einem Krankenhaus werden komplexe, medizinische Geräte verwendet, die Ergebnisdaten von Untersuchungen auf Netzwerkordnern verschiedener PCs ablegen. Da diese Geräte nicht mit Passwörtern arbeiten, dürfen die Netzwerkordner der PCs nicht Passwortgeschützt sein. Diese Sicherheitslücke ermöglicht dem Virus Conficker sich zwischen den PCs zu vermehren, indem er Netzlaufwerke die nicht Passwortgeschützt sind sucht und sich über diese Verbreitet.

Beispiel 2: Karin liest und verschickt ihre Emails über die Webseite eines Providers der ein kostenloses Webmailservice anbietet. Sie hat als Passwort ihren Usernamen um die Jahreszahl ihres Geburtsdatums erweitert. Karins gekränkter Ex-Freund hat sich im Internet einen Passwort-Cracker (ein Programm, welches automatisch Passwortkombinationen ausprobiert) heruntergeladen und ihn auf Karins Email-Account angesetzt. Innerhalb kürzester Zeit wird das Programm fündig. Von nun an kann Karins Exfreund ihre Emails lesen und auch in Karins Namen Emails verschicken.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist eigentlich einfach diese Maßnahme zu vermitteln. Software kann dabei helfen. Viele Passwort-Eingabemasken prüfen die Passwörter schon auf ihre Qualität und verweigern zu einfache Passwörter.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Zeitaufwand sowie Kosten für die Erstellung eines guten Passworts sind vollkommen vernachlässigbar. Im Notfall bietet es sich an die Anfangsbuchstaben des Refrains des Lieblingsliedes als Passwort zu verwenden. Dabei können noch Buchstaben gegen Ziffern getauscht werden (i = 1, e = 3 o.ä.).

M 4.2 BILDSCHIRMSPERRE

Relevanz für den Durchschnittsbenutzer: mittel

Eine Bildschirmsperre kann eingesetzt werden um am Bildschirm sichtbare Informationen zu verbergen, wenn man kurz den Arbeitsplatz verlassen muss. Grundvoraussetzung dabei ist, dass die Bildschirmsperre durch ein Passwort gesichert ist. Siehe M 4.1.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne Bildschirmsperre ist jegliche Information, die gerade angezeigt wird, für alle einsehbar, wenn man seinen Arbeitsplatz gerade verlassen hat. Hier ein Beispiel:

Beispiel 1: Fritz arbeitet in einem Großraumbüro. Er ist gerade dabei eine Bestellung im Internet abzuschließen. Gerade als er seine persönlichen Daten – Name, Adresse, Kreditkarteninformationen – in der Webmaske eingegeben hat, läutet sein Telefon. Sein Chef besteht darauf ihn umgehend zu sehen. Ohne sich weiter um seine Bestellung zu kümmern eilt Fritz ins Büro seines Chefs. Währenddessen wird Bob, der in der Postabteilung derselben Firma arbeitet, auf Fritz' Monitor aufmerksam und sieht sich genau an, was da zu sehen ist. Er notiert sich die Kreditkarteninformationen und alles andere was auf dem Display zu lesen ist. Einige Wochen später wundert sich Fritz über die astronomische Summe auf seiner

Kreditkartenabrechnung. Die Nachforschung der Kreditkartenfirma hat ergeben, dass mit Fritz' Karte bei etlichen Onlineshops Computerhardware gekauft und an die Firma geliefert wurde. Der Empfänger existiert in der Firma nicht und niemand in der Postabteilung will etwas über die Pakete gewusst haben.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist eigentlich einfach diese Maßnahme zu vermitteln. Niemand würde seine Brieftasche oder seinen Reisepass irgendwo offen liegen lassen während er nicht in der Nähe ist. Genauso wenig sollte ein PC offen zugänglich zurückgelassen werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme erfordert eine einmalige Einstellung im Betriebssystem, danach reicht ein Mausklick um den Bildschirm zu sperren. Auch zusätzliche Kosten entstehen dadurch nicht.

M 4.3 REGELMÄßIGER EINSATZ EINES ANTI-VIREN-PROGRAMMS

Relevanz für den Durchschnittsbenutzer: hoch

Viren sind ein sehr verbreitetes Problem im IT-Bereich, vor allem beim Einsatz von weit verbreiteten Betriebssystemen wie etwa Windows. Die Gefahr die von Computer-Viren ausgeht betrifft Durchschnittsbenutzer sehr direkt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Die Gefahren die von Computerviren ausgehen können, sind sehr unterschiedlich, können aber von nervigen Meldungen bis zum kompletten Verlust aller Daten reichen. Hier ein paar Beispiele:

Beispiel 1: Karl hat auf seinem Computer kein Anti-Viren-Programm installiert und klickt auch auf jeden Email-Anhang, den er geschickt bekommt. In einem dieser Anhänge war ein Trojaner versteckt welcher sich unbemerkt im Hintergrund installiert hat. Von da an werden alle von Karl verwendeten Eingaben protokolliert und viele seiner Passwörter und andere persönliche Information ohne sein Wissen ins Netz verschickt und können dort missbraucht werden. Jetzt wundert sich Karl auf einmal, wieso auf seiner kleinen Homepage plötzlich

massenhaft Daten zu finden sind, die er nie dort hochgeladen hat.

Beispiel 2: Susanne hat klugerweise ein Anti-Viren-Programm installiert aber da sie die automatische Aktualisierungsaufforderung des Programms so genervt hat, hat sie die automatische Aktualisierung deaktiviert. Sie surft auf vielen Webseiten herum und auf einer dieser Seiten wird ihr ein Virus untergeschoben, da das installierte Anti-Viren-Programm nicht aktuell ist und den eigentlich schon bekannten Virus nicht erkennt. Von da an hat Susanne regelmäßig Programmabstürze begleitet von seltsamen Fehlermeldungen und kann sich nicht erklären warum.

Beispiel 3: Hubert hat kein Anti-Viren-Programm auf seinem Computer. Er hat bei der letzten Feier eine Menge Fotos mit seiner Digitalkamera gemacht und auf seinem Computer gespeichert. Freunde von ihm haben ihm ihre Memory-Sticks gegeben damit er die Fotos auf diese überspielen kann.

Leider war auf einem dieser Memory-Sticks ein Virus. Da kein Anti-Viren-Programm installiert ist, kann sich der Virus auf dem Computer installieren und seine Schadensroutine etwas zeitverzögert ausführen, in der Zwischenzeit hat Hubert die Memory-Sticks wieder an seine Freunde zurückgegeben. Hubert bemerkt ein paar Tage später verärgert, dass plötzlich alle seine Bilder auf dem Computer nicht mehr da, oder kaputt sind und seine Freunde sind auch nicht erfreut, weil sie jetzt einen Virus auf ihrem Memory-Stick vorfinden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass er einen Virenschutz am Computer benötigt. Allerdings muss vielen Benutzern das Programm installiert und ihnen die Grundfunktionen erklärt werden, damit sie es benutzen können.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Benutzer muss zumindest die Zeit für die Installation des Anti-Viren Programms aufwenden und die Zeit für die regelmäßige Aktualisierung desselben. Außerdem entstehen ihm dadurch auch Kosten, wenn er sich für ein kommerzielles Produkt entscheidet.

M 4.4 GEEIGNETER UMGANG MIT LAUFWERKEN FÜR WECHSELMEDIEN UND EXTERNEN DATENSPEICHERN

Relevanz für den Durchschnittsbenutzer: hoch

Datenspeicherungsmedien erfordern wie z.B. auch Bücher gewisse Aufmerksamkeit bei der Aufbewahrung um die Haltbarkeit zu maximieren. CDs bzw. DVDs können beispielsweise durch UV-Licht beschädigt werden, Magnetische Speichermedien wie Festplatten oder DAT-Tapes dürfen Magneten nicht zu nahe kommen. Festplatten sind außerdem sehr erschütterungsanfällig.

Was kann passieren wenn man die Maßnahme nicht setzt?

Die Unsachgemäße Lagerung von Datenträgern kann zum Verlust der gespeicherten Daten führen. Hier ein Beispiel:

Beispiel 1: Rainer ist semiprofessioneller Fotograf und wird regelmäßig bei Hochzeitsfeiern und anderen Anlässen gebucht. Da im Lauf der Zeit enorme Datenmengen zusammenkommen, brennt Rainer regelmäßig DVDs mit den Fotos jedes Events. Diese DVDs lagert Rainer in einer Spindel auf seinem Schreibtisch neben dem Fenster, wo sie täglich ohne Schutz der Sonne ausgeliefert sind. Als Rainers Festplatte irgendwann den Dienst verweigert, muss er feststellen, dass die DVDs inzwischen unlesbar sind, da sie der UV-Strahlung nicht standhalten konnten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht ganz einfach zu vermitteln. Das die Lagerung erheblichen Einfluss auf die Lebensdauer von Speichermedien haben kann ist nicht offensichtlich. Dennoch ist es nicht schwer die Maßnahme umzusetzen, wenn man sich mit der Tatsache abfindet.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die ordnungsgemäße Aufbewahrung von Speichermedien kann durchaus einige Zeit in Anspruch nehmen. Auch die Kosten können unter den entsprechenden Umständen schnell anwachsen. In den meisten Fällen reicht es aber schon auf Kleinigkeiten zu achten.

M 4.10 PASSWORTSCHUTZ FÜR TK-ENDGERÄTE

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.1

M 4.13 SORGFÄLTIGE VERGABE VON IDS

Relevanz für den Durchschnittsbenutzer: gering

Diese Maßnahme richtet sich in erster Linie an Administratoren von UNIX-ähnlichen Betriebssystemen. Es ist bei solchen insbesondere darauf zu achten, dass User-IDs nur einmalig vergeben werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollten User-IDs mehrfach vergeben werden, können die betroffenen User auf die Daten der jeweils anderen zugreifen, da das System zwischen den einzelnen Benutzern nicht unterscheiden kann. Hier ein Beispiel:

Beispiel 1: Ewald benutzt seit kurzer Zeit Linux auf seinem PC. Da er zusammen mit seiner Freundin wohnt, möchte er auch für sie einen Account auf seinem Computer einrichten. Dazu kopiert er in der entsprechenden Konfigurationsdatei nur die Zeile mit seinem Benutzernamen und ändert dann den Namen, die numerische UserID behält er für den Account seiner Freundin aber bei. Nun ändert er nur noch das Passwort und zeigt seiner Freundin wie sie den PC mitbenutzen kann. Eines Tages verirrt sich Ewalds Freundin in Ewalds Home-Verzeichnis. Da das Betriebssystem nicht zwischen Ewald und seiner Freundin unterscheiden kann, hat sie vollen Zugriff auf seine Daten und löscht versehentlich einige Verzeichnisse.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht ganz einfach zu vermitteln. Es ist nicht ganz offensichtlich warum zwei User, die unterschiedlich heißen, für das System doch ein und derselbe sein sollen. Wenn man sich aber mit diesem Umstand vertraut macht, ist es nicht schwierig diese Maßnahme umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der korrekte Umgang mit den Tools von UNIX-ähnlichen Systemen schließt das versehentliche Anlegen von doppelten User-IDs bereits aus. Damit ist kein zusätzlicher Zeitaufwand nötig. Es entstehen auch keine Kosten.

M 4.14 OBLIGATORISCHER PASSWORTSCHUTZ UNTER UNIX**Relevanz für den Durchschnittsbenutzer: hoch**

Siehe M 4.1.

M 4.19 RESTRIKTIVE ATTRIBUTVERGABE BEI UNIX-SYSTEMDATEIEN UND -VERZEICHNISSEN**Relevanz für den Durchschnittsbenutzer: gering bis mittel**

Beim Einsatz von UNIX-ähnlichen Betriebssystemen ist darauf zu achten, die Rechtevergabe möglichst restriktiv zu gestalten. Benutzern sollte der Schreib- (und in gewissen Fällen auch der Lese-)Zugriff auf fremde Dateien bzw. Systemdateien verweigert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn Benutzer die Rechte haben alle Dateien zu verändern, können versehentlich notwendige Dateien für den Betrieb des Systems verändert oder gelöscht werden. Hier ein Beispiel:

Beispiel 1: Christian ist neu in der Linux-Gemeinde. Bei der Installation ist ihm irgendwann ein Fehler unterlaufen und er hat zufällig Schreib- und Lese-Rechte auf alle Dateien (root-Zugang) erhalten. Einige Zeit geht alles gut und Christian ist zufrieden mit seinem neuen Betriebssystem. Eines Tages löscht Christian versehentlich die Datei „fstab“ aus dem Verzeichnis „etc“. Damit weiß sein Betriebssystem nicht mehr welche Datenträger in Christians PC eingebaut sind und kann nicht mehr hochfahren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu

vermitteln?

Diese Maßnahme ist gerade bei neuen Benutzern von UNIX-ähnlichen Systemen nicht leicht zu vermitteln. Die Trennung von Benutzer und Administrator ist aber bei genauer Betrachtung ein deutlicher Sicherheitsvorteil gegenüber anderer Betriebssysteme.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Das Beachten dieser Maßnahme verursacht keine Kosten. Auch der Zeitaufwand ist im Normalfall vernachlässigbar, da die Standardeinstellungen bereits mit dieser Maßnahme konform gehen.

M 4.27 PASSWORTSCHUTZ AM TRAGBAREN PC

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.1.

M 4.28 SOFTWARE-REINSTALLATION BEI BENUTZERWECHSEL EINES TRAGBAREN PC

Relevanz für den Durchschnittsbenutzer: hoch

Sollte ein PC, insbesondere ein tragbarer, den Benutzer wechseln, ist es empfehlenswert die Software neu zu installieren. Einerseits wird dadurch die Performance verbessert, andererseits werden eventuell sensible Daten gelöscht. Auch eventuell vorhandene Viren werden so beseitigt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn ein PC den Benutzer wechselt, und der Vorbesitzer keine Neuinstallation vornimmt, kann der neue Besitzer auf alle Dateien des Vorbesitzers zugreifen. Hier ein Beispiel:

Beispiel 1: Dieter möchte sein Notebook bei einem Online-Auktionshaus verkaufen. Das Notebook ist noch in einem guten Zustand und schon bald hat sich ein Käufer gefunden.

Dieter verschiebt noch einige Dateien in den Papierkorb und bereitet das Notebook für den Versand vor. Einige Tage später nimmt der neue Besitzer des Notebooks dieses von der Post entgegen und bemerkt beim ersten Hochfahren bereits, dass der Verkäufer seine persönlichen Daten mit dem Notebook mit verkauft hat. Dieter hat ohne darüber Nachzudenken gespeicherte TAN-Codes inklusive Onlinebanking-LOGIN-Daten von seiner Bank, Kreditkarteninformationen und seinen gesamten Email-Verkehr mit dem Notebook verkauft. Außerdem findet der neue Besitzer einige sehr private Fotos...

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach zu vermitteln. Es würde auch niemand der eine Brieftasche verkauft, dem neuen Besitzer sein ganzes Bargeld überlassen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Das umsetzen dieser Maßnahme kann einiges an Zeit in Anspruch nehmen – die bewahrte Privatsphäre sollte aber jedem Benutzer diesen Zeitaufwand wert sein.

M 4.29 EINSATZ EINES VERSCHLÜSSELUNGSPRODUKTES FÜR TRAGBARE PCS

Relevanz für den Durchschnittsbenutzer: mittel

Insbesondere bei Tragbaren PCs bietet sich der Einsatz eines Verschlüsselungsproduktes ein, welches eine Sichere Speicherung von Dateien ermöglicht, die auch bei physischem Zugriff auf das Speichermedium standhält.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein Verzicht auf diese Maßnahme kann den Verlust von sensiblen Daten zur Folge haben. Hier ein Beispiel:

Beispiel 1: Dominik hat eine revolutionäre Methode zur Energiegewinnung entdeckt. Alle Informationen wie Messergebnisse, Baupläne und Effizienzberechnungen sind auf seinem Notebook gespeichert. Auf dem Weg zu einer Konferenz bei der Dominik diese neue Methode präsentieren möchte wird sein Notebook gestohlen. Da Die Dateien ohne einen

Sicherheitsmechanismus gespeichert wurden, hat der Dieb Zugriff darauf.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einigermaßen einfach zu vermitteln. Analog zu einem Tresor im Haushalt kann in gewissen Szenarien der Einsatz einer Verschlüsselungssoftware für bestimmte Dokumente sehr nützlich sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Das Umsetzen dieser Maßnahme kann einiges an Zeit in Anspruch nehmen. Moderne Betriebssysteme bringen bereits Software zum Verschlüsseln von Dateien oder Verzeichnissen mit sich. Es gibt auch etliche kostenlose Programme zum Download, welche die selbe Funktionalität bieten.

M 4.30 NUTZUNG DER IN ANWENDUNGSPROGRAMMEN ANGEBOTENEN SICHERHEITSFUNKTIONEN

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Viele Standardprodukte im IT-Bereich bieten gewisse Sicherheitsfunktionen. Auch wenn viele davon nur von mittelmäßiger Qualität sind, können sie Unbefugte behindern und mögliche Schäden verringern. Beispiele hierfür wären : Passwortschutz bei Programmaufruf, automatische Zwischenspeicherung von Dokumenten, Verschlüsselung von Dateien...

Was kann passieren wenn man die Maßnahme nicht setzt?

Jede nicht gesetzte Maßnahme erleichtert einem Unbefugten den Zugriff. Auch wenn manche Sicherheitsmaßnahmen einen Angreifer mit entsprechendem Knowhow nur kurzfristig bremsen können, können sie weniger versierte Angreifer vielleicht ganz aufhalten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach zu vermitteln. Eine „geschenkte“ einfach anzuwendende

Sicherheitsmaßnahme soll eingesetzt werden. Das schwieriger zu vermittelnde Wissen ist, welche Software welche Sicherheitsmaßnahmen mitbringt und wie diese aktiviert werden können.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Das Umsetzen diese Maßnahme sollte weder nennenswerten Zeitbedarf noch zusätzliche Kosten mit sich bringen.

M 4.31 SICHERSTELLUNG DER ENERGIEVERSORGUNG IM MOBILEN EINSATZ

Relevanz für den Durchschnittsbenutzer: mittel

Tragbare PCs sind auf Akkus zur Stromversorgung angewiesen. Da insbesondere bei älteren Akkus die Entladung im unteren Kapazitätsbereich sehr schnell erfolgen kann, sollten Dokumente regelmäßig gespeichert bzw. gesichert werden. Weiters sollten die Reststrom-Anzeigen des mobilen Geräts im Auge behalten werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein plötzlicher Einbruch der Stromversorgung kann zu Fehlern bei der Datenspeicherung und damit zu Datenverlusten führen. Hier ein Beispiel:

Beispiel 1: Oliver sitzt mit seinem Notebook in einem Kaffeehaus und verwendet designt einen Flyer für ein Fest. Das Betriebssystem seines Notebooks warnt Oliver davor, dass der Akku in kürze keinen Strom mehr liefern wird. Oliver ist überzeugt, dass die Zeit noch reicht um den Flyer fertig zu machen. Gerade als er sein Kunstwerk speichern möchte, wird der Bildschirm schwarz. Daheim lädt Oliver den Akku wieder, vom Flyer ist aber nichts mehr zu finden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach zu vermitteln. Ein elektronisches Gerät kann ohne Strom nicht funktionieren – daher muss auf den Ladezustand von Akkus geachtet werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Das Umsetzen diese Maßnahme verursacht keinen zusätzlichen Zeitaufwand und auch keine Kosten.

M 4.32 PHYSIKALISCHES LÖSCHEN DER DATENTRÄGER VOR UND NACH VERWENDUNG

Relevanz für den Durchschnittsbenutzer: hoch

Wenn Datenträger ausgetauscht werden, sollten diese einerseits zum Selbstschutz vor schädlichen Programmen vor der ersten Verwendung und andererseits nach der letzten Verwendung zum Schutz der Privatsphäre gelöscht werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn diese Maßnahme nicht zur Anwendung kommt, können verschieden Probleme daraus resultieren. Einerseits können Datenträger, die von einem anderen Benutzer übernommen werden mit Schädlicher Software verseucht sein, welche den eigenen PC befallen kann. Andererseits kann der nachfolgende Verwender des Datenträgers wenn dieser vor der Übergabe nicht gelöscht wird, auf eventuell sensible Daten zugreifen. Hier ein Beispiel:

Beispiel 1: Monika übernimmt von ihrem Bruder eine externe Festplatte, die ihm inzwischen zu klein ist. Natürlich freut sich Monika und beginnt sofort die Festplatte zu verwenden ohne sie vorher zu kontrollieren. Leider hat Monikas Bruder zuvor einige Software aus dem Internet geladen und sich dabei einen Virus eingefangen, der auch die externe Festplatte befallen hat. Dieser Virus breitet sich nun auch auf Monikas PC aus.

Beispiel 2: Emil hat im Lauf der Jahre etliche Festplatten gefüllt und immer wenn er auf ein größeres Modell umgestiegen ist, hat er die alte Festplatte in einer Schublade abgelegt. Inzwischen hat er so viele unverwendete Festplatten, dass er beschließt einige davon los zu werden. Er löscht einfach die Dateien von der Festplatte und verkauft sie über ein Forum. Der Käufer ist sehr Neugierig und analysiert mit Software die es im Internet gibt, ob eventuell gelöschte Dateien wiederhergestellt werden können. Tatsächlich kann er den Großteil des ursprünglichen Inhaltes wieder herstellen und so in Emils Dateien herumschnüffeln.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist schwierig zu vermitteln. Es ist nicht intuitiv zu verstehen, dass gelöschte Dateien so lange nicht wirklich gelöscht sind, bis sie überschrieben wurden. Dennoch empfiehlt es sich Software zu verwenden die Datenträger wirklich löscht indem sie vollständig mit zufälligen Daten füllen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Software zum Überschreiben – und damit endgültigen Löschen – ist zum Teil kostenlos, allerdings ist abhängig von der Größe des Datenträgers die Laufzeit dieser Programme unter Umständen beträchtlich.

M 4.33 EINSATZ EINES VIREN-SUCHPROGRAMMS BEI DATENTRÄGERAUSTAUSCH UND DATENÜBERTRAGUNG**Relevanz für den Durchschnittsbenutzer: hoch**

Wenn Daten ausgetauscht werden – egal ob das über ein Netzwerk oder durch Übergabe eines Datenträgers geschieht – ist der Einsatz eines Viren-Suchprogrammes unersetzlich.

Was kann passieren wenn man die Maßnahme nicht setzt?

Das unkontrollierte Akzeptieren und Verwenden von Daten kann unter Umständen einem Virus ermöglichen den PC zu befallen. Hier ein Beispiel:

Beispiel 1: Michael tauscht regelmäßig mit seinen Freunden Dateien aus. Meistens geschieht das durch den Austausch von USB-Sticks. Da Michael keinen Virenschanner verwendet, kann er auch den USB-Stick seines Freundes nicht überprüfen. Nichts ahnend öffnet Michael eine der Dateien auf dem Datenträger und schon ist sein PC von einem Virus befallen. In regelmäßigen Abständen startet sein Computer jetzt neu und ist allgemein sehr instabil.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu

vermitteln?

Diese Maßnahme ist einfach zu vermitteln. Auch im echten Leben sollte man auf ein Mindestmaß an Hygiene achten und so wird man intuitiv die getragene Wäsche von einem Anderen vor dem Anziehen waschen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Zusätzliche Kosten werden durch diese Maßnahme nicht verwendet, wenn man bereits einen Virens Scanner einsetzt. Auch der Zeitbedarf ist in den meisten Fällen vernachlässigbar.

M 4.34 EINSATZ VON VERSCHLÜSSELUNG, CHECKSUMMEN ODER DIGITALEN SIGNATUREN

Relevanz für den Durchschnittsbenutzer: mittel

Siehe M 4.22 und M 4.29.

M 4.35 VERIFIZIEREN DER ZU ÜBERTRAGENDEN DATEN VOR VERSAND

Relevanz für den Durchschnittsbenutzer: hoch

Wenn Daten ausgetauscht werden, sollte darauf geachtet werden, dass das Übertragungsmedium nur die gewünschten Informationen enthält. Siehe auch M 4.32.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte bei der Übergabe ein nicht kontrollierter Datenträger verwendet werden, so kann dieser noch andere Daten enthalten, welche der Empfänger nicht kennen sollte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist schwierig zu vermitteln. Es ist nicht intuitiv zu verstehen, dass gelöschte Dateien so lange nicht wirklich gelöscht sind, bis sie überschrieben wurden. Daher empfiehlt es sich spezielle Lösch-Software zu verwenden, die Dateien vollständig löscht, indem sie sie

mit Zufallsdaten überschreibt.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Eine Kontrolle vor dem Versand nimmt wenig Zeit in Anspruch. Auch die eventuelle Kontrollsoftware ist höchstens einmalig zu bezahlen und damit sind die Kosten überschaubar.

M 4.38 ABSCHALTEN NICHT BENÖTIGTER LEISTUNGSMERKMALE

Relevanz für den Durchschnittsbenutzer: mittel

Zur Steigerung des Sicherheitsniveaus sollten nicht benötigte Leistungsmerkmale abgeschaltet werden. Das gilt für die oftmals nicht verwendete Bluetooth-Funktionalität des Handys genauso wie für die Druckerfreigabe in Windows-Betriebssystemen wenn kein Drucker installiert ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Nicht genutzte Leistungsmerkmale können Unberechtigten einen Angriffspunkt bieten. Da diese Merkmale nicht genutzt werden bemerkt man ein eventuell unerwartetes Verhalten oft nicht. Damit haben Angreifer mehr Zeit Schaden anzurichten. Hier ein Beispiel:

Beispiel 1: Paula ist seit kurzem stolze Besitzerin eines Mobiltelefons das wesentlich mehr Funktionen bietet, als Paula je benutzen wird. In den ersten Stunden mit dem neuen Handy hat Paula über Bluetooth ihren Lieblingsklingelton und einige Fotos geschickt bekommen. Seit dieser Zeit ist ihr Handy im Bluetooth-Empfangsmodus. Als sie eines Tages in der U-Bahn sitzt, befindet sich unter anderem ein Übeltäter in ihrer Nähe der mit einem besonderen Programm die nähere Umgebung nach Bluetooth-fähigen Handys absucht. Paulas Handy taucht dabei auf und unter Ausnutzung eines Programmierfehlers in der Bluetoothsoftware von Paulas Handy kann der Übeltäter Paulas Fotos, sowie Kontakte und Nachrichten herunterladen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einigermaßen einfach zu vermitteln. Voraussetzung ist aber, sich mit dem betreffenden Gerät vertraut zu machen und eventuell das Handbuch zu Rate zu ziehen

um zu entscheiden, welche Funktionen nötig sind und welche nicht.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann einige Zeit in Anspruch nehmen, bis man mit dem Gerät vertraut ist und beurteilen kann welche Funktionen wichtig sind. Kosten entfallen bei dieser Maßnahme hingegen.

M 4.44 PRÜFUNG EINGEHENDER DATEIEN AUF MAKRO-VIREN

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.3, M 4.33.

M 4.56 SICHERES LÖSCHEN UNTER WINDOWS-BETRIEBSSYSTEMEN

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Es ist zu beachten, dass Dateien beim Löschen nicht physikalisch vom Datenträger gelöscht werden, sondern nur die Verweise auf diese Datensegmente entfernt werden. Damit ist es möglich den Inhalt von lange gelöschten Dateien auszulesen. Insbesondere beim Löschen unter Windows-Betriebssystemen ist zu beachten, dass, wenn nicht anders gefordert, Dateien nur in den Papierkorb verschoben werden. Es ist daher nötig den Papierkorb regelmäßig zu entleeren, damit dieser nicht zu viel Speicherplatz verbraucht und zu unübersichtlich wird. Zur sicheren Löschung von Dateien oder Datenträgern empfiehlt sich Software welche in der Lage ist die Daten auf der Festplatte zu überschreiben. Siehe M 4.32.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne „Sicheres Löschen“ besteht die Gefahr, dass gelöschte Dateien wiederhergestellt werden können. Das kann insbesondere bei der Übergabe von Datenträgern problematisch sein. Hier ein Beispiel:

Beispiel 1: Mathilda verwendet ihren USB-Stick manchmal um Dokumente für Präsentationen

immer zur Hand zu haben. Nach einer Präsentation löscht sie die Daten vom USB Stick indem sie die Dateien markiert und dann den Menüpunkt löschen auswählt. Mathilda weiß nicht, dass dabei die Dateien nicht wirklich gelöscht werden sondern nur die Einträge aus der Verzeichnisstruktur entfernt werden. Als Mathildas USB-Stick gestohlen wird, ist sie noch froh, dass sie kurz zuvor alles gelöscht hat. Leider ist der Dieb im Besitz eines Programmes zur Datenwiederherstellung. Kurz darauf ist Mathilda schockiert als sie über die vertraulichen Unternehmens-Interna in der Zeitung liest.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist schwierig zu vermitteln. Es ist nicht intuitiv zu verstehen, dass gelöschte Dateien so lange nicht wirklich gelöscht sind, bis sie überschrieben wurden. Dennoch empfiehlt es sich Software zu verwenden die Datenträger wirklich löscht, indem sie vollständig mit zufälligen Daten füllen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Software zum Überschreiben – und damit endgültigen Löschen – ist zum Teil kostenlos, allerdings ist abhängig von der Größe des Datenträgers die Laufzeit dieser Programme unter Umständen beträchtlich.

M 4.57 DEAKTIVIEREN DER AUTOMATISCHEN CD-ROM-ERKENNUNG

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Die Autoplay-Funktion für Wechseldatenträger (CDs/DVDs/USB-Sticks) in Windows-Betriebssystemen sollte abgeschaltet werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Viele Viren verbreiten sich beispielsweise über die Autostart Funktion bei USB-Sticks. Wenn ein verseuchter USB-Stick an den PC angesteckt wird, missbraucht er die Autoplay-Funktion um schadhafte Software auszuführen. Hier ein Beispiel:

Beispiel 1: Andreas möchte einige Dokumente in einem Copyshop ausdrucken. Dazu speichert

er alles Nötige auf einem USB-Stick den er dann dem Angestellten im Copyshop übergibt. Der USB-Stick landet im PC, welcher Virenverseucht ist. Der Virus erkennt das neue Speichermedium und legt eine Kopie von sich selbst als Autostart-Datei am USB-Stick ab. Als Andreas mit den Ausdrucken zurückkehrt und den USB-Stick wieder an seinem PC anschließt (auf dem leider kein Virens Scanner installiert ist) wird die Autostart-Datei ausgeführt und damit auch Andreas' PC mit dem Virus verseucht.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach zu vermitteln. Der Benutzer sollte Interesse daran haben, nur ausgewählte Programme zum ausgewählten Zeitpunkt auszuführen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist schnell und kostenlos umzusetzen. Es erfordert nur einige Mausklicks um die Autoplay-Funktion abzuschalten.

M 4.64 VERIFIZIEREN DER ZU ÜBERTRAGENDEN DATEN VOR WEITERGABE / BESEITIGUNG VON RESTINFORMATIONEN

Relevanz für den Durchschnittsbenutzer: hoch

Bei der elektronischen Weitergabe gelten die selben Richtlinien wie beim Versand von Datenträgern. Siehe M 4.35.

M 4.75 SCHUTZ DER REGISTRIERUNG UNTER WINDOWS NT/2000/XP

Relevanz für den Durchschnittsbenutzer: hoch

Für den laufenden Betrieb wichtige Dateien und Verzeichnisse eines Betriebssystems sollten für Benutzer keinesfalls schreibbar, eventuell auch nicht lesbar sein. Siehe M 4.19, M 4.53.

M 4.78 SORGFÄLTIGE DURCHFÜHRUNG VON KONFIGURATIONSÄNDERUNGEN

Relevanz für den Durchschnittsbenutzer: hoch

Die Veränderung von Konfigurationsdateien sollte im laufenden Betrieb sehr sorgfältig durchgeführt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Einzelne Komponenten bzw. das ganze System können in ihrer Stabilität beeinträchtigt werden, wenn Konfigurationsänderungen unüberlegt vorgenommen werden. Hier ein Beispiel:

Beispiel 1: Ludwig ändert das Administratorenpasswort seines PCs. Da er gerade etliche andere Dinge im Kopf hat, vergisst er das Passwort sicher zu hinterlegen. Nach der Änderung muss er seinen Administratorenaccount lange nicht verwenden und so vergisst Ludwig das Passwort. Als einige Wochen später wieder Änderungen anstehen, versucht Ludwig das Administratorenkonto zu aktivieren, aber es gelingt ihm nicht. Er hat sich damit aus seinem PC ausgesperrt und kann keine Änderungen mehr durchführen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahme zu vermitteln – wichtige Entscheidungen sollten in jedem Fall, nicht nur im IT-Bereich wohl überlegt getroffen werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht keine zusätzlichen Kosten, allerdings kann das bewusste Konfigurieren – dazu gehört unter anderem auch das Lesen von Dokumentation – einige Zeit in Anspruch nehmen.

M 4.82 SICHERE KONFIGURATION DER AKTIVEN NETZKOMponentEN

Relevanz für den Durchschnittsbenutzer: hoch

Da immer mehr Haushalte neben kabelgebundenem Internet auch mit WLAN-Routern ausgestattet sind, nimmt die Bedeutung der sicheren Konfiguration von aktiven Netzkomponenten immer weiter zu.

Was kann passieren wenn man die Maßnahme nicht setzt?

Häufig werden aktive Netzkomponenten ohne das Wissen ihrer Besitzer betrieben. In diesem Fall wird Außenstehenden der Zugang zum Netzwerk erleichtert. Hier ein Beispiel:

Beispiel 1: Volker betreibt ein kleines Designermöbelgeschäft. Von seinem Internetprovider hat er im Kombiangebot einen WLAN-Router aufgestellt bekommen. Da sich Volker für derartige Dinge nicht weiter interessiert, weiß er nicht, dass er ein frei zugängliches WLAN betreibt. Gegenüber dem Möbelladen befindet sich ein kleines Kaffeehaus in dem regelmäßig Kunden mit Notebooks zu Gast sind. Eines Nachmittags besucht ein Jugendlicher mit Notebook das Kaffeehaus und wird auf Volkers WLAN aufmerksam. Ohne Hindernisse gelingt es dem Jugendlichen in Volkers Netzwerk aufgenommen zu werden. So gelingt es dem Jugendlichen auch schnell auf Volkers Buchhaltungs-PC zuzugreifen und Einblick in alle Finanzdaten zu nehmen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht ganz einfach diese Maßnahme zu vermitteln – teilweise betreiben Benutzer Netzkomponenten ohne davon zu wissen bzw. diese „gekauft“ zu haben. Es ist daher nötig, Benutzerhandbücher zu lesen und sich ein Bild über den Funktionsumfang von Geräten zu machen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursachte keine zusätzlichen Kosten, kann aber einige Zeit in Anspruch nehmen.

M 4.83 UPDATE/UPGRADE VON SOFT- UND HARDWARE IM NETZBEREICH

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Sollte von den Herstellern aktualisierte Softwareversionen zur Verfügung gestellt werden, sollten diese installiert werden. Bei enorm veralteter Hardware empfiehlt sich auch der Austausch selbiger um das Sicherheitsniveau sowie die Produktivität zu steigern.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn bestehende Sicherheitslücken nicht gefüllt werden, ermöglicht bzw. vereinfacht das einem potentiellen Angreifer eine Attacke. Hier ein Beispiel:

Beispiel 1: Ernst betreibt einen WLAN-Router, der nur die überholte WEP-Verschlüsselung beherrscht. Diese Verschlüsselungsmethode ist sehr einfach zu überlisten, und genau das gelingt einem Eindringling, welcher sich auf Ernsts Kosten illegale Inhalte aus dem Internet herunterlädt. Ernst hätte das durch eine kleine Investition – nämlich die Anschaffung eines aktuelleren WLAN-Routers verhindern können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht ganz einfach diese Maßnahme zu vermitteln – die Einstellung, an einem funktionierenden Gerät nicht herum zu basteln, ist tief verwurzelt.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann sowohl Kosten als auch Zeit beanspruchen. In den meisten Fällen sollten aber beide Punkte innerhalb eines akzeptablen Rahmens liegen.

M 4.94 SCHUTZ DER WWW-DATEIEN**Relevanz für den Durchschnittsbenutzer: mittel**

Beim Einsatz von Webseiten ist es nötig auf die Absicherung der WWW-Dateien zu achten. Diese dürfen keinesfalls von Unbefugten veränderbar sein. Eventuell ist es auch nötig die Dateien vor lesendem Zugriff zu schützen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ungeschützte Dateien können von Unbefugten verändert werden. Damit können Informationen für Besucher von Webseiten verfälscht werden. Hier ein Beispiel:

Beispiel 1: Peter hat sich bereit erklärt für seinen Sportverein eine Webseite zu erstellen. Er kümmert sich auch darum diese Webseite online zu stellen. Um sich die Arbeit zu erleichtern hat Peter auf ein kleines Content Management System zurückgegriffen. Das System befindet sich zurzeit noch in Entwicklung und weist noch große Sicherheitslücken auf (worauf die Programmier auch deutlich hinweisen). Nach der Veröffentlichung der Homepage dauert es nicht lange, bis ein Hacker Inhalte verfälscht hat und so finden sich plötzlich rassistische Äußerungen auf der Startseite des Sportvereins. Da Peter der Zuständige ist bekommt er schon bald Besuch von der Polizei.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer die Maßnahme zu vermitteln, allerdings ist die Umsetzung nicht immer so einfach, wie es auf den ersten Blick erscheint. Neben den Zugriffsberechtigungen für die Dateien gibt es unter Umständen noch andere Zugriffsmöglichkeiten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann sehr viel Zeit in Anspruch nehmen. Kosten müssen nicht zwangsläufig entstehen.

M 4.98 KOMMUNIKATION DURCH PAKETFILTER AUF MINIMUM BESCHRÄNKEN

Relevanz für den Durchschnittsbenutzer: hoch

Für Durchschnittsbenutzer bieten sich sogenannte Desktop-Firewalls an, um die Kommunikation auf ein Minimum zu beschränken. Je mehr Kommunikation möglich wäre, desto mehr mögliche Angriffspunkte bietet ein System. Moderne Betriebssysteme bringen normalerweise rudimentäre Firewallfunktionen – welche zum Teil sehr ausbaufähig sein können – mit.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein Verzicht auf Paketfilter bewirkt, dass jedes Datenpaket beim Betriebssystem ankommt. Dadurch können potentielle Fehler im Betriebssystem ausgenutzt werden, was dazu führt, dass ein Angreifer die Kontrolle über das Betriebssystem übernehmen kann.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Da moderne Betriebssysteme mit Paketfilterfunktionalitäten ausgeliefert werden, ist diese Maßnahme einfach umzusetzen. Es ist auch einfach an Benutzer zu vermitteln, ohnehin zur Verfügung stehende Schutzmechanismen einzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme lässt sich schnell umsetzen und verursacht nicht zwangsläufig zusätzliche Kosten. Eine feinere Auswahl, welche Pakete das Betriebssystem erreichen dürfen, kann einige Zeit in Anspruch nehmen.

M 4.99 SCHUTZ GEGEN NACHTRÄGLICHE VERÄNDERUNGEN VON INFORMATIONEN**Relevanz für den Durchschnittsbenutzer: mittel**

Dateien, die weitergegeben werden, können im Normalfall vom Empfänger auch be- oder verarbeitet werden. Das muss nicht immer im Sinne des Erstellers sein. Um die Bearbeitung von Dokumenten offensichtlich zu machen, gibt es digitale Signaturen. Die Wahl des passenden Dateiformates erschwert das Bearbeiten zusätzlich.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn Dokumente in herkömmlichen Formaten ausgetauscht werden, kann der Empfänger die enthaltenen Informationen verfälschen und in verfälschter Form anderen zukommen lassen. Auch eine auszugsweise Weiterverarbeitung ist durch die Weitergabe elektronischer Daten problemlos möglich.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Die Umsetzung kann allerdings problematisch sein. Besondere Dateiformate erfordern unter Umständen eigene Programme zur Anzeige, digitale Signaturen machen nur Sinn, wenn alle möglichen Leser des Dokumentes wissen, dass ursprünglich eine digitale Unterschrift enthalten war.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme lässt sich ohne großen Zeitaufwand umsetzen, die Kosten können dabei allerdings schnell steigen.

M 4.101 SICHERHEITSGATEWAYS UND VERSCHLÜSSELUNG

Relevanz für den Durchschnittsbenutzer: mittel

Wenn Dateien über offene Netzwerke verschickt werden sollten diese im Bedarfsfall verschlüsselt werden. Das kann auf Seiten des Clients, wie auch auf Seiten des Servers geschehen. Für Durchschnittsbenutzer eignet sich dabei die Verschlüsselung auf Client-Seite besser, da es einige kostenlose Software (GnuPG) gibt.

Was kann passieren wenn man die Maßnahme nicht setzt?

Eine unverschlüsselte Übertragung von Daten über das Internet vereinfacht bzw. ermöglicht es potentiellen Übeltätern den Kommunikationsvorgang zu belauschen. Hier ein Beispiel:

Beispiel 1: Alice und Bob wollen sich verabreden. Zur Absprache des Treffpunkts kommunizieren sie über Email. Weder Alice noch Bob verwenden Verschlüsselungsprodukte. Der eifersüchtigen Eve gelingt es die Emails von Alice und Bob zu belauschen und so erfährt sie von dem geheimen Treffen. Natürlich kann Eve die beiden nicht einfach gewähren lassen und so beschließt sie mit Wasserballons bewaffnet zur vereinbarten Zeit am Treffpunkt zu warten und Alice und Bob eine böse Überraschung zu bereiten. Hätten Alice und Bob ihre Emails verschlüsselt, wäre ihnen die ungewollte Dusche erspart geblieben.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Auch im echten Leben wird niemand Informationen, die nur für eine Person gedacht sind, an eine Plakatwand heften. Der Einsatz von Verschlüsselung half schon immer geheime Informationen auch wirklich geheim zu halten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert bei der ersten Anwendung ein wenig Zeit für die Konfiguration, der regelmäßige Einsatz ist allerdings nicht aufwendig und verursacht auch keine Kosten.

M 4.105 ERSTE MAßNAHMEN NACH EINER UNIX-STANDARDINSTALLATION**Relevanz für den Durchschnittsbenutzer: mittel**

Wie bei jedem aktuellen Betriebssystem sollten Accounts durch ein gutes Passwort (siehe M 4.1) geschützt werden. Außerdem sollten umgehend nach der Installation verfügbare Updates installiert werden um mögliche bekannte Sicherheitslücken zu schließen. Für Durchschnittsbenutzer ist diese Maßnahme ausreichend. Im Serverbetrieb sollten von Administratoren auch unnötige Dienste (bei einer Desktop Installation entfallen diese im Normalfall ohnehin) abgestellt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn ein neuer Benutzer diese anfänglichen wichtigen Schritte ignoriert, schadet er erstens seiner subjektiven Erfahrung mit einem Betriebssystem, da außer Sicherheitsupdates häufig auch zusätzliche, oder verbesserte Funktionalität durch Updates installiert wird. Zweitens bleiben Sicherheitslücken geöffnet und ermöglichen Übeltätern das einbrechen in das System. Hier ein Beispiel:

Beispiel 1: Da Gerald für sein Betriebssystem immer viel Geld ausgegeben hat, ärgert er sich maßlos über regelmäßige Abstürze und Virenbefall. Er beschließt einmal ein UNIX-nahes Betriebssystem auszuprobieren, welches kostenlos angeboten wird. Nach der Installation einer eher veralteten Distribution will Gerald sofort loslegen und beginnt im Internet zu surfen. Kurze zeit Später wird Gerald Opfer eines Skript-Kiddies (also einem Möchtegern-Hacker der nur fertige Programme, welche Sicherheitslücken ausnutzen, ausprobiert), das Gerald's Festplatten löscht. Hätte Gerald alle Sicherheitsupdates installiert wäre das nicht geschehen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Jedes moderne Betriebssystem bietet Funktionen um

Updates einzuspielen. Diese sollten regelmäßig – am besten automatisch – installiert werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert nur wenig Zeit und verursacht keine Kosten.

M 4.107 NUTZUNG VON HERSTELLER-RESSOURCEN

Relevanz für den Durchschnittsbenutzer: mittel

Hersteller-Ressourcen (Handbücher, Foren, FAQs) stellen eine wichtige Informationsquelle dar, welche in Problemfällen zu einer schnellen Lösung führen können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn Hersteller-Ressourcen nicht genutzt werden, können Probleme unter Umständen langfristig bestehen, woraus zusätzlicher Schaden entstehen kann.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist eigentlich einfach zu vermitteln. Bei Problemen ist es naheliegend im Handbuch nachzuschlagen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht keine Kosten. Allerdings kann das selbstständige Problemlösen mithilfe von Handbuch und FAQs einige Zeit in Anspruch nehmen.

M 4.114 NUTZUNG DER SICHERHEITSMECHANISMEN VON MOBILTELEFONEN

Relevanz für den Durchschnittsbenutzer: mittel

Mobiltelefone bieten einige Sicherheitsmaßnahmen welche auch von Durchschnittsbenutzer

verwendet werden sollten. In erster Linie sollte von Durchschnittsbenutzern die PIN-Abfrage beim Anschalten stets aktiviert sein.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte ein Mobiltelefon ohne Pin-Code Abfrage gestohlen werden, kann der Dieb damit telefonieren. Außerdem ist ein Zugriff auf die gespeicherten Kontakte und Kurznachrichten möglich.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist eigentlich einfach zu vermitteln. Die Standardeinstellung ist bereits, dass der PIN-Code abgefragt wird.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht keine Kosten. Der Zeitaufwand zum eingeben des PINs ist minimal.

M 4.134 WAHL GEEIGNETER DATENFORMATE

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Beim Austausch von Dateien sollte auf geeignete Datenformate geachtet werden. Zum Austausch von Microsoft Word Dokumenten eignet sich beispielsweise das .rtf (RichTextFormat) besser, da es von mehreren Programmen verarbeitet werden kann. Ein weiterer Vorteil ist, dass dieses Format keine Makroviren enthalten kann.

Was kann passieren wenn man die Maßnahme nicht setzt?

Manche Dateiformate können Metainformationen enthalten. Unter Umständen ist es nicht im Sinne des Erstellers einer Datei, wenn diese beim Austausch übermittelt werden. Hier ein Beispiel:

Beispiel 1: Karin erstellt im Lauf einiger Wochen eine Seminararbeit mit dem Textprogramm

Microsoft Word. Karin weiß nicht, dass ihre Version von Word nicht nur den aktuellen Inhalt speichert, sondern auch vorhergegangene Versionen. Da Karin große Teile ihrer Arbeit von einem anderen Studenten übernommen und dann verändert hat, wird ihr diese Versions-Speicherung zum Verhängnis als ihr Professor bei der Abgabe die älteren Versionen ansieht.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Leider ist diese Maßnahme sehr schwer zu vermitteln. Durchschnittsbenutzer wissen oft nicht, welche Zusatzinformationen in Dateien gespeichert sind, da sie von den Programmen nicht darüber informiert werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme nimmt wenig Zeit in Anspruch. Kosten entstehen dadurch keine.

M 4.135 RESTRIKTIVE VERGABE VON ZUGRIFFSRECHTEN AUF SYSTEMDATEIEN

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Siehe M 4.20 und M 4.53.

M 4.146 SICHERER BETRIEB VON WINDOWS 2000/XP

Relevanz für den Durchschnittsbenutzer: hoch

Die Sicherheitsmechanismen von Betriebssystemen sollten unbedingt eingesetzt werden. Windows 2000/XP bieten Funktionen zur Systemwiederherstellung sowie zum Schutz vor schädlicher Software. Zusätzlich ist eine Firewall inkludiert. Weitere Sicherheitsmerkmale betreffen den Betrieb innerhalb einer Domain und sollten in diesem Fall vom Administrator aktiviert und konfiguriert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Die Betriebssystemeigenen Sicherheitsmechanismen dienen insbesondere auch dem Schutz von Sicherheitslücken. Diese Mechanismen nicht einzusetzen erleichtert es Angreifern diese Lücken auszunutzen. Hier ein Beispiel:

Beispiel 1: Richard hat – um Platz zu sparen – die Funktion „Systemwiederherstellung“ seines Windows-PCs abgeschaltet. In einer einschlägigen Newsgruppe liest er über einen neu veröffentlichten Treiber für sein Mainboard. Diesen will sich Richard sofort herunterladen und installieren. Nach dem notwendigen Neustart funktioniert sein PC nicht mehr. Richard versucht von der Installations-CD zu booten und das System wiederherzustellen. Leider gelingt dies nicht, da Richard diese Funktion ja abgeschaltet hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Im Grunde ist diese Maßnahme einfach zu vermitteln. Insbesondere da moderne Betriebssysteme ihre Sicherheitsmechanismen bei der Grundinstallation bereits aktivieren. Benutzer müssten diese Funktionen also willentlich abschalten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme nimmt eigentlich keine Zeit in Anspruch. Auch Kosten entstehen dadurch keine.

M 4.168 AUSWAHL EINES GEEIGNETEN ARCHIVSYSTEMS

Relevanz für den Durchschnittsbenutzer: hoch

Beim Einsatz einer Backuplösung ist es nötig diese entsprechend der eigenen Bedürfnisse und der vorhandenen Ressourcen zu wählen. Unter anderem ist es wichtig Punkte wie „Erweiterbarkeit“, „Zugriffszeit“ oder „Kapazität“ zu beachten, um die Archivierung der Daten längerfristig nutzen zu können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Falls bei der Anschaffung bzw. Umsetzung einer Backuplösung keine Rücksicht auf die oben genannten Punkte genommen wird, können Platzprobleme (und damit notwendigerweise der Verlust älterer Daten) oder überhöhte Kosten auftreten. Hier ein Beispiel:

Beispiel 1: Eberhart hat zur Archivierung der Daten seiner Firma einen PC mit 4 Festplatten, welche in einem Raid-Verbund zusammengeschlossen sind angeschafft. Die Kapazität der

Festplatte wurde zu gering berechnet und so geht Eberhart nach einigen Monaten der Speicherplatz aus. Um Geld zu sparen, entschließt er sich einige ältere Daten zu löschen und so wieder Platz zu schaffen. Als durch einen Virenbefall auf Eberharts PC einige wichtige Dokumente verschwinden, bemerkt Eberhart, dass diese sich unter den gelöschten alten Daten befanden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist eigentlich einfach zu vermitteln, in eigentlich allen anderen Bereichen des Lebens ist es sich vor einer größeren Entscheidung über Bedürfnisse und mögliche zukünftige Ereignisse Gedanken zu machen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann einige Zeit in Anspruch nehmen – Kosten können im besten Fall aber sogar eingespart werden.

M 4.173 REGELMÄßIGE FUNKTIONS- UND RECOVERYTESTS BEI DER ARCHIVIERUNG

Relevanz für den Durchschnittsbenutzer: hoch

Auch Durchschnittsbenutzer sollten regelmäßig überprüfen ob ihr Backupsystem funktioniert und ob Daten aus dem Backup auch wiederherstellbar sind.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wird auf eine regelmäßige Überprüfung der gesicherten Daten verzichtet, kann man sich im Ernstfall nicht darauf verlassen, dass Sicherheitskopien der Daten existieren. Hier ein Beispiel:

Beispiel 1: Ulrike speichert ihre wichtigen Daten regelmäßig auf optischen Datenträgern. Sie vertraut dabei darauf, dass die erstellten CDs funktionieren. Kurz nachdem sie eine CD erstellt hat beginnt ihre Festplatte zu pfeifen und funktioniert wenig später überhaupt nicht mehr. Noch ziemlich ruhig greift Ulrike zu ihrer letzten erstellten CD, doch als sie diese ins Laufwerk einlegt zeit ihr PC keine Daten an, die eingelegte CD wird überhaupt nicht erkannt. Ulrike findet heraus, dass etliche ihrer gebrannten CDs keine Daten enthalten und damit wertlos

sind.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Ein gewisses Maß an Misstrauen vorausgesetzt, sollten auch Durchschnittsbenutzer einsehen, dass es nötig ist gelegentlich zu überprüfen ob ein Speichervorgang funktioniert hat.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann etwas Zeit in Anspruch nehmen, verursacht aber keine weiteren Kosten.

M 4.177 SICHERSTELLUNG DER INTEGRITÄT UND AUTHENTIZITÄT VON SOFTWAREPAKETEN

Relevanz für den Durchschnittsbenutzer: hoch

Niemals sollte man Software ausführen, deren Ursprung man nicht kennt. Insbesondere bei Datei-Anhängen in Emails, fremden USB-Sticks oder Downloads aus dem Internet ist Vorsicht geboten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn man unbedacht Programme ausführt, können diese Malware enthalten. Dabei kann es sich um Software zum Ausspionieren von Passwörtern, Trojanische Pferde oder Backdoors installieren. Hier ein Beispiel:

Beispiel 1: Karl hat auf seinem Computer kein Anti-Viren-Programm installiert und klickt auch auf jeden Email-Anhang den er geschickt bekommt. In einem dieser Anhänge war ein Trojaner versteckt, welcher sich unbemerkt im Hintergrund installiert hat. Von da an werden alle von Karl verwendeten Eingaben protokolliert und viele seiner Passwörter und andere persönliche Information ohne sein Wissen ins Netz verschickt und können dort missbraucht werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Schon früh wird Kindern vermittelt keine Süßigkeiten von Fremden anzunehmen. Ähnlich vorsichtig sollte man mit Software umgehen die man zugeschickt bekommt oder von zweifelhaften Homepages runterlädt.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist weder mit Zeitaufwand noch Kosten verbunden.

M 4.194 SICHERE GRUNDKONFIGURATION EINES APACHE-WEBSERVERS

Relevanz für den Durchschnittsbenutzer: gering

Bei der Installation aus Binärpaketen gibt es wenig zu beachten. Die Installationsroutinen der Binär-Pakete sorgen für eine korrekte Installation. Einige Konfigurationsoptionen können zur Verbesserung der Sicherheit abgeschaltet werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Eine Standardinstallation von Apache ermöglicht es gewisse Informationen über den Server, auf dem Apache läuft, abzufragen. Das kann einem Angreifer im Zweifelsfall die Arbeit erleichtern.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Es gibt Unmengen von Konfigurationsanleitungen für Apache die Durchschnittsbenutzer sowie Fortgeschrittenen ansprechen. Es ist nur nötig den Benutzern zu vermitteln, dass eine Standardkonfiguration nicht automatisch sicher ist.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist für Durchschnittsbenutzer mit wenig Zeitaufwand verbunden. Kosten entfallen.

M 4.195 KONFIGURATION DER ZUGRIFFSSTEUERUNG BEIM APACHE-WEBSEVER

Relevanz für den Durchschnittsbenutzer: gering

Einige Konfigurationsoptionen des Webservers Apache können zur Verbesserung der Sicherheit verändert werden. So gibt es die Möglichkeit nur Besucher von bestimmten IP-Adressen zuzulassen. Diese Maßnahme ist aber eigentlich nur für Entwicklerumgebungen oder Intra-Web-Lösungen geeignet.

Was kann passieren wenn man die Maßnahme nicht setzt?

Eine Standardinstallation von Apache ermöglicht es von jedem Ort der Welt diesen Webserver zu erreichen. Natürlich ist das Risiko für einen Hackerangriff in diesem Fall höher, als wenn nur bekannte Hosts zugreifen dürften.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Es gibt Unmengen von Konfigurationsanleitungen für Apache die Durchschnittsbenutzer sowie Fortgeschrittenen ansprechen. Es ist nur nötig den Benutzern zu vermitteln, dass eine Standardkonfiguration nicht automatisch sicher ist.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist für Durchschnittsbenutzer mit wenig Zeitaufwand verbunden. Kosten entfallen.

M 4.199 VERMEIDUNG GEFÄHRLICHER DATEIFORMATE

Relevanz für den Durchschnittsbenutzer: hoch

Email ist mittlerweile ein wichtiger Übertragungsweg für Viren und Würmer. Aus diesem Grund können Emails, die nicht frei von Attachements und nicht im Plaintext-Format sind, möglicherweise gefährlich sein. Daher gilt es einerseits den Mail-Client dahingehend zu

konfigurieren, dass vor dem Anzeigen von Dateianhängen der Benutzer darauf hingewiesen wird, und andererseits dafür zu sorgen, dass für Emails im HTML-Format die Ausführung von Java-Code abgeschaltet wird.

Was kann passieren wenn man die Maßnahme nicht setzt?

Bei Emails mit Attachements besteht die Gefahr, ausführbare Dateien geschickt zu bekommen, welche schädliche Software wie Viren oder Würmer enthalten können. Ebenso besteht bei HTML-formatierten Emails die Gefahr, dass Programmcode ohne das Wissen des Benutzers ausgeführt wird, welcher möglicherweise Schaden anrichten kann. Hier ein Beispiel:

Beispiel 1: Heinz öffnet alle Dateianhänge, die er in Emails entdeckt. Mit einem der Anhänge installiert sich ein Wurm auf Heinz' Computer der sich erstmal an alle Kontakte aus Heinz' Adressbuch weiterversendet und unbemerkt alle Tastatureingaben von Heinz protokolliert und regelmäßig ins Internet schickt. Zusätzlich installiert der Wurm eine sogenannte Backdoor, über die es dem Programmierer des Wurms jederzeit möglich ist, Heinz' PC fernzusteuern.

Beispiel 2: Silke hat ihren Mailclient dahingehend konfiguriert, ihr das Leben so bequem wie möglich zu machen und einfach alles, wozu er in der Lage ist, darzustellen. Als sie eines Tages ein Mail von einem unbekanntem Absender öffnet, beginnt ihr Computer plötzlich Internetbrowserfenster zu öffnen. In einigen der Fenster erkennt Silke Angebote für Medikamente, in anderen werden illegale Film und Musik-Downloads angeboten und plötzlich friert Silkes PC wegen Überlastung ein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist schwierig zu vermitteln. Die Sicherheitstechnisch korrekten Einstellungen führen oft dazu, dass Emails gar nicht, oder nicht korrekt dargestellt werden. Daher bevorzugen Durchschnittsbenutzer häufig die unsichereren aber bequemeren Einstellungen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme ist mit etwas Zeitaufwand aber ohne zusätzliche Kosten umzusetzen.

M 4.229 SICHERER BETRIEB VON PDAS

Relevanz für den Durchschnittsbenutzer: mittel

In der Regel werden PDAs in Verbindung mit anderen IT-Systemen, beispielsweise dem Arbeitsplatzrechner verwendet. Dabei ist es wichtig gelegentlich zu überprüfen, ob die zu synchronisierenden Verzeichnisse keine unbekannt Dateien enthalten. Weiters kann es vorteilhaft sein, Virenerkennungssoftware, welche inzwischen von immer mehreren Hersteller auch für PDAs angeboten wird, zu verwenden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Es sind bereits einige Viren für PDAs veröffentlicht worden. Diese bisher bekannten Viren richten noch keinen Schaden an, es ist aber mit schädlichen Viren zu rechnen. Weiters droht bei der Synchronisierung mit dem Arbeitsplatzrechner die Gefahr, dass Dateien auf den PDA kopiert werden die möglicherweise Schaden anrichten können. Hier ein Beispiel:

Beispiel 1: David verwendet seinen PDA unterwegs um Emails abzurufen, im Internet zu surfen und sogar um Musik anzuhören. Da er noch nie von Viren für PDAs gehört hat, besucht David auch Webseiten, die er auf seinem PC nicht besuchen würde. Auf einer dieser Webseiten fängt sich David einen Virus ein, der speziell für PDAs entwickelt wurde. Unbemerkt verschickt der Virus Davids Kontakte und Termine an einen unbekanntes Server. Davids PDA stürzt regelmäßig ab und auch die Laufzeit des Akkus wird plötzlich immer kürzer.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist schwierig zu vermitteln. Von Viren für PCs hat eigentlich jeder Benutzer schon gehört, von Viren für PDAs wissen die wenigsten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann Kosten verursachen und auch einige Zeit in Anspruch nehmen.

M 4.231 EINSATZ ZUSÄTZLICHER SICHERHEITSWERKZEUGE FÜR PDAS

Relevanz für den Durchschnittsbenutzer: mittel

Durch den Einsatz von zusätzlichen Sicherheitswerkzeugen – in erster Linie Verschlüsselungssoftware und Virenscannern – können PDAs geschützt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Viren für PDAs existieren bereits und werden in Zukunft sicher an Bedeutung zunehmen. Die davon ausgehende Bedrohung gleicht der im PC-Bereich bekannten.

PDAs sowie Mobiltelefone mit PDA-Funktionalität werden häufig gestohlen – ohne den Einsatz von Verschlüsselungssoftware sind die Daten auf dem Gerät nicht geschützt. Hier ein Beispiel:

Beispiel 1: Gernot ist Manager einiger bekannter Musiker. In seinem PDA hat er Kontaktdaten von etlichen Berühmtheiten gespeichert. In einer belebten Fußgängerzone spürt Gernot einen Stoß und kurze Zeit später bemerkt er, dass sein PDA gestohlen wurde. Am nächsten Tag entdeckt er im Internet Kontaktadressen zu allen Stars, die in seinem PDA gespeichert wurden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht schwierig zu vermitteln. Bei kleinen portablen Geräten ist es nicht verwunderlich, dass diese häufig gestohlen werden. Es sollte im Interesse jedes Benutzers sein, zumindest die Daten zu schützen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann zusätzliche Kosten verursachen, wenn das entsprechende Sicherheitswerkzeug käuflich erworben werden muss. Der Zeitaufwand kann vernachlässigt werden.

M 4.237 SICHERE GRUNDKONFIGURATION EINES IT-SYSTEMS

Relevanz für den Durchschnittsbenutzer: hoch

Im Anwenderbereich sind moderne Betriebssysteme weniger auf Sicherheit als auf Benutzerfreundlichkeit getrimmt. Manche Funktionen stellen dabei unter Umständen ein Sicherheitsrisiko dar. Es gilt zu entscheiden, welche Prioritäten gesetzt werden sollen. Insbesondere für Durchschnittsbenutzer reicht es zumeist automatische Sicherheitsupdates vom Hersteller zu installieren und einen Virenschanner sowie eine lokale Firewall einzurichten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne Virenschanner bzw. Firewall stehen alle Türen für jede Art von Malware, Viren und Hacker offen. Hier ein Beispiel:

Beispiel 1: Auf Alfreds Computer ist ein bekanntes Betriebssystem installiert. Alfred hat sich gegen die Standardeinstellungen entschieden und verzichtet sowohl auf Sicherheitsupdates, als auch auf die Firewallfunktionen des Betriebssystems. Unvermeidlicherweise kommt es dazu, dass Alfred sich einen Virus einfängt. Sein Betriebssystem wird instabil und stürzt immer wieder ab. Alfred kommt nicht auf die Idee, dass ein Virus schuld sein könnte und vermutet eine defekte Hardwarekomponente. Er gibt Geld für einen neuen Prozessor und Speicher aus, und bemerkt keine Verbesserung.

Beispiel 2: Daniel verwendet keine Firewall, da er glaubt, dass eine Firewall seinen PC langsamer machen würde. Da der Computer ungeschützt mit dem Internet verbunden wird, gelingt es einem Hacker in Daniels PC einzudringen und einen kleinen Server zum Datenaustausch zu installieren. Von nun an dient Daniels Computer einer Gruppe von Hackern als Speicherplatz, auf dem auch etliche illegale Dateien gespeichert werden. Abgesehen von den hohen Netzwerklasten könnte Daniel sogar für die illegalen gespeicherten Dateien verantwortlich gemacht werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach umzusetzen. Moderne Betriebssysteme werden schon mit diversen Sicherheitsmechanismen ausgeliefert und weisen bereits bei der Installation darauf hin, dass diese verwendet werden sollten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme lässt sich schnell und ohne zusätzliche Kosten umsetzen.

M 4.238 EINSATZ EINES LOKALEN PAKETFILTERS

Relevanz für den Durchschnittsbenutzer: hoch

Der Einsatz eines Paketfilters lohnt sich in jedem Fall und ist nicht nur für Server sondern auch für Arbeitsplatz-PCs sinnvoll. Siehe M 4.237.

M 4.247 RESTRIKTIVE BERECHTIGUNGSVERGABE UNTER WINDOWS XP

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.19, M 4.20, M 4.149.

M 4.248 SICHERE INSTALLATION VON WINDOWS XP

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.136, M 4.146, M 4.237.

M 4.249 WINDOWS XP SYSTEME AKTUELL HALTEN

Relevanz für den Durchschnittsbenutzer: hoch

Windows XP bietet eine Funktion zum automatischen aktualisieren des Betriebssystem. Diese Funktion ist extrem wertvoll und sollte in jedem Fall aktiviert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Durch Updates werden Sicherheitslöcher geschlossen. Zusätzlich können dem Betriebssystem neue Funktionen hinzugefügt werden. Wenn ein Betriebssystem nicht aktualisiert wird bleiben Sicherheitslücken bestehen und erhöhen die Wahrscheinlichkeit für Sicherheitsvorfälle. Hier ein Beispiel:

Beispiel 1: Markus hat die automatische Aktualisierungsfunktion seines Betriebssystems seit dem ersten Tag abgeschaltet, da er die Neustarts, welche auf eine Aktualisierung folgen nicht ausstehen kann. Sein Betriebssystem ist daher mit Sicherheitslücken gespickt, was aber Markus nicht davon abhält mit seinem PC ins Internet zu gehen. Kurz nach der Veröffentlichung eines Wurms wird auch Markus' Computer infiziert. Die Festplatte beginnt zu rattern und kurz darauf erscheint ein Bluescreen. Von nun an lässt sich der PC nicht mehr booten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist einfach umzusetzen. Moderne Betriebssysteme weisen bereits bei der Installation auf die Möglichkeit automatischer Aktualisierungen hin, und empfehlen eindeutig, diese zu benutzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist ohne Zeitaufwand und ohne Kosten umzusetzen.

M 4.251 ARBEITEN MIT FREMDEN IT-SYSTEMEN

Relevanz für den Durchschnittsbenutzer: hoch

Wenn fremde IT-Systeme verwendet werden – sei es in einem Internetcafe, bei einem Bekannten/Verwandten oder an einem öffentlich zugänglichen Portal – ist insbesondere beim Einsatz von USB-Sticks oder anderen Medien zur Datenspeicherung oder Weiterleitung (z.B. auch via Email) auf besondere Vorsicht zu achten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Bei fremd administrierten Systemen weiß man normalerweise nichts über den Sicherheitsstandard. Sollte beispielsweise kein – oder kein aktueller – Virens scanner vorhanden sein, besteht die Gefahr einer Infektion. Wenn Mailwürmer ihr Unwesen treiben oder der Computer sogar von einem Hacker kontrolliert wird, besteht die Gefahr, dass eingegebene Email-Adressen als Spam-Ziel oder Wurm-Empfänger genutzt werden. Hier ein Beispiel:

Beispiel 1: Elfriede besucht während eines Urlaubs in Tunesien ein Internetcafe um ihren Eltern eine elektronische Postkarte zukommen zu lassen und sich selbst ihre bisher geschossenen Fotos zu schicken. Als Elfriede die Speicherkarte ihrer Kamera in das Lesegerät steckt, infiziert ein Virus die Speicherkarte. Ohne etwas davon zu wissen verschickt Elfriede ihre Fotos und auch die Postkarte für ihre Eltern. Als Elfriede aus ihrem Urlaub heimkehrt wundert sie sich, dass ihre Mailbox mit tausenden neuen Nachrichten gefüllt ist. Im Minutenabstand treffen neue Mails ein, die sich alle als Spam herausstellen. Auch Elfriedes Eltern berichten über Unmengen von Spam seitdem die Postkarte eingetroffen ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht einfach umzusetzen. Auch wenn auf den ersten Blick alles in Ordnung scheint kann auf einem Computer Software installiert sein, die alle Eingaben protokolliert. Tatsächlich gibt es kaum Möglichkeiten sich bei der Verwendung eines fremden Systems, auf ein Mindestmaß an Sicherheit verlassen zu können.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist unter Umständen mit einem Hohen Zeitaufwand verbunden. Kosten entfallen allerdings.

M 4.253 SCHUTZ VOR SPYWARE

Relevanz für den Durchschnittsbenutzer: hoch

Zum Schutz vor Spyware empfiehlt es sich gewisse Einstellungen am Browser zu treffen, sowie regelmäßig Softwareupdates einzuspielen und ein Virensuchprogramm einzusetzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Bei Spyware handelt es sich um Schadsoftware, welche heimlich Daten sammelt und an Dritte übermittelt. Dabei kann es sich um Daten über das Internet-Surf-Verhalten handeln, oder aber auch um protokollierte Eingaben. Damit kann ein potentieller Angreifer Details über den Benutzer und seinen PC Sammeln und diese im Bedarfsfall einsetzen oder aber weiterverkaufen. Hier ein Beispiel:

Beispiel 1: Mario kümmert sich, was seinen Computer betrifft, wenig um seine Privatsphäre. Daher ist sein PC auch mit Spyware verseucht, die sich beim Besuch einiger Webseiten installiert hat. Die meisten dieser Programme beobachten nur wie lange Mario im Internet ist und welche Webseiten er besucht. Eines dieser Spywareprogramme protokolliert aber jeden Tastendruck mit, und übermittelt diese an einen Hacker. Dieser kann ohne Probleme Usernamen und Passwörter mitlesen, sowie den Inhalt von Emails die Mario verschickt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme einfach umzusetzen. Automatische Updates sollten aktiviert sein, die Browsereinstellungen sollten vor der Ausführung von JavaScripts und Applets sowie ActiveX Elementen zumindest nachfragen. Ebenso sollte ein Virenschanner zur Standardsoftware auf jedem PC gehören.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert keinen zusätzlichen Zeitaufwand und auch keine weiteren Kosten.

M 4.274 SICHERE GRUNDKONFIGURATION VON SPEICHERSYSTEMEN

Relevanz für den Durchschnittsbenutzer: mittel

Für Durchschnittsbenutzer die ein Speichersystem betreiben wollen, gibt es zusätzlich zu M 4.237 nichts zu beachten.

M 4.275 SICHERER BETRIEB EINES SPEICHERSYSTEMS

Relevanz für den Durchschnittsbenutzer: mittel

Für Durchschnittsbenutzer die ein Speichersystem betreiben wollen, gibt es zusätzlich zu M 4.146 und M 4.152 nichts zu beachten.

M 4.293 SICHERER BETRIEB VON HOTSPOTS

Relevanz für den Durchschnittsbenutzer: mittel

Beim Einsatz eines Hotspots ist darauf zu achten, dass das Netzwerk vom WLAN getrennt und nur über ein Sicherheitsgateway zu erreichen ist. Weiter empfiehlt es sich auf alle Fälle WLAN-Spezifische Sicherheitsmechanismen wie WPA bzw. WPA2 zu verwenden. Der Betrieb eines Hotspots ermöglicht prinzipiell jedem Fremden Zugang zum WLAN und damit dem Internet. Durchschnittsbenutzer sollten im Zweifelsfall davon absehen, einen Hotspot zu betreiben um das eigene Netzwerk zu schützen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein offener Hotspot ermöglicht jedem Passanten Zugriff aufs WLAN. Wenn dabei auf Sicherheitsmechanismen verzichtet wird, bedeutet das zugleich Zugriff auf das Netzwerk und damit alle PCs in dem Netzwerk.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist grundsätzlich einfach umzusetzen. Dennoch gibt es vieles zu beachten und daher sollten Durchschnittsbenutzer vom Betrieb eines Hotspots absehen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann einige Zeit in Anspruch nehmen, verursacht aber keine weiteren Kosten.

M 4.294 SICHERE KONFIGURATION DER ACCESS POINTS

Relevanz für den Durchschnittsbenutzer: hoch

WLAN Access Points sollten grundsätzlich so konfiguriert werden, dass sie für Fremde nicht zugänglich sind. Dazu gehört es, das Netzwerk nicht bekannt zu geben. Weiters sollten die zur Verfügung stehenden Sicherheitsmechanismen wie WPA bzw. WPA2 genutzt werden um den Zugang einzuschränken. Außerdem ist darauf zu achten, sicherheitsrelevante Konfigurationswerte von Access Points niemals im Auslieferungszustand zu belassen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein nicht gesicherter Access Point, ein sogenannter Hotspot, ermöglicht jedem Passanten Zugriff aufs WLAN. Wenn dabei auf Sicherheitsmechanismen verzichtet wird, bedeutet das zugleich Zugriff auf das Netzwerk und damit alle PCs in dem Netzwerk. Hier ein Beispiel:

Beispiel 1: Susanne hat sich zu ihrem neuen Notebook auch einen WLAN-Router gekauft, damit sie ohne Kabelsalat von ihrer Couch aus Internetsurfen kann. Susanne wundert sich bei der Installation noch, wie problemlos alles voran geht – einfach nur anstecken und erreicht ihr WLAN – und schon bald liest sie von ihrer Couch aus Emails. Einige Zeit später klingelt es an der Tür und Susanne staunt nicht schlecht, als sie einem Polizisten gegenübersteht, der sie beschuldigt auf einem Video-Portal im Internet ein terroristisches Drohvideo gepostet zu haben. Natürlich hat Susanne nichts damit zu tun, aber ein böartiger Passant konnte über das ungeschützte WLAN das Video hochladen. Susanne kann sich noch an den Abend erinnern, als ihre Internetverbindung so langsam erschien, und sie sich dachte es würde wohl mal wieder Windows schuld sein.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist grundsätzlich einfach umzusetzen. Es gilt allerdings besonders darauf zu achten, keine Standardwerte (insbesondere bei Passwörtern) zu verwenden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann einige Zeit in Anspruch nehmen, verursacht aber keine weiteren Kosten.

M 4.306 UMGANG MIT PASSWORT-SPEICHER-TOOLS**Relevanz für den Durchschnittsbenutzer: hoch**

Beim Einsatz von Passwort-Speicher-Tools, sogenannten Passwort-Safes ist es wichtig auf gewisse Kriterien zu achten. Auf den Inhalt des Safes darf keinesfalls Zugriff durch Unberechtigte möglich sein. Das bedeutet einerseits, dass der Passwort-Safe ein Master-Passwort unterstützen und fordern muss, und sich dieses keinesfalls zur Erhöhung der Usability merken darf. Auch dürfen die Daten nicht im Klartext auf Datenträgern gespeichert

werden sondern müssen auf alle Fälle verschlüsselt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ein schlechtes, oder falsch eingesetztes Passwort-Speicher-Tool hat den großen Nachteil, dass es den Zugriff auf alle Passwörter eines Users bietet. Hier ein Beispiel:

Beispiel 1: Michael hat sich bei etlichen Onlinediensten angemeldet und kommt inzwischen mit den verschiedenen Passwörtern, die er gewählt hat, nicht mehr klar. Daher investiert er einen kleinen Betrag in eine Software die als sogenannter Passwort-Safe fungiert. Fleißig notiert Michael alle Passwörter in dem Programm, ohne sich über die genaue Funktion Gedanken zu machen. Michael verzichtet auf ein Masterpasswort und so kann jeder auf das Programm zugreifen und die Passwörter auslesen. Ein Angreifer erlangt so Zugriff auf Michaels Passwörter und verwendet nun Michaels Email-Account zum versenden von Spam-Mails.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Allerdings erfordert diese Maßnahme etwas Recherche und auch Konsequenz seitens des Benutzers.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Software welche diese Funktionalität bereitstellt gibt es zum Teil gratis oder schon in Betriebssysteme integriert. Die Konfiguration und der korrekte Einsatz dieser Software kann einige Zeit in Anspruch nehmen.

M 5 MAßNAHMENKATALOG KOMMUNIKATION

Der Maßnahmenkatalog 5 umfasst alle erdenklichen Kommunikationsformen. Angefangen von Telefon- und Fax- über Email- und VoIP-Lösungen werden weit verbreitete Medien und Protokolle auf Vertraulichkeit sowie Manipulierbarkeit getestet.

M 5.9 PROTOKOLLIERUNG AM SERVER

Relevanz für den Durchschnittsbenutzer: mittel

Siehe M 4.25, M 4.47, M 4.54, M 4.106.

M 5.10 RESTRIKTIVE RECHTEVERGABE

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Siehe M 4.53, M 4.135.

M 5.23 AUSWAHL EINER GEEIGNETEN VERSANDART FÜR DEN DATENTRÄGER

Relevanz für den Durchschnittsbenutzer: mittel

Beim Versand von Datenträgern ist es wichtig darauf zu achten, dass eine Beschädigung ausgeschlossen wird. Insbesondere gilt das für optische Datenträger (CDs, DVDs) sowie für mechanische Datenträger (Festplatten).

Was kann passieren wenn man die Maßnahme nicht setzt?

Beim Versand können durch schlechte Behandlung Datenträger zerstört werden. So reagieren beispielsweise Festplatten schlecht auf Erschütterungen, CDs bzw. DVDs werden leicht zerkratzt und damit unlesbar. Hier ein Beispiel:

Beispiel 1: Gerald möchte seinem Cousin eine Festplatte, die er mit seiner Musiksammlung bespielt hat schicken. Gerald steckt die Festplatte in ein Luftpolsterkuvert und gibt es bei der Post auf. Leider sind die Postbeamten nicht gerade vorsichtig und so muss die Festplatte einige Erschütterungen durch Stürze einstecken. Als Gerald's Cousin das Kuvert öffnet und die Festplatte anstecken möchte, wird sie in seinem Computer nicht erkannt. Außerdem macht die Festplatte seltsame Geräusche.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen, wenn man sich über die Funktionsweise von Datenträger informiert hat. Es sollte jedem Benutzer klar sein, dass Datenträger jeder beliebigen Art nicht unzerstörbar sind.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme lässt sich in jedem Fall schnell und kostengünstig umsetzen.

M 5.26 TELEFONISCHE ANKÜNDIGUNG EINER FAXSENDUNG

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Wenn vertrauliche oder finanzwirksame Inhalte über Fax versandt werden, ist es in jedem Fall empfehlenswert den Empfänger im Vorhinein auf das Fax aufmerksam zu machen, damit dieser das Fax sofort entgegen nehmen kann.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn bei wichtigen Daten der Empfänger eines Faxes nicht vorher informiert wird, ist nicht gewährleistet, dass der gewünschte Empfänger der Erste ist, der das Fax zu Gesicht bekommt.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit geringen Kosten verbunden, der Zeitaufwand ist sehr gering.

M 5.27 TELEFONISCHE RÜCKVERSICHERUNG ÜBER KORREKTEN FAXEMPFBANG**Relevanz für den Durchschnittsbenutzer: mittel bis hoch**

Bei wichtigen Fax-Sendungen sollte beim Empfänger nachgefragt werden, ob eine vollständige Übertragung gelungen ist. Neuere Fax-Geräte erstellen allerdings bereits einen Sendebericht, welcher in den meisten Fällen als Bestätigung der erfolgreichen Sendung ausreicht.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne die Rückfrage ob ein Fax erfolgreich angekommen ist, kann man – insbesondere bei älteren Geräten, welche keinen Sendebericht erstellen – nicht davon ausgehen, dass die Sendung erfolgreich war. Insbesondere bei Termingebundenen Sendungen kann diese Unsicherheit Probleme bereiten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit geringen Kosten verbunden, der Zeitaufwand ist ebenfalls gering.

M 5.28 TELEFONISCHE RÜCKVERSICHERUNG ÜBER KORREKTEN FAXABSENDER**Relevanz für den Durchschnittsbenutzer: hoch**

Beim Erhalt einer wichtigen oder ungewöhnlichen Faxesendung sollte man die Möglichkeit in Betracht ziehen, sich beim Faxabsender zu vergewissern, ob die betreffende Nachricht auch

wirklich von ihm geschickt wurde.

Was kann passieren wenn man die Maßnahme nicht setzt?

Man kann bei einem (unerwartetem) Fax nicht sicher sein, dass es wirklich vom angeblichen Absender geschickt wurde. So kann beispielsweise ein öffentlich Zugängliches Faxgerät eines Unternehmens oder Amtes genutzt werden, um dem Empfänger eine gefälschte Nachricht zukommen zu lassen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit geringen Kosten verbunden, der Zeitaufwand ist ebenfalls gering.

M 5.36 VERSCHLÜSSELUNG UNTER UNIX UND WINDOWS NT

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Siehe M 4.22 und M 4.29.

M 5.45 SICHERHEIT VON WWW-BROWSERN

Relevanz für den Durchschnittsbenutzer: hoch

Jeder Benutzer, der Webseiten besuchen will, muss einen WWW-Browser verwenden. Es gibt verschiedenste Programme von verschiedenen Herstellern – empfehlenswerte Browser werden ständig gewartet und verbessert, daher ist es – wie für alle anderen Programme – relevant regelmäßige Sicherheitsupdates zu installieren. Genauso wichtig ist es die eingebauten Sicherheitsfunktionen von aktuellen Browsern (z.B. gegen Phishing) einzusetzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Genauso wie viele andere Programme enthalten auch WWW-Browser Sicherheitslücken. Mit einem veralteten Browser läuft der Benutzer Gefahr, durch den Besuch bestimmter Webseiten schädlicher Software alle Türen zu öffnen. Hier ein Beispiel:

Beispiel 1: Erikas PC ist schon einige Jahre alt – genauso wie die Software auf dem PC. Ihr Browser bietet noch keine Schutzmechanismen vor Phishing-Seiten oder XSS-Attacken. Als Erika ein Email bekommt, in dem sie darauf hingewiesen wird, dass sie sich bei ihrem Onlinebanking-Service aus Wartungsgründen anmelden und einige Daten aktualisieren muss macht sie das auch sofort. Sie klickt also auf den Link im Email und wird auf eine Hacker-Seite umgeleitet, auf der ihre Informationen abgefragt werden. Ohne es zu wissen, übermittelt Erika ihre persönlichen Daten und Login-Informationen an eine kriminelle Organisation. Ein aktueller Browser hätte Erika auf die Gefahr hinweisen können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen, aktuelle Browser weisen selbstständig auf Aktualisierungen hin, der User muss nur noch zustimmen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist nicht mit Kosten verbunden, der Zeitaufwand ist vernachlässigbar.

**M 5.51 SICHERHEITSTECHNISCHE ANFORDERUNGEN AN DIE
KOMMUNIKATIONSVERBINDUNG TELEARBEITSRECHNER-INSTITUTION****Relevanz für den Durchschnittsbenutzer: mittel**

Für Telearbeiter gelten besondere Richtlinien. Die Vertraulichkeit und Integrität der übertragenen Daten muss sichergestellt werden. Obwohl diese Maßnahme für Durchschnittsbenutzer von großer Bedeutung sein kann, ist es auf jeden Fall nötig diese Maßnahme unter Anleitung eines Administrators umzusetzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Der Verzicht auf diese Maßnahme kann dazu führen, dass die Kommunikation zwischen Arbeitsplatz und Telearbeitsplatz von unauthorisierten Dritten belauscht und sogar manipuliert werden kann. Fehler bei der Datenübertragung können im schlimmsten Fall die ganze Arbeit des Telearbeiters zunichte machen und damit hohe Kosten verursachen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht einfach umzusetzen und sollte unbedingt mit Hilfe eines Administrators realisiert werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahme kann sowohl einen hohen Zeitaufwand als auch enorme Kosten mit sich bringen.

M 5.57 SICHERE KONFIGURATION DER MAIL-CLIENTS

Relevanz für den Durchschnittsbenutzer: mittel

Die sichere Konfiguration von Mail-Clients beinhaltet unter anderem den Einsatz von verschlüsselten Kommunikationsmethoden (SSL, TLS). Weiters ist es wichtig keine Passwörter im Programm zu speichern und die Email-Anzeige auf Klartext zu stellen, um eventuell versteckte Skripte in HTML-E-mails nicht auszuführen. Für Attachements sollte ein aktueller Virens Scanner zur Verfügung stehen, um die Gefahr von Viren und Trojanern zu verringern.

Was kann passieren wenn man die Maßnahme nicht setzt?

Durch unsichere Email-Clients können schädliche Programme, welche per Email verschickt werden, ausgeführt werden. Dadurch kann großer Schaden am betroffenen PC entstehen. Zusätzlich ist zu beachten, dass die Kommunikation leicht ablauschbar ist, und damit Passwörter und Usernamen mitgelauscht werden können, wenn keine Verschlüsselung eingesetzt wird. Hier ein Beispiel:

Beispiel 1: Hans will sich das Leben so bequem wie möglich machen. Daher aktiviert er alle erdenklichen Funktionen seines Email-Clients, und stellt sogar ein, dass JavaScript-Elemente

von Emails ausgeführt werden, um bloß kein Detail eines Emails zu verpassen. Er bekommt ein HTML-formatiertes Email zugesandt welches er – obwohl ihm der Absender unbekannt ist – sofort öffnet. Plötzlich wird der PC immer langsamer und nur kurze Zeit später stürzt er mit einem Blue Screen ab. Im letzte Email, das Hans geöffnet hat waren einige Zeilen Programmcode versteckt, welche automatisch ausgeführt wurden und wichtige Dateien des Betriebssystems verändert bzw. gelöscht hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Bei aktuellen Email-Clients sind viele risikobehaftet Funktionen standardmäßig abgeschaltet.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht keine Kosten, der Zeitaufwand ist relativ gering.

M 5.63 EINSATZ VON GNUPG ODER PGP

Relevanz für den Durchschnittsbenutzer: hoch

Der Einsatz von Verschlüsselungsprodukten – insbesondere im Email-Bereich erhöht das Sicherheitsniveau enorm. Durch Verschlüsselung bzw. Signaturen kann die Vertraulichkeit geschützt werden, und die Authentizität von Dateien oder Nachrichten kann überprüft werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn man Nachrichten oder Dateien zugeschickt bekommt, ist es ohne Hilfsmittel unmöglich zu überprüfen, ob der Inhalt einem Dritten bekannt oder verändert wurde. Hier ein Beispiel:

Beispiel 1: Leo verschickt wichtige Finanzinformationen via Email an seinen Geschäftspartner Gerd. Einem Hacker gelingt es diese Emails abzufangen. Die Informationen enthalten wertvolle Hinweise über einen bevorstehenden Börsengang von Leos Firma. Der Hacker wird diese Informationen nutzen und enorme Aktiengewinne einfahren. Damit nicht genug verfälscht der Hacker auch noch die Zahlen der Nachricht und leitet sie an Gerd weiter. Gerd

vertraut auf die Informationen seines Partners Leo und trifft dadurch einige folgenschwere Entscheidungen, die hohe finanzielle Verluste mit sich bringen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Umsetzung der Maßnahme erfordert ein gewisses Grundwissen. Wenn aber erstmal die Software für die Verschlüsselung installiert ist, ist es einfach die Maßnahme anzuwenden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Anfänglich erfordert die Maßnahme einige Zeit. Kosten fallen nicht zwangsläufig an, da es viele Open Source Lösungen gibt.

M 5.64 SECURE SHELL

Relevanz für den Durchschnittsbenutzer: hoch

Sollte der Einsatz von Terminal-Programmen nötig sein, sollte unbedingt das SSH Protokoll verwendet werden. Telnet bzw. FTP sind Klartextprotokolle, die von dritten ohne Aufwand mitgelesen werden können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn man anstelle von SSH oder SFTP Telnet, ftp oder ähnliche Klartextprotokolle verwendet, kann ein unauthorisierter Dritter alle Informationen – inklusive übertragener Usernamen und Passwörter – mitlesen. Hier ein Beispiel:

Beispiel 1: Erika bekommt von ihrer Universität einen Email-Zugang zur Verfügung gestellt. Auf einer veralteten Homepage hat sie eine Anleitung gefunden, wie man die Emails direkt am Server lesen kann. Sie meldet sich via Telnet mit ihrem Usernamen und Passwort auf dem Mailserver an. Ein anderer User überwacht alle Verbindungen zu dem Server und wird sofort auf Erikas Usernamen und Passwort aufmerksam. Auch ihre Emails kann er lesen und lernt auf diesem Weg sehr viel über Erika. Immer wieder besucht er „zufällig“ dieselben Veranstaltungen wie Erika und ihre Freundinnen, besucht dieselben Lokale. Eines Abends spricht er Erika an ...

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Inzwischen akzeptiert ein Großteil der Server keine Telnet-Verbindungen mehr. Insofern ist man ohnehin gezwungen die Maßnahme umzusetzen. Einen großen Teil der Verantwortung für die Umsetzung dieser Maßnahme sollten eigentlich Administratoren tragen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert kaum Zeit und verursacht auch keine Kosten.

M 5.66 VERWENDUNG VON SSL**Relevanz für den Durchschnittsbenutzer: hoch**

SSL wird unter anderem bei der WWW-Nutzung als Sicherheitsprotokoll eingesetzt. Dabei wird das gesamte Datenaufkommen verschlüsselt zwischen Server und Browser übertragen. Für einen sinnvollen Einsatz ist es nötig, aufmerksam auf eventuelle Fehlermeldungen des Browsers zu achten – dieser würde nämlich auch bemerken, wenn die Verschlüsselung nicht vertrauenswürdig ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne Verschlüsselung lassen sich alle Anfragen an einen Web-Server beobachten. Das enthält auch eventuell übertragene Passwörter und Benutzernamen. Hier ein Beispiel:

Beispiel 1: Simon erhält ein Email, welches anscheinend von seiner Bank kommt. Darin ist ein Link zu einer Homepage enthalten, wo sich Simon mit seinen Onlinebankingdaten anmelden soll. Als er die Seite besucht, macht ihn sein Browser darauf aufmerksam, dass die Verschlüsselung über ein unbekanntes Zertifikat erfolgt. Simon ignoriert den Hinweis und meldet sich auf der gefälschten Bank-Seite mit seinen Daten an. Ein Hacker ist jetzt im Besitz von Simons Bank-Daten.

Beispiel 2: Der 16jährige Markus ist in einem Forum für Jugendliche angemeldet. Sein

neugieriger Vater liest die unverschlüsselte Anmeldung seines Sohnes im Forum mit. Spät abends meldet sich Markus Vater in dem Forum unter dem Namen seines Sohnes an und sieht sich um, womit sein Sohn so beschäftigt ist. Am nächsten Tag wird Markus von seinen Freunden gefragt warum er am Vorabend nicht mit ihnen reden wollte...

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Umsetzung der Maßnahme erfordert einige Aufmerksamkeit. Fehlermeldungen müssen genau gelesen und entsprechend behandelt werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Umsetzung der Maßnahme erfordert nur etwas Aufmerksamkeit bei einem Sicherheitsvorfall. Ansonsten geschieht alles im Hintergrund.

M 5.68 EINSATZ VON VERSCHLÜSSELUNGSVERFAHREN ZUR NETZKOMMUNIKATION

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 5.63, M 5.64, M 5.66

M 5.69 SCHUTZ VOR AKTIVEN INHALTEN

Relevanz für den Durchschnittsbenutzer: hoch

Moderne Browser bieten unzählige Sicherheitsmechanismen um den PC vor aktiven Inhalten zu schützen. Diese Sicherheitsmechanismen sollten in jedem Fall aktiviert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Durch das Besuchen von bestimmten Webseiten können aktive Inhalte schädliche Aktionen auf dem PC des Benutzers ausführen. So können beispielsweise Viren verbreitet oder Dateien verändert werden. Hier ein Beispiel:

Beispiel 1: Michael verwendet einen veralteten Webbrowser und hat keine Sicherheitsmechanismen aktiviert. Er ist gerade auf der Suche nach seltenen Musikstücken und kommt dabei auf eine Homepage, über die ein Spionageprogramm verbreitet wird. Aufgrund der fehlenden Sicherheitsvorkehrungen des Browsers installiert sich das Spionageprogramm. Von nun an werden alle Aktivitäten von Michael im Internet überwacht und an einen Server zur Auswertung weitergeleitet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Empfohlene Schutzvorkehrungen sind bei der Installation eines Browsers in der Regel ohnehin aktiviert.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist ohne weitere Kosten und nur mit minimalem Zeitaufwand verbunden.

M 5.72 DEAKTIVIEREN NICHT BENÖTIGTER NETZDIENSTE

Relevanz für den Durchschnittsbenutzer: mittel

Siehe M 4.12, M 4.38.

M 5.91 EINSATZ VON PERSONAL FIREWALLS FÜR INTERNET-PCS

Relevanz für den Durchschnittsbenutzer: hoch

Personal Firewalls können den PC eines Benutzers vor unrechtmäßigen Zugriffen schützen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne Personal Firewall kann grundsätzlich jedes Programm Verbindung zum Internet herstellen. Ebenso ist es jedem Internetbesucher eine Verbindung zu jedem anderen

Computer aufzubauen, der nicht durch eine Firewall geschützt wird. Hier ein Beispiel:

Beispiel 1: Sebastian hat noch nie über die Verwendung einer Firewall nachgedacht. Als er ein Email öffnet und den enthaltenen Anhang öffnet, installiert sich ohne sein Wissen ein Server-Dienst auf seinem Computer der Hackern den Zugriff auf seine Daten ermöglicht. Ohne es zu wissen betreibt Sebastian jetzt eine File-Sharing Plattform, für die er, rechtlich gesehen, auch zur Verantwortung gezogen werden kann.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Moderne Betriebssysteme werden mit Firewall-Funktionalität ausgeliefert und weisen auch darauf hin, dass diese Funktionen genutzt werden sollten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Ein Grundschutz ist ohne hohen Zeitaufwand und ohne zusätzliche Kosten umzusetzen. Professionell konfigurierte Firewalls nehmen allerdings einige Zeit in Anspruch.

M 5.96 SICHERE NUTZUNG VON WEBMAIL

Relevanz für den Durchschnittsbenutzer: hoch

Webmail ist grundsätzlich eine Benutzerfreundliche Möglichkeit seine Emails zu lesen. Auf alle Fälle ist es nötig darauf zu achten, dass der Anbieter eine verschlüsselte Verbindung anbietet, um Benutzernamen und Passwörter sowie den Inhalt der Emails zu schützen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Da das Hypertext Transport Protokoll (HTTP) ein Klartextprotokoll ist, können unverschlüsselt übertragene Usernamen und Passwörter, sowie der Inhalt von Hypertext-Dokumenten von unberechtigten Dritten mitgelesen, oder auch verändert werden. Damit ist eine sichere Kommunikation über Webmail nur möglich, wenn sie mittels SSL verschlüsselt wird.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Es ist nur nötig, darauf zu achten, dass eine gültige Verschlüsselungsform eingesetzt wird.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme erfordert in der Regel keine zusätzlichen Kosten. Der Zeitaufwand ist im Normalfall auch vernachlässigbar, da inzwischen kaum Webmail Provider existieren, die keine SSL-Verschlüsselung anbieten.

M 5.98 SCHUTZ VOR MISSBRAUCH KOSTENPFLICHTIGER EINWAHLNUMMERN**Relevanz für den Durchschnittsbenutzer: gering bis mittel**

Bei der Nutzung eines Modems zur Verbindung mit dem Internet besteht die Gefahr, durch Verwendung einer falschen Nummer den Überblick über die Kosten zu verlieren. Eine falsche Nummer kann unter anderem durch sogenannte Dialer, bzw. beim Aufruf von kostenpflichtigen Services ins Wählprogramm gelangen. Durch die zunehmende Verbreitung von Breitbandinternetzugängen und dem Rückgang von Modems verliert diese Maßnahme an Bedeutung.

Was kann passieren wenn man die Maßnahme nicht setzt?

Bei Verwendung von kostenpflichtigen Mehrwertnummern kann man sehr leicht den Überblick über die laufenden Kosten der Internetnutzung verlieren. Insbesondere wenn man nach der Nutzung einer kostenpflichtigen Einwahlnummer die Verbindung nicht beendet, oder aber für die regelmäßige Internetnutzung auch die kostenpflichtige Einwahlnummer verwendet.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach umzusetzen. Allerdings ist Konsequenz seitens der Nutzer nötig. Alternativ können auch Administratoren Mehrwertnummern sperren, um so jede Gefahr auszuschließen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme verursacht weder Kosten noch hohen Zeitaufwand.

M 5.108 KRYPTOGRAPHISCHE ABSICHERUNG VON E-MAIL

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme kann auch für Durchschnittsbenutzer hilfreich sein. Siehe M 5.63, M 5.68.

M 5.110 ABSICHERUNG VON E-MAIL MIT SPHINX (S/MIME)

Relevanz für den Durchschnittsbenutzer: hoch

Diese Maßnahme kann auch für Durchschnittsbenutzer hilfreich sein. Siehe M 5.63, M 5.68, M5.108.

M 5.121 SICHERE KOMMUNIKATION VON UNTERWEGS

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 4.29, M 4.31, M 4.28, M 4.229, M 4.230

M 5.122 SICHERER ANSCHLUSS VON LAPTOPS AN LOKALE NETZE

Relevanz für den Durchschnittsbenutzer: mittel

Als mobile Geräte haben Laptops ein höheres Gefährdungspotential als stationäre IT-Systeme. Für Durchschnittsbenutzer reichen im Allgemeinen jedoch dieselben Sicherheitsmechanismen wie für Stand-PCs. (Siehe M 4.136, M 4.137, M 4.151, M 4.248).

Was kann passieren wenn man die Maßnahme nicht setzt?

In Firmennetzen können Laptops, die gleichberechtigt in ein LAN angeschlossen werden, ein Sicherheitsrisiko darstellen, da sie Zugriff auf alle Netzwerkressourcen haben.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Die Umsetzung ist allerdings schwierig zu realisieren und sollte durch Administratoren erfolgen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme kann hohe Kosten verursachen und viele Arbeitsstunden in Anspruch nehmen.

M 5.139 SICHERE ANBINDUNG EINES WLANS AN EIN LAN**Relevanz für den Durchschnittsbenutzer: hoch**

Bei der Einbindung eines WLANs in eine LAN muss besonderes Augenmerk auf die Sicherheit gelegt werden. Siehe M 4.293.

Was kann passieren wenn man die Maßnahme nicht setzt?

Insbesondere frei zugängliche WLANs – sog. Hotspots ermöglichen einen leichten Zugang auf ein Netzwerk. Wenn das LAN nicht vor dem WLAN abgesichert wird, besteht die Gefahr, dass Unberechtigte auf Ressourcen aus dem LAN zugreifen können. Hier ein Beispiel:

Beispiel 1: Willi hat zusätzlich zu dem Netzwerk, welches seinen PC mit den PCs seiner Söhne verbindet ein WLAN eingerichtet, um mit dem Laptop überall im Haus eine Verbindung zum Internet und zu seinen Dokumenten zu haben. Leider hat Willi vergessen, sein WLAN abzusichern und auch sein restliches Netzwerk nicht vom WLAN getrennt und so kommt es dazu, dass sich eines Tages ein Passant vor Willis Haus mit dem WLAN verbinden kann und Zugriff auf alle Daten von Willis PC hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist einfach zu vermitteln. Wenn man Angst vor einem Einbruch durchs Kellerfenster hat, sollte man auch den Keller mit einer Sicherheitstür vom restlichen Haus trennen. Das Umsetzen der Maßnahme ist allerdings nicht ganz einfach, da die Sicherheit in vielen Fällen der Nutzbarkeit im Wege steht.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Maßnahme ist mit vertretbarem Zeitaufwand zu realisieren, zusätzliche Kosten entfallen, da es unzählige Open-Source Lösungen gibt, die sich mit dem Problem befassen.

M 5.141 REGELMÄßIGE SICHERHEITSCHECKS IN WLANS

Relevanz für den Durchschnittsbenutzer: gering bis mittel

Es gibt viele – zum Teil kostenlose – Programme um WLANs auf ihre Sicherheit hin zu überprüfen. Zu einem großen Teil ist der Umgang mit diesen Programmen leider relativ komplex, wodurch sie für Durchschnittsbenutzer nicht geeignet sind.

Was kann passieren wenn man die Maßnahme nicht setzt?

Regelmäßige Sicherheitschecks sind eine hilfreiche Methode um Sicherheitslücken zu entdecken. Viele Tools die man zum Testen verwenden kann, werden auch von Hackern eingesetzt um eventuelle Sicherheitslücken auszunutzen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Die Maßnahme ist nicht ganz einfach umzusetzen. Die Programme zum Testen von WLANs sind in der Regel nicht wirklich benutzerfreundlich und erfordern einige Lernzeit.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Prinzipiell ist die Maßnahme ohne Kosten umzusetzen. Der Zeitaufwand – insbesondere zum Erlernen der Werkzeuge – ist allerdings nicht zu unterschätzen

M 6 MAßNAHMENKATALOG NOTFALLVORSORGE

Der Maßnahmenkatalog 6 umfasst alle Punkte zur Notfallvorsorge. Dabei werden sowohl Verhaltensmaßregeln für einen eingetretenen Notfall aufgestellt, als auch Schritte zur Schadensminimierung für mögliche Sicherheitsvorfälle vorgestellt.

M 6.13 ERSTELLUNG EINES DATENSICHERUNGSPLANS

Relevanz für den Durchschnittsbenutzer: hoch

Für Durchschnittsbenutzer ist eine geregelte Datensicherung eine der wichtigsten Sicherheitsvorkehrungen. Aus diesem Grund sollten sich auch Durchschnittsbenutzer überlegen, welche Daten sie auf alle Fälle sichern wollen und in welchem Intervall Daten gesichert werden. Insbesondere sollte auch auf Konfigurationsdaten geachtet werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Eine unregelmäßige, oder unvollständige Sicherung von Datenbeständen, kann im schlimmsten Fall den vollständigen Verlust von Daten bedeuten. Auf jeden Fall ist aber die Wiederherstellung von Daten, die nicht regelmäßig gesichert wurden zeit- und auch kostenintensiv. Hier ein Beispiel:

Beispiel 1: Gustav will sich seit einiger Zeit selbstständig machen. Sein gesamter Business-Plan ist auf seiner Festplatte gespeichert. Manchmal denkt er daran und startet händisch ein Backup einiger Daten. An dem Tag als seine Festplatte auf einmal nicht mehr funktionieren will, lag sein letztes Backup etwa ein (arbeitsintensives) Monat zurück. Um die Arbeit des letzten Monats wieder herzustellen, muss sich Gustav an eine professionelle Datenrettungsfirma wenden. Die Wiederherstellung seiner Daten kostet Gustav 2500€.

Beispiel 2: Gerd speichert regelmäßig den Inhalt seines Dokumenten-Ordners verschlüsselt auf dem PC seines Freundes. Durch einen Virenangriff wird Gerds Festplatte gelöscht. Glücklicherweise sind wichtige Dokumente gesichert. Gerd macht sich daran seinen PC neu zu installieren und spielt auch erfolgreich die gesicherten Daten zurück. Für etliche komplexe Programme fehlt Gerd aber die Konfiguration, welche natürlich nicht in dem „Dokumente-Ordner“ abgelegt war. Gerd benötigt ganze 2 Wochen bis sei PC wieder voll einsatzfähig ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme lässt sich einfach an Benutzer vermitteln. Es gibt etliche einfach zu bedienende Backup-Lösungen. Speicherplatz wird immer billiger und damit sollte niemand mehr ein gutes Argument gegen eine regelmäßige Datensicherung haben.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Sicherung seiner Daten ist gerade für Durchschnittsbenutzer mit überschaubarem Speicherbedarf weder kosten- noch zeitintensiv. Es gibt genügend kostenlose Lösungen die sich automatisch um die Sicherung kümmern und auch der nötige Speicherplatz ist inzwischen nicht mehr teuer.

M 6.16 ABSCHLIEßEN VON VERSICHERUNGEN**Relevanz für den Durchschnittsbenutzer: hoch**

Im Privatbereich, sowie auch in kleinen und mittelständischen Unternehmen sollten Benutzer, die um ihre Daten besorgt oder sogar von ihnen abhängig sind auch Versicherungen berücksichtigen. Natürlich kann eine Versicherung keinen Sicherheitsvorfall verhindern – der entstandene Schaden kann dadurch allerdings eingeschränkt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn es zu einem Sicherheitsvorfall kommt, kann unter Umständen finanzieller Schaden daraus folgen. Dieser kann einerseits durch Verzögerungen durch Wiederherstellung von Infrastruktur oder aber auch durch den Verlust von unwiederbringlichen Gütern entstehen. Hier ein Beispiel:

Beispiel 1: Alfred hat soeben ein neues Firmengebäude bezogen. Einige Prototypen für Produkte, die er in Zukunft vertreiben möchte lagern zusammen mit Verträgen und Informationen über Interessenten an seinen Produkten in einem Raum des neuen Firmengebäudes. Im Drunter und Drüber des Umzugs hat bisher niemand an den Abschluss von Versicherungen gedacht. Ausgerechnet jetzt bricht ein Feuer aus, als sich Putzmittel bei einem Funkenflug durch die letzten Arbeiten in dem Gebäude entzünden. Rasend schnell breitet sich das Feuer aus und zerstört alles was ihm im Weg steht erbarmungslos. Auch

Alfreds Prototypen und Daten fallen den Flammen zum Opfer. Aufgrund der fehlenden Versicherung bleibt Alfred auf den enormen Kosten, die durch das Feuer entstanden sind, sitzen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht schwer zu vermitteln. In den Köpfen der meisten Menschen sind zumindest Haushaltsversicherungen fest eingespeichert. Wenn man im Vorhinein überlegt, welche Versicherungen wirklich Sinn machen, ist auch ein Beratungsgespräch bei den Versicherungspartnern empfehlenswert.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme ist überschaubar. Zumindest ein – besser wären natürlich einige – Termin(e) bei Versicherungsberatern ist nötig. Die Kosten für eine Versicherung sind abhängig von der Deckungssumme und können natürlich sehr hoch sein.

M 6.19 DATENSICHERUNG AM PC

Relevanz für den Durchschnittsbenutzer: hoch

Für Durchschnittsbenutzer ist diese Maßnahme mit eine der wichtigsten, da dadurch nach einem (Sicherheits)Vorfall die wirklich wichtigen Daten – die in die der Nutzer Arbeit gesteckt hat, gesichert erhalten bleiben. Details hierzu siehe dazu M 6.13.

M 6.20 GEEIGNETE AUFBEWAHRUNG DER BACKUP-DATENTRÄGER

Relevanz für den Durchschnittsbenutzer: hoch

Regelmäßige Sicherungskopien nutzen dem Benutzer nur, wenn sie von einem Sicherheitsvorfall nicht auch in Mitleidenschaft gezogen werden. Daher ist es wichtig, auf die geeignete Aufbewahrung der Backup-Datenträger zu achten.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn es zu einem Sicherheitsvorfall kommt, der auch Backupdatenträger beeinträchtigt, ist im schlimmsten Fall mit dem endgültigen Verlust von Daten zu rechnen. Hier ein Beispiel:

Beispiel 1: Bernhard hat bereits am eigenen Leib erfahren wie wichtig Sicherheitskopien sein können. Seit einem Vorfall vor einigen Jahren speichert er die wichtigen Daten von seinem Notebook immer zusätzlich zu auf einem USB-Stick ab. Diesen USB-Stick lässt Bernhard immer an seinem Notebook stecken, da er es sowieso nur daheim verwendet. Eines Tages wird bei Bernhard eingebrochen. Der Dieb stiehlt unter anderem auch Bernhards Notebook – leider ist er nicht so nett den USB-Stick mit Bernhards Daten abzustecken und für Bernhard zurück zu lassen.

Beispiel 2: Rainer ist semiprofessioneller Fotograf und wird regelmäßig bei Hochzeitsfeiern und anderen Anlässen gebucht. Da im Lauf der Zeit enorme Datenmengen zusammenkommen, brennt Rainer regelmäßig DVDs mit den Fotos jedes Events. Diese DVDs lagert Rainer in einer Spindel auf seinem Schreibtisch neben dem Fenster, wo sie täglich ohne Schutz der Sonne ausgeliefert sind. Als Rainers Festplatte irgendwann den Dienst verweigert, muss er feststellen, dass die DVDs inzwischen unlesbar sind, da sie der UV-Strahlung nicht standhalten konnten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht ganz einfach zu vermitteln. Das die Lagerung erheblichen Einfluss auf die Lebensdauer von Speichermedien haben kann, ist nicht offensichtlich. Dennoch ist es nicht schwer die Maßnahme umzusetzen, wenn man sich mit der Tatsache abfindet.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die ordnungsgemäße Aufbewahrung von Speichermedien kann durchaus einige Zeit in Anspruch nehmen. Auch die Kosten können unter den entsprechenden Umständen schnell anwachsen. In den meisten Fällen reicht es aber schon auf Kleinigkeiten zu achten.

Relevanz für den Durchschnittsbenutzer: hoch

Da auch optische Datenträger wie CDs bzw. DVDs nicht unbegrenzt haltbar sind, empfiehlt es sich für gekaufte Software Sicherheitskopien anzulegen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte es nötig sein, Software ein zweites Mal zu installieren, ist es nötig, die Installationsmedien zur Verfügung zu haben. Sollten der Zugriff auf diese unmöglich sein, hilft nur ein Neukauf, der, je nach Software, sehr teuer werden kann. Hier ein Beispiel:

Beispiel 1: Kurt nutzt in seinem Architekturbüro verschiedene Computerprogramme, von denen einige sehr teuer waren. Kurt verlässt sich darauf, dass die Installations-CDs sicher in seinen Büromöbel verwahrt sind. Durch unglückliche Umstände verschüttet Kurt eine stark ätzende Flüssigkeit über seinem Schreibtisch von der auch einiges bis in die Schubladen durchsickert. Kurt bemerkt das Problem zu spät. Einige originale CDs von den teuren 3D-Programmen wurden zerstört. Eine neuerliche Installation ist damit unmöglich, es sei den Kurt kauft das Programm erneut.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist schwierig zu vermitteln (siehe M 6.20) aber einfach umzusetzen. Es ist nur darauf zu achten, dass Sicherheitskopien immer getrennt von den Originalen aufbewahrt werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme ist gering, das Kopieren einer CD oder DVD dauert nicht lange und geschieht im Hintergrund. Auch die Kosten sind gering.

M 6.22 SPORADISCHE ÜBERPRÜFUNG AUF WIEDERHERSTELLBARKEIT VON DATENSICHERUNGEN

Relevanz für den Durchschnittsbenutzer: hoch

Zur Sicherheit sollten Backups gelegentlich auf ihre Wiederherstellbarkeit überprüft werden. Im Ernstfall zu bemerken, dass die gesichert geglaubten Daten nur Datenmüll sind, wäre fatal.

Was kann passieren wenn man die Maßnahme nicht setzt?

Der Verzicht auf gelegentliche Test-Wiederherstellungen kann dazu führen, dass Fehler bei der Datensicherung nicht bemerkt werden und im Ernstfall Daten nicht wiederherstellbar sind. Hier ein Beispiel:

Beispiel 1: Doris verwendet eine kommerzielle Backuplösung bei der auch Speicherplatz im Preis enthalten ist. Aufgrund sehr positiver Erfahrungsberichte vertraut sie dem Service blind. Was sie zu ihrem Pech nicht weiß, ist dass ihre Netzwerkkarte defekt ist und beim Versenden von Daten gelegentlich einige Bytes verschluckt. Als Doris eines Tages eine versehentlich gelöschte Datei aus ihrem Backup zurückholt und öffnet, stellt sie fest, dass anstelle der erwarteten Informationen nur zufällige Zeichenketten zu lesen sind.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Diese Maßnahme ist nicht schwer zu vermitteln. Es ist eigentlich logisch, dass man nicht blind auf seine Sicherheitsvorkehrungen vertraut sondern diese gelegentlich auf Funktionstüchtigkeit überprüft.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme ist gering. Es reicht im Grunde stichprobenweise Daten wiederherzustellen um auf die Funktionstüchtigkeit des Systems schließen zu können. Zusätzliche Kosten entstehen dabei keine.

M 6.23 VERHALTENSREGELN BEI AUFTRETEN EINES COMPUTER-VIRUS

Relevanz für den Durchschnittsbenutzer: hoch

Wenn ein Virus auf einem PC entdeckt wird, ist es wichtig diesen umgehen du entfernen. Außerdem sollten andere Benutzer, mit denen ein Datenaustausch stattgefunden hat,

gewarnt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Die Gefahren, die von Viren ausgehen, sind sehr unterschiedlich. Von lästigen Meldungen bis zu gelöschten Daten oder veröffentlichten Informationen im Internet ist eigentlich alles möglich. Hier ein Beispiel:

Beispiel 1: Martin hat auf seinem Computer ein Anti-Viren-Programm installiert. Er lässt auch automatisch die Aktualisierungen des Virenprogramms durchführen – das war die Standardeinstellung des Programmes. Als Martin ein Email mit angehängtem Virus öffnet, meldet sein Virens scanner die Gefahr. Martin liest die Meldung nicht genau und klickt auf „Ignorieren“. Auch eine erneute Meldung nach einigen Minuten, dass Martins PC von einem Virus befallen ist ignoriert Martin. Obwohl er oft genug gewarnt wurde lässt Martin dem Virus alle Freiheiten sich zu verbreiten und Schaden anzurichten.

Beispiel 2: Claudias PC ist von einem Virus befallen. Während der Virens scanner alle Dateien durchsucht und reinigen will, kopiert Claudia einige Fotos auf einen USB Stick den sie ihrer Freundin Ulrike geben will. Während der USB stick noch mit dem Computer verbunden ist kopiert sich auch der Virus auf den USB Stick. Der Virens scanner meldet, dass der Virus entfernt wurde und Claudia macht sich auf den Weg zu Ulrike. Als diese den USB-Stick mit den Fotos in Empfang nimmt und auch gleich ansteckt, infiziert der Virus auch Ulrikes PC. Einige Wichtige Daten von Ulrike werden im Internet veröffentlicht.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass Virenschutz am Computer nötig ist. Allerdings muss vielen Benutzern das Programm installiert und ihnen die Grundfunktionen erklärt werden, damit sie es benutzen bzw. überhaupt eines benutzen können.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten können durch Gratis-Software minimiert werden. Zeit muss nur bei der Installation (und eventuell bei der Aktualisierung) aufgewendet werden.

M 6.24 ERSTELLEN EINES NOTFALL-BOOTMEDIUMS

Relevanz für den Durchschnittsbenutzer: mittel

Sollte sich ein Computer nicht mehr starten lassen, kann es oft hilfreich sein ein alternatives Bootmedium zur Hand zu haben. Es gibt unzählige kostenlose CD-Images die man brennen kann, um im Notfall eventuell noch auf Daten zugreifen zu können.

Was kann passieren wenn man die Maßnahme nicht setzt?

Grundsätzlich ist diese Maßnahme nicht wirklich nötig wenn man regelmäßige Sicherheitskopien speichert. Im schlimmsten Fall – wenn man diese Maßnahme nicht setzt – muss man sich eventuell um Festplatten-Ersatz kümmern und jegliche Software neu installieren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass ein Notfallbootmedium hilfreich sein kann. Es ist allerdings wesentlich schwieriger den Umgang mit diesen Bootmedien zu vermitteln. Ungeübte Benutzer könnten damit sogar zusätzlichen Schaden verursachen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten für diese Maßnahme sind vernachlässigbar, es fällt nur eine leer-CD an. Der Zeitaufwand für das Erstellen des Bootmediums ist auch sehr gering, die Arbeit damit kann allerdings langwierig sein.

M 6.25 REGELMÄßIGE DATENSICHERUNG DER SERVER-FESTPLATTE

Relevanz für den Durchschnittsbenutzer: mittel

Wenn Durchschnittsbenutzer einen Server betreiben ist die regelmäßige Datensicherung mindestens so wichtig wie bei herkömmlichen PCs.

Was kann passieren wenn man die Maßnahme nicht setzt?

Der Verzicht auf regelmäßige Datensicherung kann im schlimmsten Fall zum Verlust von wichtigen Daten führen. Hier ein Beispiel:

Beispiel 1: Ernst betreibt einen Server für sein Studentenwohnheim, auf dem Musik und Video-Daten, sowie Fotos gespeichert und für alle Bewohner des Heims zugänglich gemacht werden. Ernst nimmt es mit der Datensicherheit aber nicht so ernst, und hat noch nie ein Backup von den Dateien gemacht. Als bei einem Unwetter durch einen Blitzeinschlag die Festplatten des Servers vernichtet werden, gehen alle Fotos und Videos verloren. Die Bewohner des Studentenheims sind seit diesem Vorfall nicht allzugut auf Ernst zu sprechen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass eine regelmäßige Datensicherung insbesondere auch bei Serveranwendungen notwendig ist. Allerdings muss man Benutzern eventuell Starthilfe beim Umgang mit Backuplösungen bieten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten können durch Gratis-Software minimiert werden. Je nach Speicherbedarf können die Kosten und auch der Zeitaufwand für Datensicherung recht stark steigen.

M 6.27 SICHERES UPDATE DES BIOS

Relevanz für den Durchschnittsbenutzer: gering

Das BIOS ist ein essentieller Bestandteil in jedem PC. Gelegentlich kann es nötig sein, neuere vom Hersteller zur Verfügung gestellte Versionen des BIOS zu installieren. Wenn man sich dabei an die Vorgaben des Herstellers hält, kann dabei eigentlich nichts passieren.

Was kann passieren wenn man die Maßnahme nicht setzt?

Unsachgemäßes Vorgehen bei der Aktualisierung des BIOS kann dazu führen, dass ein PC unbrauchbar wird. In diesem Fall hat der Hersteller noch die Möglichkeit das BIOS zu ersetzen. Das bedeutet im Schlimmsten Fall ist der PC zum Händler zu bringen und einige Tage nicht verfügbar. Es besteht allerdings keine Gefahr für gespeicherte Daten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, sich bei gewissen Vorgängen genau an die Anleitung zu halten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand beim Aktualisieren des BIOS sollte keine Rolle spielen, es sollte auf jeden Fall in Ruhe erfolgen. Kosten für ein BIOS-Update nach der Anleitung des Herstellers entfallen.

M 6.31 VERHALTENSREGELN NACH VERLUST DER SYSTEMINTEGRITÄT**Relevanz für den Durchschnittsbenutzer: mittel bis hoch**

Sollte ein Sicherheitszwischenfall eintreten gilt es einige Regeln zu befolgen. Es sollten laufende Programme beendet werden und der Computer sollte heruntergefahren werden. Je nach aufgetretenem Zwischenfall bzw. Notwendigkeit einer Ausforschung der Schuldigen sollte eine Komplettdatensicherung durchgeführt werden. Ausführbare Daten sollten überprüft werden und eventuell aus gesicherten Kopien wieder hergestellt werden. Eventuell kann es auch nötig sein alle Passwörter zurückzusetzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Je nach Art des Zwischenfalls können verschiedene Folgen auftreten. Bei einem Hackerangriff beispielsweise bleiben dem Hacker alle Türen offen. Falls Viren aufgetreten sind können Datenverluste die Folge sein. Bei Hardware-Fehlern, sowie einer defekten Festplatte, können – wenn es nicht schon passiert ist – Daten zerstört und eventuell auch einwandfreie Backups mit fehlerhaften Daten überschrieben werden. Hier ein Beispiel:

Beispiel 1: Max' Computer wird von einem Hacker attackiert, welcher sich auch recht schnell Zugang verschaffen kann. Max bemerkt, dass er auf gewisse Dateien keinen Zugriff mehr hat und dass sein PC viel langsamer ist als gewohnt. Außerdem findet Max eine Kopie von einem aktuellen Kinofilm, den Max nicht heruntergeladen hat. Trotz all dieser seltsamen Ereignisse schöpft Max keinen Verdacht und geht ihnen nicht auf den Grund. Der Hacker kann lange Zeit

mit Max' Computer machen was er möchte.

Beispiel 2: Karl wird vom Betriebssystem auf seinem PC darauf hingewiesen, dass die eingebaute Festplatte fehleranfällig ist. Karl ignoriert diese Meldungen und geht seiner Tätigkeit wie gewohnt nach. Er führt auch weiterhin regelmäßig seine Backups aus bis eines Tages die Festplatte gar nicht mehr funktioniert. Als Karl auf die Ersatzfestplatte die Sicherheitskopien wiederherstellen will bemerkt er, dass die gesicherten Dateien nur noch Datenmüll enthalten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es kann schwierig sein, Benutzern zu vermitteln, wann möglicherweise Gefahr droht, da manche Programme oder Downloads gelegentlich langsamer sind wenn ein Hintergrundprozess gerade Ressourcen verbraucht. Auch sind einige der Maßnahmen (z.B. Komplettdatensicherung, Untersuchung der gesicherten Daten) Durchschnittsbenutzern nicht wirklich zumutbar, da fundiertes Wissen benötigt wird.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Diese Maßnahmen können einiges an Zeit in Anspruch nehmen und – wenn man dazu nicht selbst in der Lage ist – auch enorme Kosten verursachen.

M 6.32 REGELMÄßIGE DATENSICHERUNG

Relevanz für den Durchschnittsbenutzer: hoch

Regelmäßige Datensicherung schützt unwiederbringliche – in der Regel selbst erstellte – Daten davor, durch einen Sicherheitszwischenfall zerstört zu werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Ohne regelmäßige Datensicherung droht auch der Verlust von wichtigen Daten. Das kann durch versehentliches Löschen, Viren, Hardwarefehler oder ähnliches geschehen. Hier ein Beispiel:

Beispiel 1: Markus ist nie ohne sein Notebook unterwegs und nutzt auch gerne die Möglichkeit unterwegs zu arbeiten. Leider vergisst er regelmäßig darauf Sicherheitskopien seiner Arbeit zu machen. Eines Tages wird in der U-Bahn sein Notebook gestohlen. Neben dem überaus ärgerlichen finanziellen Verlust ist damit auch die Arbeit der letzte Tage zunichte gemacht worden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Sicherheitskopien sollten für wichtige Daten selbstverständlich sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten und Zeitaufwand für Sicherheitskopien hängen von der zu sichernden Datenmenge ab. Da aber Speicherplatz sowohl online, als auch offline immer günstiger wird, sind die Kosten auf alle Fälle überschaubar.

M 6.33 ENTWICKLUNG EINES DATENSICHERUNGSKONZEPTS

Relevanz für den Durchschnittsbenutzer: mittel

Bei umfangreicheren Daten empfiehlt es sich ein Konzept zur Datensicherung zu erstellen, um den Platzbedarf im Griff zu haben und auch die Performance des Systems nicht zu beeinflussen. Unter anderem sollten Backups automatisiert werden. Um den Platzbedarf im Griff zu haben, gibt es die Möglichkeit inkrementelle Datensicherung zu machen. Auch bietet es sich an regelmäßige Backups außerhalb der Arbeitszeit durchzuführen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn bei großen Datenmengen auf ein Datensicherungskonzept verzichtet wird, kann es zu Performanceeinbrüchen kommen. Außerdem können die Sicherheitskopien unübersichtlich werden und es besteht die Gefahr, dass Daten „übersehen“ werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist relativ einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Im Allgemeinen wird es aber für Durchschnittsbenutzer nicht wirklich nötig sein, ein Konzept zur Datensicherung zu erstellen, da die Datenmenge überschaubar sein sollte.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Kosten und Zeitaufwand für Sicherheitskopien hängen immer von der zu sichernden Datenmenge ab. Da aber Speicherplatz sowohl online als auch offline immer günstiger wird, sind die Kosten auf alle Fälle überschaubar.

M 6.38 SICHERUNGSKOPIE DER ÜBERMITTELTEN DATEN

Relevanz für den Durchschnittsbenutzer: hoch

Falls Daten nur zum Zweck der Übermittlung an Zweite erstellt werden, sollte eine Kopie – mindestens bis zum bestätigten Erhalt des Originals – aufbewahrt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollten beim Transport der Daten Schäden auftreten kann ohne Kopie der Originaldaten kein erneuter Versand erfolgen. Hier ein Beispiel:

Beispiel 1: Alex bereitet gelegentlich im Auftrag eines gemeinnützigen Vereins Unfalldaten grafisch auf. Immer wenn er mit einer Ausarbeitung fertig ist, brennt er die Daten auf eine CD und versendet die CD per Post. Die Originaldaten löscht er von seinem Computer um Platz zu sparen. Als Alex wieder einmal eine fertige CD verschickt geht bei der Post etwas schief und die CD kommt nie an. Nach einigen Tagen wird beiden Seiten klar, dass die CD nicht mehr ankommt. Die Arbeit einiger Tage ist zunichte gemacht und die Deadline ist inzwischen auch überschritten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln und es dürfte dem Instinkt jedes Durchschnittsbenutzers widersprechen dieser Maßnahme zuwider zu handeln.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Sowohl Kosten als auch Zeitaufwand spielen bei dieser Maßnahme keine Rolle.

M 6.40 REGELMÄßIGE BATTERIEPRÜFUNG/-WECHSEL**Relevanz für den Durchschnittsbenutzer: mittel**

Im Rahmen von Wartungsarbeiten sollten auch Batterien von sicherheitsrelevanten Bauteilen regelmäßig kontrolliert werden. Anfängen von Rauchmeldern über Alarmanlagen bis hin zu Computern können funktionierende Batterien das Sicherheitsniveau erhöhen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Batterien deren Kapazität nicht mehr ausreicht, haben das Versagen der Geräte, die sie mit Strom versorgen sollten, zur Folge. Hier ein Beispiel:

Beispiel 1: Christian hat für seine WG vor einigen Jahren einen Rauchmelder besorgt, da bei Partys häufig getrunken wird und einige Bewohner Raucher sind. In all der Zeit hat niemand den Zustand der Batterien geprüft und so hat auch niemand bemerkt, dass die Batterien des Rauchmelders keinen Strom mehr liefern. Eines Abends schläft einer der Bewohner mit brennender Zigarette ein. Es kommt zum unvermeidlichen Wohnungsbrand, den die restlichen Mitbewohner erst bemerken, als sie hustend erwachen. Durch reines Glück können alle Bewohner der WG von der Feuerwehr gerettet werden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht ganz einfach diese Maßnahme an Durchschnittsbenutzer zu vermitteln, da Batterien häufig nur in Notfällen zum Einsatz kommen und dadurch oft vergessen werden. Gerade im Notfall sollten die Batterien aber funktionieren.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten und auch der Zeitaufwand für das Ersetzen von Batterien sollte für die meisten

Durchschnittsbenutzer gering sein, da es nur eine überschaubare Anzahl von betroffenen Geräten geben sollte.

M 6.41 ÜBUNGEN ZUR DATENREKONSTRUKTION

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Siehe M 6.22

M 6.44 DATENSICHERUNG UNTER WINDOWS NT

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 6.32

M 6.45 DATENSICHERUNG UNTER WINDOWS 95

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 6.32

M 6.47 AUFBEWAHRUNG DER BACKUP-DATENTRÄGER FÜR TELEARBEIT

Relevanz für den Durchschnittsbenutzer: hoch

Siehe M 6.20.

M 6.49 DATENSICHERUNG EINER DATENBANK

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Beim Einsatz von Datenbank ist in jedem Fall auf Datensicherung Wert zu legen, da insbesondere Datenbanken nicht ohne weiteres aus Dateien wiederhergestellt werden können. Die korrekte Sicherung von Datenbanken ist daher wichtig.

Was kann passieren wenn man die Maßnahme nicht setzt?

Da die meisten Datenbanken Informationen auf mehrere Dateien verteilt abspeichern, verliert man, auch wenn nur eine Datei beschädigt wird, alle Daten. Für Durchschnittsbenutzer ist es daher besonders wichtig, regelmäßig Dumps von Datenbanken zu speichern. Ansonsten ist eine erfolgreiche Wiederherstellung einer einmal zerstörten Datenbank sehr schwierig. Hier ein Beispiel:

Beispiel 1: Hubert programmiert Web-Applikationen und hat dafür einen Webserver und eine Datenbank auf seinem PC installiert. Regelmäßig werden alle aktualisierten Dateien auf seinem PC gesichert. Während seiner Arbeit stürzt Huberts PC ab und beschädigt dabei einige Dateien auf der Festplatte. Hubert kann alle Dateien aus dem Backup wiederherstellen – seine Datenbank lässt sich aber trotzdem nicht öffnen, obwohl er die Dateien aus dem Backup wiederhergestellt hat. Mit einem Datenbank-Dump hätte Hubert die Datenbank sichern und problemlos wiederherstellen können.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht ganz einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Wenn man aber auf ein automatisiertes Backup zurückgreifen kann, ist auch ein Datenbankenbackup für Durchschnittsbenutzer kein Problem.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Effizient lässt sich diese Maßnahme für Durchschnittsbenutzer nur mit automatisierten Backups umsetzen, da anderenfalls ein enormes Maß an Konsequenz von Seiten des Benutzers notwendig wäre.

M 6.50 ARCHIVIERUNG VON DATENBESTÄNDEN

Relevanz für den Durchschnittsbenutzer: gering

Wenn Datenbanken regelmäßig „gedumpt“ werden, muss das Ergebnis – in der Regel eine Text-Datei – wie jede andere Datei auf dem Computer gesichert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn bewusst oder unbewusst auf die Sicherung von diesen Datenbank-Exporten verzichtet wird, ist eine Wiederherstellung des Datenbestandes nicht mehr möglich.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es erfordert nur einmalig zusätzliche Arbeit beim Einrichten der Sicherungskopien, ab diesem Zeitpunkt erfolgt auch die Sicherung des Datenbank-Dumps automatisch.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Wenn bereits ein Backupsystem im Einsatz ist fallen weder Kosten noch Zeitaufwand ins Gewicht.

M 6.52 REGELMÄßIGE SICHERUNG DER KONFIGURATIONSDATEN AKTIVER NETZKOMPONENTEN

Relevanz für den Durchschnittsbenutzer: mittel bis hoch

Bei Sicherheitskopien sollte immer auf Konfigurationsdaten geachtet werden. Mit gesicherter Konfiguration gestaltet sich sowohl eine Wiederherstellung, als auch eine Neukonfiguration eines Services wesentlich einfacher.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wenn bewusst oder unbewusst auf die Sicherung von Konfigurationsdaten verzichtet wird, ist es schwieriger ein ausgefallenes Service wieder in Stand zu setzen, da die teilweise schwierige

Konfigurationsarbeit erneut gemacht werden muss.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es erfordert nur einmalig zusätzliche Arbeit beim einrichten der Sicherungskopien, ab diesem Zeitpunkt erfolgt auch die Sicherung der Konfigurationsdaten automatisch.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Wenn bereits ein Backupsystem im Einsatz ist fallen weder Kosten noch Zeitaufwand ins Gewicht.

M 6.54 VERHALTENSREGELN NACH VERLUST DER NETZINTEGRITÄT

Sollte sich ein Netzwerk auf unerwartete Weise verhalten, gilt es auf Seite des Benutzers einige Aktionen zu setzen.

Relevanz für den Durchschnittsbenutzer: hoch

Bei Arbeiten im Netzwerk gilt es für Benutzer – sollte sich das Netzwerk unerwartet verhalten – umgehend die aktive Arbeit zu speichern, sowie alle Programme die das Netzwerk verwenden zu beenden. Gegebenenfalls sollte der Administrator informiert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Eine Veränderung der Netzperformance kann auf missbräuchliche Nutzung oder auch Konfigurationsarbeiten hindeuten. In jedem Fall kann es zu Inkonsistenzen bei Daten kommen. Hier ein Beispiel:

Beispiel 1: Hubert arbeitet an einer verteilten Datenbank. Er aktualisiert etliche Datensätze. Als er seine Arbeit speichern will, bekommt er von seinem Client die Meldung, dass der Server

nicht erreichbar ist. Im Abstand von 10 Sekunden versucht Hubert immer wieder seine Daten zu speichern. Nach 5 Minuten hat er damit Erfolg und damit haben sich die Fehlermeldungen für Hubert erledigt. Durch die schlechte Netzverbindung hat der Speichervorgang allerdings nicht funktioniert. Dadurch wurde eine ganze Tabelle der Datenbank korrumpiert. Die Wiederherstellung der Tabelle aus dem Backup dauerte 2 Tage.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Wenn es bei Vorgängen im Netzwerk wiederholt oder dauerhaft zu Problemen kommt sollte diesen in jedem Fall auf den Grund gegangen werden. Das kann zuhause durch den Benutzer selbst erfolgen, oder in einem Betrieb durch einen IT-Administrator..

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Fehlersuche in einem Netzwerk kann natürlich einiges an Zeit bzw. Kosten verschlingen. Dementsprechend werden Benutzer in ihrem Heimnetzwerk eine etwas höher Toleranzgrenze haben, in Betrieben, welche hohe Verfügbarkeitsanforderungen an ihre Netzwerke haben, wird der Nutzen die Kosten aber in jedem Fall überwiegen.

M 6.56 DATENSICHERUNG BEI EINSATZ KRYPTOGRAPHISCHER VERFAHREN

Bei Kryptographischen Verfahren darf die Frage der Datensicherheit nicht vernachlässigt werden. Insbesondere muss die Speicherung kryptographischer Schlüssel sowie der Konfigurationsdaten abzuwägen.

Relevanz für den Durchschnittsbenutzer: hoch

Für Durchschnittsbenutzer gibt es keinen Unterschied zur Sicherung unverschlüsselter Daten. Je nach Verschlüsselungsalgorithmus müssen eventuell gesondert Vorkehrungen zur Entschlüsselung der Daten getroffen werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wie bei allen Maßnahmen, die mit Datensicherung zu tun haben, sind im schlimmsten Fall

Daten für immer verloren. Hier ein Beispiel:

Beispiel 1: Karl benutzt zum Speichern bestimmter Dokumente eine Verschlüsselungssoftware. Damit kann ein Dieb der Karls Notebook stiehlt beispielsweise seine Bankdaten nicht nutzen. Karl legt regelmäßig Sicherheitskopien dieser verschlüsselten Dateien ab, allerdings hat Karl vergessen auch von dem 2048bit langen Schlüssel ein Backup zu speichern. Karls Notebook wird durch einen Fahrradunfall – zum Glück ist Karl nichts passiert – kaputt. Auf dem Ersatzgerät installiert Karl wieder dasselbe Verschlüsselungsprogramm wie zuvor und stellt auch seine gesicherten Daten wieder her. Erst jetzt merkt Karl, dass er seine privaten Dokumente nicht mehr entschlüsseln kann, da der Schlüssel für immer verloren ist.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Sicherheitskopien sollten für wichtige Daten selbstverständlich sein. In speziellen Fällen müssen immer auch Konfigurationsdaten gespeichert werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten für diese Maßnahme sind – wenn erst ein Backupsystem eingesetzt wird – minimal. Der zusätzliche Platz- bzw. Zeitbedarf beim Speichern von Konfigurationsdaten fällt dabei nicht ins Gewicht.

M 6.64 BEHEBUNG VON SICHERHEITSVORFÄLLEN

Relevanz für den Durchschnittsbenutzer: hoch

Sollte ein Sicherheitszwischenfall eingetreten sein, müssen umgehend Gegenmaßnahmen getroffen werden um den Schaden einzugrenzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sicherheitszwischenfälle, gegen die nichts unternommen wird, erhöhen die Gefahr einer Verbreitung. Die Ausmaße des Schadens, der aus einem Sicherheitszwischenfall folgen kann,

können sich dadurch vergrößern. Hier ein Beispiel:

Beispiel 1: Huberts Virens Scanner meldet bei einer Routineüberprüfung, dass eine Datei mit einem Virus verseucht ist. Da Hubert mit seinen Gedanken bereits bei seinem Campingurlaub ist, ignoriert er die Meldung des Virens scanners. Der Virus verschickt sich über das Email-Adressbuch an Huberts Kontakte. Nach der erfolgreichen Verbreitung beginnt der Virus mit seiner zerstörerischen Tätigkeit und überschreibt alle Dokumente auf Huberts PC mit sinnlosen Daten.

Beispiel 2: Als Sabine von ihrem Damenabend heimkommt stellt sie vor ihrer Wohnungstür fest, dass ihr Schlüssel verschwunden ist. Sehr verärgert tritt Sabine gegen ihre Wohnungstür welche sich widerstandslos öffnen lässt. In ihrer Wohnung herrscht Chaos, Sabines Schubladen sind durchwühlt worden und schnell bemerkt Sabine das Fehlen ihres Schmuckes. Gegen den Rat von allen Freunden und Verwandten tauscht Sabine das Schloss ihrer Wohnungstür nicht aus, sie verwendet ihren Reserveschlüssel und vertraut darauf, dass sie kein zweites Mal überfallen werden würden. Leider lag Sabine falsch, keine Woche später steht Sabine wieder vor offenen Türen, diesmal sind ihre Stereoanlage und ihr Fernseher verschwunden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwierig Benutzern zu vermitteln, dass auf einen Sicherheitsvorfall reagiert werden muss um den Schaden einzugrenzen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Je nach aufgetretenem Sicherheitsvorfall können sowohl Zeitaufwand als auch Kosten hoch sein. So können Sicherheitsschlösser beispielsweise sehr teuer sein.

M 6.65 BENACHRICHTIGUNG BETROFFENER STELLEN

Nach einem Sicherheitszwischenfall müssen alle davon betroffenen Stellen informiert werden. Insbesondere gilt das für Stellen, die direkt Schäden erleiden könnten oder bei der Behebung helfen können.

Relevanz für den Durchschnittsbenutzer: mittel

Sollte ein Sicherheitszwischenfall eingetreten sein, müssen betroffene Benutzer umgehend darüber informiert werden, bzw. müssen die Benutzer die zuständige IT-Sicherheitsstelle (in Betrieben o.ä.) darüber in Kenntnis setzen.

Was kann passieren wenn man die Maßnahme nicht setzt?

Nicht gemeldete Sicherheitszwischenfälle können dazu führen, dass der entstehende Schaden größer bzw. weiter verbreitet wird. Hier ein Beispiel:

Beispiel 1: Auf Karls PC verschwinden gelegentlich Daten. Karl vermutet, dass er sie versehentlich gelöscht hat und kümmert sich nicht weiter darum anstatt seinem Systemadministrator bescheid zu geben. Nach einem langen Wochenende bemerkt Karl dass große Teile seiner Dokumente nicht mehr aufzufinden sind. Karls Kollegen haben dieselben Probleme. Ohne es zu wissen wurde Karl Opfer eines neuen Makrovirus, welcher sich über Emails in der gesamten Abteilung verbreitet hat. Karl hätte den Schaden minimieren können, wenn er sofort gehandelt hätte.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist eher schwierig Benutzern einerseits zu vermitteln, dass sie bei unerwartetem Verhalten hellhörig werden, gleichzeitig aber nicht paranoid zu werden. Dazu gehört es einen Sicherheitsvorfall als solchen zu erkennen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Sowohl Zeitaufwand, als auch Kosten für diese Maßnahme sind überschaubar. Benutzer können Sicherheitsvorfälle im alltäglichen Computerbetrieb erkennen und melden bzw. im Heimbetrieb selbst tätig werden.

Relevanz für den Durchschnittsbenutzer: hoch

Nach einem Sicherheitsvorfall sollte es im Interesse jedes Benutzers sein, etwas für die Zukunft zu lernen. Für einen optimalen Lerneffekt sollte die Nachbearbeitung nicht vernachlässigt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Der Verzicht auf diese Maßnahme würde im schlimmsten Fall zu einer Wiederholung des Sicherheitsvorfalles führen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist relativ schwierig, Benutzern zu vermitteln, dass man aus dem Schaden noch was lernen kann. Nur zu oft lässt sich beobachten, dass dieselben Fehler immer wieder gemacht werden.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand für diese Maßnahme kann enorm sein. Meistens würde aber schon einen kurze Analyse der Fragen „Was ist passiert?“, „Warum ist es passiert?“ und „Wie kann man solche Probleme in Zukunft verhindern?“ ausreichen, um eventuelle Fehler zu erkennen und in Zukunft zu vermeiden.

M 6.67 EINSATZ VON DETEKTIONSMAßNAHMEN FÜR SICHERHEITSVORFÄLLE

Neben der Prävention sollte auch der Detektion von Sicherheitsvorfällen ausreichend Aufmerksamkeit geschenkt werden. Mögliche Maßnahmen wären die Installation von Alarmanlagen, Viren-Scanner oder Checksummen-Systeme.

Relevanz für den Durchschnittsbenutzer: hoch

Für zahlreiche Bedrohungsszenarien gibt es Methoden, diese Frühzeitig zu erkennen und möglicherweise abzuwenden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Je länger ein Sicherheitsvorfall unerkannt bleibt, desto schwerwiegender können die potentiellen Folgen sein. Hier ein paar Beispiele:

Beispiel 1: Karl verwendet kein Antiviren-Programm. Von einer zweifelhaften Quelle lädt er sich virenverseuchte Software auf seinen PC. Von diesem Zeitpunkt passieren regelmäßig eigenartige Dinge. Der PC wird immer langsamer und stürzt oft ab. Karl bekommt oft Benachrichtigungen über Emails, die nicht zugestellt werden konnten. Diese Vorkommnisse ignoriert Karl einfach, bis er eines Tages seine Kreditkartenabrechnung zugestellt bekommt, laut der er tausende Euro ausgegeben haben soll.

Beispiel 2: Hubert hat verwendet einen Virens Scanner der automatisch regelmäßig aktualisiert wird. Auch Sicherheitskopien macht Hubert regelmäßig. Insgesamt ist er bei seinem Computersystem sehr auf Sicherheit bedacht – ganz im Gegensatz zu seiner Erdgeschosswohnung. Seine Wohnungstür wird durch ein einziges Schloss der einfachsten Ausführung gesichert. Außerdem lässt Hubert liebend gern die Fenster offen stehen wenn er die Wohnung verlässt, und lädt damit Einbrecher regelrecht ein, sich bei ihm zu bedienen. Genau das geschieht eines Tages auch, und da Hubert auch keine Alarmanlage installiert hat, haben die Einbrecher genügend Zeit die ganze Wohnung leer zu räumen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer Benutzern die Vorteile von Detektionsmaßnahmen zu vermitteln. Allerdings muss vielen Benutzern der Umgang mit diesen Detektionsmaßnahmen vermittelt werden. Gerade bei Virens Scannern ist es beispielsweise notwendig sich mit den Meldungen des Programms zu befassen und regelmäßig Updates zu installieren.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand sowie der Kostenaufwand sind von den jeweiligen Maßnahmen abhängig. Ein Virens Scanner ist schnell installiert und teilweise auch kostengünstig bis kostenlos einsetzbar. Eine Alarmanlage kann allerdings schnell ins Geld gehen. Zusätzlich ist der Einbau einer Alarmanlage eine zeitintensive Tätigkeit.

M 6.71 DATENSICHERUNG BEI MOBILER NUTZUNG DES IT-SYSTEMS

Mobile Geräte wie Notebooks sind in der Regel nicht ständig mit dem Netzwerk verbunden. Daher ist während längerer offline-Zeiten eine Sicherung auf externe Datenträger nötig.

Relevanz für den Durchschnittsbenutzer: hoch

Auch beim Einsatz von Notebooks sollte man regelmäßige Sicherheitskopien machen. Wenn es keine Möglichkeit zur Speicherung auf einem zweiten PC gibt (z.B. während einer Bahnfahrt) sollten Sicherheitskopien auf externe Datenträger durchgeführt werden. Man kann nie vorhersehen, wann eine Komponente kaputt geht oder gestohlen wird.

Was kann passieren wenn man die Maßnahme nicht setzt?

Wie bei allen Maßnahmen in denen es um Sicherheitskopien geht sind im schlimmsten Fall Daten für immer verloren oder nur mit enormem Aufwand und hohen Kosten wiederherstellbar. Hier ein Beispiel:

Beispiel 1: Hubert fährt übers Wochenende zu Freunden. Die lange Zugfahrt möchte er nutzen, um weiter an seiner Diplomarbeit zu feilen. Nach einigen Stunden fleißiger Arbeit legt Hubert eine Pause ein. Über der Lektüre einer Zeitung nickt er für einige Minuten ein. Als er aufwacht ist sein Notebook zusammen mit dem Mitreisenden aus dem Abteil verschwunden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Sicherheitskopien sollten für wichtige Daten selbstverständlich sein.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten für diese Maßnahme sind minimal – ein USB-Stick für die wichtigsten aktuellen Daten reicht für den mobilen Einsatz. Für den stationären Einsatz sollte es einen Backup-Mechanismus geben.

M 6.72 AUSFALLVORSORGE BEI MOBILTELEFONEN

Wie PDAs sollten auch Mobiltelefone mit einem PC synchronisiert werden. Die Kontrolle des Ladezustandes des Akkus sollte in regelmäßigen Abständen erfolgen.

Relevanz für den Durchschnittsbenutzer: mittel

Jeder Mensch kann einmal in die Lage kommen, eine Notrufnummer wählen zu müssen. Zumindest aus diesem Grund sollte der Ladezustand des Akkus regelmäßig kontrolliert werden. Außerdem stehen Diebstähle von Mobiltelefonen an der Tagesordnung und häufig ist der größte Schaden, der dabei entsteht der Verlust aller gespeicherten Telefonnummern.

Was kann passieren wenn man die Maßnahme nicht setzt?

Im Notfall ist ein leer-telefoniertes Handy völlig nutzlos. Auch verlorenen Telefonnummern können zu ärgerlichen Situationen führen. Hier ein Beispiel:

Beispiel 1: Sabines liebstes Hobby ist das Telefonieren und Verschicken von Kurzmitteilungen. Eine volle Akkuladung überdauert bei Sabine nur selten einen ganzen Tag. Eines Abends beobachtet Sabine einen Einbruch in ihrer Nachbarschaft. Sie greift zu ihrem Handy und will die Polizei verständigen, muss aber feststellen, dass ihr Akku wieder einmal leer ist. Sabine sieht sich nach weiteren Passanten oder einer Telefonzelle um, bis sie aber eine gefunden hat, sind die Einbrecher mit ihrer Beute bereits entkommen.

Beispiel 2: Karl verwendet alle Funktionen seines Telefons. Notizblock, Telefonbuch, TODO-Liste, Terminverwaltung, Photoalbum und Email-Client. Karl verzichtet aber darauf sein Handy mit seinem Notebook zu synchronisieren. Durch eine unglückliche Verkettung alltäglicher Ereignisse findet Karl auf schmerzhaft Weise heraus, dass sein Telefon nicht schwimmen kann. Auch nach einer angemessenen Trockenzeit lässt sich Karls Handy nicht wieder anschalten. Karl hat keinen Zugriff auf seine Termine, und da auch seine gespeicherten Telefonnummern verloren sind, kann er den genauen Zeitpunkt für den wichtigen Termin mit den Investoren nicht erfragen.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Sicherheitskopien sollten für alle Daten selbstverständlich sein, und für Notfälle sollte immer ein wenig

Akkulaufzeit über bleiben.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten für diese Maßnahme entfallen im Grunde, da der Platzbedarf beim Synchronisieren mit dem PC minimal ist. Die Funktionalität zum Synchronisieren bringen beinahe alle aktuellen Handys mit. Der Zeitaufwand ist ebenfalls minimal. Um ein wenig Akkulaufzeit aufzusparen ist eventuell ein wenig Zurückhaltung nötig.

M 6.74 NOTFALLARCHIV

Ein Notfallarchiv enthält Sicherungsdaten, mit denen das Gesamtsystem in sich konsistent wieder hergestellt werden kann. Es sollte keinesfalls durch die gleiche Schadensursache zerstört werden wie beschädigten Produktionsdaten.

Relevanz für den Durchschnittsbenutzer: hoch

Im Idealfall sollten Sicherungskopien nicht in der Nähe des zu sichernden PCs gelagert werden. Diese Maßnahme sollte auch von Durchschnittsbenutzern berücksichtigt werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Nach einem Schadensfall sollte ein Zugriff auf die gesicherten Daten möglich sein. Anderenfalls sind Sicherungskopien natürlich nutzlos. Hier ein Beispiel:

Beispiel 1: Hubert ist selbständiger Webdesigner und Grafiker. Seine Workstation administriert er selbst, und kümmert sich auch regelmäßig um Backups seiner Daten. Extra dafür hat er sich einige externe USB-Festplatten zugelegt, die er in seinem Büro neben dem PC lagert. Nach einem langen Wochenende wird Hubert vor seinem Büro von der Feuerwehr empfangen. Durch einen Kabelbrand ist sein gesamtes Büro den Flammen zum Opfer gefallen. Neben seinem PC wurde auch die Sammlung von USB-Festplatten und damit all seine bisherigen Aufträge und Kundendaten zerstört.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu

vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es wird jedem Benutzer einleuchten, dass im Notfall ein „externes“ Backup hilfreich wäre.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Je nach Art der Umsetzung dieser Maßnahme können die Kosten natürlich ein großer Faktor sein. Es gibt auch kostenlose gemeinschaftliche Methoden, bei denen alle Mitglied einen Teil ihres Speicherplatzes anderen Mitgliedern für (verschlüsselte!!!) Sicherheitskopien zur Verfügung stellen. Der Zeitaufwand unterscheidet sich nicht maßgeblich von Backups auf USB-Festplatten oder ähnlichem.

M 6.76 ERSTELLEN EINES NOTFALLPLANS FÜR DEN AUSFALL VON WINDOWS 2000/XP/2003-SYSTEMEN

Ausfälle von Server oder Workstations sind im betrieblichen Umfeld in der Regel mit eingeschränkter Produktivität verbunden. Aus diesem Grund sollte es – wo nötig – einen Notfallplan geben um zumindest die Dauer der Ausfälle zu minimieren.

Relevanz für den Durchschnittsbenutzer: mittel

Für Durchschnittsbenutzer wird es sich im Allgemeinen nicht rentieren in einen ausgeklügelten Notfallplan für den Ausfall eines PCs zu investieren. Wichtig ist, dass Daten gesichert und wichtige Vorgänge (wie Installationen bzw. bestimmte Einstellungen) dokumentiert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Nach einem Schadensfall erschwert ein fehlendes Backup und fehlende Dokumentation die Rückkehr zu einem funktionierenden System. Hier ein Beispiel:

Beispiel 1: Sabine betreibt auf ihrem PC neben ihrer herkömmlichen Software auch einen Webserver und ein Wiki um diverse Kontakte und Termine zu verwalten sowie TODO-Listen zu

führen. Sie speichert regelmäßig ihre wichtigsten Daten bei einem Anbieter von Backuplösungen. Eines Tages fällt ein besonders bösartiges Virus über Sabines PC herein, welcher Daten vollkommen zerstört. Sabine muss ihren PC neu aufsetzen. Leider hatte sie vergessen die Konfiguration ihres Webservers und Wikis zu dokumentieren. Sie muss sich die schwierige Einstellungsarbeit erneut antun.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es gibt etliche – auch kostenlose – Programme welche sich um die regelmäßige und effiziente Sicherung von Daten auf einem PC kümmern.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten sind auf alle Fälle überschaubar, Festplatten sind inzwischen sehr kostengünstig und die Software, die sich um die Datensicherung kümmert, gibt es teilweise kostenlos. Außerdem gibt es Anbieter von Backupdiensten, die zusätzlich zur Software, auch Speicherplatz gratis zur Verfügung stellen bzw. verkaufen. Bei der Dokumentation von Installationen und Einstellungen ist ein wenig Konsequenz beim Benutzer gefragt. Der Nutzen im Notfall rechtfertigt den zusätzlichen Aufwand aber auf alle Fälle.

M 6.78 DATENSICHERUNG UNTER WINDOWS 2000/XP

Relevanz für den Durchschnittsbenutzer: hoch

Regelmäßige Datensicherungen ermöglichen in einem Schadensfall, dass Daten wieder hergestellt werden können und ersparen damit auch dem Durchschnittsbenutzer jede Menge Arbeit und Ärger.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte nach einem Schadensfall kein Backup existieren, ist die Wiederherstellung bzw. die Wiederbeschaffung im besten Fall sehr zeitaufwendig. Im schlimmsten Fall sogar unmöglich. Hier ein Beispiel:

Beispiel 1: Hubert ist gerade dabei seine Diplomarbeit fertig zu stellen. Seine Arbeit umfasst inzwischen 120 Seiten. Gerade als Hubert zum letzten Mal auf „Speichern“ klickt stürzt sein PC mit einer unverständlichen Fehlermeldung ab. Aus reiner Bequemlichkeit hat Hubert darauf verzichtet seine Arbeit an einem anderen Ort zu sichern. Nach diesem Vorfall startet Huberts PC nicht mehr. Hubert baut die Festplatte aus seinem PC aus und bringt sie zu einem Freund. Gemeinsam stellen sie fest, dass Huberts Diplomarbeit nicht mehr lesbar ist. Hubert muss die Arbeit des gesamten Semesters noch einmal machen.

Beispiel 2: Karl speichert sein Projektstagebuch auf dem USB-Stick den er immer bei sich führt. Er hält es nicht für nötig die Daten vom USB-Stick noch an einem anderen Ort zu speichern – immerhin enthalten USB-Sticks ja keine beweglichen Teile, sind also immun gegen Erschütterungen und außerdem hält sein USB-Stick ja schon 3 Jahre ohne ein einziges Problem. Als Karl eines Abends auf die Straßenbahn wartet klingelt sein Handy. Karl zieht es ohne weiter nachzudenken aus seiner Tasche und nimmt dabei ohne es zu merken seinen USB-Stick gleich mit. Dieser fällt wie es das Schicksal will genau vor die Räder der gerade eintreffenden Straßenbahn. Dieser Belastung ist auch der beste USB-Stick nicht gewachsen. Karls Daten sind ein für alle mal verloren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es gibt etliche – auch kostenlose – Programme welche sich um die regelmäßige und effiziente Sicherung von Daten auf einem PC kümmern.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten sind auf alle Fälle überschaubar, Festplatten sind inzwischen sehr kostengünstig und die Software, die sich um die Datensicherung kümmert, gibt es teilweise kostenlos. Außerdem gibt es Anbieter von Backupdiensten, die zusätzlich zur Software auch Speicherplatz gratis zur Verfügung stellen bzw. verkaufen.

M 6.89 NOTFALLVORSORGE FÜR EINEN APACHE-WEBSEVER

Relevanz für den Durchschnittsbenutzer: mittel

Wenn Durchschnittsbenutzer einen Webserver betreiben, sollten sie in erster Linie für die

Sicherung der HTML-Dokumente sorgen. Weiters ist es wichtig jeden Schritt der Installation und Konfiguration zu dokumentieren.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte nach einem Schadensfall an einem Webserver ein Backup oder Dokumentation fehlen, ist die Wiederherstellung in jedem Fall sehr zeitaufwendig. Sollte beispielsweise der Webshop eines Betriebes betroffen sein, können dadurch auch finanzielle Einbußen entstehen. Hier ein Beispiel:

Beispiel 1: Sabine handelt über einen Webshop mit Modeschmuck, den sie selbst erzeugt. Auf ihrem Webserver gibt es kein automatisches Backup und sie kümmert sich auch nicht darum ein händisches Backup zu machen. Eines Tages stößt der Star einer Internationalen Film-Produktion auf Sabines Webshop und will für eine Premierenfeier Schmuck bei Sabine bestellen. Gerade in diesem Moment stürzt der Webserver auf dem Sabines Webshop läuft ab und zerstört dabei Sabines Onlineshop. Da Sabine kein Backup hat dauert der neuerliche Aufbau einige Wochen. Inzwischen hat der Star auf Sabines Schmuck vergessen und Sabine ihre Chance auf gratis Publicity auf dem roten Teppich verspielt.

Beispiel 2: Hubert besucht während seiner Weltreise regelmäßig Internetcafés, von denen aus er Fotos von seiner Kamera auf seinen Blog hoch lädt. Hubert ist richtig stolz auf seine Fotos und wird von den Lesern seines Blogs in den höchsten Tönen gelobt. Als wieder ein Besuch in einem Internetcafe ansteht findet Hubert auf seinem Blog weder Bilder noch Text. Was er jedoch findet ist ein Mail von dem Anbieter des Blogger-Services der erklärt, dass ein Erdbeben etliche Festplatten seiner Server zerstört habe. Weiters hoffe er, dass Hubert, wie in den AGBs empfohlen, Sicherungskopien seiner Fotos und Blog-Einträge habe. Hubert hat natürlich keine Sicherungskopien mehr, aber ab jetzt den festen Vorsatz in Zukunft Sicherungskopien zu machen.

Beispiel 3: Karl musste vor einiger Zeit in der Schule für ein Projekt einen Webserver installieren. Er entschied sich für Apache, welchen er mühsam für den Betrieb mit SSL und etlichen zusätzlichen Modulen wie etwa php konfigurierte. Damals hat Karl sein Vorgehen nicht protokolliert. Heute steht er erneut vor der Aufgabe einen Apache-Webserver zu installieren, da er sich Angeboten hat für einige Freunde Homepages online zu stellen. Da sich Karl nicht genau erinnern kann was er damals gemacht hat, muss er sich erneut alles mühsam erarbeiten.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahmen an Durchschnittsbenutzer zu vermitteln. Es braucht allerdings ein gewisses Maß an Konsequenz bei der Dokumentation seiner Tätigkeiten und der Sicherung seiner Daten an zumindest einer zweiten Stelle.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Die Kosten bei dieser Maßnahme sind je nach Vorgehen minimal. Der Zeitaufwand insbesondere beim Dokumentieren kann einiges ausmachen, ist aber in jedem Fall geringer als der Zeitaufwand bei einer Neuinstallation.

M 6.90 DATENSICHERUNG UND ARCHIVIERUNG VON E-MAILS

E-Mails gehören wie alle anderen Dokumente und Userdaten gesichert.

Relevanz für den Durchschnittsbenutzer: hoch

Emails können auch bei Durchschnittsbenutzern eine wichtige Rolle spielen. Daher sollten diese in jedem Fall gesichert werden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Immer größere Teile des Lebens können inzwischen über das Internet abgewickelt werden. Dabei ersetzen Emails die herkömmliche Post. Verlorene Emails können daher etliche unangenehme Folgen haben. Hier ein Beispiel:

Beispiel 1: Karl lernt in einem Lokal eine Frau kennen, sie unterhalten sich und verbringen einen schönen Abend. Zum Abschied überreicht Karl ihr seine Visitenkarte mit seiner Emailadresse. Tags darauf trifft bei Karl eine Email mit der Telefonnummer seiner Traumfrau ein und Karl nimmt sich vor am Abend anzurufen. Karl erledigt noch einiges während, ohne sein Wissen, durch einen Virus seine gesamten Emails gelöscht werden. Als Karl wieder nach Hause kommt und sieht, dass seine Emails verschwunden sind, kann er sein Pech gar nicht fassen – er hat sich weder Telefonnummer noch Email-Adresse seiner Bekanntschaft notiert.

Beispiel 2: Hubert bestellt im Internet in einem Onlineshop. Er bezahlt mit Kreditkarte und freut sich, als ihm die Bestellbestätigung als Email zugestellt wird schon auf sein Paket. Drei Wochen nach der Bestellung ist noch immer kein Paket eingetroffen. Zusätzlich löscht Hubert versehentlich die Bestellbestätigung. Einige Tage später – noch immer ist kein Paket eingetroffen – ruft Hubert bei dem Onlineshop an und möchte sich nach seiner Bestellung erkundigen. Da Hubert aber das Email mit der Bestellbestätigung verloren hat, kann ihm der Angestellte des Shops auch keine Auskunft geben. Erst mit Hilfe der Kreditkartenabrechnung kann das Paket nachverfolgt werden. Es stellt sich heraus, dass das Paket ordnungsgemäß zugestellt wurde. Laut Auskunft des Angestellten hat Hubert eine falsche Lieferadresse angegeben – aber auch das kann Hubert jetzt nicht mehr kontrollieren, da er keine Bestellbestätigung mehr hat.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist einfach diese Maßnahme umzusetzen. Am einfachsten wäre es Beispielsweise alle Emails als Kopie an eine zweite Emailadresse weiterzuleiten. Dafür kann man sich bei diversen Webmailanbietern einen gratis Account zulegen. Eine andere Möglichkeit ist es im Backup das Datenverzeichnis seines Mail-Clients einzuschließen.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Sowohl Zeitaufwand als auch Kosten für die Speicherung der Emails sind minimal.

M 6.95 AUSFALLVORSORGE UND DATENSICHERUNG BEI PDAS

PDAs stellen durch ihre Natur ein gewisses Sicherheitsrisiko dar. Einerseits bieten sie eine Möglichkeit gewisse Tätigkeiten unterwegs durchzuführen, andererseits sind PDAs ein beliebtes Ziel für Diebe. Benutzer von PDAs müssen auf alle Fälle die Daten von ihrem Gerät an einem anderen Ort sichern und den Akkuladezustand im Auge behalten.

Relevanz für den Durchschnittsbenutzer: mittel

Bei Durchschnittsbenutzer sind PDAs inzwischen vor allem in Handys integriert und werden zum größten Teil als Wecker oder MP3-Player verwendet. In jedem Fall sollten sich auch Durchschnittsbenutzer darüber im Klaren sein, dass regelmäßiges Synchronisieren mit einem

PC essentiell ist. Speicherung von Backups auf z.B. Compact Flash Karten ist kein dauerhafter Ersatz für eine Synchronisierung.

Was kann passieren wenn man die Maßnahme nicht setzt?

Falls ein PDA verloren geht, gestohlen wird, oder aufgrund eines Defekts nicht mehr einsetzbar ist, kann es ohne Sicherheitskopien der Daten zu unbequemen Situationen durch verpasste Termine kommen. Hier ein Beispiel:

Beispiel 1: Karl verwendet seinen PDA um sein Leben zu strukturieren. Angefangen von beruflichen, sowie privaten Terminen bis zu Telefonnummern, Adressen und seinem privaten Tagebuch speichert er alles auf seinem PDA. Karl hat bisher noch nie einen Gedanken daran verschwendet, dass sein PDA wie alle elektronischen Geräte womöglich irgendwann nicht mehr funktionieren könnte. Natürlich passiert das unausweichliche und eines Tages bleibt das Display seines PDAs schwarz. Da Klaus aufgrund des Alters des Geräts keinen Garantieanspruch mehr hat, betritt er auf dem Weg zur Arbeit das Geschäftlokal eines Handy- und PDA-Spezialisten. Dieser kann zwar das Display des Geräts reparieren, die Daten sind aber verloren. Karl muss mühsam alle Telefonnummern und Termine wiederbeschaffen, da er seinen PDA nie mit seinem PC synchronisiert hat.

Beispiel 2: Auch Sabine speichert ihre Termine in ihrem PDA. Im Gegensatz zu Karl synchronisiert sie ihren PDA regelmäßig mit ihrem PC. An einem Mittwochmorgen verschläft Sabine, vollkommen gestresst stürmt sie aus dem Haus, nur um auf dem Weg zu ihrem Vorstellungsgespräch zu bemerken, dass der Akku ihres PDAs vollkommen leer ist. Sabine kann sich nicht erinnern, ob ihr Termin um 13.00 oder um 14.00 war und kommt zu spät. Ihr Traumjob ist bereits vergeben.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass ein PDA regelmäßig synchronisiert und der Akku aufgeladen werden muss.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Zeitaufwand, sowie die Kosten für diese Maßnahme sind gleich null. In der Regel starten PDAs das Synchronisationsprotokoll von alleine sobald sie ans Kabel angesteckt werden.

M 6.96 NOTFALLVORSORGE FÜR EINEN SERVER

Bei der Sicherung von Daten ist es insbesondere bei Servern wichtig auch Konfigurationdaten zu sichern.

Relevanz für den Durchschnittsbenutzer: mittel

Wenn man Server(dienste) einsetzt, ist auf alle Fälle auf die zusätzliche Sicherung von Konfigurationsdaten zu achten. Bei Durchschnittsbenutzern werden sich aber im Normalfall kaum klassische Server finden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte im Ernstfall ein Server neu aufgesetzt werden müssen, erspart man sich einiges an Zeit und Arbeit wenn die letzte aktuelle Konfiguration zur Hand ist. Hier ein Beispiel:

Beispiel 1: Hubert ist für den Verein der Kaninchenzüchter in seiner Heimatstadt der IT-Beauftragte. Um den Mitgliedern des Vereins ein Kommunikationsmedium zur Verfügung zu stellen, installiert Hubert einen Mailserver mit Accounts für alle Mitglieder. Außerdem präsentiert sich der Verein über die Homepage, die auf dem Server gespeichert ist. Zusätzlich gibt es ein Forum für Mitglieder des Vereins sowie Interessierte. Durch einen Angriff von einer Hackergruppe werden alle Datenbestände gelöscht. Hubert als IT-Beauftragter hat natürlich regelmäßige Backups von den Mailboxen, Homepages sowie Forenbeiträgen gemacht, allerdings hat er nicht daran gedacht die Konfiguration seines Servers auch zu sichern. Alle Informationen über Accounts, die Einstellungen des Mailservers und Spamfilters sowie die Access Control Lists des Forums sind unwiederbringlich verloren gegangen. Hubert muss alles wieder neu konfigurieren.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass bei einem bestehenden Backup auch Konfigurationsdaten bedacht werden sollten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Wenn bereits ein Backup besteht, sind sowohl der zusätzliche Zeitaufwand wie auch die Kosten für die Speicherung der Konfigurationsdaten vernachlässigbar.

M 6.99 REGELMÄßIGE SICHERUNG WICHTIGER SYSTEMKOMPONENTEN FÜR WINDOWS SERVER 2003

Bei der Sicherung von Daten ist es insbesondere bei Servern wichtig auch Konfigurationdaten zu sichern.

Relevanz für den Durchschnittsbenutzer: mittel

Wenn man Server(dienste) einsetzt, ist auf alle Fälle auf die zusätzliche Sicherung von Konfigurationsdaten zu achten. Bei Durchschnittsbenutzern werden sich aber im Normalfall kaum klassische Server finden.

Was kann passieren wenn man die Maßnahme nicht setzt?

Sollte im Ernstfall ein Server neu aufgesetzt werden müssen, erspart man sich einiges an Zeit und Arbeit, wenn die letzte aktuelle Konfiguration zur Hand ist. Hier ein Beispiel:

Beispiel 1: Susanne hat sich vor einiger Zeit als Wochenendprojekt vorgenommen einen Home-NAS-Server für ihre Musik und Film-Sammlung einzurichten. Sie stellt also ihre Medien-Dateien über Samba ihrem PC und ihrem Notebook zur Verfügung. Zusätzlich speichert sie ihre Dateien regelmäßig auf einer USB-Festplatte in einem anderen Zimmer und im Lauf der Zeit erweitert sie ihren NAS-Server um einige zusätzliche Funktionen. So speichert dieser automatisch Susannes bevorzugte PodCasts und ein Programm archiviert ihre Photos welche Susanne natürlich mit in ihr Backup aufnimmt. Nach einem starken Gewitter muss Susanne feststellen, dass von ihrem NAS-Server nicht mehr viel Funktionierendes über ist. Da sich Susanne inzwischen so an die praktischen Funktionen gewöhnt hat, macht sie sich erneut an die Arbeit und muss alle Funktionen wieder händisch konfigurieren. Sie benötigt dafür 4 Tage.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu

vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass bei einem bestehenden Backup auch Konfigurationsdaten bedacht werden sollten.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Wenn bereits ein Backup besteht, sind sowohl der zusätzliche Zeitaufwand wie auch die Kosten für die Speicherung der Konfigurationsdaten vernachlässigbar.

M 6.102 VERHALTENSREGELN BEI WLAN-SICHERHEITSVORFÄLLEN

Relevanz für den Durchschnittsbenutzer: hoch

In etlichen Haushalten und kleinen Betrieben finden sich WLANs. Teilweise werden diese sogar unwissentlich und ungesichert betrieben und bieten Passanten gratis Zugang zum Internet und auch zum eigenen Netzwerk. Daher ist es wichtig zu erkennen wann sich ein WLAN nicht wie vorgesehen Verhält und zu wissen was in so einem Fall zu tun ist.

Was kann passieren wenn man die Maßnahme nicht setzt?

Die Betreiber eines WLANs sind grundsätzlich Verantwortlich für selbiges, wobei natürlich Unwissenheit nicht vor Strafe schützt. Hier ein paar Beispiele:

Beispiel 1: Karl hat von seinem Internetprovider ein ADSL-Modem mit eingebautem WLAN-Router zur Selbstinstallation zugeschickt bekommen. Da Karl technisch versiert ist und Bedienungsanleitungen prinzipiell nicht liest, schließt er sein Modem an die Telefonleitung und seinen Computer an und freut sich über seine neue schnelle Internetverbindung. Peter – Karls zwielichtiger Nachbar – wird von seinem Notebook darauf hingewiesen, dass ein neues WLAN in Reichweite ist und verbindet sich natürlich mit selbigem. Während Peter etliche Downloads startet, fällt Karl auf, dass seine neue schnelle Internetverbindung immer wieder Aussetzer aufweist und immer wieder langsamer ist als erwartet. Nach dem ersten Monat bekommt Karl die Abrechnung von seinem Anbieter und muss feststellen, dass er sein Downloadvolumen erheblich überschritten hat und einen hohen Betrag nachzahlen muss.

Beispiel 2: Hubert bemerkt, dass sein WLAN nicht erreichbar ist, als er die WLAN-Funktionalität seines neuen Handys testen möchte (bislang hat Hubert seinen Computer nur

über Netzwerkkabel an seinem Router angeschlossen, das WLAN hat er nur einmal für seinen Studienkollegen aufgedreht, der ihn mit seinem Notebook besucht hatte). Hubert ignoriert das eigenartige Phänomen ganz zur Freude von Bernd, der heimlich die Kontrolle über Huberts WLAN-Router übernommen hat. Anstatt den WLAN-Router abzuschalten, oder auch nur zu versuchen das Problem über das Webinterface zu untersuchen (Hubert hätte gemerkt, dass etwas nicht stimmen kann, da Bernd das Passwort geändert hat), ermöglicht Hubert, ohne es zu wissen, Bernd weiterhin den freien Zugang zu seinem Netzwerk. Bernd hat zu Huberts Glück aber ein Gewissen und ist damit zufrieden zu wissen, dass er Huberts Netzwerk kontrolliert, er nutzt diese Macht aber nicht aus um Hubert zu schaden.

Maßnahme schwer umzusetzen und/oder schwer an einen Durchschnittsbenutzer zu vermitteln?

Es ist nicht schwer einem Benutzer zu vermitteln, dass er ein außergewöhnliches Verhalten seines WLANs ernst nimmt und kontrolliert.

Maßnahme mit hohem Zeitaufwand und/oder Kosten verbunden?

Der Benutzer muss im Grunde nur auf dem Web-Interface das eigentlich alle WLAN-Router anbieten, nachsehen, welche Geräte mit den Router verbunden sind um zu sehen ob ein unerwünschter Teilnehmer im Netzwerk ist. Verbunden mit einem guten Passwort fürs Webinterface, sowie einer passenden Sicherung des WLANs sollte ein Durchschnittsbenutzer ohne großen Zeitaufwand und ohne zusätzliche Kosten ausreichend geschützt sein.

ZUSAMMENFASSUNG

Maßnahmen aus den BSI-Katalogen, die in dieser Liste nicht aufscheinen, wurden von uns als nicht sinnvoll bewertet.

Mithilfe dieser Auflistung lassen sich nun einige Ergebnisse festhalten. Der wohl wichtigste Punkt ist, dass durch die von uns angeführten Maßnahmen ein Rückschluss auf die wichtigsten und auch häufigsten Themen möglich ist. Gerade diese eignen sich hervorragend für den Einbau in ein Spielkonzept, da sie zum einen Teil sehr vielfältig sind, andererseits aber für die breite Masse an möglichen Nutzern geeignet sind. Die Hauptanliegen, die somit auf alle Fälle in einem Spiel abgedeckt werden sollten sind

„Sichere deine Daten“

„Kenne dein System“

„Kenne deine Einrichtung“

„Aktualisiere deine Software“

„Schalte unnötige Services ab“

„Bewahre dein gesundes Misstrauen“

Diese Liste, bzw. „TODO-Liste“ könnte bereits eine große Vielfalt an Fehlern, die aufgrund von Unwissenheit oder Unachtsamkeit entstehen, verhindern. Es kann somit von Grund auf ein neues und verbessertes Sicherheitsbewusstsein geschaffen werden, das nicht nur privaten Benutzern weiterhelfen könnte, sich in der komplexen Welt der IT-Sicherheit auszukennen und somit Schäden zu vermeiden. Der Grundstock der damit gelegt werden könnte hat Weiters den Vorteil, dass er beliebig erweiterbar ist und auf sämtliche Benutzer angepasst werden kann. Rund um die genannten Schlagworte könnte man nun beginnen ein Spiel zu kreieren, an welchem die Spieler sowohl Spaß haben, als auch ihr Verständnis für die Sicherheitsproblematik in der IT Schulen können.

WIE SOLL DAS WISSEN VERMITTELT WERDEN

Da ein sehr unspezifisches aber breit gefächertes Wissen vermittelt werden soll, ist die Wahl auf die Variante „Simulativer Unterricht“ gefallen. Das fundamentale Wissen kann gut auf spielerische Art und Weise vermittelt werden. Auch ist die Zielgruppe auf spielerische Art einfacher zu erreichen, da ein gut gemachtes Spiel durch den Spielspaß Menschen längerfristig motivieren kann sich mit einem Thema zu befassen, für das sie sich eigentlich nicht interessieren. Daher soll der Spielspaß auf keinen Fall zu kurz kommen.

Auf diese Art kann in der breiten Masse Sicherheitsbewusstsein geschaffen werden, sodass sich Privatpersonen und kleine Betriebe selbst um ein Mindestmaß an Sicherheit kümmern können.

BESTANDSAUFNAHME

Die Mischung aus Bildung und Unterhaltung erzielt bekannterweise gute Ergebnisse beim Lernvorgang, jedoch existiert ein derartiger, spielerischer Ansatz zur Awarenessbildung im Securitybereich bisher noch nicht. Der explizit als "Edutainment" ausgewiesene Ansatz, sich spielerisch mit der Thematik Viren/Virenschanner¹³ zu befassen, vermittelt beispielsweise keine Motivation sich genauer mit dieser Bedrohung zu befassen. Ein weiteres Beispiel ist „bSafe Bingo“¹⁴ - im Grunde eine gute Idee. Es handelt sich hierbei um herkömmliches Bingo (5 in einer Reihe) mit dem Unterschied, dass das laufende Spiel endet und für eine gewisse Zeit auch kein Neues mehr beginnt, sobald es bei einem der Mitarbeiter/Mitspieler zu einer Verletzung kommt. Das funktioniert vielleicht als kleiner Ansporn zusätzliche Vorsicht am Arbeitsplatz walten zu lassen, vermittelt aber auch kein Wissen wie mit bestimmten Gefahrensituationen umzugehen ist.

Weiters wird nicht vermittelt wie es zu Gefahrensituationen kommen kann, wie etwa durch

¹³<http://www.neupart.dk/cmseasy/cmseasy.nsf/0/EFC472198EEEC63EC1256C95005FB9E4?opendocument&expand=&lang=UK>

¹⁴ http://www.safetystar.net/HTML/b-safe_bingo.HTML

die Unwissenheit um Gefahren, durch Leichtgläubigkeit (z.B. Bei SPAM-E-mails welche oft als Nachricht von Banken getarnt sind), Halbwissen, schlechte Planung ohne Einbeziehung von Sicherheitsaspekten oder aber falsche Einschätzung der benötigten Ressourcen für ein brauchbares Sicherheitskonzept.

DAS SPIEL UND DIE SPIELMECHANIK

ÜBERLEGTE SPIELVARIANTEN

Wie sind also zu dem Ergebnis gekommen, dass voraussichtlich der spielerische Ansatz der Erfolgreichste sein dürfte, um Wissen über das Thema Sicherheit im IT-Bereich an Durchschnittsbenutzer zu vermitteln.

Die nächste Frage die es jetzt zu beantworten gilt ist: „Was für ein Spiel ist für diesen Zweck überhaupt geeignet?“

Ein Computerspiel scheidet für uns als Variante im Vorhinein aus, da ein Durchschnittsbenutzer idealerweise schon Wissen über IT-Sicherheit vermittelt bekommen haben sollte, bevor er mit einem Computer arbeitet. Also haben wir uns überlegt, dass ein klassisches Gesellschaftsspiel ein brauchbarer Ansatz ist.

Aber auch ein Gesellschaftsspiel kann man auf verschiedenste Weisen gestalten. Wir haben uns einige Varianten überlegt und diese auf ihre Eignung für unser Ziel, nämlich einem Durchschnittsbenutzer Wissen zum Thema IT-Sicherheit möglichst einfach zu vermitteln, untersucht. Dabei muss neben der Wissensvermittlung vor allem überprüft werden, ob das Spiel nicht zu komplex/schwierig wird bzw. ob es überhaupt Spaß macht, denn nur Spiele die auch unterhaltsam sind werden freiwillig gespielt werden.

Zur Beschreibung der überlegten Spielvarianten verwenden wir folgendes Schema:

- Kurzbeschreibung: Hier wird kurz erklärt um was für eine Art von Spiel es sich handelt.
- Spielweise: Eine kurze Erläuterung wie die Spielmechanik bei dieser Spielvariante funktionieren soll.
- Spielziel: Was ist das Spielziel, was muss man erreichen um bei dem Spiel zu gewinnen?
- Spaßfaktor: Was macht den Reiz/Spaß bei der Spielvariante aus?
- Wissensvermittlung: Wie erfolgt die Wissensvermittlung bei dieser Variante und wie umfangreich ist diese?
- Vorteile: Wo liegen die Vorteile der vorgestellten Spielvariante?
- Nachteile: Was sind die Nachteile der vorgestellten Spielvariante?
- Beispiel des Spielverlaufs: Die Beschreibung einer kurzen fiktiven Spielszene um besser darzustellen wie das Spiel funktionieren soll.

SPIELVARIANTE 1 – DAS KARTENSPIEL

Kurzbeschreibung: Ein Kartenspiel für zwei oder mehrere Personen mit Angriffs- und Verteidigungskarten sowie Ereigniskarten.

Spielweise: Das Spielgeschehen läuft in Runden ab, wobei immer der Spieler, welcher gerade am Zug ist, Angriffe ausspielen kann und externe Ereigniskarten aufdecken kann bzw. muss. Für gute Aktionen (z.B. für einen erfolgreichen Angriff oder aber das erfolgreiche Abwehren eines Angriffs) gibt es dann Punkte bzw. könnte man auch für manche schlechte Aktionen Punkte abziehen. Das Ganze geht so lange rundenweise weiter, bis eine Ereigniskarte das Spielende einläutet. Sobald das Spielende erreicht ist, werden die Punkte, die bei gelungenen Angriffs- oder Verteidigungsaktionen gesammelt wurden, zusammengezählt.

Spielziel: Am Ende des Spiels mehr Punkte gesammelt zu haben als die anderen Mitspieler.

Spaßfaktor: Diese Variante wird vor allem mit vielen Spielern sehr lustig, da nie klar ist wer in der nächsten Runde wen attackieren wird und wann das eigentliche Spielende erreicht sein wird.

Wissensvermittlung: Durch die Angriffskarten (z.B. Hacken, Viren, etc.) und die Verteidigungskarten (Firewall, Antiviren-Software, usw.) kann ein guter Überblick über Gefahren und Verteidigungsmöglichkeiten (sprich Maßnahmen) gegeben werden.

Vorteile: Das Spiel ist einfach zu erlernen und der Spaßfaktor erhöht sich quasi mit der Anzahl der Spieler, die an dem Spiel teilnehmen (bis zu einer gewissen festzulegenden maximalen Spieleranzahl).

Nachteile: Das Spiel wird nur eine kleine Auswahl der Sicherheitsproblematik an die Spieler übermitteln können (begrenzt durch die Anzahl der Karten).

Beispiel eines Spielverlaufs: Spieler A ist am Zug und spielt die Angriffskarte „Hackerangriff - Stufe 2“ aus. Spieler B will mit der Karte „Firewall – Stufe 2“ verteidigen. Die aufgedeckte Ereigniskarte sagt jedoch „Schlecht konfigurierte Firewall, alle Firewalls haben diese Runde nur Stufe 1.“ Daher gelingt Spieler A sein Angriff und er bekommt Punkte für den gelungenen Hackerangriff.

SPIELVARIANTE 2 – EIN BRETTSPIEL MIT KARTEN UND WÜRFELN

Kurzbeschreibung: Ein Brettspiel für zwei oder mehrere Spieler mit Würfeln, Ereignisfeldern und Kauf- und Verkaufsmöglichkeiten von Schutzmechanismen (Karten).

Spielweise: Man muss vom Start zum Ziel kommen und dabei möglichst viele Punkte (oder Geld oder ähnliches) erwirtschaften. Der Würfelwurf bestimmt dabei, wie weit man fahren muss. Die Wege sind teilweise gegabelt und man muss sich an der Weggabelung für einen Weg entscheiden. Dabei kann man am Weg auf Gefahrenfelder, Ereignisfelder oder auf Felder kommen, bei denen man Schutzmechanismen einkaufen kann.

Zusätzlich gibt es eine Art „Mensch-Ärgere-Dich-Nicht“-Regel: wenn ein Spieler auf dasselbe Feld kommt, auf dem gerade ein anderer Spieler steht, passiert etwas mit einer der beiden Spielfiguren (die Konsequenz wird ausgewürfelt).

Spielziel: Spielziel wird es sein vom Start so schnell wie möglich zum Ziel zu kommen und dabei möglichst wenig Punkte/Geld zu verlieren bzw. viele Punkte/Geld zu gewinnen. Wer im Ziel ist bekommt pro Runde, welche die anderen Mitspieler länger brauchen um ins Ziel zu gelangen, noch Punkte/Geld dazu. Wenn alle Spieler im Ziel sind endet das Spiel.

Spaßfaktor: Der Spaßfaktor ist hoch, da das Spiel selbst stark vom Würfelglück abhängt und die „Mensch-Ärger-Dich-Nicht“-Regel zusätzlich für Spannung sorgt.

Wissensvermittlung: Die Wissensaneignung über die Schutzmechanismen erfolgt durch die übers Spielfeld verteilten Gefahrenfelder bzw. Ereignisfelder aber auch durch die Karten.

Vorteile: Diese Variante ist leicht verständlich, abwechslungsreich und lustig durch den unvorhersehbaren Ablauf.

Nachteile: Die Wissensübermittlung ist durch die Anzahl der Gefahrenfelder, Schutzmechanismen (Karten) sowie Ereignisfelder beschränkt.

Beispiel eines Spielverlaufs: Spieler A hat gewürfelt und muss auf ein Gefahrenfeld, wo er die Karte „Virenangriff“ als Ereignis zieht. Zum Glück hat er aber den Schutzmechanismus „Anti-Viren-Programm“ vorher erworben und kann mit dieser Karte den Virenangriff abwehren - nichts ist passiert.

Spieler B hat auch gewürfelt und kommt auf dasselbe Feld wie Spieler A.

Durch Auswürfeln wird entschieden das Spieler A ein Feld weiter muss auf das nächste Gefahrenfeld wo er das Ereignis „Phishing-Attacke“ zieht und Spieler B auf dem Feld stehenbleibt wo ein „Virenangriff“ auf ihn lauert. Spieler B hat keinen Schutz gegen „Virenangriff“ und verliert Punkte. Spieler A hat aber auch keinen Schutz gegen „Phishing-Attacke“ und verliert ebenfalls Punkte.

SPIELVARIANTE 3 – DIE BRETTSPIELVARIANTE MIT EINEM FLEXIBEL GESTALTBAREM SPIELBRETT, MINIATUREN, WÜRFELN UND KARTEN

Kurzbeschreibung: Eine Variante für zwei oder bevorzugt mehrere Spieler, mit Miniaturen, Würfeln, Karten und einem flexibel gestaltbarem Spielbrett.

Man begibt sich in dieser Variante als Computer in die schöne, aber gnadenlose Welt des Internets und muss diverse Aufgaben bestehen.

Spielweise: Ein Spieler wird die „böse“ Seite spielen (nennen wir diesen Spieler den „Netztroll“), welcher das Spielfeld nach einer Anleitung aufbaut. Die anderen spielen einen Computer/Programmierer/Datenkurier der durch das Netz „wandert“. Dargestellt wird dieser Charakter als Miniatur welche an einer bestimmten Stelle des Spielfelds aufgestellt wird.

Die Spieler bekommen dann einen bzw. mehrere Aufträge (z.B. „Hole die Daten von Punkt A und bringe sie sicher nach Punkt B“ – oder um auch die Rolle des Angreifers zu ermöglichen „Stiehl die Daten der Firma XY“), welche der „Netztroll“ – oder auch der Spieler, der die Firma XY besitzt, verhindern muss.

Die Computer/Programmierer/Datenkuriere, welche die Spieler spielen, haben gewisse Fähigkeiten (Virusresistenz, Geschwindigkeit, etc.), welche die Aktionsmöglichkeiten auf dem Spielbrett bestimmen. Rundenweise kommen jetzt der Netztroll und dann die anderen Spieler an die Reihe und können diverse Aktionen ausführen.

Spielziel: Das Spielziel kann von Auftrag zu Auftrag sehr verschieden sein.

Spaßfaktor: Dieser Variante würde es nicht an Skurrilität mangeln und sie würde dementsprechend lustig sein.

Wissensvermittlung: Durch das Attackiert werden / Attackieren und Abwehren von Gefahren und Ereignissen kann viel Wissen an die Spieler vermittelt werden, vor allem da diese Variante leicht um komplexere Szenarien und Informationen erweiterbar ist und theoretisch so beliebige neue Spielverläufe hinzugefügt werden können.

Vorteile: Das System ist durch die Aufträge sehr flexibel und erweiterbar, zudem kommt der Spaßfaktor durch die Rollenverteilung und die Spielwelt, die so geschaffen wird, nicht zu kurz.

Nachteile: Das Spiel ist aufwändig zu erstellen und nicht ganz einfach zu erlernen. Zudem braucht man mindestens drei Spieler, damit es wirklich Spaß macht. Auch kann die Spielzeit, abhängig vom Auftrag, sehr lange werden. Desweiteren würde diese Variante vermutlich nur eine jüngere Zielgruppe ansprechen.

Beispiel eines Spielverlaufs: Es ist ein Spiel mit drei Spielern, einer spielt den Netztroll und zwei andere die Computer. Die Spieler (Computer 1 und Computer 2) haben den Auftrag Daten von Punkt A nach Punkt B zu bringen. Da die Daten für einen Computer zu viel sind, teilen sie die Daten auf Computer 1 und Computer 2 auf. Auf dem Weg zu Punkt B versucht der Netztroll ihre Festplatten durch einen „Bösartigen Virusangriff“ zu zerstören und schafft dies bei Computer 1 auch. Glücklicherweise hat Computer 1 die Karte „Datenbackup auf externer Festplatte“ und verliert so die Daten doch nicht. Computer 1 und Computer 2 bringen die Daten sicher nach Punkt B und haben so den Auftrag erfüllt.

SPIELVARIANTE 4 – DAS QUIZSPIEL

Kurzbeschreibung: Ein Quiz-Spiel für zwei oder mehrere Spieler mit einem farbigem Spielbrett, Ereigniskarten und Würfeln.

Spielweise: Die Spieler oder Spielerteams kommen rundenweise zum Zug. Man muss einerseits würfeln um vorwärts zu kommen, andererseits auch die Fragen richtig beantworten, die man dann gestellt bekommt. Zudem kann der Würfelwurf auch noch durch gezogene Ereigniskarten beeinflusst werden.

Spielziel: Ziel ist es durch eine glückliche Hand beim Würfeln, als auch durch das richtige Beantworten von Fragen schließlich als Erster ins Ziel zu kommen.

Spaßfaktor: Der Spaßfaktor wird vor allem durch das Würfelglück und die gezogenen Zufallsereignisse geprägt, sowie durch witzige Fragestellungen und Antwortmöglichkeiten bei den Quiz-Karten.

Wissensvermittlung: Durch die vielen Fragen und Antworten auf den Quizkarten kann viel Wissen übermittelt werden.

Vorteile: Da man leicht neue Quizkarten hinzufügen kann, kann so eine große Menge an Information ins Spiel gebracht werden.

Nachteile: Wahrscheinlich wird das Spiel schnell für Leute langweilig, die sich schon auskennen bzw. die alle Fragen und Antworten bereits kennen. Umgekehrt frustrierend könnte es für Leute sein, die sich überhaupt nicht bei den Fragen auskennen.

Beispiel eines Spielverlaufs: Spielergruppe 1 beantwortet die gestellte Frage richtig (*Frage: „Was ist eine gute Maßnahme die hilft, wenn einmal ein Datenträger mit wichtigen Daten kaputtgeht?“ Antwort: „Ein regelmäßiges Backup der Daten auf einem anderen Datenträger.“*). und darf die Augenzahl des vorher getätigten Würfelwurfs auch am Spielfeld weiterfahren. Spielergruppe 2 beantwortet die ihnen gestellte Frage nicht richtig, darf ihren Würfelwurf also nicht ziehen. Allerdings ziehen sie auch das Ereignis, dass alle Spieler auf gelben Feldern 4 Felder vorrücken dürfen. Da sie selbst auf einem gelben Feld stehen, dürfen sie trotz Nichtbeantwortung der Frage 4 Felder vorrücken.

SPIELVARIANTE 5 – DAS KARTENSPIEL ERGÄNZT DURCH WÜRFEL

Kurzbeschreibung: Ein Kartenspiel für zwei oder mehrere Spieler mit Computer-, Angriffs- und Verteidigungskarten, sowie Würfel und Ereigniskarten.

Spielweise: Man muss versuchen eine gewisse Anzahl an Computern zu erobern bzw. genug vorher definierte Zusatzziele zu erreichen. Dies passiert rundenweise durch Würfeln, wobei Angriffe durch Schutz- und weitere Angriffskarten erschwert bzw. erleichtert werden können.

Ereigniskarten machen das Spiel zusätzlich spannend.

Spielziel: Ziel ist es eine gewisse Anzahl an Computern zu erobern und/oder Zusatzziele zu erreichen.

Spaßfaktor: Der Spaßfaktor in Variante 5 ist sehr hoch und hängt viel vom Würfelglück bzw. dem Würfelpech ab. Dazu spielt jeder gegen jeden und vor allem bei vielen Spielern wird diese Variante für viel Unterhaltung sorgen.

Wissensvermittlung: Die Wissensübermittlung passiert durch das Kennenlernen welche Verteidigung gegen welchen Angriff wirkt, sowie durch Beschreibungen auf den Ereigniskarten.

Vorteile: Das Spiel ist leicht zu erlernen und macht vor allem mit mehreren Spielern sehr viel Spaß.

Nachteile: Die Wissensübermittlung ist durch die Anzahl der Karten im Spiel begrenzt. Zudem würde bei dieser Variante eher der Spielspaß im Vordergrund stehen und weniger die Wissensvermittlung.

Beispiel eines Spielverlaufs: Spieler A möchte Spieler B einen Computer mit der Karte „Hackerangriff“ wegnehmen und müsste mit 5 sechseitigen Würfeln mindestens auf 15 Würfelaugen kommen um den Computer übernehmen zu können. Vorher hat er zudem die Ereigniskarte „schlecht konfiguriertes System“ ausgespielt, welches die Verteidigung des Angegriffenen zudem noch um 3 Punkte schwächt, er jetzt also nur 12 Würfelaugen würfeln müsste, um beim Angriff erfolgreich zu sein.

Spieler B hat seinen Computer allerdings mit der Verteidigungskarte „Firewall“ geschützt, wodurch die Schwierigkeit auf 20 erhöht wird. Spieler A schafft bei seinem Würfelwurf aber nur 19 und Spieler B kann so den Computer behalten.

DIE VON UNS GEWÄHLTE SPIELVARIANTE IM DETAIL

Nach vielen Diskussionen haben wir beschlossen, ein Brettspiel zu erstellen, bei dem es Ereigniskarten, Angriffs- sowie Verteidigungskarten und Würfeln gibt. Diese Variante haben wir vor allem deshalb gewählt, weil sie viele Vorteile der vorher vorgestellten Varianten bietet und nur wenige von den Nachteilen.

Diese Variante bietet die Vorteile, dass sie leicht zu verstehen ist, kein Wissen um die Gefahren im IT-Bereich voraussetzt, von zwei oder mehreren Spielern gespielt werden und voraussichtlich viel Spaß machen kann. Zudem kann man bei Bedarf das Spiel auch erweitern und damit das Wissensgebiet ausweiten, in dem man neue Angriffs-, Verteidigungs- und Ereigniskarten dem Spiel hinzufügt. Zunächst wollen wir nun das Grundgerüst des Spiels erklären:

Kurzbeschreibung: Ein Brettspiel, bei dem es kein Ziel-Feld gibt, sondern welches nur ein Start-Feld über welches man immer wieder zieht wenn man das Spielfeld „umrundet“, hat. Es gibt Angriffskarten, mit denen man andere Mitspieler attackieren kann, Verteidigungskarten, mit denen man sich gegen Angriffe verteidigen kann, verschiedene Arten von Feldern auf dem Spielbrett, auf denen man vordefinierte Aktionen ausführen darf/muss, wie etwa Ereignisfelder, auf denen ein Ereignis eintritt (bestimmt durch eine gezogene Ereigniskarte) .

Spielweise: Jeder Spieler repräsentiert ein Team, welches ein IT-Projekt fertig stellen soll und dabei zwangsläufig mit vielen Problemen der IT konfrontiert werden wird. Die Spieler kommen nacheinander an die Reihe und dürfen würfeln und dann, je nachdem auf welches Feld sie mit ihrer Spielfigur gezogen sind, Aktionen ausführen. Man sammelt Punkte durch gewisse Aktionen und kann diese durch andere auch wieder verlieren. Punkteabzüge kann es etwa durch nicht abgewehrte Angriffe von Mitspielern oder böse Ereignisse geben, Punktegewinne durch das erfolgreiche Abwehren von Angriffen, positive Ereignisse und dem Passieren des Start-Feldes.

Spielziel: Das Spielziel ist es, als Erster die geforderte Punkteanzahl zu erreichen und damit das IT-Projekt erfolgreich abzuschließen.

Spaßfaktor: Der Spaßfaktor dürfte sehr hoch sein, da dieses Spiel eine hohe Zufallskomponenten mitbringt und die meisten Aktionen neben einer Karte zusätzlich durch einen Würfelwurf bestimmt werden. Da die Spieler sich auch gegenseitig attackieren können und sowohl mit Punktegewinn als auch mit Punkteverlust gearbeitet wird, kann sich theoretisch ein Spielverlauf in wenigen Zügen komplett ändern. Damit bleibt auch die

Langzeitmotivation erhalten, da es kein Patentrezept für das Spiel gibt mit dem man automatisch gut abschneiden wird.

Wissensübermittlung: Die Wissensvermittlung erfolgt durch das Wissen welcher Angriff bzw. welches negative Ereignis mit welcher Verteidigungskarte bzw. mit welchen Verteidigungskarten abgewehrt werden kann. Zudem stehen auf den Karten und in der Anleitung Kurzbeschreibungen zu den Ereignissen. Die Kartenanzahl kann theoretisch auch durch Erweiterungen erhöht werden.

Vorteile: Diese Variante ist leicht zu erlernen, sorgt auch für längerfristigen Spielspaß, vor allem mit mehr Mitspielern. Die Wissensvermittlung kann zwar nur in einem beschränkten Rahmen passieren, ist dafür aber sehr einprägsam. Das Spiel kann theoretisch auch mit neuen Angriffs-, Verteidigungs- sowie Ereigniskarten oder anderen Spielfeldverläufen erweitert werden und so mehr Wissen in das Spiel gepackt werden.

Nachteile: Die Wissensvermittlung ist durch die Anzahl der Karten beschränkt. Da diese Spielvariante aber theoretisch durch eine gewisse Anzahl an Zusatzkarten erweitert werden kann, kann man diesem Problem zumindest begrenzt abhelfen.

Beispiel eines Spielverlaufs: siehe die nachfolgende Anleitung

BESCHREIBUNG DES SPIELES „DAMN IT! – DIE VERRÜCKTE WELT DER IT“.

WORUM GEHT ES BEI DEM SPIEL?

Mehrere Teams kämpfen darum, schneller als die konkurrierenden Teams ein IT-Projekt fertigzustellen. Dabei wird natürlich alles gemacht, um die Konkurrenz zu behindern und selbst schnell voranzukommen. Aber auch werden Ereignisse auftreten, die in der IT-Welt nun einmal vorkommen können. Jeder Spieler übernimmt eines dieser Teams und versucht durch das Sammeln von Punkten die geforderte Punktezahl zu erreichen und damit das IT-Projekt erfolgreich abzuschließen.

EMPFOHLENES ALTER

10-99

SPIELLÄNGE

zwischen 30 und 75 Minuten

MÖGLICHE SPIELERANZAHL

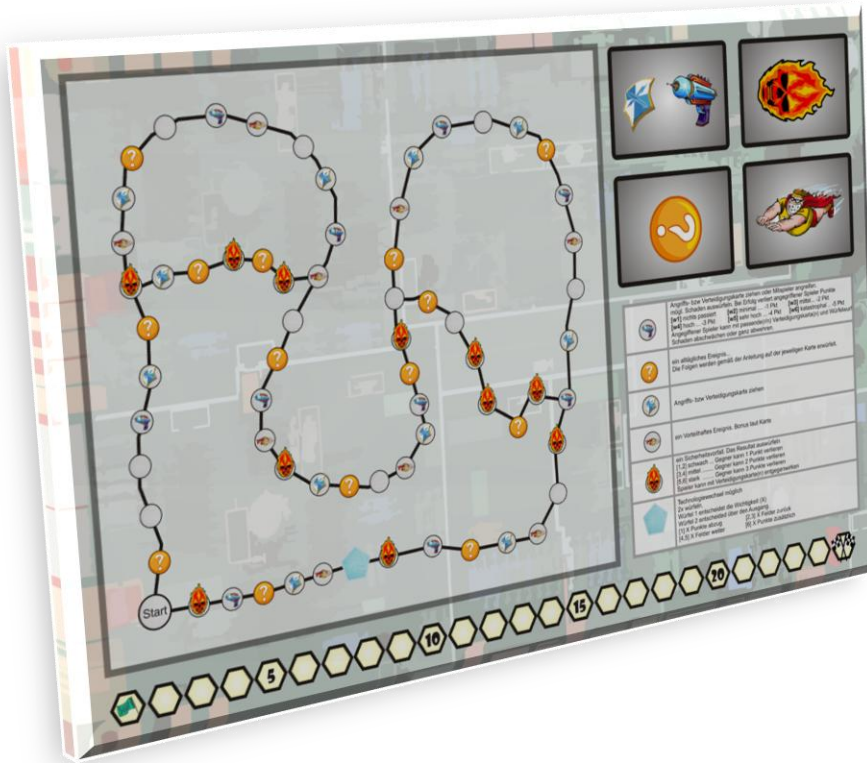
2-6

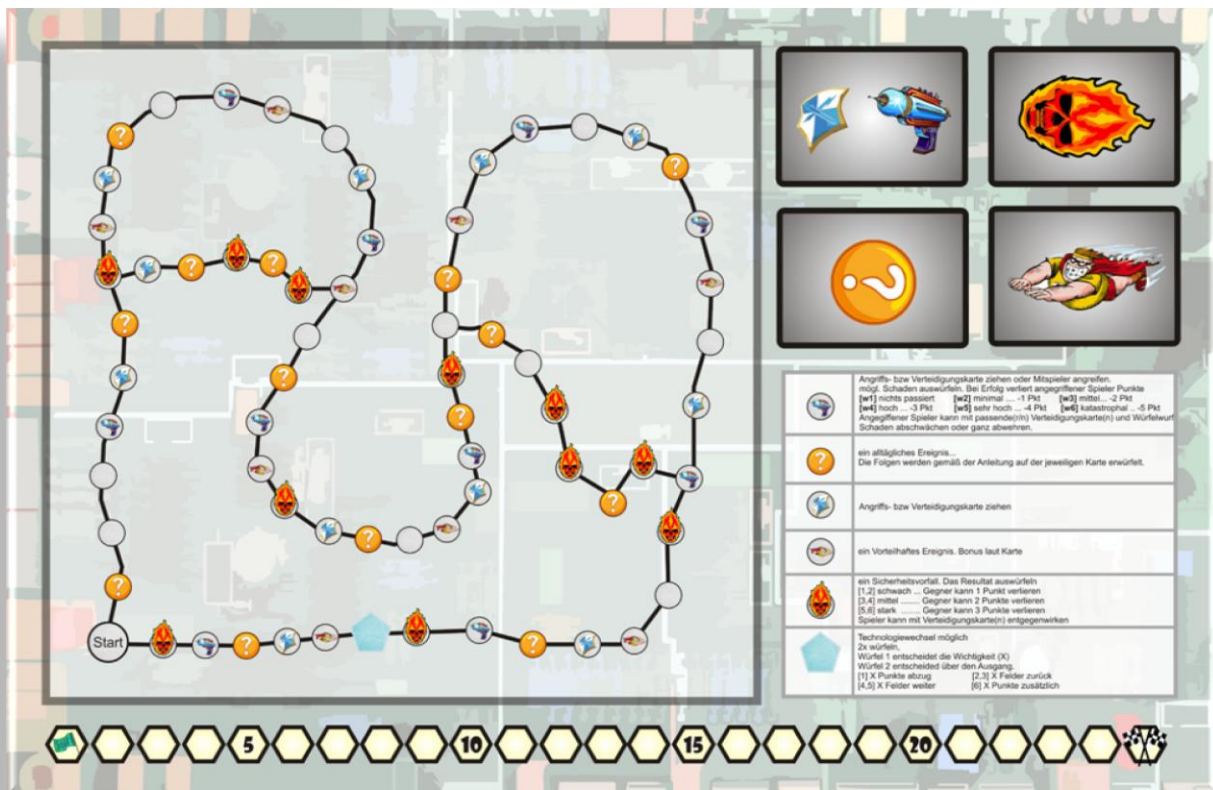
INHALT DES SPIELS

- 1 Spielbrett
- 6 Spielfiguren
- 6 Markierungssteine
- 54 Angriffs-/Verteidigungskarten (20 Angriffskarten und 34 Verteidigungskarten)
- 10 Ereigniskarten für positive Ereignisse
- 14 Ereigniskarten für negative Ereignisse
- 10 Ereigniskarten für zufällige Ereignisse
- 1 Würfel (sechseitig)
- 1 Anleitung

DAS SPIELBRETT

Die Quellen (siehe Quellenangaben S001-S009) beziehen sich auf die verwendeten Grafiken. Diese wurden jeweils in den Programmen Photoshop bzw Corel Draw bearbeitet und in die hier vorliegende Form gebracht.





DIE PUNKTELEISTE



SPIELAUFBAU

- Zuerst wird das Spielbrett aufgestellt.
- Die Spielfiguren werden auf das Startfeld gesetzt.
- Die zu den Spielfiguren gehörenden Markierungssteine auf der Punkteanzeige auf 0 (grüne Flagge) setzen.
- Einen Kartenstapel aus den Angriffs-/Verteidigungskarten erstellen und gut durchmischen. Danach bekommt jeder Mitspieler 5 von diesen Karten und der Rest wird auf den dafür vorgesehenen Platz (übereinstimmende Grafik am Kartenrücken) am Spielbrett gelegt.
- Einen Kartenstapel aus den Ereigniskarten für positive Ereignisse erstellen, diesen durchmischen und dann auf den dafür vorgesehenen Platz (übereinstimmende Grafik am Kartenrücken) am Spielbrett legen.

- Einen Kartenstapel aus den Ereigniskarten für negative Ereignisse erstellen, diesen durchmischen und dann auf den dafür vorgesehenen Platz (übereinstimmende Grafik am Kartenrücken) am Spielbrett legen.
- Einen Kartenstapel aus den Ereigniskarten für zufällige Ereignisse erstellen, diesen durchmischen und dann auf den dafür vorgesehenen Platz (übereinstimmende Grafik am Kartenrücken) am Spielbrett legen.
- Jeder Mitspieler würfelt einmal mit dem sechsseitigen Würfel. Der Spieler mit der höchsten Augenzahl beginnt. Sollten mehrere Spieler diese Augenzahl haben wird unter diesen der Vorgang solange wiederholt bis ein klarer Sieger des Stechens feststeht. Dieser Spieler darf dann beginnen. Nach dessen Zug kommt der nächste Spieler im Uhrzeigersinn an die Reihe.

SPIELABLAUF

EIN SPIELZUG FOLGT FOLGENDEM SCHEMA

- 1 x Würfeln mit dem sechsseitigen Würfel. Mit der Spielfigur dann die Augenzahl an Feldern am Spielbrett weiterziehen (im Uhrzeigersinn). Sollte sich der Weg am Spielbrett gabeln darf der Spieler entscheiden welche Abzweigung er nimmt.
- Sollte auf dem Feld, auf dem die Spielfigur zum Stehen kommt, eine Aktion möglich sein, wird diese durchgeführt. Sollte sich dabei der Punktestand eines Spielers ändern, wird der Markierungsstein des Mitspielers auf der Punkteanzeige entsprechend an die richtige Stelle gesetzt. Bei Punkteverlust kann man dabei nicht unter 0 Punkte sinken. Sollte man bei der Aktion Karten vom Angriffs-/Verteidigungskartenstapel ziehen können und man hat dann mehr als 8 Angriffs/Verteidigungskarten (A/V) auf der Hand, müssen überzählige A/V-Karten in den A/V-Kartenstapel hineingemischt werden, wobei der Spieler selbst entscheiden kann welche Karten er abgeben will.
- Sollte ein Spieler jetzt 25 Punkte oder mehr haben, ist das Spiel zu Ende und dieser Spieler hat gewonnen. Ansonsten ist der nächste Spieler an der Reihe.

ES GIBT FOLGENDE MÖGLICHKEITEN AN PUNKTE ZU KOMMEN:

- Das Start-Feld passieren (8 Punkte) oder direkt darauf zum stehen kommen. (10 Punkte).
- Durch die Auswirkung eines positiven Ereignisses.
- Das erfolgreiche Durchführen einer Verteidigungsaktion.
- Manche Zufallsereignisse.
- Am „Neue Technologie“-Feld

DIE SPIELFELDER UND DARAUF MÖGLICHE AKTIONEN:

Das Start-Feld



Dies ist das Feld an dem alle Spielfiguren am Anfang stehen. Wenn ein Spieler mit seiner Spielfigur im Laufe des Spiels dieses Feld passiert bekommt er 8 Punkte. Sollte die Spielfigur direkt auf dem Start-Feld zum Stehen kommen, gibt es sogar 10 Punkte.

Leeres Feld



Hier kann keine Aktion durchgeführt werden.

Ereignisfeld – positives Ereignis



Kommt man auf dieses Feld, wird die oberste Karte vom Kartenstapel mit den positiven Ereignissen abgehoben, dann gewürfelt und dann auf der Karte nachgesehen, welchen Effekt das Würfelerggebnis hat. Anschließend wird die Karte wieder in den Kartenstapel mit den positiven Ereignissen hineingemischt.

Ereignisfeld – schlechtes Ereignis

Kommt man auf dieses Feld, wird die oberste Karte vom Kartenstapel mit den schlechten Ereignissen abgehoben und nachgesehen, um welches negative Ereignis es sich handelt.

Negative Ereignisse können durch bestimmte Verteidigungskarten abgewehrt werden. Sollte der Spieler eine oder mehrere dieser Verteidigungskarten in seinem Besitz haben, kann er versuchen mit einer Verteidigungsaktion (siehe Verteidigungsaktion) das Ereignis abzuwehren.



Sollte die Verteidigungsaktion erfolgreich sein, bekommt der Spieler einen Punkt dazu.

Sollte er mangels Verteidigungskarten keine Verteidigungsaktion durchführen können oder schlägt die Verteidigungsaktion fehl, muss der Spieler würfeln und das Würfelergebnis hat dann folgenden Effekt:

- 1-2: einmal Aussetzen
- 3-4: -1 Punkt (auf der Punkteanzeige)
- 5: -2 Punkte (auf der Punkteanzeige)
- 6: -3 Punkte (auf der Punkteanzeige)

Die Karte mit dem schlechten Ereignis wird wieder in den Kartenstapel hineingemischt.

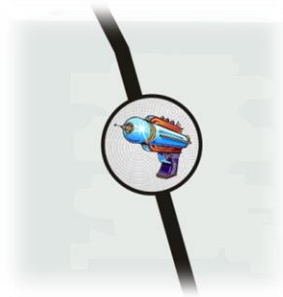
Eventuell eingesetzte Verteidigungskarten müssen in den Kartenstapel mit den Angriffs-/Verteidigungskarten hineingemischt werden.

Ereignisfeld – zufälliges Ereignis



Kommt man auf dieses Feld, wird die oberste Karte vom Kartenstapel mit den zufälligen Ereignissen abgehoben, dann gewürfelt und dann auf der Karte nachgesehen, welchen Effekt das Würfelergebnis hat. Anschließend wird die Karte wieder in den Kartenstapel mit den zufälligen Ereignissen hineingemischt.

Das Angriffsfeld



Auf diesem Feld hat man entweder die Möglichkeit eine Angriffsaktion (siehe Angriffsaktion) auf einen beliebigen Mitspieler durchzuführen oder man darf würfeln, ob man eine Karte vom A/V-Kartenstapel abheben darf. Das Würfelergebnis hat dabei folgenden Effekt:

- 1-3: Man darf keine Karte abheben.
- 4-6: Man darf eine Karte abheben.

Das Verteidigungsfeld



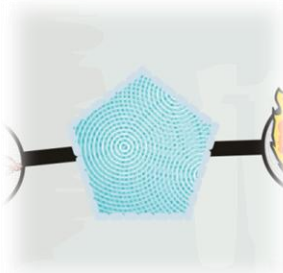
Hier hat man die Möglichkeit, eine Karte vom A/V-Kartenstapel abzuheben(ansonsten passiert nichts).

Das "Neue Technologie"-Feld:

Am Feld „Neue Technologie “ muss zweimal gewürfelt werden um festzulegen wie gut oder wie schlecht die neue Technologie funktioniert.

Der erste Wurf bestimmt wie stark sich die neue Technologie auswirken wird. Nennen wir den gewürfelten Wert „X “.

Der zweite Wurf bestimmt wie sich die neue Technologie auswirkt.



Würfelergebnis / Effekt

- 1: man verliert „X“ Punkte
- 2: man muss „X“ Felder zurückfahren
- 3-4: Kein Effekt
- 5: man fährt „X“ Felder weiter
- 6: man bekommt „X“ Punkte dazu

EIN FELD AUF DEM BEREITS ANDERE MITSPIELER STEHEN

Wenn man auf einem Feld landet, auf dem bereits ein oder mehrere Mitspieler stehen, kann man eine Angriffsaktion auf einen dieser Mitspieler durchführen, vorausgesetzt man hat eine Angriffskarte.

DIE ANGRIFFSAKTION

Eine Angriffsaktion kann dann durchgeführt werden, wenn man selbst eine Angriffskarte besitzt und die eigene Spielfigur entweder auf einem Angriffsfeld zu stehen kommt oder aber auf einem Feld wo ein anderer Mitspieler bereits steht.

Auf einem Angriffsfeld kann man eine Angriffsaktion auf einen beliebigen Mitspieler vornehmen.

Wenn man auf ein Feld kommt, auf dem bereits ein oder mehrere Mitspieler stehen, kann man auf einen dieser Mitspieler eine Angriffsaktion durchführen. Eventuelle Aktionen auf diesem Feld (z.B. das Karten ziehen auf einem Ereignisfeld) müssen aber vor der Angriffsaktion durchgeführt werden.

Wenn man einen Mitspieler angreift legt man diesem die entsprechende Angriffskarte vor. Auf dieser Angriffskarte steht ein Wert, der angibt wie schwierig es ist diesen Angriff abzuwehren und es stehen dort auch die Gegenmaßnahmen/Verteidigungskarten die gegen diesen Angriff helfen würden.

Der angegriffene Mitspieler kann dann entscheiden, ob er eine Verteidigungsaktion durchführen will bzw. kann. Sollte er dies nicht machen, oder aber die Verteidigungsaktion fehlschlagen, dann wird der Effekt ausgewürfelt den dieser Angriff hat.

Würfelergebnis / Effekt

- 1: Glück gehabt. Nichts passiert.
- 2: Minimaler Schaden (-1 Punkt bei Erfolg)
- 3: Mittlerer Schaden (-2 Punkte bei Erfolg)
- 4: Hoher Schaden (-3 Punkte bei Erfolg)
- 5: Sehr hoher Schaden (-4 Punkte bei Erfolg)
- 6: Ein großes Desaster (-5 Punkte bei Erfolg)

Nach der Angriffsaktion, egal ob sie erfolgreich war oder nicht, wird die Angriffskarte in den A/V-Kartenstapel hineingemischt.

DIE VERTEIDIGUNGSAKTION

Eine Verteidigungsaktion kann man dann durchführen, wenn eine Angriffskarte auf einen ausgespielt wurde oder wenn man auf ein Ereignisfeld gezogen ist, auf dem dann ein schlechtes Ereignis eintreten würde. Damit man die Verteidigungsaktion durchführen kann, muss man zumindest eine Verteidigungskarte in den Händen halten, die gegen das entsprechende negative Ereignis, bzw. die Angriffskarte helfen würde (steht auf der entsprechenden Angriffskarte bzw. der Ereigniskarte).

Auf Angriffskarten und Ereigniskarten mit schlechten Ereignissen steht ein Zahlenwert.

Dieser gibt an wie hoch man würfeln muss um den Angriff bzw. das Ereignis abzuwehren.

Dieser Wert ist davon abhängig, wieviele Gegenmaßnahmen es gegen diesen Angriff bzw. dieses Ereignis gibt.

Anzahl Gegenmaßnahmen / Zahlenwert der für eine erfolgreiche Verteidigungsaktion erreicht oder überboten werden muss.

- 4 Gegenmaßnahmen:Schwierigkeit 7
- 3 Gegenmaßnahmen:Schwierigkeit 6
- 2 Gegenmaßnahmen:Schwierigkeit 5
- 1 Gegenmaßnahme: Schwierigkeit 4

Man muss also einmal würfeln. Jede Verteidigungskarte die eingesetzt wird um den Angriff bzw. das negative Ereignis abzuwehren bringt einen Bonus auf den Wurf. Man darf so viele Verteidigungskarten einsetzen wie man will, nur müssen diese auch gegen die Angriffsaktion bzw. das negative Ereignis helfen. Verteidigungskarten gibt es in jeweils zwei Varianten, in Stärke 1 (ein Schild / +1 auf den Würfelwurf) und in Stärke 2 (zwei Schilde / +2 auf den Würfelwurf).

Sollte der Bonus der Verteidigungskarten bereits ausreichen um den Wert zu erreichen, muss nicht extra gewürfelt werden.

Alle eingesetzten Verteidigungskarten müssen nach der Verteidigungsaktion wieder in den A/V-Kartenstapel hineingemischt werden, egal ob die Verteidigungsaktion erfolgreich war oder nicht.

Eine erfolgreiche Verteidigungsaktion bringt dem Verteidiger einen Zusatzpunkt ein.

Beispiel: Spieler A spielt die Angriffskarte „Hacker“ auf Spieler B aus. Diese Angriffskarte hat die Schwierigkeit 7 und kann durch die vier Verteidigungskarten „Firewall“, „Gutes Passwort“, „Richtige Rechtevergabe“ und „gesichertes WLAN“ abgewehrt werden.

Spieler B hat zufällig die Verteidigungskarten „Firewall“ (Stufe 2) und „richtige Rechtevergabe“ (Stufe 1) und setzt diese auch ein. Das bedeutet er hat damit einen Bonus von 3 Punkten. Um die Schwierigkeit 7 zu erreichen und damit den Angriff abzuwehren müsste er dann eine 4 oder höher würfeln.

Die Quellen (siehe Quellenangaben K0001-K0060) beziehen sich auf verwendete Bilder oder Grafiken. Diese wurden jeweils in den Programmen Photoshop bzw Corel Draw bearbeitet und in die hier vorliegende Form gebracht.

10 ANGRIFFSKARTEN (JEWEILS 2 MAL – INSGESAMT 20 KARTEN)

Effekt:

- 1: Nichts passiert.
- 2: Minimaler Schaden (-1 Punkt bei Erfolg)
- 3: Mittlerer Schaden (-2 Punkte bei Erfolg)
- 4: Hoher Schaden (-3 Punkte bei Erfolg)
- 5: Sehr hoher Schaden (-4 Punkte bei Erfolg)
- 6: Ein großes Desaster (-5 Punkte bei Erfolg)

Karte	Angriffsform	Verteidigungsmöglichkeit	Quelle
	Social Engineering	Schulungen, gesundes Misstrauen	K0019
	Diebstahl Einbruch	Sicherheitstüren/Sicherheitsfenster, Backup, Versicherung, Verschlüsselung	K0018



Virus / Wurm

Antivirensoftware, Sicherheitsupdates, Firewall

K0016



WLAN-Sniffing

Verschlüsselung, Gesichertes WLAN

K0039



Hacker

Firewall, Gutes Passwort, Richtige Rechtevergabe, gesichertes WLAN

K0015



Trojanisches Pferd

Antivirensoftware, gesundes Mißtrauen

K0037



Dumpster
Diving

Richtiges Entsorgen/richtiges
Löschen

K0036



Phishing

Gesundes Misstrauen, Schulung

K0038



Sabotage

motivierte Mitarbeiter,
Sicherheitstüren/Sicherheitsfenster,
richtige Rechtevergabe, gesundes
Misstrauen

K0040






Passwort
cracken

gutes Passwort

K0041

17 VERTEIDIGUNGSKARTEN (2 SETS: EINMAL IN STÄRKE 1 UND EINMAL IN STÄRKE 2)
 INSGESAMT 34 KARTEN.

Karte	Verteidigungsmaßnahme	schützt vor:	Quelle
 <p>The card features a background image of a computer monitor displaying a virus scanner interface. A text box on the screen reads: 'Antivirensoftware', 'Virens Scanner erkennen und entfernen Computerviren.', and 'Zu beachten: regelmäßig Updates einspielen'. The card is part of a set with a vertical 'SICHERHEIT' banner on the left.</p>	Antivirensoftware	Virus/Wurm, Trojanisches Pferd, Virenbefall	K0008
 <p>The card features a background image of a server rack. A text box on the screen reads: 'Backup', 'Backups sind Sicherheitskopien von wichtigen Daten.', and 'Zu beachten: regelmäßig, am besten automatisch durchführen'. The card is part of a set with a vertical 'SICHERHEIT' banner on the left.</p>	Backup	Diebstahl/Einbruch, Datenträgerfehler, Sturzschaden, Verlust	K0007
 <p>The card features a background image of a computer keyboard. A text box on the screen reads: 'richtige Entsorgung und Löschen', 'Richtiges Löschen von Datenträgern erfordert, daß jegliche Information mehrfach mit Zufallsdaten überschrieben wird.', and 'Dokumente müssen vor der Entsorgung zerstört werden.'. The card is part of a set with a vertical 'SICHERHEIT' banner on the left.</p>	richtige Entsorgung und Löschen	Dumpster Diving, falsche Entsorgung	K0012



Passwort

Hacker, Passwort cracken

K0005



Rechtevergabe

Hacker, Vandalismus/Sabotage, Sabotage

K0014



Versicherung

Diebstahl/Einbruch, Einbruch, Sturzschaden, Verlust

K0025



Richtige Klimatisierung

Schlechte Klimatisierung, falsche Lagerung

K0034



Sicherheitsupdates

Virus/Wurm,
Virenbefall

K0009



Gesichertes WLAN

WLAN-Sniffing,
gesichertes WLAN

K0010



Verschlüsselung

Diebstahl/Einbruch,
WLAN-Sniffing

K0011



Firewall

Virus/Wurm, Hacker,
Virenbefall

K0013



USV

Unwetter, Stromausfall

K0033



Sicherheitstüren und Fenster

Diebstahl/Einbruch, Vandalismus/Sabotage, Sabotage

K0035



Gesundes Misstrauen

Social Engineering, Trojanisches Pferd, Phishing, Sabotage, Vandalismus/Sabotage

K0042



Schulung

Social Engineering, Phishing, Spamwelle, falsche Lagerung, Menschliches Versagen

K0043



motivierte Mitarbeiter

Vandalismus/Sabotage, Sabotage

K0045



Brandschutz

Feuer

K0044

EREIGNISKARTEN IM SPIEL

Ereigniskarten werden nach der Benutzung wieder in den Kartenstapel zurückgemischt.

14 NEGATIVE EREIGNISSE: (INSGESAMT 14 KARTEN)

Würfelergebnis/Effekt

1-2: Einmal Aussetzen

3-4: -1 Punkt

5: -2 Punkte

6: -3 Punkte

Karte	Negatives Ereignis	Maßnahme dagegen...	Quelle
	Unwetter	USV / Überspannungsschutz	K0001
	Einbruch	Sicherheitstüren/Sicherheitsfenster, Versicherung	K0004



Stromausfall

USV / Überspannungsschutz

K0026



Virenbefall

Antivirensoftware, Sicherheitsupdate,
Firewall

K0028



Spamwelle

Schulung

K0029



Feuer

Brandschutz

K0002



Schlechte
Klimatisierung

Klimatisierung

K0003



Datenträgerfehler

Backup

K0030



Sturzscha-den

Backup, Versicherung

K0031



falsche Lagerung

Schulung, richtige Klimatisierung

K0032



Sabotage

motivierte Mitarbeiter, gesundes Misstrauen, richtige Rechtevergabe, Sicherheitstüren/Sicherheitsfenster

K0040



falsche Entsorgung

richtige Entsorgung/richtiges Löschen

K0048



Verlust

Versicherung, Backup

K0049



Fehlverhalten




Schulung

K0050

10 POSITIVE EREIGNISSE: (INSGESAMT 10 KARTEN)

Zur Erklärung:

Nochmal würfeln bedeutet, dass man dies wie einen zusätzlichen Zug betrachten darf. Wenn man noch zweimal oder dreimal würfeln darf gilt folgendes: Es wird ebenfalls als ein zusätzlicher Zug betrachtet, die Würfelwürfe werden dabei einfach zusammengezählt.

Karte	positives Ereignis	Würfelergebnis / Effekt	Quelle
 <p>Upgrade Verbindung</p> <p>Schnellere Datentransferraten erhöhen die Produktivität.</p> <p>Würfeln ... 1-2 : +1 Punkt 3-4 : +2 Punkte 5-6 : +3 Punkte</p>	Upgrade Verbindung	1-2: +1 Punkt 3-4: +2 Punkte 5-6: +3 Punkte	K0020
 <p>Prozessor Upgrade</p> <p>Besser Hardware erleichtert die Arbeit.</p> <p>Würfeln: 1-2 : 1 A/V Karte abheben 3-4 : 2 A/V Karten abheben 5-6 : 3 A/V Karten abheben</p>	Prozessorupgrade	1-2: 1 Karte abheben 3-4: 2 Karten abheben 5-6: 3 Karten abheben	K0021
 <p>Besseres Backupsystem</p> <p>Ein verbessertes Backupsystem verringert die Wartezeit im Falle einer Wiederherstellung.</p> <p>Würfeln: 1-2 : 1 A/V Karte abheben 3-4 : 2 A/V Karten abheben 5-6 : 3 A/V Karten abheben</p>	Besseres Backup-System	1-2: 1 Karte abheben 3-4: 2 Karten abheben 5-6: 3 Karten abheben	K0022



motivierte Mitarbeiter

1-2:	noch einmal würfeln	
3-4:	noch zweimal würfeln	K0023
5-6:	noch dreimal würfeln	



Schulungen

1-2:	1 Karte abheben	
3-4:	2 Karten abheben	K0024
5-6:	3 Karten abheben	



Open Source Alternativen

1-2:	+1 Punkt	
3-4:	+2 Punkte	K0027
5-6:	+3 Punkte	



Bessere Verschlüsselung

1-2:	noch einmal würfeln	
3-4:	noch zweimal würfeln	K0046
5-6:	noch dreimal würfeln	



Bessere Klimatisierung

1-2: +1 Punkt

3-4: +2 Punkte

5-6: +3 Punkte

K0034



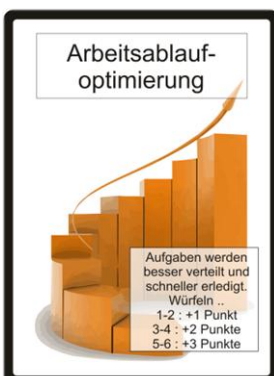
Neue Sicherheitstüren
und Fenster

1-2: noch einmal würfeln

3-4: noch zweimal würfeln

5-6: noch dreimal würfeln

K0035



Arbeitsablauf-
optimierung

1-2: +1 Punkt

3-4: +2 Punkte

5-6: +3 Punkte

K0047

10 ZUFALLSEREIGNISSE (INSGESAMT 10 KARTEN)

add Würfelwürfe: Nochmal würfeln bedeutet, dass man dies wie einen neuen Zug betrachten darf. Bei zweimal würfeln: Würfelwürfe zusammenzählen und als einen Zug betrachten.

Karte	Zufallsereignis	Würfelergebnis / Resultat	Quelle
	Gesetzesänderung	1: 2 Runden aussetzen 2: 1 Runde aussetzen 3-4: nichts passiert 5: noch einmal würfeln 6: noch zweimal würfeln	K0051
	Änderung der Zugriffsrechte	1: -2 Punkte 2: -1 Punkte 3: eine Karte ablegen 4: eine Karte ziehen 5: +1 Punkt 6: +2 Punkte	K0052
	Neue Software	1: 2 Runden aussetzen 2: 1 Runde aussetzen 3-4: nichts passiert 5: noch einmal würfeln 6: noch zweimal würfeln	K0053



Neuer Mitarbeiter

- 1: -1 Punkt
 2: eine Runde aussetzen
 3-4: nichts passiert
 5: noch einmal würfeln
 6: +1 Punkt
- K0054



Neues Gebäude

- 1: -2 Punkte
 2: -1 Punkt
 3-4: nichts passiert
 5: +1 Punkt
 6: +2 Punkte
- K0055



Consultant

- 1: 2 Karten ablegen
 2: 1 Karte ablegen
 3-4: nichts passiert
 5: 1 Karte ziehen
 6: 2 Karten ziehen
- K0056



Besucher

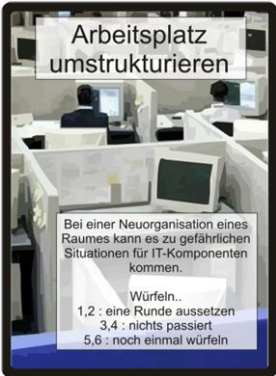
- 1-2: -1 Punkt
 3-4: nichts passiert
 5-6: +1 Punkt
- K0057



Datentransfer

- 1: 2 Runden aussetzen
- 2: 1 Runde aussetzen
- 3-4: nichts passiert
- 5: noch einmal würfeln
- 6: noch zweimal würfeln

K0058



Arbeitsplatz umstrukturieren

- 1-2: einmal aussetzen
- 3-4: nichts passiert
- 5-6: noch einmal würfeln

K0060



Kooperation

- 1: -2 Punkte
- 2: -1 Punkte
- 3-4: nichts passiert
- 5: +1 Punkte
- 6: +2 Punkte

K0059

ARBEITSAUFTEILUNG

Vorwort	Andreas Weiner
Sicherheit und Sicherheitsverständnis	Alexander Piskernik
Allgemein	Alexander Piskernik
IT	Alexander Piskernik
Didaktische Verfahren	Alexander Piskernik
Frontalunterricht	Alexander Piskernik
Diskussionsrunden	Alexander Piskernik
Lernen durch Lehren / Selbststudium / Studienzirkel	Alexander Piskernik
eLearning / Programmierter Unterricht	Alexander Piskernik
Learning by Doing	Alexander Piskernik
Simulativer Unterricht / Spielerisches Lernen	Alexander Piskernik
Wer ist die Zielgruppe	Alexander Piskernik
Was soll vermittelt werden	Alexander Piskernik
Maßnahmenkatalog des BSI	Andreas Weiner
Einführung	Andreas Weiner
M 1 Maßnahmenkatalog Infrastruktur	Andreas Weiner
M 2 Maßnahmenkatalog Organisation	Andreas Weiner
M 3 Maßnahmenkatalog Personal	Andreas Weiner
M 4 Maßnahmenkatalog Hardware und Software	Alexander Piskernik
M 5 Maßnahmenkatalog Kommunikation	Alexander Piskernik
M 6 Maßnahmenkatalog Notfallvorsorge	Alexander Piskernik
Wie soll das Wissen vermittelt werden	Alexander Piskernik
Bestandsaufnahme	Alexander Piskernik
Das Spiel und die Spielmechanik	Andreas Weiner
Überlegte Spielvarianten	Andreas Weiner
Spielvariante 1 – Das Kartenspiel	Andreas Weiner
Spielvariante 2 – Ein Brettspiel mit Karten und Würfeln	Andreas Weiner
Spielvariante 3 – Die Brettspielvariante mit einem flexibel gestaltbarem Spielbrett, Miniaturen, Würfeln und Karten	Andreas Weiner
Spielvariante 4 – Das Quizspiel	Andreas Weiner
Spielvariante 5 – Das Kartenspiel ergänzt durch Würfel	Andreas Weiner
Die von uns gewählte Spielvariante im Detail	Andreas Weiner
Anleitung zu dem Spiel „Damn IT! – Die verrückte Welt der IT“.	Andreas Weiner
Worum geht es bei dem Spiel?	Andreas Weiner
Empfohlenes Alter	Andreas Weiner
Voraussichtliche Spiellänge	Andreas Weiner
Mögliche Spieleranzahl	Andreas Weiner
Inhalt des Spiels	Andreas Weiner
Das Spielbrett	Andreas Weiner

Die Punkteleiste	Andreas Weiner
Spielaufbau	Andreas Weiner & Alexander Piskernik
Spielablauf	Andreas Weiner & Alexander Piskernik
Ein Spielzug folgt folgendem Schema	Andreas Weiner & Alexander Piskernik
Es gibt folgende Möglichkeiten an Punkte zu kommen	Andreas Weiner
Die Spielfelder und darauf mögliche Aktionen	Andreas Weiner & Alexander Piskernik
Ein Feld auf dem bereits andere Mitspieler stehen	Andreas Weiner
Die Angriffsaktion	Andreas Weiner
Die Verteidigungsaktion	Andreas Weiner
Karten im Spiel	Andreas Weiner
Angriffskarten	Andreas Weiner
Verteidigungskarten	Andreas Weiner
Ereigniskarten	Andreas Weiner
negative Ereignisse	Andreas Weiner
positive Ereignisse	Andreas Weiner
Zufallsereignisse	Andreas Weiner
Graphische Umsetzung Spielbrett und Karten	Alexander Piskernik & Andreas Weiner
Arbeitsaufteilung	Alexander Piskernik & Andreas Weiner
Resümee	Andreas Weiner
Literaturverzeichnis	Alexander Piskernik
Appendix - Spielanleitung	Andreas Weiner & Alexander Piskernik

RESÜMEE

Viele Gefahren lauern im IT-Bereich, aber es gibt auch genug Maßnahmen, mit denen man sich vor diesen schützen kann. Für viele davon muss man kein IT-Experte sein um sie umsetzen zu können.



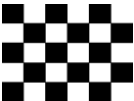


Wir hoffen mit dem von uns gestaltetem Spiel dazu beitragen zu können, dass viele Nutzer sich dieser Gefahren bewusst werden und auch ein paar Maßnahmen kennenlernen, mit denen sie diesen begegnen können, denn gerade im IT-Bereich ist der Spruch „Unwissenheit ist ein Segen“ fehl am Platz.





LITERATURVERZEICHNIS

WISSENSCHAFTLICHE QUELLEN

- ¹ http://de.wikipedia.org/wiki/E-Learning#Formen_des_E-Learning, 23.4.09
- ² <http://secondlife.com>, 23.4.09
- ³ <http://www.e-learning3d.de/>, 23.4.09
- ⁴ http://de.wikipedia.org/wiki/Handlungsorientierter_Unterricht, 23.4.09
- ⁵ <http://isc.sans.org/survivaltime.HTML>, 3.7.09
- ⁶ <http://www.amazon.de/>, ASIN (=eindeutige Produktbezeichnung): B000R9UVHQ, 20.6.09
- ⁷ <http://www.parland.de/spiele.HTML>, 20.6.09
- ⁸ <http://www.huchandfriends.de/page/de/Die-Spiele/Spiele-Detail.php?oid=65>, 20.6.09
- ⁹ <http://www.herz-spiele.de/25.html>, 20.6.09
- ¹⁰ https://www.bsi.bund.de/cln_136/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/inhalt_node.HTML, 23.4.09
- ¹¹ <https://www.bsi.bund.de>, 23.4.09

QUELLEN DER GRAFIKEN FÜRS SPIELBRETT

- | | | |
|------|---|---|
| S001 |  | http://www.tallemu.com/ , 16.8.09 |
| S002 |  | http://2.bp.blogspot.com/_2BDMdp9MIIM/SeeWjzINYQI/AAAAAAAAA0M/ZWIoRoPJxfs/s320/finish_flag.png , 16.8.09 |
| S003 |  | http://www.flags-and-anthems.com/media/flags/flag-start-finish-checkered-flag.gif , 16.8.09 |
| S004 |  | http://www.fotosearch.de/bthumb/IMZ/IMZ001/jba0708.jpg , 16.8.09 |
| S005 |  | http://www.quizilla.com/user_images/Q/QU/QUI/QUIZILLAQUIZZERRR200/1247333595_7962_full.jpeg , 16.8.09 |

- S006  <http://www.jerseyhotheadz.com/Images/new-skull-11.png>, 16.8.09
- S007  <http://www.duperman.de/dupi/pics/91-Speed-Dupi.jpe>, 16.8.09
- S008  <http://www.elby-designs.com/asm-2/others/asm2-pcb.jpg>, 16.8.09
- S009  <http://members.dokom.net/m.richhardt/images/Startflagge.jpg>, 16.8.09

QUELLEN DER GRAFIKEN FÜR KARTEN

- K0001 http://blog.256bit.org/uploads/blitz_03.jpg, 29.8.09
- K0002 <http://www.n24.de/media/ fotos/bildergalerien/pekinghotelbrand/02-Hotel-feuer2-ap.jpg>, 29.8.09
- K0003 <http://rcspiritualdirection.com/blog/wp-content/uploads/2009/05/desert-tree-sophie-jacobson.jpg>, 29.8.09
- K0004 [http://www.polizeibericht.ch/thumb_uc_19638_w250_Rickenbach_SZ_Einbruch_im_Tschuetschi_\(Archivbild_Einbrecher_Kap_o_Solothurn\).jpg](http://www.polizeibericht.ch/thumb_uc_19638_w250_Rickenbach_SZ_Einbruch_im_Tschuetschi_(Archivbild_Einbrecher_Kap_o_Solothurn).jpg), 29.8.09
- K0005 http://buckeyesecure.osu.edu/pmwiki/uploads/SafeComputing/password_star.jpg, 29.8.09
- K0006 <http://www.cooldesignideasblog.net/wp-content/uploads/2007/10/hamster-paper-shredder.jpg>, 29.8.09
- K0007 http://www.edge10.de/images/NAS400_gr.jpg, 29.8.09
- K0008 http://www.virensan.com/uploads/File/dreamstime_2474124.jpg, 29.8.09
- K0009a <http://www.hitech-blog.com/wp-content/2K008/10/update.png>, 29.8.09
- K0009b <http://www.pioneer.be/images/eur/support/AVIC-HD3I.jpg>, 29.8.09
- K0010a http://www.avm.de/de/Presse/Pressefotos/Fotos/AVM_FRITZBox_Fon_WLAN_7170_und_Stick.jpg, 29.8.09
- K0010b <http://static.howstuffworks.com/gif/lock1.jpg>, 29.8.09
- K0011 http://www.mondolithic.com/wp-content/uploads/2K008/09/sciam_cryptography_final.jpg, 29.8.09
- K0012 <http://www.microsoft.com/library/media/1033/windowsxp/images/using/setup/maintain/67396-delete-key.jpg>, 29.8.09
- K0013 <http://www.martintechnology.com/images/firewall.jpg>, 29.8.09
- K0014 http://www.harrisbuyshouses.com/attachments/Image/Shake_Hands2.jpg, 29.8.09
- K0015 <http://www.haydar-isik.com/pictures/hacker.jpg>, 29.8.09
- K0016 <http://www.nK00b-hackz.de/zello/muster/wallpaper/worms.shot.jpg>, 29.8.09
- K0017 <http://mividaessuegno.files.wordpress.com/2K009/03/light-virus-1.jpg>, 29.8.09
- K0018 <http://www.kbds.at/images/geldtaschendiebstahl.jpg>, 29.8.09
- K0019 <http://billmullins.files.wordpress.com/2K008/06/windowsliverwriterhowfakeroquesoftwareaffectsrealpeople-c293social-engineering4.jpg>, 29.8.09
- K0020 <http://www.ihk-niederbayern.de/typo3temp/pics/c93215621c.jpg>, 29.8.09
- K0021 http://www.n24.de/media/import/dpaserviceline/dpaserviceline_2K0081125_16/17_19648978originallarge-4-3-8K00-134-468-2556-2284.jpg, 29.8.09
- K0022 <http://www.stahnke.dk/gallerifotos/Harddisk2777.jpg>, 29.8.09
- K0023 <http://www.drivenleaders.com/wp-content/uploads/2K008/08/motivation.jpg>, 29.8.09
- K0024 <http://www.successandstyle.ch/Bilder/Schulung.jpg>, 29.8.09
- K0025 <http://repairstemcell.files.wordpress.com/2K009/02/insurance.jpg>, 29.8.09
- K0026 http://fotowettbewerb.hispeed.ch/original/279472/kerzenlicht/kerzenlicht_licht_rot_kerze_schwarz.jpg, 29.8.09
- K0027a <http://www.start-to-web.ch/uploads/pics/tux.jpg>, 29.8.09
- K0027b <http://www.shellium.org/files/pictures/3d-gnu-head.jpg>, 29.8.09

- K0027c http://www.freeware-download.com/blog/wp-content/uploads/2K009/02/firefox_huge-3K00x288.png, 29.8.09
- K0027d <http://www.gimp.org/about/wilber-huge-alpha.png>, 29.8.09
- K0028 <http://www.orchideenvereinkaernten.at/images/virus.jpg>, 29.8.09
- K0029 <http://www.konfabulieren.com/pix/spam.jpg>, 29.8.09
- K0030 http://www.minibild.de/images/data/media/10/Festplatten_Headcrash.jpg, 29.8.09
- K0031 http://barefootrunner.org/reflections/gravity_032909.gif, 29.8.09
- K0032 http://www.datenambulanz.de/u/press_photo/DSCF1904.JPG, 29.8.09
- K0033 <http://www.logo-edv.de/aktuell/belkin-usv-superior.jpg>, 29.8.09
- K0034 <http://bilder.afterbuy.de/images/30812/NMA35K00.jpg>, 29.8.09
- K0035 <http://www.berliner-tresor.de/safe/images/stories/sicherheitstuer.jpg>, 3.9.09
- K0036 <http://tastybooze.com/wp-content/uploads/2K009/04/dumpster-dive-1024x768.jpg>, 3.9.09
- K0037 http://upload.wikimedia.org/wikipedia/commons/e/ee/Kon_trojanski_RB.jpg, 3.9.09
- K0038 <http://www.shapingyouth.org//wp-content/uploads/2K009/01/phishing.jpg>, 3.9.09
- K0039a http://almhaus-saualpe.at/CMS_Almhaus_Saualpe/images/wlan%201.jpg, 3.9.09
- K0039b <http://media.photobucket.com/image/crosshair/mvician/German41.jpg>, 3.9.09
- K0040 <http://www.linke-t-shirts.de/images/cover9K00/DLF61086.jpg>, 3.9.09
- K0041 http://c3rb3r.openwall.net/mdcrack/screenshots/MDCrack-NG_big.jpg, 3.9.09
- K0042 http://trustedadvisor.com/public/image/Oppressive%20Mistrust%20iStock_K00K0006165526Small.jpg, 3.9.09
- K0043 <http://aqua-services.de/cms/upload/schulung.jpg>, 3.9.09
- K0044 <http://images.clipartof.com/small/31033-Clipart-Illustration-Of-A-Man-Calmly-Extinguishing-Flames-With-A-Fire-Extinguisher.jpg>, 3.9.09
- K0045 http://www.sciencepark.at/var/sciencepark/storage/images/media/images/news/wie_stellt_man_ein_gutes_team_zusammen/7669-1-ger-DE/wie_stellt_man_ein_gutes_team_zusammen_imagelarge.jpg, 3.9.09
- K0046 http://re-coded.co.uk/images/Software/raptor8_Encrypted.jpg, 3.9.09
- K0047 http://www.axxom.de/uploads/consulting_orange.jpg, 3.9.09
- K0048 <http://www.charlywerder.ch/Filmmacher/abfall.jpg>, 3.9.09
- K0049 http://blog.steuerberaten.de/privat/wp-content/uploads/2K008/12/verlust-arto-fotolia_9756269_xs.jpg, 3.9.09
- K0050 <http://desireforspiritualgrowth.files.wordpress.com/2K009/06/human-error1.jpg>, 3.9.09
- K0051 <http://blog.tmcnet.com/beyond-voip/judge.jpg>, 3.9.09
- K0052 <http://www.ohanaware.com/weblog/wp-content/uploads/2K009/07/Permissions-Reset-Icon.png>, 3.9.09
- K0053 <http://media.bestofmicro.com/Windows-7-Versionen,U-2-220106-13.jpg>, 3.9.09
- K0054 <http://smallbusinessonlinecommunity.bankofamerica.com/servlet/JiveServlet/download/1078-1514/freelancerimage.JPG>, 3.9.09
- K0055 http://de.structurae.de/files/photos/1610/seagram_building_52_back.jpg, 3.9.09
- K0056 http://www.hauni.com/fileadmin/pics/hauni/company/press_pictures/consulting_rgb_01.jpg, 3.9.09
- K0057 http://press.gophila.com/uploads/photos/990_l.jpg, 3.9.09
- K0058 http://www.telekom-presse.at/Datentransfer_sxc_a.jpg, 3.9.09
- K0059 http://www.s-u-h-steuerberatung.de/Bilder/kooperation_s_und_h_steuerberatungs_gmbh.JPG, 3.9.09
- K0060 <http://iemprogram.com/blog/wp-content/uploads/2K009/07/cubicle.jpg>, 3.9.09

APPENDIX

ANLEITUNG

DAMN IT! DIE VERRÜCKTE WELT DER IT

Der Umgang mit Informationstechnologie (IT) kann einige Gefahren mit sich bringen wie man weiß. Im Spiel Damn IT! gilt es möglichst schnell ein IT-Projekt erfolgreich über die Bühne zu bringen und dies bevor das die Konkurrenz tut. Die Gefahren, die im Umgang mit IT lauern, können diesem Vorhaben so manchen Stein in den Weg legen und auch die Konkurrenz spielt nicht gerade fair. Wer also wird diesen harten Weg bis zur Fertigstellung des IT-Projekts als Erster erfolgreich meistern können?

MÖGLICHE ANZAHL AN MITSPIELERN

2-6

SPIELAUFBAU

Als Erstes wird das Spielbrett so aufgestellt, dass alle Mitspieler es gut erreichen können. Jeder Mitspieler nimmt sich eine Spielfigur und den dazugehörigen, sprich gleichfarbigen, Markierungsstein.

Die Spielfiguren werden dann auf das Startfeld und die Markierungssteine auf die Punkteleiste auf das Feld mit der grünen Fahne (= 0 Punkte) gesetzt.

SPIELKARTEN



Es gibt vier Arten von Spielkarten: die Angriffs/Verteidigungskarten (abgekürzt A/V-Karten, links oben), die Ereigniskarten für negative Ereignisse (rechts oben), die Ereigniskarten für zufällige Ereignisse (links unten) und die Ereigniskarten für positive Ereignisse (rechts unten).

Aus jedem Kartentyp wird ein Stapel gebildet und dieser dann jeweils gut gemischt. Die Karten-Stapel werden dann auf die entsprechenden Positionen am Spielbrett abgelegt. Jeder Spieler bekommt aus dem A/V-Kartenstapel verdeckt fünf Karten. Dies sind die Handkarten des jeweiligen Spielers.

WER FÄNGT AN?

Jetzt wird entschieden welcher Spieler anfangen darf. Dazu würfelt jeder mit dem sechsseitigen Würfel und wer die höchste Augenzahl erreicht, darf anfangen. Sollten mehrere Spieler das höchste Würfelergebnis haben, würfeln diese weiter bis schlussendlich ein Sieger feststeht. Dieser darf dann den ersten Spielzug machen.

DAS SPIELZIEL

Wessen Markierungsstein als erstes 25 Punkte, sprich das Feld mit den beiden Zielflaggen, erreicht, hat das IT-Projekt erfolgreich beendet und ist damit der Sieger.

WIE GESPIELT WIRD

Die Spieler führen in Damn IT! der Reihe nach ihre Spielzüge durch, solange bis ein Spieler das Spielziel erreicht. Der Anfangsspieler macht den ersten Spielzug und nach Beendigung von diesem darf der nächste Spieler im Uhrzeigersinn seinen Spielzug machen und so weiter.

EINEN SPIELZUG DURCHFÜHREN

Bei einem Spielzug würfelt der Spieler zuerst mit dem sechsseitigen Würfel. Dann zieht er die Spielfigur die gewürfelte Zahl an Felder den Weg entlang weiter. Sollte sich dabei der Weg am Spielbrett gabeln hat der Spieler selbst die Wahl welchen Weg er nehmen will. Je nachdem, auf welchem Feld die Spielfigur zu stehen kommt, muss bzw. kann man als Spieler bestimmte Aktionen durchführen. Bei diesen Aktionen kann der Spieler oder auch ein Mitspieler Punkte dazu gewinnen oder verlieren.

GEWINN UND VERLUST VON PUNKTEN

Punkteveränderungen werden vorgenommen indem die Markierungssteine auf der Punkteleiste bei Punktegewinn die entsprechenden Felder vor- bzw. bei Punkteverlust zurückgezogen werden.

Wichtig! Bei Punkteverlust kann man nicht unter 0 Punkte (sprich das Feld mit der grünen Fahne) kommen.

DIE HANDKARTEN

Handkarten sind A/V-Karten, die der Spieler auf der Hand hat und vor den anderen Mitspielern verdeckt hält. Wichtig! Ein Spieler darf nie mehr als 7 A/V-Karten auf der Hand haben. Sollte er nachdem er A/V-Karten abgehoben hat mehr als 7 Kartenauf der Hand haben muss er die überzähligen Karten in den A/V-Kartenstapel zurückmischen. Dabei darf sich der Spieler selbst aussuchen welche A/V-Karten er abgibt.

DIE SPIELFELDER

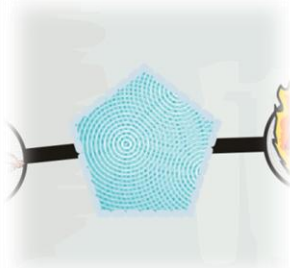
DAS STARTFELD



Ein Spieler, der mit seiner Spielfigur das Startfeld passiert, erhält 8 Punkte. Kommt die Spielfigur des Spielers sogar direkt auf dem Startfeld zu stehen erhält er 10 Punkte.

Das Überqueren des Startfelds repräsentiert das Erreichen eines Meilensteins bei dem IT-Projekt.

DAS „NEUE TECHNOLOGIE“-FELD



Wenn die Spielfigur eines Spielers auf dem Feld „Neue Technologie“ zu stehen kommt, wird bei dem IT-Projekt des Spielers eine neue Technologie eingeführt. Ob sich diese bewährt, nichts bringt oder sogar dem Projekt schadet wird mittels zweier Würfelwürfen entschieden.

Der erste Würfelwurf entscheidet wie stark sich die neue Technologie auswirken wird. Wir nennen das gewürfelte Ergebnis des ersten Wurfs jetzt einmal X.

Der zweite Würfelwurf entscheidet was dann effektiv passiert:

Würfel-ergebnis	Effekt
1	Man verliert „X“ Punkte. (die neue Technologie bringt leider massive Nachteile)
2	Man muss „X“ Felder zurückfahren (die neue Technologie ist leider ein Rückschritt)
3, 4	Kein Effekt (Die Einführung der neuen Technologie wirkt sich nicht auf das IT-Projekt aus)
5	Man fährt „X“ Felder weiter (die neue Technologie bedeutet einen leichten Fortschritt)
6	Man bekommt „X“ Punkte dazu (die neue Technologie bietet massive Vorteile und bringt das IT-Projekt voran)

DIE A/V-FELDER



Wenn die Spielfigur eines Spielers auf diesem Feld zu stehen kommt kann dieser eine A/V-Karte vom A/V-Kartenstapel abheben und seinen Handkarten hinzufügen und einen Angriff auf einen beliebigen Mitspieler starten (mehr dazu bei „Angriff und Verteidigung“).



Wenn die Spielfigur eines Spielers auf diesem Feld zu stehen kommt kann dieser eine A/V-Karte vom A/V-Kartenstapel abheben und seinen Handkarten hinzufügen.

ANGRIFFSAKTION

Ein Angriff auf einen Mitspieler, also der Versuch dessen IT-Projekt> zu sabotieren, ist in folgenden Situationen möglich:

Wenn die Spielfigur eines Spielers auf einem Feld zu stehen kommt, auf dem schon ein oder mehrere Spielfiguren anderer Mitspieler stehen, kann der Spieler einen der Mitspieler angreifen. Zuerst ist aber die normale Aktion auf diesem Feld durchzuführen. Sollte er im Zuge der Aktion von dem Spielfeld wegfahren müssen, kann er keinen Mitspieler dort angreifen.

Ein Angriff auf einen beliebigen Mitspieler ist dann möglich, wenn die eigene Spielfigur auf einem A/V-Feld zu stehen kommt.

Um einen Angriff durchzuführen benötigt der angreifende Spieler eine Angriffs-Karte in den Handkarten. Auf einer Angriffs-karte steht links unten ein Zahlenwert und im Text steht mit welchen Maßnahmen bzw. Verteidigungskarten man sich gegen den Angriff verteidigen kann.

Sollte ein Angriff erfolgreich sein, dann schadet man dem IT-Projekt des angegriffenen Mitspielers. Der Schaden wird dann vom Angreifer ausgewürfelt:

Würfelwurf	verursachter Schaden
1	Nichts passiert
2	-1 Punkt (Minimaler Schaden)
3	-2 Punkte (Mittlerer Schaden)
4	-3 Punkte (Hoher Schaden)
5	-4 Punkte (Sehr hoher Schaden)
6	-5 Punkte (Ein großes Desaster)

Egal ob der Angriff erfolgreich war oder nicht, die Angriffskarte wird danach in den A/V-Kartenstapel gemischt.

VERTEIDIGUNGSAKTION

Ein angegriffener Mitspieler hat die Möglichkeit sich zu verteidigen wenn er zumindest eine Verteidigungskarte in der Hand hält die auf der Angriffskarte als mögliche Gegenmaßnahme steht. Sollte er so eine nicht haben, ist eine Verteidigung gegen den Angriff nicht möglich und der Angriff ist automatisch erfolgreich. Es können auch mehrere verschiedene Verteidigungskarten zur Verteidigung eingesetzt werden.

Die Verteidigung funktioniert wie folgt:

Auf der Angriffskarte steht ein Zahlenwert. Dieser muss mit einem Würfelwurf, zu welchem der Verteidigungswert der Verteidigungskarten addiert wird, überboten werden. Der Verteidigungswert einer Verteidigungskarte ist durch die Anzahl der Schilde links unten angegeben (also entweder 1 oder 2).

Für eine erfolgreiche Verteidigung wird der Verteidiger mit einem Punkt belohnt, da die richtigen Sicherheitsmaßnahmen offenbar rechtzeitig ergriffen worden sind.

Egal ob die Verteidigung erfolgreich war oder nicht, es werden danach alle verwendeten Verteidigungskarten in den A/V-Kartenstapel gemischt.

Ein Angriff auf einen Mitspieler, also der Versuch dessen IT-Projekt zu sabotieren, ist in folgenden Situationen möglich:

Wenn die Spielfigur eines Spielers auf einem Feld zu stehen kommt, auf dem schon ein oder mehrere Spielfiguren anderer Mitspieler stehen, kann der Spieler einen der Mitspieler angreifen. Zuerst ist aber die normale Aktion auf diesem Feld durchzuführen. Sollte er im

Zuge der Aktion von dem Spielfeld wegfahren müssen, kann er keinen Mitspieler dort angreifen.

Ein Angriff auf einen beliebigen Mitspieler ist dann möglich, wenn die eigene Spielfigur auf einem A/V-Feld zu stehen kommt.

Wenn eine Spielfigur auf einem Ereignisfeld zu stehen kommt, muss der jeweilige Spieler eine Karte von dem entsprechendem Ereigniskartenstapel abheben und das Resultat des Ereignisses wird dann ausgewürfelt. Die Auswirkung des Würfelergebnisses steht dann auf der abgehobenen Ereigniskarte. Wenn das Ereignis vorbei ist wird die Ereigniskarte wieder in den entsprechenden Ereigniskartenstapel gemischt.

DIE EREIGNISFELDER

EREIGNISFELDER FÜR NEGATIVE EREIGNISSE



Wenn die Spielfigur eines Mitspielers auf einem Ereignisfeld für schlechte Ereignisse zu stehen kommt, muss dieser eine Karte vom Ereigniskartenstapel für schlechte Ereignisse abheben. Das schlechte Ereignis funktioniert genau wie ein Angriff auf den Spieler.

Sollte dieser Spieler also passende Verteidigungskarten in den Handkarten haben, kann er sich gegen das schlechte Ereignis verteidigen. Sollte die Verteidigung erfolgreich sein werden die eingesetzten Verteidigungskarten in den A/V-Kartenstapel zurück gemischt. Für einen erfolgreich abgewehrten Angriff gibt es hierbei keine Punkte.

Sollte die Verteidigung misslingen oder man sich gegen das Ereignis nicht verteidigen können wird so der verursachte Schaden ausgewürfelt:

Würfelnwurf	verursachter Schaden
1 oder 2	Einmal Aussetzen. Die Behebung des Schadens dauert einfach.
3 oder 4	-1 Punkt (Minimaler Schaden)
5	-2 Punkte (Mittlerer Schaden)
6	-3 Punkte (Hoher Schaden)

Die Ereigniskarte wird anschließend in den Kartenstapel für schlechte Ereignisse zurück gemischt.

EREIGNISFELDER FÜR ZUFÄLLIGE EREIGNISSE



Wenn die Spielfigur eines Mitspielers auf einem Ereignisfeld für zufällige Ereignisse zu stehen kommt, muss dieser eine Karte vom Ereigniskartenstapel für zufällige Ereignisse abheben. Was geschieht wird durch den Text auf der Karte festgelegt.

Wenn das Ereignis vorbei ist wird die Ereigniskarte wieder in den entsprechenden Ereigniskartenstapel gemischt.

EREIGNISFELDER FÜR POSITIVE EREIGNISSE



Wenn die Spielfigur eines Mitspielers auf einem Ereignisfeld für positive Ereignisse zu stehen kommt, muss dieser eine Karte vom Ereigniskartenstapel für positive Ereignisse abheben. Was geschieht wird durch den Text auf der Karte festgelegt.

Wenn das Ereignis vorbei ist wird die Ereigniskarte wieder in den entsprechenden Ereigniskartenstapel gemischt.

Viel Spass beim Spielen!