A Datenschutz und Datensicherheit (Staatlich)

Dieses Kapitel beschäftigt sich mit dem Thema Datenschutz und Datensicherheit aus dem staatlichen Blickwinkel. Dies bedeutet, dass Richtlinien angegeben werden, welche Datenschutz und Datensicherheit aus staatlicher Sicht sichern sollen.

A.1 Absicherung der Kommunikationskanäle (Z07.03)

Unter der Absicherung von Kommunikationskanälen wird in der IT-Sicherheit die Wahrung von sechs unterschiedlichen Schutzzielen verstanden:

A.1.1 Authentizität

Unter Authentizität ist der Nachweis der Identität einer Partei A gegenüber einer Partei B zu verstehen. Hierdurch wird sichergestellt, dass sich eine dritte Partei C nicht fälschlicherweise als Partei A ausgeben kann und somit unberechtigter Weise deren Berechtigungen zum Lesen, Schreiben oder Verändern von Daten nutzen kann.

Eine Authentifizierung kann einseitig oder beidseitig erfolgen. Üblicherweise authentifiziert sich bei der einseitigen Authentifizierung nur der Server gegenüber dem Client und bei der gegenseitigen Authentifizierung zusätzlich der Client gegenüber dem Server. Ob eine ein- oder beidseitige Authentifizierung genutzt werden soll, muss in der Praxis anhand der Sensitivität der ausgetauschten Informationen entschieden werden.

Als Methode zur Authentifizierung ist ein Verfahren zu wählen, welches zum Zeitpunkt der Implementierung mit einem hohen Sicherheitsniveau eingestuft wird. Zum Zeitpunkt der Erstellung dieses Dokuments wäre beispielsweise TLS 1.3 (*Transport Layer Security* o.D.) als solches Verfahren zu nennen. Sollte das Sicherheitsniveau dieses Verfahrens in Zukunft nicht mehr ausreichen, muss laut aktuellem Stand der Technik ein neues Verfahren zur Authentifizierung etabliert werden.

A.1.2 Vertraulichkeit

Unter Vertraulichkeit von Daten wird in der IT-Sicherheit verstanden, dass die enthaltenen Informationen für Außenstehende nicht einsehbar sind. Vertraulichkeit von Daten wird in der Regel durch deren Verschlüsselung erreicht. Mit der Verschlüsselung der Daten werden aus lesbaren Informationen unlesbare Datenblöcke, die es unbefugten Personen unmöglich machen, Informationen aus diesen zu gewinnen.

Die Kommunikation zwischen Server und Client erfolgt in vielen Fällen über einen unsicheren Kanal. Die Kommunikation über einen solchen Kanal birgt hohe Gefahren, da übertragene Daten und Informationen mittels Sniffing (*Sniffer* o.D.) leicht ausgelesen beziehungsweise mitgeschnitten werden können. Um einen solchen Angriff ausschließen zu können, ist es notwendig, die Kommunikation zu verschlüsseln.

Hierzu ist ein Verfahren zu wählen, welches zum Zeitpunkt der Implementierung mit einem hohen Sicherheitsniveau eingestuft wird. Zum Zeitpunkt der Erstellung dieses Dokuments wäre beispielsweise TLS 1.3 (*Transport Layer Security* o.D.) als solches Verfahren zu nennen, um Daten auf dem Transport-Layer zu verschlüsseln. In bestimmten Fällen bspw. bei hochgradig sensitiven (evtl. militärischen) Informationen könnten zukünftig sogar Methoden implementiert werden, welche die übertragenen Daten bereits auf dem Physical-Layer verschlüsseln. Sollte das Sicherheitsniveau des eingesetzten Verfahrens in Zukunft nicht mehr ausreichen, muss laut aktuellem Stand der Technik ein neues Verfahren zur Authentifizierung etabliert werden.

A.1.3 Integrität

Unter Integrität von Daten ist zu verstehen, dass sich diese zum Zeitpunkt des Eintreffens beim Empfänger in einem unmodifizierten Zustand befinden und dass eventuelle Versuche die Daten zu verändern erkannt werden.

Auch hier ist wieder ein Verfahren zu wählen, welches zum Zeitpunkt der Implementierung mit einem hohen Sicherheitsniveau eingestuft wird. Zum Zeitpunkt der Erstellung dieses Dokuments wäre ebenfalls TLS 1.3 (ebd.) als solches Verfahren zu nennen. Sollte das Sicherheitsniveau dieses Verfahrens in Zukunft nicht mehr ausreichen, muss laut aktuellem Stand der Technik ein neues Verfahren zur Authentifizierung etabliert werden.

A.1.4 Verfügbarkeit

Verfügbarkeit im Sinne der IT-Sicherheit bezeichnet die Tatsache, dass die Funktionen eines IT-Systems ständig bzw. innerhalb einer vorgegebenen Zeit, zur Verfügung stehen und die Funktionalität des IT-Systems nicht vorübergehend oder dauerhaft beeinträchtigt ist. In diesem Zusammenhang kann auch die Verfügbarkeit von Informationen bzw. Daten bedeutend sein.

Die Verfügbarkeit ist einerseits durch den betreuenden Systemadministrator, durch entsprechende Verfahren zur Verfügbarkeitssteigerung, sicherzustellen. Hierzu gehören beispielsweise die redundante Auslegung von Servern oder die Verwendung von Loadbalancern.

Andererseits können Baumaßnahmen die Verfügbarkeit von Systemen einschränken. Dies kann bspw. durch das Aufstellen von Funkmasten mit einem entsprechend starken Magnetfeld oder durch die Beschädigung von Leitungen durch Bauarbeiten geschehen. Aufgrund dessen sollte bei der Entscheidung bzgl. Baumaßnahmen ein Mitarbeiter mit entsprechendem Fachwissen beteiligt werden, sodass solchen Problematiken im Vorhinein entgegengewirkt werden kann.

A.1.5 Verbindlichkeit

Verbindlichkeit bedeutet im Kontext der IT-Sicherheit, das sämtliche Aktionen einer Instanz eindeutig zugeordnet und nicht geleugnet werden können.

Mechanismen zum Sicherstellen der Verbindlichkeit sind beispielsweise detaillierte Log-Files. Diese sollten als Mindestanforderung die IP-Adresse, das Zugriffsdatum und die angefragten Dateien enthalten.

A.1.6 Anonymität

Anonymität ist die Geheimhaltung der Identität einer Instanz (wie beispielsweise einer Einzelperson oder einer Gruppe von Akteuren).

Völlige Anonymität wird nur in wenigen Anwendungsfällen benötigt und kann auch nie zu 100% garantiert werden. Der in der Praxis wesentlich öfter anzutreffende Fall ist die Pseudonymisierung durch beispielsweise die Verwendung von Pseudonymen.

Sollte in einem der verwendeten Systeme eine Pseudonymisierung gewünscht sein, so kann diese beispielsweise dadurch erreicht werden, dass sich Nutzer der Applikation eigene Nutzernamen aussuchen können. Sollte tatsächlich eine vollständige Anonymisierung von Nöten sein, so kann beispielsweise über die Verwendung des TOR-Netzwerks nachgedacht werden. Zusätzlich müsste für ein solches System eine Logging-Policy erstellt werden, welche die Protokollierung und Archivierung von Verbindungsnachweisen untersagt.

Allerdings gilt auch hier, dass die Sicherheit des verwendeten Verfahrens regelmäßig verifiziert werden muss und im Ernstfall ein anderes zum aktuellen Stand der Technik als „sicher anonymisierendes“ Verfahren implementiert werden muss.

A.1.7 Fazit - Kommunikationskanäle

Zusammenfassend kann festgehalten werden, dass zum aktuellen Stand der Technik sämtliche Kommunikationskanäle zur Sicherung von Authentizität, Vertraulichkeit und Integrität zumindest mittels TLS 1.3 zu schützen sind. Die Verfügbarkeit ist durch den Administrator des ent-

sprechenden Systems sicherzustellen, die Verbindlichkeit durch das Führen von detaillierten Log-Files. Sollte eine Anonymisierung gewünscht sein, so ist zunächst zwischen einer tatsächlichen oder eine Pseudo-Anonymisierung zu unterscheiden und dann ein entsprechendes Verfahren auszuwählen.

A.2 Richtlinien

Im Folgenden werden anhand der definierten Zielsetzungen Richtlinien erstellt, welche die Sicherung von Datenschutz und Datensicherheit im staatlichen Kontext fördern. Die Definition der Richtlinien basiert dabei auf den in der Praxis bewährten Standards ISO27000-Reihe (siehe *ISO-27000-Reihe* o.D.), BSI-Grundschutz (siehe *BSI-Grundschutz* o.D.) und Datenschutz-Grundverordnung (siehe *Datenschutz Grundverordnung* o.D.).

A.2.1 Richtlinien zu Datenfreigabe und Datenweitergabe an Förderer der Projekte (Z07.01) - basierend auf BSI-Grundschutz M4.64

Sollte das Projekt von externen Quellen gefördert werden, so ist es zwingend notwendig, diese entsprechend zu prüfen. Externe Quellen fördern Projekte in der Regel nicht aus Nächstenliebe sondern verfolgen oft eigene Ziele, welche konträr zur eigentlichen Intention des Projekts stehen können.

Aufgrund dessen sollten potentielle Förderer, die ein berechtigtes Interesse an der Sammlung von Daten über jugendliche Mitbürger aufweisen kategorisch ausgeschlossen werden. Ebenso sollte unabhängig von der in Aussicht gestellten Summe, ein Ausschluss von potentiellen Förderern erfolgen, deren Sitz in Ländern mit fraglichen Datenschutzbestimmungen liegt.

Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen Vor der Weitergabe von Dateien an externe Partner, unabhängig von der Art der Weitergabe (bspw. E-Mail, Datenträgeraustausch, Veröffentlichung auf einem Webserver) sollten diese dahingehend überprüft werden, ob sie Restinformationen enthalten, die nicht zur Veröffentlichung bestimmt sind. Hiermit soll sichergestellt werden, dass nur die tatsächlich benötigten Informationen weiter gegeben werden.

Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich sind auch die Aktionen, welche dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standard-Software wie z. B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen des Benutzers gespeichert. Hierzu gehören bspw. Kommentare in Word, welche durch das Ändern der Schriftfarbe auf „weiß“ unsichtbar erscheinen oder gefaltete und somit ausgeblendete Zeilen und Spalten in Excel-Dokumenten.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, welcher zur Erstellung der Datei verwendet wurde.

Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr. Um Restinformationen zu beseitigen, kann die Datei in einem anderen Dateiformat abgespeichert werden, z. B. als „Nur-Text“ oder als „HTML“ , können die Nutzdaten in eine zweite Instanz derselben Standard-Software kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte.

Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie. Um der Weitergabe von Informationen vorzubeugen, die ursprünglich mit Wissen der Ersteller eingebracht worden sind, wie z. B. als „verborgen“ formatierter Text, dessen Vorhandensein dann aber vergessen wurde, kann es sinnvoll sein, die Datei ausdrucken. Dabei sollten dann alle Optionen aktiviert werden, die beim Drucken versteckte Informationen ausgeben. Hierzu gehören bspw. der in Word unter „Ansicht“ befindliche Punkt „Kommentare in Ihrem Dokument anzeigen“.

Restinformationen/Slack-Bytes Beim Datenträgeraustausch kann sogenannter Slack-Space ein Problem darstellen. Jedes Betriebssystem hat eine kleinste physikalische Speichereinheit mit festgelegter Größe. Unter DOS ist dies ein Sektor und umfasst 512 Byte. Bei Unix-Systemen ist dies ein Block, die Größe eines Blocks hängt dabei von der eingesetzten Unix-Variante ab. Unter DOS werden die einzelnen Sektoren einer Partition logisch zu Zuordnungseinheiten (Cluster) zusammengefasst. Wie viele Sektoren einen Cluster bilden, hängt von der Größe der Partition ab. Wird eine Datei geöffnet, werden ihr ein oder mehrere Cluster zugeordnet.

Die letzte Zuordnungseinheit wird dabei nicht vollständig benutzt, wenn die Dateigröße der zu

speichernden Datei nicht zufällig ein Vielfaches der Clustergröße ist.

Dies verbraucht Speicherplatz. Der durchschnittliche Speicherplatzverbrauch hierdurch steigt mit der Clustergröße. Deshalb sollte die Clustergröße bei der Erstellung von Partitionen nicht zu groß wählt werden. Da die benötigte Clustergröße einer Partition von ihrer Verwendung abhängt (bspw. Primäre OS Partition, Datenspeicher für kleine/große Daten, etc.), wird an dieser Stelle auf eine explizite Größenempfehlung verzichtet. Es sei aber darauf hingewiesen, dass die Wahl der Clustergröße von der voraussichtlichen Größe der auf der Partition zu speichernden Daten abhängig sein sollte.

Ein anderes Problem hierbei ist, dass (bei DOS-basierten Betriebssystemen) die restlichen Bytes des letzten Clusters bzw. Blocks mit zufällig im Hauptspeicher stehenden Bytes aufgefüllt werden, sogenannten Slack-Bytes. Diese können sinnlose Einträge, Informationen über die Dateistruktur, aber auch Passwörter enthalten. Auch bei einem Kopiervorgang von einem Datenträger auf den anderen kann die Datei je nach Clustergröße mit Slack-Bytes aufgefüllt werden.

Vor der Weitergabe von Dateien sollte sichergestellt werden, dass diese keine Slack-Bytes mehr enthalten. Dies kann mit Hilfe eines geeigneten Editors (z. B. Hex-Editor) überprüft werden. Sollten dabei Slack-Bytes gefunden werden, so sind diese zu überschreiben.

Daneben haben viele Windows-Applikationen das Problem, dass das jeweilige Programm bei der Bearbeitung einer Datei den in Anspruch genommenen Speicherplatz nicht durchgehend mit Applikationsdaten überschreibt, sondern dass Lücken entstehen können, die ebenfalls alte Datenbestände des IT-Systems enthalten. Deshalb sollte das Betriebssystem regelmäßig und automatisiert von Junk-Files, temporäre Dateien, nicht mehr benötigte Log-Files, etc. befreit werden.

Verborgener Text / Kommentare Eine Datei kann Textpassagen enthalten, die als "versteckt" oder "verborgen" formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche **Zusatzinformationen gelöscht** werden. Besonders gefährlich sind beispielsweise Excel-Dateien, die gefaltete Spalten enthalten, in denen sich oftmals Zusatzinformationen befinden, die nicht für den Empfänger bestimmt sind. Ein Formatwechsel kann hier hilfreich sein.

Änderungsmarkierungen Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten. Falls dem so ist, müssen diese **Änderungsmarkierungen gelöscht** werden.

Versionsführung In praktisch allen aktuellen Office-Suites gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in einer Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu sehr großen Dateien führen, z. B. wenn Graphiken mitgeführt werden. **Auf keinen Fall sollte die Option "Version beim Schließen automatisch speichern"** gewählt werden, da hier bei jedem Schließen einer Datei die komplette Vorgängerversion zusätzlich gespeichert wird.

Dateieigenschaften Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wieder zu finden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter (nicht nur der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den Bearbeiter beeinflusst werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält. Gegebenenfalls sind die entsprechenden Dateien dann vor der Weitergabe zu bearbeiten.

Schnellspeicherung Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.

Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor eine weitere Anwendung ausgeführt wird, die viel Speicherplatz in Anspruch nimmt,

- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

Die Einhaltung dieser Richtlinien sollte in regelmäßigen Abständen durch den Datenschutzbeauftragten stichprobenartig geprüft werden. Sollte hierbei eine nicht unerhebliche Menge an Verstößen festgestellt werden, so sollten nochmals Schulungen stattfinden, in denen die Arbeitnehmer auf die Wichtigkeit der erstellten Richtlinien hingewiesen und deren Zweck erläutert wird.

A.2.2 Richtlinien zur Organisation des Patchmanagements (Z07.04) - basierend auf BSI-Grundschutz B1.14

Patchmanagement umfasst drei Teilaspekte für die jeweils einzeln Richtlinien erstellt werden müssen.

Informationsbeschaffung über Sicherheitslücken der Systeme Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen werden. Sicherheitsrelevante Updates oder Patches für die eingesetzte Hard- und Software müssen gegebenenfalls installiert werden. Sind keine entsprechenden Updates oder Patches verfügbar, so muss eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden. Es ist daher sehr wichtig, dass sich die Systemadministratoren regelmäßig über neu bekannt gewordene Schwachstellen informieren. Informationsquellen zu diesem Thema sind beispielsweise:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI)
  (siehe http://www.bsi.bund.de/)
- Hersteller bzw. Distributoren von Programmen und Betriebssystemen. Diese informieren oft registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.
- Computer Emergency Response Teams (CERT s).
  Dies sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten Advisories über aktuelle Schwachstellen in Hard-

und Softwareprodukten und geben Empfehlungen zu deren Behebung. Verschiedene Organisationen oder Verbände unterhalten eigene CERTs. Das ursprüngliche CERT der Carnegie Mellon Universität diente als Vorbild für viele weitere derartige Teams und ist heute eine Art "Dach-CERT": Computer Emergency Response Team / Coordination Center (CERT/ CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, Telefon: +1-412-268-7090 (24-Stunden-Hotline), E-Mail: cert@cert.org, WWW : http://www.cert.org Die CERT-Mitteilungen werden in Newsgruppen (comp.security.announce und info.nsfnet.cert) und über Mailinglisten (Aufnahme durch E-Mail an: cert-advisory-request@cert.org) veröffentlicht. In Deutschland existieren unter anderem folgende CERTs:

- CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn, Telefon: 0228 99-9582-222, Fax: 022899-9582-5427, E-Mail: certbund@bsi.bund.de, WWW: https://www.bsi.bund.de/certbund/
- DFN-CERT, Zentrum für sichere Netzdienste GmbH, DFN-CERT, DFN-CERT Services GmbH, Sachsenstraße 5, D-20097 Hamburg, Telefon: 040-808077-555, Fax: -556, E-Mail: info@dfn-cert.de, WWW: http://www.dfn-cert.de.
- An verschiedenen Hochschulen existieren CERTs, die auch Informationen öffentlich zur Verfügung stellen. Ein Beispiel ist das RUS-CERT der Universität Stuttgart (siehe http://cert.uni-stuttgart.de).
- Hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen oder Mailinglisten. In solchen Foren werden Hinweise auf existierende oder vermutete Sicherheitslücken oder Fehler in diversen Betriebssystemen und sonstigen Softwareprodukten diskutiert. Besonders aktuell sind meist die englischsprachigen Mailinglisten wie Bugtraq, von denen es an vielen Stellen öffentlich zugängliche Archive gibt, beispielsweise unter
  http://www.securityfocus.com.

- Manche IT -Fachzeitschriften veröffentlichen ebenfalls regelmäßig Beiträge mit einer Übersicht über neue Sicherheitslücken in verschiedenen Produkten. Idealerweise sollten sich

die Administratoren und der IT-Sicherheitsbeauftragte bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine „unabhängige" Informationsquelle zu benutzen. Die Administratoren sollten jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein

bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, muss rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann. Hierzu muss der Datenschutzbeauftragte durch den zuständigen Administrator benachrichtigt werden, um in gegenseitiger Abstimmung eine Lösung zu erarbeiten.

Sicherstellung der Integrität und Authentizität von Softwarepaketen bzw. Patches
Durch unvorsichtiges Ausführen von Programmen, die aus „unsicheren" Quellen stammen, kann beträchtlicher Schaden entstehen. Schadsoftware (so genannte Malware) kann beispielsweise Programme zum Ausspähen von Passwörtern, Trojanische Pferde oder Backdoors auf einem Computer installieren, oder ganz einfach Daten beschädigen oder löschen.

Typische Quellen für solche Schadsoftware sind beispielsweise Programme, die sich als Bildschirmschoner, Virenscanner oder sonstige Hilfsprogramme ausgeben, und per E-Mail unter gefälschten Absenderadressen an sehr viele Empfänger verschickt werden. Oft laden auch unvorsichtige Anwender die Programme aus dem Internet herunter und installieren sie ohne Überprüfung.

Zwei Beispiele, bei denen durch die Überprüfung vorhandener digitaler Signaturen Schaden

hätte vermieden werden können, sind ein Vorfall vom März 2002, bei dem die Distribution des Pakets OpenSSH auf dem ftp-Server des OpenSSH-Projekts manipuliert wurde, und ein ähnlicher Vorfall vom September 2002, bei dem dies mit der Distribution des Mailservers sendmail geschah. In beiden Fällen wurden in die Distributionen Trojanische Pferde eingeschleust, die zu einer Kompromittierung des Rechners führen konnten, auf dem die Pakete kompiliert wurden. **In beiden Fällen hätte eine Überprüfung der vorhandenen digitalen Signaturen die Manipulation aufdecken können.**

Selbst wenn ansonsten keine Verschlüsselungs- oder Signaturtechniken zum Einsatz kommen, sollte die Nutzung in dem Umfang, wie er in dieser Maßnahme beschrieben wird, in Erwägung gezogen werden.

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Dies gilt besonders für Updates oder Patches, die normalerweise nicht mehr auf Datenträgern ausgeliefert werden. Die meisten Hersteller und Distributoren bieten zu diesem

Zweck Prüfsummen an, die zumindest eine Prüfung der Integrität eines Paketes erlauben. Die Prüfsummen werden dabei meist auf den Webseiten der Hersteller veröffentlicht oder auch per E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren, wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeugten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese vor der Installation des Paketes überprüft werden. Hierzu muss von dem heruntergeladenen Software-Paket mit Hilfe eines Tools wie bspw. HashMyFiles (siehe *Prüfsummen berechnen und vergleichen* o.D.) die entsprechende Prüfsumme berechnet und mit der vom Hersteller bereitgestellten Prüfsumme verglichen werden.

Eine Überprüfung der Authentizität kann mit Prüfsummen jedoch nicht erfolgen. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von Public-Key-Servern verfügbar. Häufig werden die Prüfsummen mit einem der Programme PGP oder GnuPG erzeugt.

Ergibt die Prüfung, dass es sich um eine gültige Signatur des jeweiligen Herstellers handelt, so resultiert daraus ein deutlich höherer Grad an Vertrauenswürdigkeit für das Paket, als lediglich durch das Vorhandensein einer Prüfsumme.

Das bei Linux-Distributionen verbreitete Paketverwaltungssystem RPM (Redhat Package Manager) hat ebenso wie das Paketverwaltungssystem der Debian-Distribution bereits eine integrierte Überprüfungsfunktionalität.

Manchmal führen selbst die eingebauten Software-Updatemechanismen des jeweiligen Betriebssystems oder der Anwendungssoftware keine Prüfsummenvergleiche durch. Wenn möglich, sollte allerdings bei jedem Softwarepaket vor dem Einspielen ein Prüfsummencheck durchgeführt werden.

Ferner sind nicht alle Prüfsummenvergleiche ohne Mitwirkung der Anwender durchführbar, da die hierfür erforderlichen Checksummen, Signaturen oder Zertifikate von den Herstellern nicht auf eine einheitliche Weise bereitgestellt werden. Daher ist häufig eine manuelle Verifikation auf den Herstellerseiten oder die Anpassung der URLs in der Patch- und Änderungssoftware nötig.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall vor

der Installation des Pakets überprüft werden.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der öffentliche Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit dem entsprechenden privaten Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einer CD-ROM des Herstellers, von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public Key Server.

Zur Überprüfung von Prüfsummen und digitalen Signaturen müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein. Außerdem müssen die Administratoren genügend Zeit haben, die entsprechenden Programme im Arbeitsalltag einzusetzen und sich mit der Bedienung vertraut zu machen.

Von einem Bezug von Patches und Änderungen per E-Mail ist aus verschiedenen Gründen abzuraten. Die Herkunft von E-Mails ist ohne Einsatz zusätzlicher Sicherheitsmechanismen schwer festzustellen und die Empfängeradressen in den Institutionen sind oft Verteilerlisten, deren Adresse leicht zu erraten ist. Patches und Änderungen können außerdem mittlerweile sehr umfangreich sein. Viele Unternehmen und Behörden haben die Größe von E-Mail-Anhängen beschränkt und verbieten unter Umständen zudem die Annahme ausführbarer Anhänge. Ferner werden durch die großen Datenmengen die E-Mail-Systeme unnötig belastet. Daher kann eine rechtzeitige Verfügbarkeit der Software-Änderungen, welche besonders bei Sicherheitspatches kritisch sein kann, via E-Mail nicht ausreichend gewährleistet werden.

Des Weiteren bieten einige Hersteller an, Änderungen und Patches dem Kunden direkt auf Datenträgern zuzusenden. Auch in diesem Fall sollten die Patches und Änderungen möglichst anhand von Prüfsummen oder digitalen Signaturen verifiziert werden, denn Absender-Angaben auf Postsendungen und Hersteller-Logos auf CD s und DVDs lassen sich leicht fälschen.

Ein weiterer Aspekt zur Prüfung der Echtheit der Aktualisierung können vom Hersteller veröffentlichte Nachrichten auf seiner Webseite, per Newsletter oder über ähnliche Kanäle sein. Einige Hersteller haben Zyklen und Zeitpunkte etabliert, zu denen in der Regel systematisch Informationen über Änderungen veröffentlicht werden.

Dokumentation der Veränderungen an den bestehenden Systemen Um einen reibungslosen Betriebsablauf zu gewährleisten, muss der Administrator einen Überblick über das System haben bzw. sich verschaffen können. Dieses muss auch für seinen Vertreter möglich sein, falls der Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um

Prüfungen des Systems (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können.

Daher sollten die Veränderungen, die Administratoren (unabhängig davon, ob es sich bei diesen um Mitarbeiter oder externe Techniker handelt) am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.

Bei **Installation neuer Betriebssysteme** oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.

Unter Unix müssen ausführbare Dateien, auf die auch andere Benutzer als der Eigentümer Zugriff haben oder deren Eigentümer root ist, vom Systemadministrator freigegeben und dokumentiert werden. Insbesondere müssen Listen mit den freigegebenen Versionen dieser Dateien geführt werden, die außerdem mindestens das Erstellungsdatum, die Größe jeder Datei und Angaben über evtl. gesetzte s-Bits enthalten. Sie sind Voraussetzung für den regelmäßigen Sicherheitscheck und für Überprüfungen nach einem Verlust der Integrität.

Fazit Patchmanagement Zusammenfassend kann für das Patchmanagement festgehalten werden, dass eine regelmäßige Prüfung auf Informationen zu neuen Sicherheitslücken- und Patches anhand von mindestens zwei verschiedenen Quellen durchzuführen ist. Vor der Installation eines Patches ist dessen Authentizität zu prüfen. Außerdem muss nach erfolgter Installation eine Dokumentation der Änderung erfolgen.

A.2.3 Richtlinien zur Wartung von Soft- und Hardware (Z07.04) - basierend auf BSI-Grundschutz M2.4

Als Maßnahmen vor und nach Wartungs- und Reparaturarbeiten sind durch den betreffenden Abteilungsleiter in Abstimmung mit der IT-Abteilung folgende Punkte einzuplanen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.

- Wartungstechniker müssen sich auf Verlangen ausweisen.

- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.

- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.

- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach „Eindringtiefe" des Wartungspersonals, Passwortänderungen erforderlich. Im PC-Bereich sollte ein Computer-Viren-Check durchgeführt werden.

- Nach den Wartungsarbeiten sollten die Geräte mit einem aktuellen Computer-Viren-Schutz-programm auf Schadsoftware überprüft werden.

- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).

- Beauftragte Firmen sollten schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien (z. B. Brandschutz, VdS 2008 Schweiß-, Löt- und Trennschleifarbeiten) beachten. Dies gilt für alle Tätigkeiten, bei denen eine direkte oder indirekte Gefahr für Gebäude oder Menschen entstehen können. Letztlich kommt es darauf an, dass das vor Ort eingesetzte Personal mit diesen Regeln vertraut ist.

- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

A.2.4 Richtlinien zur Vergabe von sicheren Passwörtern (Z07.05)

Im Wandel der Zeit, werden immer leistungsstärkere Computer hergestellt, wodurch diese immer mehr Rechenoperationen ausführen können. Dementsprechend fällt es immer leichter Passwörter zu knacken. Aus diesem Grund müssen immer wieder zeitliche Empfehlungen sowie Komplexitätsempfehlungen an Passwörter aktualisiert werden.

Zeitliche Empfehlungen Aktuelle zeitliche Empfehlungen bezüglich Passwörtern sind Tabelle 36 zu entnehmen.

Windows NT	Windows 2000/XP/2003	Ab Windows Vista und Server 2008	Mindestempfehlung
Maximales Kennwortalter	Maximales Kennwortalter	Maximales Kennwortalter	90 Tage
Minimales Kennwortalter	Minimales Kennwortalter	Minimales Kennwortalter	1 Tag
Minimale Kennwortlänge	Minimale Kennwortlänge	Minimale Kennwortlänge	8 Zeichen
Kennwortzyklus	Kennwortchronik erzwingen	Kennwortchronik erzwingen	3 Versuchen
Konto sperren | Konto zurücksetzen nach	Zurücksetzungsdauer des Kontosperrungszählers	Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten
Dauer der Sperrung	Kontosperrdauer	Kontosperrdauer	60 Minuten
Benutzer muss sich anmelden, um Kennwort zu ändern	n/v	n/v	Deaktiviert
n/v	Kennwort muss Komplexitäts-voraussetzungen entsprechen	Kennwort muss Komplexitäts-voraussetzungen entsprechen	Aktiviert
n/v	Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert

Abbildung 36: Zeitliche Empfehlungen (Quelle: *Zeitliche Empfehlungen für Passwörter* o.D.)

Empfehlungen zur Komplexität Die folgenden Empfehlungen zur Komplexität von Passwörtern basieren auf Empfehlungen des BSI (siehe *Passwörter* o.D.):

Bei der Wahl eines Passwortes sind Ihrer Kreativität keine Grenzen gesetzt. Wichtig ist, dass Sie sich das Passwort gut merken können. Hierfür gibt es unterschiedliche Hilfsstrategien: Der eine merkt sich einen Satz und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man unter Umständen noch bestimmte Buch-

staben in Zahlen oder Sonderzeichen. Die andere nutzt einen ganzen Satz als Passwort oder reiht unterschiedliche Wörter, verbunden durch Sonderzeichen, aneinander.

Grundsätzlich gilt: Je länger, desto besser. Ein gutes Passwort sollte mindestens acht Zeichen lang sein. (Ausnahme: Bei Verschlüsselungsverfahren für WLAN wie zum Beispiel WPA und WPA2 sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren - das geht zum Beispiel beim Hacken von Online-Accounts nicht.)

Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, beispielsweise Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+?). Manche Anbieter von Onlinediensten machen technische Vorgaben für die verwendbaren bzw. zu verwendenden Zeichen. Wenn Ihr System Umlaute zulässt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese eventuell nicht eingegeben werden können.

Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter. Das vollständige Passwort sollte möglichst nicht in Wörterbüchern vorkommen. Es sollte zudem nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie äsdfghöder ”1234abcd”bestehen. Manche Anbieter gleichen Passwörter gegen eine sogenannte ”black listäb, in der genau solche nicht geeigneten Passwörter hinterlegt sind. Möchte man sie nutzen, erhält man einen Hinweis, dass das Passwort in dieser Form nicht zugelassen wird bzw. nicht sicher ist.

Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist nicht empfehlenswert.

Wichtige Passwörter sollten in regelmäßigen Abständen geändert werden. Warum, erklären wir unter Umgang mit Passwörtern.

Nutzen Sie einen Passwortmanager, um Ihre unterschiedlichen Passwörter gut verwalten zu können.

Um auch bei Krankheits- oder Todesfällen auf sämtliche geschäftlichen Daten zugreifen zu können, sollte die IT-Abteilung die Möglichkeit haben, Passwörter im Notfall zurückzusetzen. Ein solches Vorgehen ist allerdings zwingend zu dokumentieren.

Fazit Richtlinien zu Passwörtern Zusammenfassend kann festgehalten werden, dass Passwörter den vorgegebenen zeitlichen und Komplexitäts- Anforderungen entsprechen müssen. Die Anforderungen sind regelmäßig auf ihre Aktualität zu prüfen und gegebenenfalls zu aktualisieren.

A.2.5 Richtlinien zur Speicherung erhobener Benutzerdaten (Z07.06) - basierend auf DSGVO Kapitel 3

Um konform mit der DSGVO zu sein, sind bei der Speicherung und Verarbeitung von personenbezogenen Daten mehrere Grundsätze zu beachten:

- Rechtmäßigkeit der Verarbeitung und Bedingungen für die Einwilligung: Betroffene müssen ihre Einwilligung zur Verarbeitung der betreffenden personenbezogenen Daten für den entsprechenden Zweck erteilen. Hierzu ist es notwendig, ein entsprechendes Formular zu entwerfen, welches von jedem Beteiligten unterzeichnet bzw. nachvollziehbar bestätigt werden muss, bevor Daten erhoben werden (DSGVO Art. 6.1.a).
- Der Verantwortliche muss in der Lage sein, dieses Formular auf Verlangen vorzuzeigen und somit nachzuweisen, dass die entsprechende Person der Verarbeitung und Speicherung von personenbezogenen Daten zugestimmt hat (DSGVO Art. 7.1).
- Außerdem ist sicherzustellen, dass die zustimmende Person entweder das 16te Lebensjahr vollendet hat oder die Zustimmung durch einen Träger elterlicher Verantwortung erfolgt (DSGVO Art. 8)

Des Weiteren ist sicherzustellen, dass die folgenden Rechte der betroffenen Personen gewahrt bleiben:

Recht auf Auskunft der personenbezogenen Daten (DSGVO - Art. 15)

- Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:
  - die Verarbeitungszwecke;
  - die Kategorien personenbezogener Daten, die verarbeitet werden;

- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

- Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

- Die IT-Abteilung stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, für die betroffene Person zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

- Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Recht auf Berichtigung und Löschung (DSGVO - Art. 16,17)

- Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. 2Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung ? zu verlangen.

- Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

  - Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

  - Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

  - Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

  - Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

  - Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

  - Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

- Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Recht auf Widerspruch (DSGVO - Art. 21)

- Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und

Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

- Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

- Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

- Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

- Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

- Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Zum Einreichen eines Widerspruchs werden von verschiedenen Institutionen, wie bspw. der Verbraucherzentrale Musterbriefe angeboten (siehe *Musterbriefe zum Thema Digitale Welt* o.D.).

A.3 Richtlinien zur Absicherung von privaten und digitalen Geräten (Z07.07)

Auf den Einsatz privater Geräte sollte im betrieblichen Kontext soweit möglich verzichtet wer-

den, da diese ein schwer kalkulierbares Sicherheitsrisiko darstellen. Sollte auf den Einsatz solcher

Geräte allerdings nicht verzichtet werden können, so sind diese entsprechend der Richtlinien aus Kapitel „Datenschutz und Datensicherheit (Bürgerlich)“ abzusichern. Die Erfüllung dieser Richtlinien ist von der IT-Abteilung zu prüfen und muss die folgenden Punkte umfassen:

- Ausführungskontrolle
- Virenschutz
- personal Firewall
- Benutzerverwaltung
- Logging

A.4 Minimierung der Angriffsfläche (Z07.08)

Cyber-Kriminalität hat viele Gesichter. Das Klischee des einsamen Hackers, welcher unter diabolischen Gelächter Terminals mit giftgrünen Kommandos füllt, ist in der heutigen Zeit längst überholt. Cyber-Kriminelle finden sich in sämtlichen sozialen Schichten, haben unterschiedliche technische Kenntnisse und verfügen über verschiedene Ressourcen. Die von einem Angreifer potentiell durchführbaren Angriffe sind an die Ausprägung dieser Attribute gekoppelt. So haben beispielsweise Geheimdienste andere technische Möglichkeiten als die Nachbarskinder, welche sich in dubiosen Foren Kenntnisse zu Wireshark angelesen haben. Hieraus lässt sich folgern, dass Angreifer anhand von Attributen klassifizierbar sind, wodurch es Sicherheitsanalysten möglich ist Angreifermodelle zu definieren, diesen passende Angriffsschemata zuzuweisen und somit potentielle Bedrohungen zu identifizieren.

Im Folgenden wurde beispielhaft eine solche Betrachtung durchgeführt und entsprechende Angreifermodelle definiert. Diese Angreifermodelle können in Zukunft genutzt werden, um für jedes System potentielle Angriffe zu identifizieren und auf Basis der Angreifermodelle anhand einer qualitativen Risikoanalyse Risiken zu priorisieren, den Umgang mit diesen Risiken zu definieren und diese durch entsprechende Gegenmaßnahmen zu minimieren.

A.4.1 Definition der Angreifermodelle

Zur Klassifizierung der Angreifer müssen zunächst Attribute definiert werden. Hierzu wurden im ersten Schritt vier Attribut-Kategorien identifiziert:

- Rolle

- Verhalten

- Rechenkapazität
- technische Vorkenntnisse

Rolle

Das Attribut "Rolle" definiert in diesem Kontext, über welchen spezifischen Background der potentielle Angreifer verfügt. So kann ein Cyber-Krimineller in diesem Modell folgende Rollen annehmen:

- Außenstehender
- User
- Server-Hoster
- Entwickler

Verhalten

Das Attribut "Verhalten" klassifiziert das Vorgehen des potentiellen Angreifers. So kann der Angreifer entweder "passiv/beobachtend" vorgehen, was bedeutet, dass nur Daten gelesen werden, ohne dass eine Manipulation dieser Daten erfolgt. Des Weiteren könnte der Angreifer "aktiv/beobachtend" vorgehen, was bedeutet, dass dieser zwar keine Daten manipuliert, aber versucht, die gelesenen Daten zu entschlüsseln. Schlussendlich könnte der Angreifer auch "aktiv/-verändernd" operieren, was eine bewusste Manipulation von Daten bedeuten würde.

Rechenleistung

Das Attribut "Rechenleistung"definiert, ob der Angreifer nur einen privaten Rechner zur Durchführung des Angriffs verwendet oder ob Großrechner bzw. Botnets zum Einsatz kommen.

Technische Vorkenntnisse

Das letzte Attribut definiert die technischen „Vorkenntnisse" des potentiellen Angreifers im Bezug auf die angegriffene Ressource. "Keine" bedeutet hier, dass der Angreifer über keine Vorkenntnisse im Bezug auf die Architektur der Ressource verfügt. "Vollständige Kryptoarchitektur" bedeutet, dass der Angreifer über verwendete Protokolle und Sicherheitsmechanismen im Bilde ist und genau weiß, welche Instanzen in welchen Szenarien miteinander kommunizieren. Schlussendlich kann der Angreifer auch Kenntnisse über die verwendete Hard- und Software wie beispielsweise Schnittstellen verfügen.

Um beim Erstellen einer Bedrohungsanalyse keine Bedrohungen außer Acht zu lassen, ist es wichtig, realistische Angreifermodelle mit möglichst unterschiedlichen Attributen zu erstellen, da verschiedene Angreifer unterschiedliche Angriffsmethoden verwenden würden. Abbildung 37 zeigt die Klassifizierung von sechs solcher Angreifermodelle, die unter Berücksichtigung der definierten Attribute ein möglichst breites Spektrum an potentiellen Cyber-Kriminellen abdecken.

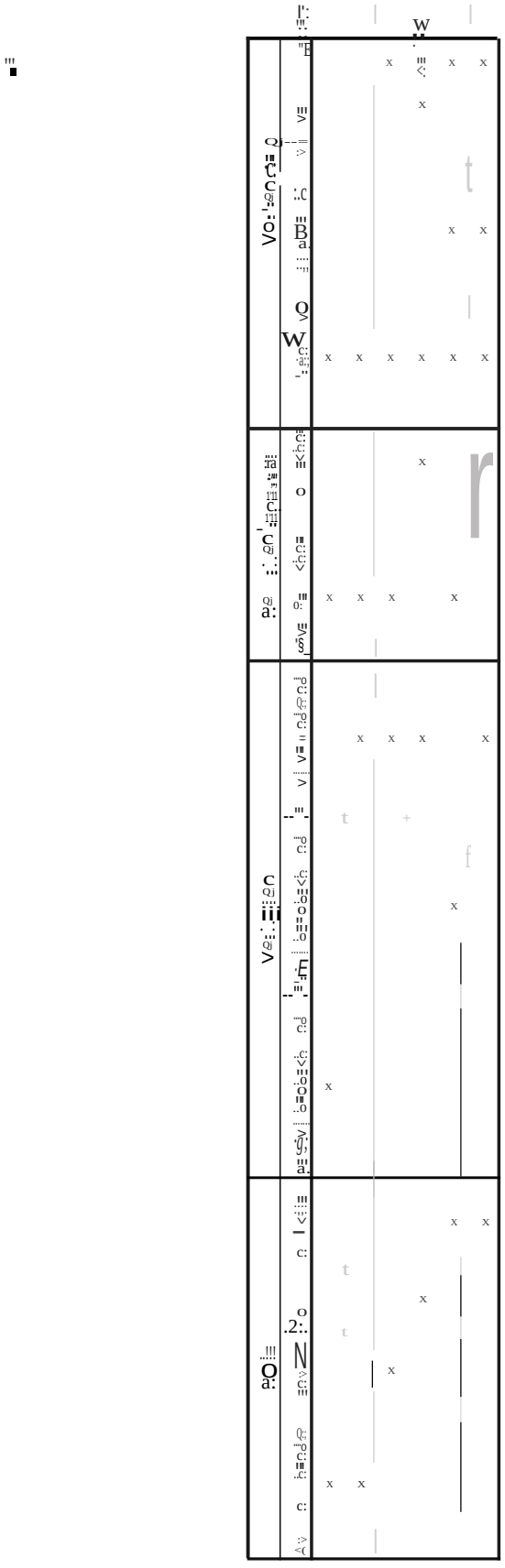

Abbildung 37: Definition der Angreifermodelle

Aus der obigen Tabelle 37 lassen sich folgende potentielle Angreiferprofile ablesen und zugehörige Angriffsschemata zuweisen:

Außenstehender, passiv/beobachtend, Privat Rechner, keine Vorkenntnisse

Der Angreifer hat nur geringe Ressourcen in Form eines Privatrechners und keine Vorkenntnisse im Bezug auf die verwendete Architektur. Außerdem geht der Angreifer lediglich passiv/beobachtend vor. Aufgrund dieser Definition bleibt dem potentiellen Angreifer nur die Möglichkeit, existierenden Netzwerkverkehr abzuhören (Sniffing). Da der Angreifer nur passiv vorgeht, kann er nur dann Informationen aus dem Netzwerkverkehr extrahieren, wenn dieser nicht verschlüsselt ist.

Außenstehender, aktiv/verändernd, Privat Rechner, keine Vorkenntnisse

Die Ressourcen und Vorkenntnisse des Angreifers verändern sich im Vergleich zum vorherigen Profil nicht, allerdings ist das Vorgehen des potentiellen Angreifers nun aktiv/verändernd. Das bedeutet, dass im Gegensatz zum vorherigen Profil mit gelesene, verschlüsselte Daten insofern einen Nutzen für den Angreifer bieten, als dass er versuchen könnte, diese zu entschlüsseln, um daraus Informationen zu gewinnen.

Außerdem kann der potentielle Angreifer beispielsweise folgende Angriffe ausführen:

- Man-in-the-Middle
- Replay-Angriff
- XXS
- DoS
- Passwort-Cracking
- Portscanning
- Session Hijacking
- (No)SQLInjection

User, aktiv/verändernd, Privat Rechner, keine Vorkenntnisse

~~Der Angreifer verhält sich analog zum vorherigen Profil, ist aber zusätzlich User. Hieraus ergeben~~

sich folgende zusätzliche Angriffsmöglichkeiten:

- Chosen Plaintext Angriff
- Gefälschte Daten an den Server senden

Server-Hoster, aktiv/verändernd, Groß-Rechner, verwendete Hardware (serverseitig)

Der Angreifer ist der Hoster des Servers, kennt somit die serverseitige Architektur und besitzt entsprechende Hardware. Außerdem verhält er sich aktiv/verändernd. Hieraus ergeben sich beispielsweise folgende weiterführende Angriffsmöglichkeiten:

- Datenbank Passwort Cracking
- Anlegen falscher Datensätze
- Manipulation des SSL-Handshakes
- Abschalten des Servers
- RAM freezen und Daten auslesen

Entwickler, aktiv/beobachtend, Privat Rechner, sämtliche Vorkenntnisse

Der Angreifer ist Entwickler und verfügt dementsprechend über sämtlichen architektonischen Kenntnisse bzgl. der angegriffenen Ressource. Der Angreifer verhält sich lediglich aktiv/beobachtend, was bedeutet, dass dieser Daten abfängt und deren Verschlüsselung knackt, was dem Angreifer wesentlich leichter als einem Außenstehendem fällt, da dieser als Entwickler Zugriff auf die verwendete Kryptoarchitektur hat.

Entwickler, aktiv/verändernd, Groß-Rechner, sämtliche Vorkenntnisse

Der Angreifer ist ebenfalls Entwickler,verhält sich aber im Gegensatz zum vorherigen Profil aktiv/verändernd und hat Zugriff auf Groß-Rechner oder Bot-Netze, was eine Entschlüsselung der abgefangenen Daten wahrscheinlicher macht. Zusätzlich könnte der Angreifer Backdoors in Updates einschleusen, was ihm neben dem Abhören von Daten ebenfalls Manipulationen ermöglicht.

A.4.2 Fazit - Angreiferprofile

Die aufgelisteten Angreiferprofile sind lediglich beispielhaft zu verstehen und müssen je nach

Kontext des zu prüfenden Systems angepasst werden. Allerdings geben diese bereits einen Ein-

blick in potentielle Angreiferprofile und die von diesen Profilen durchführbaren Angriffe. Hierdurch kann eine Abschätzung erfolgen, inwiefern entsprechende Angriffe realistisch sind, was wiederum zur Einschätzung des jeweiligen Risikofaktors und somit zu einer Priorisierung der Risiken genutzt werden kann. Hierdurch ist es dann möglich, zu entscheiden, welche Risiken akzeptiert und welche als so gravierend eingestuft werden müssen, als das entsprechende Gegenmaßnahmen definiert werden sollten.

A.5 Richtlinien zur Entsorgung von (privaten) Geräten - (Z07.09)

Sollten private Geräte im professionellen Umfeld genutzt werden, so sind diese nach Ende ihres Lifecycles analog zu Firmengeräten zu entsorgen. Das bedeutet, dass eventuell enthaltene Speichermedien mehrfach überschrieben werden, damit eventuell sensitive Informationen nicht von Dritten ausgelesen werden können. Je nachdem wie sensitiv die enthaltenen Informationen sind, bietet auch das Schreddern des Datenträgers eine Alternative.

A.6 Richtlinien zur (privaten) Internetnutzung während der Arbeitszeiten - (Z07.10)

Arbeitszeit ist zwar Arbeitszeit, aber was spricht dagegen, in der Pause kurz den Facebook-Status zu prüfen? Arbeitnehmern muss klar gemacht werden, dass die private Internetnutzung durch ein Gerät im Unternehmensnetzwerk eine potentielle Sicherheitslücke darstellt. Das bedeutet, dass an Arbeitsrechnern sofern möglich eine Beschränkung auf vom Arbeitgeber als sicher eingestufte und / oder zum Arbeiten notwendige Seiten erfolgen muss. Eine solche Beschränkung kann beispielsweise durch die Verwendung eines Proxy-Servers (siehe *Proxy* o.D.) erfolgen.

A.7 Richtlinien zur Verarbeitung von Metadaten - (Z07.11)

Selbst bei verschlüsselter Kommunikation kann, durch Abfangen von die Kommunikation betreffenden Metadaten (siehe *Metadaten* o.D.), ein Rückschluss auf die kommunizierenden Parteien und dementsprechend eine Profilbildung erfolgen. Metadaten fallen auch in anderen Kontexten, wie beispielsweise dem automatisiertem Übertragen von Verbrauchsdaten (Wasser, Strom, etc.) an. Sollten solche Maßnahmen zur Debatte stehen, so ist es notwendig, dass dem Bürger gegenüber eine entsprechende Stellungnahme zu dieser Thematik erfolgt. Optimal wäre es hierbei, auf möglichst lokale Anbieter zu setzen und Metadaten nicht länger zu speichern, als dass diese zur Verarbeitung benötigt werden. Dies würde dem Bürger ein Gefühl von Sicherheit vermitteln und könnte dazu beitragen, dessen Abwanderung entgegen zu wirken.

A.8 Förderung des Sicherheitsbewusstseins von Angestellten - (Z07.12)

Eine Kette ist immer nur so stark, wie ihr schwächste Glied - dieser bekannte Spruch gilt auch im Kontext der IT-Sicherheit und das schwächste Glied ist in der Regel der Nutzer. Selbst perfekt ausgefeilte Sicherheitsrichtlinien und durch sichere Passwörter geschützte Systeme nutzen nichts, wenn der Nutzer bspw. durch Social Engineering (*Was ist Social Engineering?* o.D.) dazu gebracht werden kann, sein Passwort an einen Außenstehenden zu verraten.

Aus diesem Grund ist es notwendig, **die Angestellten in regelmäßigen Abständen (bspw. jährlich) durch Schulungen zum Thema Datenschutz und Datensicherheit zu sensibilisieren**. Diese Schulungen sollten zur Kostenreduktion wenn möglich durch den internen Datenschutzbeauftragten durchgeführt werden.

B Datenschutz und Datensicherheit (Bürgerlich)

B.1 Richtlinien zur Absicherung von privaten digitalen Geräten (Z07.07)

Private digitale Geräte wie Smartphones, Tablets und Laptops sollten entsprechend, der aktuellen Richtlinien, abgesichert werden. Dazu gehören folgende Kernpunkte:

- Ausführungskontrolle: Die Ausführungskontrolle verhindert den Start von ausführbaren Dateien aus Verzeichnissen, in die der Benutzer schreiben kann. Durch diesen Mechanismus wird verhindert, dass beispielsweise heruntergeladene oder von zu Hause mitgebrachte Dateien, die möglicherweise infiziert sind, am APC ausgeführt werden.
- Virenschutz: Das Virenschutzprogramm prüft Dateien auf schädliche Inhalte. Mit dem Virenschutzprogramm auf dem APC werden auch Dateien auf Wechselmedien geprüft, die nicht das zentrale Sicherheits-Gateway passieren.
- Personal Firewall: Die Personal Firewall kontrolliert ein- und ausgehende Verbindungen. Damit schützt sie den APC vor Zugriffen von außen und verhindert, dass beliebige Anwendungen Daten versenden können.
- Gerätekontrolle: Eine Gerätekontrolle regelt, welche Geräte über externe Schnittstellen angeschlossen werden können.

- Benutzerverwaltung: Jeder Benutzer erhält ein persönliches Konto. Dabei werden dem Konto nur die Rechte zugewiesen, die der Benutzer für seine Arbeit benötigt. Die Verwaltung der Benutzer erfolgt typischerweise über einen Verzeichnisdienst.
- Logging: Relevante Ereignisse, wie beispielsweise Meldungen des Virenschutzprogramms, werden kontinuierlich erfasst, um Sicherheitsvorfälle zeitnah zu erkennen.

B.2 Richtlinien zur Entsorgung von privaten digitalen Geräten (Z07.09)

Ausgediente Geräte gehören ins Recycling. Persönliche Einträge und sensible Informationen sollte man vorher aber auf sichere Weise löschen.

Ganz gleich ob Handy, Smartphone, Tablet oder PC mit Festplatte wer einen dienstbaren elektronischen Geist mit gespeicherten Daten ausrangiert oder weiterverkauft, sollte vorher persönliche Einträge und sensible Informationen auf sichere Weise löschen, damit private Dokumente, Fotos oder auch Passwörter nicht in falsche Hände geraten. So kann man sich und der Umwelt einen nützlichen Dienst erweisen, wenn man die ausgedienten Elektronikgeräte weiterverkauft oder zum sachgerechten Recycling bringt.

Wenn auf Altgeräten, die einen Datenträger beherbergen, sensible persönliche Daten, etwa Adressen, Krankenakten oder Urlaubsfotos, gespeichert sind, sollten diese vor der Weitergabe

der Geräte unbedingt physikalisch gelöscht werden. Bei diesem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Vorgang werden die gespeicherten Daten mehrmals überschrieben. Diese etwas zeitaufwendige Prozedur macht eine Wiederherstellung von Daten unmöglich. Entsprechende Schredder-Software für die physikalische Löschung heißt zum Beispiel Eraser, Wiper oder Schredder.

Speicherkarten aus Handy oder Digitalkamera müssen in der Regel entnommen werden und mittels Kartenlesegerät sowie PC-Programm gelöscht werden. Für nicht entfernbare Speicherkarten in Smartphones gibt es spezielle Apps zum Download. Wer sich unsicher ist, wie die Daten gelöscht werden oder wo die Speicherkarte überhaupt versteckt ist, sollte einen IT-Fachmann aufsuchen.

Bei hochsensiblen Informationen empfiehlt sich eine mechanische Vernichtung des Datenträgers durch Schreddern. Dies übernehmen Firmen, die auch Akten vernichten. Beispielsweise:

- https://www.deutsche-aktenvernichtung.de
- Rhenus Becker GmbH und Co. KG, Williams Road 1, 67681 Sembach
- FileEx Akten- und Datenträgervernichtung GmbH, Charles-Lindbergh-Allee 10, 54634 Bitburg
- BHL GmbH Handel und Logistik, Amselstrasse, 54311 Trierweiler

B.3 Bewusstsein der Jugendlichen zu sicheren Passwörtern (Z07.02)

Um das Bewusstsein von Jugendlichen zu sicheren Passwörter zu steigern, könnte eine Informationsbroschüre mit den wichtigsten Informationen erstellt werden. Diese Informationsbroschüre würde von Sachbearbeitern erstellt werden, welche eine entsprechende Schulung zum Umgang sowie der Erstellung von sicheren Passwörtern erhalten haben. Die Broschüre müsste nach der Erstellung an geeigneten Stellen den Jugendlichen zugänglich gemacht werden. Dazu eignen sich zum einen Stellen an denen Jugendliche sich sammeln und treffen wie Einrichtungen wie beispielsweise Pfarrheime, Bahnhöfe und Parks und zum anderen Soziale Einrichtungen wie Schulen. In dieser Informationsbroschüre könnten die Informationen aus folgenden Unterkapiteln stehen:

B.3.1 Wieso brauche ich sichere Passwörter?

Unsichere Passwörter können sehr schnell von sogenannten „Crackern“ durch einfaches Ausprobieren gefunden werden. Diesen Leuten geht es meistens nicht darum, Daten zu klauen, zu verändern oder fremde E-Mails zu lesen, sondern sie sind auf der Suche nach einem Account über den sie ihre kriminellen Aktivitäten ungestört ausüben können.

Dabei kann es sich um Angriffe gegen einzelne Rechner, um geplante „Denial of Service"-Attacken gegen ganze Netzwerke oder um den Handel mit Waffen o.ä. handeln. In jedem dieser Fälle fällt der Verdacht zuerst auf den Inhaber des gecrackten Accounts. Dies ist in der Regel mit erheblichen Unannehmlichkeiten verbunden (Hausdurchsuchungen, Verhöre durch die Polizei/Staatsanwaltschaft usw.).

Sie können das Risiko, Opfer einer solchen „Verwechslung" zu werden erheblich senken, indem sie ihre Passwörter regelmäßig ändern und dabei auch auf die Sicherheit der Passwörter achten.

B.3.2 Wie sehen schlechte Passwörter aus?

Schlechte Passwörter sind einfache Kombinationen von Buchstaben oder Ziffern, so dass reale Wörter oder Zahlenkombinationen daraus entstehen wie zum Beispiel Namen, Orte und Geburtsdaten. Des Weiteren sind auch kurze Passwörter schlechte Passwörter. Beispiele:

- 123456
- Stefan
- 1994
- Trier

B.3.3 Wie sehen gute und sichere Passwörter aus?

Gute Passwörter sind zufällige Kombinationen aus Buchstaben, Ziffern und Sonderzeichen. Im Idealfall ist kein reales Wort in solch einem Passwort zu finden. Solche Passwörter sollten auch eine Mindestlänge von 8 Zeichen haben.

- #3Z.WJFd}
- +qaßLWUüjx
- Um7MWA+ödP.s
- HGvzs7-UÜe

B.3.4 Welche sicheren Möglichkeiten gibt es sich sichere Passwörter zu merken?

Wie man sieht können sich die meisten Menschen solche zufälligen Zeichenkombinationen schlecht merken, denn es schwierig ist eine passende „Eselsbrücke" zu finden. Aus diesem Grund können sogenannte Passworttresore verwendet werden. Passworttresore verschlüsseln alle deine Passwörter

sicher und speichern diese sicher in einer Datenbank ab. Solche Tresore nutzen dafür ein sogenanntes Masterpasswort, das im idealfall auch den Richtlinien eines sicheren Passwortes entspricht. So muss sich bei der Nutzung eines Passworttresores nur das Masterpasswort gemerkt werden, alle anderen Passwörter können bei bedarf aus dem Passworttresor ausgelesen werden.

B.4 Förderung des Bewusstseins der Jugendlichen zum Umgang mit persönlichen Daten (Z07.02)

Um das Bewusstsein von Jugendlichen zum Umgang mit personenbezogen sowie persönlichen Daten zu fördern, könnte zum einen ein Video mit einem Beispiel zum falschen Umgang mit diesen Daten erstellt werden und zum anderen eine Informationsbroschüre mit den wichtigsten Informationen erstellt werden. Ein solches Video wurde im Rahmen dieser Arbeit erstellt und wird in digitaler Form zur Verfügung gestellt. In der angesprochen Informationsbroschüre könnten die Informationen aus folgenden Unterkapiteln stehen:

B.4.1 Welche Gesetze gibt es zu personenbezogenen Daten und was ist in ihnen geregelt?

Das deutsche Bundesdatenschutzgesetz (BDSG) regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden. Es setzt die Datenschutzrichtlinie um, die durch die Datenschutz-Grundverordnung aufgehoben und ersetzt werden wird.

Landesdatenschutzgesetze sind die in den 16 Bundesländern verabschiedeten landesrechtlichen Pendants zum Bundesdatenschutzgesetz (für Behörden des Bundes und private Unternehmen). Die Landesdatenschutzgesetze gelten für die jeweiligen Landesbehörden und Kommunalverwaltungen. Sie gelten gegebenenfalls ergänzend zu spezialgesetzliche Regelungen wie zum Beispiel das Datenschutzrecht des Zehnten Buches Sozialgesetzbuch (SGB X). Die Landesdatenschutzgesetze regeln insbesondere auch die Rechtsstellung des jeweiligen Landesbeauftragten für Datenschutz.

Die Datenschutz-Grundverordnung ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

B.4.2 Was sind personenbezogene Daten?

Nach europäischem Recht und Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.

Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten ist mithin nur unter Zustimmung des Betroffenen zulässig.

B.4.3 Also nochmal genauer, was sind personenbezogene Daten?

- Name
- Adresse
- Alter
- Geburtsdatum
- Beruf
- Hobbys
- Familienstand
- Personalausweisnummer
- Telefonnummer
- Kfz-Kennzeichen
- Kontodaten
- Kreditkartendaten
- Bilder und Videos auf denen Personen zu sehen sind
- usw.

B.4.4 Wie muss ich mit diese Daten umgehen?

Ich darf diese Daten nicht ohne die Zustimmung der Person von der sie stammen weitergeben, das beinhaltet auch das Verschicken von Bildern oder Videos.

Ich sollte meine persönlichen Daten wie beispielsweise meinen Namen, Adresse und Geburtsdatum nur so selten wie möglich weitergeben.

Einmal im Netz immer im Netz Bilder die einmal verschickt oder veröffentlicht wurden, können nicht mehr mit 100 prozentiger Sicherheit gelöscht werden, was im schlimmsten Fall im späteren Leben Konsequenzen haben kann.

B.4.5 Was kann ich tun wenn personenbezogene Daten von mir ohne meine Zustimmung veröffentlicht wurden?

Bitte die Person, die die Daten veröffentlicht hat, diese wieder zu löschen.

Setze dich mit der Plattform, auf der die Daten veröffentlicht wurde, in Verbindung und bitte diese die Daten zu löschen.

Als letzten Ausweg können rechtliche Schritte, mittels eines Anwalts, in Betracht gezogen werden.

Glossar

Administration Unter Verwaltung versteht man allgemein administrative Tätigkeiten, die mit der Besorgung eigener oder fremder Angelegenheiten zusammenhängen und meist in einem institutionellen Rahmen wie Behörden, öffentlichen Einrichtungen, Unternehmen oder sonstigen Personenvereinigungen stattfinden. 46

Corporate Social Responsibility In diesem Zusammenhang spricht man von Unternehmerische Gesellschaftsverantwortung und umschreibt einen freiwilligen Beitrag der Wirtschaft, die zu einer nachhaltigen Entwicklung beiträgt, auch über die gesetzlichen Forderungen hinaus. Es handelt sich dabei um ein verantwortliches unternehmerisches Handeln der Geschäftstätigkeit (Markt), ökologische Aspekte (Umwelt), Beziehungen zu den Mitarbeitern am Arbeitsplatz (Arbeitsplatz), sowie der Austausch mit relevanten Interessengruppen (Stakeholdern).[74]. 3, 56

Customer Relationship Management CRM ist eine kundenorientierte Unternehmensphilosophie, die mit Hilfe moderner Kommunikations- und Informationstechnologien versucht, über einen längeren Zeitraum profitable Kundenbeziehungen zu festigen. Dies geschieht durch den Aufbau von ganzheitlichen und differenzierten Vertriebs-, Marketing- und Servicekonzepten.[75]. 56

Informationsmanagement Das Informationsmanagement hat die Aufgabe, integrierte Informations- und Kommunikationssysteme in ganzheitlicher Form zu gestalten. Dabei sind nicht nur Planungs-, Konzeptions-, Entwicklungs-, und Einführngsaktivitäten auszuführen, sondern auch Unterstützungsaktivitäten bei der Nutzung und bei der Pflege und Wartung des gesamten Systems relevant. Aspekte der Qualität und Wirtschaftlichkeit, der Leistungsfähigkeit und der Akzeptanz des Systems müssen dabei berücksichtigt werden.[76]. 43, 45, 51, 52, 58, 59, 72

IT-Controlling „IT-Controlling umfaßt das Controlling der Informationstechnik (IT), der (betrieblichen) Informationssysteme (IS) und der (vornehmlich rechnergestützten) Informationsverarbeitung (IV) im Unternehmen sowie der korrespondierenden Führungsprozesse der Ressource Information. [...] Das IT-Controlling umfaßt operative, administrative und strategische Aufgaben [...]“. Im Operativen sind hier beispielsweise die Betrachtung der Wirtschaftlichkeit von IT-Investitionen, die Erstellung von IT-Kennzahlen und einem geeigneten IT-Berichtswesen oder die Erstellung des IT-Budgets zu nennen.[77]. 5

[74] *Corporate Social Responsibility* o.D.
[75] Gabriel und Beier 2002b.
[76] Gabriel und Beier 2002a.
[77] *IT-Controlling (IV-Controlling, IS-Controlling)* o.D.

IT-Governance „Unter dem Begriff IT-Governance werden alle Führungs- und Steuerungsprozesse und -instrumente des IT-Managements zusammengefasst. Dabei hat die IT-Governance im Wesentlichen zwei Ziele, die es sicherzustellen gilt: Zum einen, dass die IT grundsätzlich die Geschäftsziele unterstützt und zum anderen, dass sie dies möglichst effektiv und effizient tut. [...] Ein wesentliches Ziel der IT-Governance ist die Sicherstellung klar definierter Schnittstellen sowohl zwischen IT-Abteilung und Fachbereichen als auch innerhalb der IT (Zusammenarbeitsmodell). Hierzu sind Kommunikations- und Entscheidungswege sowie -gremien zu definieren und zu etablieren. Für die IT-Governance sind am Markt einige Standardframeworks vorhanden [...] (z. B. Cobit, ITIL).“[78]. 5

IT-Personal Das IT-Personal umfasst die Mitarbeiter eines Unternehmens „zu deren Aufgaben Bereitstellung, Betrieb und Wartung der IT-Infrastruktur und die persönliche Unterstützung ihrer Nutzer gehören.“[79]. 5

IT-Prozesse IT-Prozesse sind solche Prozesse, die für die Planung der IT-Strategie sowie den Aufbau, den Betrieb und die Verbesserung von IT-Dienstleistungen durchgeführt werden. Die IT-Prozesse bilden dabei die Basis für die Definition der benötigten Kompetenzen des IT-Personals.. 5

IT-Sicherheit „IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.“[80]. 5

IT-Strategie „Eine IT-Strategie gibt die Rahmenbedingungen für das Management der Informationstechnologie eines Unternehmens vor und zeigt den Umfang und die Richtung zukünftigen Handelns auf, um langfristige Unternehmensziele zu erreichen.“[81] Eine IT-Strategie muss also beschreiben, wie ein angestrebter Soll-Zustand erreicht werden kann.. 5

Moderation Moderation ist ein Instrument, welches die Kommunikation in Teams in der Art und Weise unterstützt und ordnet, dass die Ressourcen der Teilnehmer bestmöglich zum Einsatz kommen. Sie ist weiterhin eine Arbeits- und Darstellungstechnik, die der Moderator in Arbeitsgruppen, bei Konferenzen oder in ähnlichen Situationen einsetzt. Der

[78] *IT-Governance* o.D.
[79] *Planung des hochschulweiten Bedarfs an IT-Personal* o.D.
[80] *IT-Grundschutz* o.D.
[81] *Notwendigkeit einer IT-Strategie* o.D.

Moderator bietet Hilfen methodischer Art zur Problemlösung oder auch Konfliktregelung an, ohne dabei inhaltlich Stellung zu beziehen bzw. Partei zu ergreifen[82]. 46

Share- Community Eine Share Community ist .... .[83]. 66

SMART Home Ein Smarthome ist ein System, dass .... .[84]. 66

Unternehmen Im Kapitel Arbeitergeber CSR/CRM wird oftmals von Unternehmen gesprochen. Mit Unternehmen ist hier ein kooperatives Netzwerk gemeint, dass sich mithilfe von CSR erst bildet. Es spiegelt die Beziehung der einzelnen Stakeholder dar. Nicht nur fordern sondern auch geben.. 70

Web 1.0 Die Version 1.0 des Webs, das laut Berners-Lee als das „Read-only Web" beschrieben wird, erlaubte es uns nach Informationen zu suchen und sie zu lesen. Es gab nur sehr wenige Möglichkeiten der Benutzerinteraktion oder der Inhaltserstellung.[85] Es handelte sich oft um statische Seiten die mit hyperlinks verknüpft wurden. 44

Web 2.0 Die Version 2.0 des Webs, das laut Berners-Lee als das „Read-Write Web" beschrieben wird, erlaubte es uns nach Informationen zu suchen,sie zu lesen, zu bearbeiten und eigenen Inhalt bereit zu stellen.[86] Es hat sehr viel Potenzial und hat die Landschaft des Webs in kurzer Zeit radikal verändert, betrachtet man als Beispiel YouTube oder MySpace. 44

Web 3.0 Die Version 3.0 des Webs, das laut Berners-Lee als das „Read-Write-Execute Web" beschrieben wird, ermöglicht die Lücke zwischen Menschen und computergestützen Anwendungen zu schließen. Eine der größten Herausforderungen bei der Präsentation von Informationen im Web ist, dass Anwendungen keinen Kontext für Daten bereitstellen können und daher nicht verstehen können, was relevant ist. Durch die Verwendung einer Art semantischem Markup (oder Datenaustauschformaten) könnten Daten in eine Form gebracht werden, die nicht nur für den Menschen über die natürliche Sprache zugänglich ist, sondern auch von Softwareanwendungen verstanden und interpretiert werden kann[87]. 44, 46

Web 4.0 Die Version 4.0 des Webs, beschreibt die direkte Kommunikation zwischen Menschen und computergestützen Anwendungen. Dabei findet die Kommunikation direkt zwischen dem Menschlichen Gehirn und der Anwendung statt. 46

[82] *Moderation* o.D.
[83] Gabriel und Beier 2002b.
[84] Ebd.
[85] *Web 1.0* o.D.
[86] *Web 2.0* o.D.
[87] *Web 3.0* o.D.

Literatur

Arbeitsmarkprognose 2030 (2013). url: https://www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/a756-arbeitsmarktprognose-2030.pdf?__blob=publicationFile (siehe S. 23, 25).

Beata Domanska- Szaruga, Wioletta Wereda (2011). *Management under conditions of risk and uncertainty*.

Bevölkerung: Basisdaten regional (2017). url: http://www.statistik.rlp.de/de/gesellschaft-staat/bevoelkerung-und-gebiet/basisdaten-regional/tabelle-6/ (siehe S. 10).

Bevölkerungsentwicklung in den deutschen Bundesländern bis 2035 (2017). url: https://www.iwkoeln.de/fileadmin/publikationen/2017/357919/IW-Trends_2017-03-04_Deschermeier.pdf (siehe S. 20–23, 26).

Bevölkerungsvorausberechnung Kreisfreie Stadt Trier (2013). url: http://infothek.statistik.rlp.de/MeineHeimat/content.aspx?id=101&l=1&g=07211&tp=16384 (siehe S. 11).

Bevölkerungsvorausberechnung Landkreis Trier-Saarburg (2013). url: http://infothek.statistik.rlp.de/MeineHeimat/content.aspx?id=101&l=1&g=07235&tp=16384 (siehe S. 11).

BSI-Grundschutz (o.D.). url: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (siehe S. 122).

Bundesverkehrswegeplan 2030 (2017). url: https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/BVWP/bvwp-2030-zusammenfassung.pdf?__blob=publicationFile (siehe S. 28).

Corporate Social Responsibility (o.D.). url: https://de.wikipedia.org/wiki/Corporate_Social_Responsibility (siehe S. 56, 158).

Datenschutz Grundverordnung (o.D.). url: https://dsgvo-gesetz.de/ (siehe S. 122).

Die demografische Entwicklung in Deutschland (2017). url: https://www.bpb.de/politik/innenpolitik/demografischer-wandel/196911/fertilitaet-mortalitaet-migration (siehe S. 20).

Digitale Verwaltung Rheinland-Pfalz (2018). url: https://mdi.rlp.de/fileadmin/isim/Startseite/Dokumente/Digitale_Verwaltung_Rheinland-Pfalz_-_die_E-Government-_und_IT-Strategie....pdf (siehe S. 31, 33).

Energetische Sanierung steuerlich fördern (2018). url: https://www.iwd.de/artikel/energetische-sanierung-steuerlich-foerdern-401817/ (siehe S. 37).

Gabriel, Roland und Dirk Beier (2002a). *Informationsmanagement in Organisationen* (siehe S. 52, 158).

— (2002b). *Informationsmanagement in Organisationen* (siehe S. 56, 158, 160).

— (2002c). *Informationsmanagement in Organisationen* (siehe S. 62).

— (2003). *Informationsmanagement in Organisationen* (siehe S. 4, 6).

Gräber, S., E. Ammenwerth, B. Brigl, C. Dujat, A. Große, A. Häber, C. Jostes und A. Winter (2003). *Rahmenkonzepte für das Informationsmanagement in Krankenhäusern: Ein Leitfaden* (siehe S. 2).

ISO-27000-Reihe (o.D.). url: https://de.wikipedia.org/wiki/ISO/IEC-27000-Reihe (siehe S. 122).

IT-Controlling (IV-Controlling, IS-Controlling) (o.D.). url: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Informationsmanagement lexikon/daten-wissen/Informationsmanagement/Informationsmanagement--Aufgaben-des/IT-Controlling/index.html (siehe S. 158).

IT-Governance (o.D.). url: https://www.gabler-banklexikon.de/definition/it-governance-70700 (siehe S. 159).

IT-Grundschutz (o.D.). url: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (siehe S. 159).

Jugend im Blick – Regionale Bewältigung demografischer Entwicklungen (2015). url: https://www.dji.de/fileadmin/user_upload/jugendimblick/EMPF_DRUCKEN.pdf (siehe S. 2 f.).

Jugendliche und Poltik (o.D.). url: https://www.shell.de/ueber-uns/die-shell-jugendstudie/jugend-und-politik.html (siehe S. 71).

Krcmar, Helmut (2015). *Einführung in das Informationsmanagement* (siehe S. 5).

Landflucht: DJI-Studie zeigt, was Jugendlichen einen Verbleib in der Region erleichtern würde (02. 05. 2016). url: https://idw-online.de/de/news650605 (siehe S. 43).

Langfristige Sicherung von Versorgung und Mobilität in ländlichen Räumen (2018). url: http://www.modellvorhaben-versorgung-mobilitaet.de/modellregionen/eifelkreis-bitburg-pruem/karten-daseinsvorsorge-und-kooperationsraeume/ (siehe S. 28).

Mein Kreis, meine kreisfreie Stadt (2017). url: http://infothek.statistik.rlp.de/MeineHeimat/index.aspx?id=101&l=1 (siehe S. 8).

Metadaten (o.D.). url: https://de.wikipedia.org/wiki/Metadaten (siehe S. 147).

Mit KfW-Förderung zu Ihrem Smart Home (2017). url: https://www.kfw.de/inlandsfoerderung/Privatpersonen/Bestandsimmobilie/Smart-Home/ (siehe S. 38).

Moderation (o.D.). url: https://wirtschaftslexikon.gabler.de/definition/moderation-38919 (siehe S. 160).

Musterbriefe zum Thema Digitale Welt (o.D.). url: https://www.verbraucherzentrale.de/musterbriefe/digitale-welt (siehe S. 140).

Notwendigkeit einer IT-Strategie (o.D.). url: http://4managers.de/management/themen/it-strategie/ (siehe S. 159).

Open-Source-Software in öffentlichen Einrichtungen (o.D.). url: https://de.wikipedia.org/wiki/Open-Source-Software_in_%C3%B6ffentlichen_Einrichtungen#China,_S%C3%BCdkorea_und_Japan (siehe S. 48).

Passwörter (o.D.). url: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (siehe S. 134).

Planung des hochschulweiten Bedarfs an IT-Personal (o.D.). url: https://his-he.de/fileadmin/user_upload/Veranstaltungen_Vortraege/2006/Workshop_IT-Reorganisation_2006/TOP4.pdf (siehe S. 159).

Proxy (o.D.). url: https://de.wikipedia.org/wiki/Proxy_(Rechnernetz) (siehe S. 147).

Prüfsummen berechnen und vergleichen (o.D.). url: https://winfuture.de/downloadvorschalt,2993.html (siehe S. 129).

Public Money? Public Code! (o.D.). url: https://publiccode.eu/de/ (siehe S. 48).

S.M.A.R.T. (o.D.). url: https://de.wikipedia.org/wiki/SMART_(Projektmanagement) (siehe S. 48).

Schneller surfen im ländlichen Raum (2018). url: https://www.kommune21.de/meldung_28635_Schneller+surfen+im+l%C3%A4ndlichen+Raum.html (siehe S. 38).

Sicherung von Versorgung und Mobilität (2018). url: https://www.bmvi.de/SharedDocs/DE/Publikationen/G/abschlussbericht-versorgung-mobilitaet-laendlicher-raum.pdf?_blob=publicationFile (siehe S. 29 f.).

Sniffer (o.D.). url: https://de.wikipedia.org/wiki/Sniffer (siehe S. 120).

Stadtrat (25. 05. 2014). url: https://www.trier.de/rathaus-buerger-in/stadtrat/ (siehe S. 18).

Stadtrat (01. 08. 2018). url: https://www.trier-saarburg.de/landratswahl_2013_desktop/Kreistag2014.html (siehe S. 18).

Struktur des Wohnungsbaus (2018). url: https://de.statista.com/statistik/daten/studie/202207/umfrage/struktur-des-wohnungsbaus-nach-art-der-bauleistung-in-deutschland/.

Stubenrauch, Hubert (2011a). *Städte, Landkreise, Verbandsgemeinden und Gemeinden* (siehe S. 13, 16).

— (2011b). *Städte, Landkreise, Verbandsgemeinden und Gemeinden* (siehe S. 14).

Studie: Handy-Funklöcher schrecken Jugendliche vom Wandern ab (o.D.). url: https://www.verivox.de/nachrichten/studie-handy-funkloecher-schrecken-jugendliche-vom-wandern-ab-19300/.

Transport Layer Security (o.D.). url: https://de.wikipedia.org/wiki/Transport_Layer_Security (siehe S. 119 f.).

Überblick Hochschulen Rheinland-Pfalz (2018). url: https://www.vcrp.de/hochschulen.

Was ist Social Engineering? (o.D.). url: https://www.security-insider.de/was-ist-social-engineering-a-633582/ (siehe S. 148).

Was sind Stakeholder und was bedeutet der Stakeholder-Ansatz? (15. 03. 2016). url: https://www.business-wissen.de/hb/was-sind-stakeholder-und-was-bedeutet-der-stakeholder-ansatz/ (siehe S. 48).

Web 1.0 (o.D.). url: https://www.practicalecommerce.com/Basic-Definitions-Web-1-0-Web-2-0-Web-3-0 (siehe S. 160).

Web 2.0 (o.D.). url: https://www.practicalecommerce.com/Basic-Definitions-Web-1-0-Web-2-0-Web-3-0 (siehe S. 160).

Web 3.0 (o.D.). url: https://www.practicalecommerce.com/Basic-Definitions-Web-1-0-Web-2-0-Web-3-0 (siehe S. 160).

Wir brauchen das Dorf! (20. 04. 2015). url: https://www.theeuropean.de/gerhard-henkel/10104-stadt-und-land-sind-gleichwertig (siehe S. 15).

Zeitliche Empfehlungen für Passwörter (o.D.). url: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html (siehe S. 134).

Zukunfts-Check Dorf (2014). url: https://www.bitburger-pruem.de/cms/images/stories/wirtschaft/zukunftscheckdorf/Evaluierungsbericht-14-04-