TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Handreichung zum "Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG)

Mitwirkende

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung im TeleTrusT-Arbeitskreis "Stand der Technik im Sinne des IT-Sicherheitsgesetzes" sowie für die aktive Mitgestaltung dieser Handreichung.

Projektleitung

RA Karsten U. Bartels LL.M., HK2 Rechtsanwälte
Tomasz Lawicki, The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff

Autoren

Adrian Altrhein, TÜV Informationstechnik GmbH
Sebastian Barchnicki, if(is) - Institut für Internet-Sicherheit/secunet Security Networks AG
RA Karsten U. Bartels LL.M., HK2 Rechtsanwälte
Michael Barth, genua GmbH
Oliver Dehning, Hornetsecurity GmbH
Elmar Eperiesi-Beck, eperi GmbH
Marco Fischer, procilon IT-Solutions GmbH
Steffen Heyde, secunet Security Networks AG
Tomasz Lawicki, The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Stefan Menge, Acht:Werk GmbH & Co. KG
Patrick Michaelis, The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Ramon Moerl, itWatch GmbH
Dr. Holger Mühlbauer, TeleTrusT - Bundesverband IT-Sicherheit e.V.
Markus Robin, SEC Consult Unternehmensberatung GmbH
Peter Rost, Rohde & Schwarz Cybersecurity GmbH
Dr. Norbert Schirmer, Rohde & Schwarz Cybersecurity GmbH

Weitere Mitwirkende

Björn Christiansen, 8ack GmbH
Thomas Gereke, Siemens AG
Tobias Krebs, eperi GmbH
Markus Mantzke, 8ack GmbH

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

Vorwort

TeleTrusT begrüßt das "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme "("IT-Sicherheitsgesetz", ITSiG). Dass der Gesetzgeber einen Vorstoß mit dem Ziel unternommen hat, Defizite in der IT-Sicherheit abzubauen, ist positiv zu bewerten. Fast täglich zeigen Meldungen zu Sicherheitsvorfällen in Unternehmen und Behörden, dass auch in Deutschland dringender Handlungsbedarf zur Verbesserung der IT-Sicherheit besteht.

Aus Sicht von TeleTrusT lässt die geltende Gesetzesfassung jedoch noch eine erhebliche Verbesserungen zu: bislang hat der Gesetzgeber weder Bewertungskriterien für die sicherheitsrelevanten technischen und organisatorischen Vorkehrungen benannt, noch sonstige Vorgaben zu Mindestanforderungen aufgestellt. Das Verhältnis zum technischen Datenschutz ist ebenfalls unklar. Die Ausgestaltung der Meldepflichten von IT-Sicherheitsvorfällen und die Befugnisse des BSI werfen zudem rechtliche und praktische Fragen auf.

Es ist technisch erforderlich und deshalb richtig, mit dem Gesetz nicht nur die großen Betreibern "Kritischer Infrastrukturen" (KRITIS) zu adressieren, sondern auch nicht-kritische Systeme, nämlich die Telemedienangebote wie Webseiten. Für KRITIS-Betreiber legt das geänderte BSIG dazu unter anderem den Grundstein für Branchenmindeststandards - für Telemediendienste lässt das Gesetz hingegen offen, nach welchen Maßstäben technische und organisatorische Vorkehrungen zu treffen sind und in welchem Verhältnis diese zu den Maßnahmen nach dem Bundesdatenschutzgesetz stehen.

TeleTrusT wird sich deshalb dafür einsetzen, die bestehenden Unklarheiten des IT-Sicherheitsgesetzes gemeinsam mit allen Akteuren anzugehen. Die Aktivitäten des Gesetz- und Verordnungsgebers begleitet der TeleTrusT mit der Kompetenz der organisierten IT-Sicherheitswirtschaft in Deutschland technisch, organisatorisch und rechtlich. Das gilt insbesondere auch hinsichtlich der Anforderungen des ITSiG zu Maßnahmen nach dem Stand der Technik.

TeleTrusT hat einen verbandsinternen Arbeitskreis 'Stand der Technik' initiiert, um aus Sicht der IT-Sicherheitslösungsanbieter und -berater, den betroffenen Wirtschaftskreisen Handlungsempfehlungen und Orientierung zu geben. Der Arbeitskreis und die Arbeitsgemeinschaft Recht des TeleTrusT widmen sich der Beantwortung der Frage, wie sich der jeweilige Stand der Technik im Sinne des Gesetzes in Bezug auf IT-Sicherheit bestimmen lässt und welche rechtlichen Maßgaben umzusetzen sind.
Diese Handreichung soll den anwendenden Unternehmen und Anbietern (Herstellern, Dienstleistern) gleichermaßen Hilfestellung zur Bestimmung des "Standes der Technik" geben. Das Dokument kann dabei als Referenz für Vereinbarungen zu Sicherheitsmaßnahmen bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen.

RA Karsten U. Bartels LL.M., Vorstand TeleTrusT, Bundesverband IT-Sicherheit e.V.

Dr. Holger Mühlbauer, Geschäftsführer TeleTrusT, Bundesverband IT-Sicherheit e.V.

Tomasz Lawicki, Leiter Arbeitskreis "Stand der Technik"

Inhalt

1 Einleitung

1.1 IT-Sicherheitsgesetz

Das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz (ITSiG) soll eine Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland herbeiführen. Die dadurch eingeführten Gesetzesänderungen dienen dem Schutz dieser Systeme hinsichtlich der aktuellen und zukünftigen Gefährdungen der Schutzgüter Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität. Ausweislich der Gesetzesbegründung ist das Ziel des Gesetzes die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamtes (BKA).

Bei dem IT-Sicherheitsgesetz handelt es sich um ein sogenanntes Artikelgesetz: Es dient lediglich der Änderung mehrerer anderer Gesetze. Durch das neue Gesetz wurden unter anderem Regelungen für Kritische Infrastrukturen (KRITIS) im Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG) geschaffen und gesetzliche Änderungen im Atomgesetz (AtomG), Energiewirtschaftsgesetz (EnWiG), Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) vorgenommen.

Das IT-Sicherheitsgesetz sowie dessen Gesetzesbegründung sind unter folgendem Link abrufbar: https://www.teletrust.de/it-sicherheitsgesetz/.

Die wesentlichsten Neuregelungen sieht das ITSiG für KRITIS-Betreiber sowie Unternehmen, die Telemedienangebote bereithalten, vor. Betreiber Kritischer Infrastrukturen haben nun gemäß § 8a Absatz 1 BSIG ein dem Stand der Technik entsprechendes Mindestniveau an IT-Sicherheit einzuhalten. Zudem besteht die Verpflichtung, bestimmte IT-Sicherheitsvorfälle an das BSI zu melden. Die Einstufung eines Unternehmens als Kritische Infrastruktur verläuft auf zwei Ebenen. Zum einen ist zu prüfen, ob eine Zuordnung zu einem grundsätzlich als kritisch eingestuften Sektor vorliegt (Sektorenzugehörigkeit) und zum anderen, ob eine besondere Sicherheitsrelevanz besteht (Fehlerfolgenerheblichkeit). Mittelbar sind durch die gesetzlichen Regelungen auch Dienstleister und Zulieferer von KRITIS-Betreibern betroffen.

Gemäß § 10 Absatz 1 des BSIG wurde das Bundesministerium des Innern (BMI) zum Erlass einer Rechtsverordnung ermächtigt, die festlegt, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Dabei wird auf die Bedeutung der Dienstleistungen und deren Versorgungsgrad abgestellt. Die Bundesregierung hat am 13.04.2016 dem Erlass der von Bundesinnenminister Dr. Thomas de Maizière vorgelegten Ministerverordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) zugestimmt. Dieser erste Teil der KRITIS-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes ist bereits am 03.05.2016 in Kraft getreten. Sie enthält die Maßgaben zu den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. In einem zweiten Korb, der für Anfang 2017 erwarten wird, werden die Sektoren Finanzen, Transport und Verkehr sowie Gesundheit geregelt.

Betreiber Kritischer Infrastrukturen haben gemäß § 8a Absatz 1 BSIG eine Frist von zwei Jahren nach Inkrafttreten der Rechtsverordnung, angemessene TOV zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Anbieter von Telemedienangeboten haben aufgrund des neu geschaffenen Absatzes 7 des § 13 TMG zu gewährleisten, dass ihre technischen Einrichtungen im Rahmen ihrer technischen und wirtschaftlichen Möglichkeiten durch technische und organisatorische Vorkehrungen (TOV) geschützt sind. Bei der Auswahl dieser TOV ist der Stand der Technik zu berücksichtigen. Eine Meldepflicht für Vorfälle besteht nicht. Betroffen ist dadurch jedes Unternehmen, welches ein Telemedienangebot betreibt. Die Maßgaben des Telemediengesetzes sehen im Gegensatz zu den KRITIS-Regelungen keine Übergangsfrist und keine Kleinstunternehmerausnahmeregelung vor.

1.2 Angemessenheit der Maßnahmen

Der in dieser Handreichung beschriebene "Stand der Technik" (im Folgenden auch SdT) fokussiert die durch das IT-Sicherheitsgesetz geforderten Inhalte. Es ist jedoch im Sinne des IT-Sicherheitsgesetzes zulässig, dass bei der Auswahl notwendiger Schutzmaßnahmen, die dem "Stand der Technik" entsprechen, auch die wirtschaftlichen Aspekte berücksichtigt werden. Ob eine Maßnahme wirtschaftlich ist, kann allerdings nur durch individuelle Betrachtung des eigenen Schutzbedarfes sowie der Realisierungskosten erforderlicher Maßnahmen festgestellt werden. Aus diesem Grund wurde in dieser Handreichung auf die Wirtschaftlichkeitsprüfung verzichtet.

Um die wirtschaftlich tragbaren IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe zu identifizieren, wird auf das Wirkungsklassen-Modell verwiesen, das im Rahmen einer durch TeleTrusT unterstützten Bachelorarbeit entwickelt wurde. Die Ausarbeitung ist unter folgendem Link abrufbar: https://www.teletrust.de/publikationen/broschueren/wirkungsklassen/.

1.3 Verwendungshinweis

Diese Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen. Sie ersetzt eine technische, organisatorische oder rechtliche Beratung oder Bewertung im Einzelfall nicht."

2 Abgrenzung relevanter Begriffe

2.1 Geforderter Technologiestand

Mit dem IT-Sicherheitsgesetz fordert der Gesetzgeber die Einhaltung oder zumindest die Berücksichtigung des "Stand der Technik" für die eingesetzten technischen Einrichtungen.

So beispielsweise schreibt der § 8a BSIG vor: "Betreiber kritischer Infrastrukturen sind verpflichtet… angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse zu treffen… Dabei soll der Stand der Technik eingehalten werden".
Und gemäß § 13 Absatz 7 TMG wird gefordert: "Diensteanbieter haben… sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist… Vorkehrungen… müssen den Stand der Technik berücksichtigen".

In der Gesetzgebung tauchen oftmals Begriffe wie "allgemein anerkannten Regeln der Technik", "Stand der Technik" oder auch "Stand der Wissenschaft und Technik" auf. Die verwendeten Begriffe sind unzureichend spezifiziert, denn sie definieren keine konkrete Maßnahme oder keinen technologischen Stand. Doch die Verwendung der allgemeinen Begriffe ist vom Gesetzgeber durchaus gewollt. Einerseits gibt der Gesetzestext die durch den Gesetzgeber gewollte Zielrichtung vor, andererseits bleibt der Gesetzestext unabhängig von der technologischen Entwicklung entkoppelt und ist somit stets aktuell.

Obwohl die Begriffe ähnliche Inhalte vermuten lassen, haben sie für den Gesetzgeber unterschiedliche Bedeutung:

Allgemein anerkannte Regeln der Technik
"Die Generalklausel "allgemein anerkannte Regeln der Technik" wird für Fälle mit vergleichsweise geringem Gefährdungspotenzial oder für Fälle verwendet, die auf Grund gesicherter Erfahrungen technisch beherrschbar sind.

Allgemein anerkannte Regeln der Technik sind schriftlich fixierte oder mündlich überlieferte technische Festlegungen für Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung der beteiligten Kreise (Fachleute, Anwender, Verbraucherinnen und Verbraucher und öffentliche Hand) geeignet sind, das gesetzlich vorgegebene Ziel zu erreichen und die sich in der Praxis allgemein bewährt haben oder deren Bewährung nach herrschender Auffassung in überschaubarer Zeit bevorsteht." (Quelle: Bundesministeriums für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit, Seite 4, http://hdr.bmj.de/page_b.4.html).

Stand der Technik
"Das Anforderungsniveau bei der Generalklausel "Stand der Technik" liegt zwischen dem Anforderungsniveau der Generalklausel "allgemein anerkannte Regeln der Technik" und dem Anforderungsniveau der Generalklausel "Stand von Wissenschaft und Technik".

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten - wenn dies noch nicht der Fall ist - möglichst im Betrieb mit Erfolg erprobt worden sein. Im Recht der Europäischen Union wird auch die Formulierung "die besten verfügbaren Techniken" verwendet. Dies entspricht weitgehend der Generalklausel "Stand der Technik"."

(Quelle: Bundesministeriums für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit, Seite 4, http://hdr.bmj.de/page_b.4.html).

Stand der Wissenschaft und Technik
"Die Generalklausel 'Stand von Wissenschaft und Technik' umschreibt das höchste Anforderungsniveau und wird daher in Fällen mit sehr hohem Gefährdungspotenzial verwendet. Stand von Wissenschaft und Technik ist der Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgegebene Ziel für erforderlich gehalten werden und das Erreichen dieses Ziels gesichert erscheinen lassen."
(Quelle: Bundesministeriums für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit, Seite 4, http://hdr.bmj.de/page_b.4.html).

Substitutiv für die Generalklausel "Stand der Wissenschaft und Technik" wird auch der Begriff "Stand der Wissenschaft und Forschung" verwendet.

Ausgehend von den oben aufgeführten Definitionen lassen sich die einzelnen Generalklauseln wie folgt gegenüberstellen:

Generalklausel	Entwicklungsstand	Bewährung in der Praxis	Grad der Anerkennung
Anerkannte Regeln der Technik (3)	schriftlich fixierte oder mündlich überlieferte Festlegungen vorhanden	in der Praxis allgemein bewährt	durch Anwender und Fachleute anerkannt
Stand der Technik (2)	fortschrittlicher Entwicklungsstand bezogen auf Verfahren, Einrichtungen, Betriebsweisen	in der Praxis oder Betrieb bewährt	durch führende Fachleute anerkannt
Stand der Wissenschaft und Technik (1)	fortschrittlichster Entwicklungsstand bezogen auf Verfahren, Einrichtungen, Betriebsweisen	nach wissenschaftlichen Erkenntnissen hat den Anschein einer Eignung	durch führende Fachleute aus Wissenschaft und Technik anerkannt

Tabelle 1: Gegenüberstellung der Generalklauseln

Die folgende Grafik zeigt eine Möglichkeit zur Einordnung der Generalklauseln durch Verwendung der Kriterien "Bewährung in der Praxis", "Grad der Anerkennung" sowie "des Entwicklungsstands":

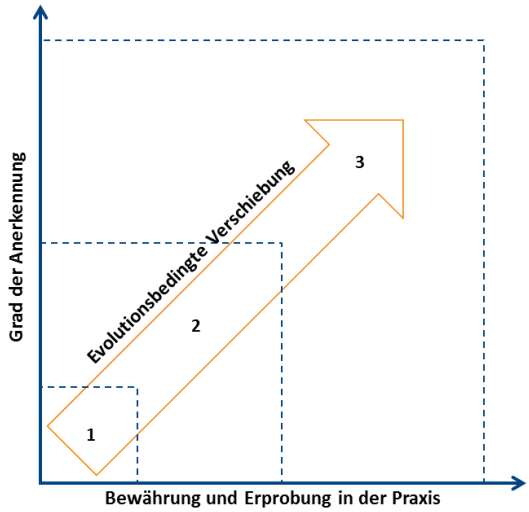

Abbildung 1: Einordnung der Generalklauseln

Die Übergänge zwischen den jeweiligen Bereichen sind nicht scharf definiert. Da sich die Technologie insgesamt weiterentwickelt, erfolgt eine kontinuierliche Verschiebung der Einordnung ausgehend vom "Stand von Wissenschaft und Technik" (in Abbildung 1 = "1") über "Stand der Technik" (2) zu den "allgemein anerkannten Regeln der Technik" (3).

Um den gesetzlich geforderten Technologiestand der IT-Sicherheit einzuhalten, bedarf es zunächst einer Schutzbedarfsanalyse sowie der Klassifizierung der Maßnahmen im Hinblick auf den erreichten Technologiestand. Aufgrund der evolutionsbedingten Verschiebung müssen die implementierten Maßnahmen kontinuierlich auf die Einhaltung des "Stands der Technik" überprüft werden. Hierfür sollte eine geeignete, messbare und nachvollziehbare Methode gewählt werden, um bei Bedarf die getroffenen Entscheidungen transparent dokumentieren zu können.

2.2 Geforderte Schutzziele

Mit den durch das ITSiG eingeführten Gesetzesänderungen werden die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität fokussiert. Mittels dieser Schutzziele können manipulierte Veränderungen des Datenzustands klassifiziert werden:

- **Verfügbarkeit**
  Die Verfügbarkeit von informationstechnischen Systemen und Komponenten ist vorhanden, wenn diese stets gemäß ihres Zwecks und Funktionsumfangs genutzt werden können.
- **Integrität**
  Die Integrität bezieht sich insbesondere auf die Daten. Dabei ist die Integrität vorhanden, wenn sichergestellt ist, dass die gesendeten Daten den Empfänger unverändert und vollständig erreichen.
- **Vertraulichkeit**
  Die Vertraulichkeit ist gegeben, wenn die schützenswerten Daten nur in der zulässigen Art und Weise ausschließlich an die Befugten verfügbar gemacht werden.
- **Authentizität**
  Die Authentizität ist vorhanden, wenn die eindeutige Identität der Kommunikationspartner (aber auch der kommunizierenden Komponenten) sichergestellt ist.

3 "Stand der Technik" wesentlicher Komponenten und Prozesse

Das ITSiG fordert die Einhaltung oder mindestens die Berücksichtigung des Stands der Technik für die eingesetzte IT-Infrastruktur. Eine weitere Konkretisierung der relevanten Systeme und Komponenten erfolgt von Seiten des Gesetzgebers nicht. Daher muss von der Einhaltung des Stands der Technik für die vollständige IT-Infrastruktur, einschließlich aller Datenübertragungs-, Datenspeicherungs- und Verarbeitungsmöglichkeiten, ausgegangen werden.

Da solche Infrastrukturen anwendungs- und branchenabhängig sind, ist eine vollumfassende Auflistung der einzelnen Komponenten im Rahmen dieser Handreichung nicht möglich. Die Autoren haben sich auf die Beschreibung des Stands der Technik für die wesentlichen Komponenten und Prozesse fokussiert. Sie wurden in den nachfolgenden funktionalen Bereichen zusammengefasst:

- Kapitel 3.1
  - Allgemeine Hinweise
- Kapitel 3.2
  - Sichere Vernetzung
  - Sicherer Internetzugang
  - Digital Enterprise Security
  - Client- und Serversicherheit
  - Mobile Security
- Kapitel 3.3
  - Prozesse

3.1 Allgemeine Hinweise

Anwendungen sind im Bereich der Verwendung im Kontext des IT-Sicherheitsgesetzes teilweise sehr speziell. Hierbei geht es beispielsweise von der einfachen sicheren E-Mail-Kommunikation bis hin zur sicheren Steuerungsfunktionalität in einem Kraftwerk. Auf Grund dessen ist es nur schwer möglich in dieser Studie eine vollumfassende Auflistung der Anwendungen zu erstellen und diese Anwendung auch zu beschreiben. Ebenfalls kann IT-Sicherheit unterschiedlich umgesetzt wegen. "Viele Wege führen nach Rom" und so gibt es auch nicht DIE EINE Umsetzung einer sicheren Architektur. Deshalb sollen hierbei wesentliche Punkte genannt werden, die als "Stand der Technik" im Sinne der heutigen Nutzbarkeit von IT-Sicherheit verstanden werden können.

Der jeweilige Schutzbedarf ist abhängig von der jeweiligen Anwendung. Gemäß IT-Sicherheitsgesetz müssen die IT-Sicherheitsziele Integrität, Authentizität, Verfügbarkeit bzw. Vertraulichkeit betrachtet werden, auch wenn Sie ggf. für die einzelne Abbildung mit unterschiedlichem Schutzbedarf bewertet werden. Dies bedeutet, dass vor allem folgende Schutzziele zu berücksichtigen sind:

- Schutz vor Angriffen zum unberechtigten Mitlesen, Ändern, Löschen von übermittelten und gespeicherten Daten
- Schutz vor Angriff auf Verfügbarkeit der jeweiligen Dienste und Daten beim Betreiber und Nutzer
- Schutz des Betriebs- und Anwendungssystemen vor unberechtigten Manipulationen, usw.

Zudem muss neben der Realisierung angemessener Schutzmaßnahmen auch das Erkennen von Angriffen auf IT-Systeme, -Dienste und Daten nach dem Stand der Technik gewährleistet werden.
Die Funktionalität zur Umsetzung der gewünschten IT-sicherheitstechnischen Anwendung muss stets vollständig und korrekt umgesetzt sein. Dies sollte von einem unabhängigen Prüfer nachvollziehbar geprüft worden sein. Die Umsetzung muss dabei stets fortschrittliche Verfahren berücksichtigen. Dies sind beispielsweise:

- 2-Faktor-Authentisierung
- gegenseitige Authentisierung
- Verschlüsselung der Kommunikation während des Transports

- Verschlüsselung der Daten (z.B. bei der Speicherung)
- Sicherung des privaten Schlüssels vor unberechtigten Kopieren
- Einsatz von sicheren Boot-Prozessen
- Sichere Software-Administration einschl. Patch-Management
- Sichere Benutzer-Administration mit aktiver Sperrmöglichkeit
- Sichere Abbildung von Netzwerkzonen zum zusätzlichen Schutz auf Netzwerk-Ebene
- Sichere Daten-Kommunikation zwischen unterschiedlichen Netzwerkzonen
- Sicheres Internet-Browsen
- Umsetzung des Need-To-Know-Prinzips
- Umsetzung des Minimal-Ansatzes (einschl. Härtung)
- Umsetzung von Logging-, Monitoring-, Reporting- und Response-Management-Systemen
- Umsetzung von Malware-Schutz
- Einsatz von sicheren Backup-Systemen zur Sicherung vor Verlust von Daten
- Mehrfache Auslegung der Systeme zur Umsetzung von Hochverfügbarkeit, etc.

"Stand der Technik" bedeutet aber auch aus Sicht der gesamten Sicherheitsfunktionalität neben einzelnen technischen Anwendungsfunktionalitäten auch die gesamte Sicherheitsarchitektur zu betrachten. Hierzu sind im Rahmen der Bedingungen folgende Punkte zu bewerten (die BNetzA fordert für die Umsetzung hinsichtlich des IT-Sicherheitskataloges gemäß EnWG §11 eine Risikoeinschätzung hoch als Standard bzw. kritisch für kritische Prozesse und Anwendungen):

■ Für den Anwender muss ersichtlich sein, unter welchen Bedingungen er das jeweilige System in der jeweiligen sicheren Konfiguration nutzen und einsetzen kann. Sollten unterschiedliche Einsatzszenarien auf einem Gerät möglich sein (z.B. Zugriff auf Office-IT über Session 1 und Zugriff auf die Prozess-IT über Session 2 ist dies optisch für den Anwender jeweils aussagekräftig darzustellen.

■ Eine ganzheitliche Sicherheitsarchitektur für das Produkt bzw. den Dienst und einer entsprechenden Dokumentation für die Evaluation durch unabhängige Dritte sollte existieren und umgesetzt sein.

■ Die verwendete Kryptographie muss modern und bis Ende des Produktlebenszyklus aktuell und sicher abgebildet werden können. Hierzu empfiehlt das BSI stets aktuell gehaltene Kataloge mit geeigneten Algorithmen.

■ Das eingesetzte Produkt bzw. der jeweilige Dienst darf keine Backdoors beinhalten, die ein Mitlesen oder gar Manipulation der Daten und Anwendungen gestatten.

■ Der Hersteller darf keine Zugriffsschnittstellen, die unabhängig vom Betreiber genutzt werden können, aufweisen.

■ Es wäre empfehlenswert, die Umsetzung der Sicherheitsfunktion von vertrauenswürdigen Dritten prüfen zu lassen.

■ Die in der Anwendung umgesetzten Prozesse (z.B. Benutzerberechtigung, Key Management etc.) sind sicher abzubilden.

Um ein Produkt hinsichtlich "Stand der Technik" zu bewerten, gibt es weitere Kriterien, die zu erfüllen sind. Dies sind die folgenden:

■ Das Produkt bzw. die Dienstleistung internationale Standards berücksichtigen und interoperabel mit Standard-Protokollen sein, soweit diese verwendet werden.

■ Wenn branchenspezifische Standards existieren, sollten diese bei dem Einsatz berücksichtigt werden.

■ Das Produkt oder die Dienstleistung muss einen störungsfreien Betrieb der Komponenten ermöglichen (Marktreife).

■ Das Produkt oder die Dienstleistung muss mit Erfolg in der Praxis erprobt worden sein.

■ Bei der Bewertung ist zu berücksichtigen, dass die Lösung als Einheit betrachtet werden muss, wenn eine Kopplung aus Hard- und Software gegeben ist.

■ Das Produkt muss hinsichtlich der Sicherheits- und der Anwendungsfunktionalität sicher updatefähig sein.

Der Hersteller der Lösung unterliegt ebenfalls in der Bewertung der Lösung Kriterien, die bei der Auswahl von Stand der Technik-Umsetzungen berücksichtigt werden müssen. Der Hersteller kann Investitionssicherheit für die jeweilige Umsetzung garantieren. Dies bedeutet, dass folgende Prüfungen erfolgen sollten:

■ Finanzieller Background des Herstellers garantiert weitere Lebenszyklen des Produktes.

■ Es existiert ein etabliertes Produktmanagement für das jeweilige Produkt und ein Roadmap für die weitere Entwicklung für den Zeitraum des Einsatzes beim Anwender.

■ Das Produkt ist während des Einsatzzeitraums nicht als Auslauf-Produkt gekennzeichnet.

■ Der Hersteller reagiert pro-aktiv auf bekannt gewordene Schwachstellen, die sein Produkt betreffen und schließt diese kurzfristig und stellt kurzfristig notwendige Software-Updates zur Verfügung.

■ Der Hersteller produziert die jeweilige Lösung in einer vertrauenswürdigen Umgebung mit vertrauenswürdigen Personal.

■ Der Hersteller beherrscht eigenständig die vollständigen Sicherheitsfunktionen und hat sich bzgl. der Sicherheitsfunktionen in keine Abhängigkeiten durch weitere Zulieferer begeben.

Sollten Zuliefer-Produkte verwendet werden, die eine geringere Vertrauenswürdigkeit aufweisen, ist durch die Sicherheitsarchitektur des Produktes und Maßnahmen im Produktionsprozess beim Hersteller zu gewährleisten, dass die Gesamtsicherheitsarchitektur hinsichtlich des definierten Schutzbedarfs bestehen bleibt.

3.2 Systeme und Komponenten

3.2.1 Sichere Vernetzung

3.2.1.1 Sichere Anbindung mobiler User / Telearbeiter

In vielen Firmen ist es notwendig, Mitarbeiter, die außer Haus sind, kontrolliert an das Firmennetz anzubinden. Bei diesen Lösungen erhält der Mitarbeiter über ein VPN Zugang zum Firmennetz oder einem Teil davon. Je nach Lösung hat der Mitarbeiter gleichzeitig Zugriff auf das Internet. In diesem Fall muss besonders dafür Sorge getragen werden, dass hier kein direkter Zugang aus dem Internet in das Firmennetzwerk geschaffen wird. Der Bedrohung durch Malware an dieser Stelle muss durch sichere technische Lösungen begegnet werden.

Als kritischer Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb dieser Geräte besondere Aufmerksamkeit zugute kommen. Entsprechende Lösungen sollten nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Im besten Fall ist die Lösung ohne Umweg direkt vom Hersteller zu beschaffen.

Die Schutzziele für solche Lösungen sind:

- Vertraulichkeit, Integrität und Authentizität des VPN-Zugangs und der übertragenen Daten sicherstellen
- Vertraulichkeit und Integrität der Firmendaten schützen
- Vertraulichkeit der kryptographischen Schlüssel sicherstellen
- Integrität der durchgeleiteten Daten sicherstellen

- Authentizität der durchgeleiteten Daten sicherstellen.

Eine Remote Access Lösung muss ein sicheres VPN zur Verfügung stellen. Das Gerät des Anwenders (z.B. Laptop des Telearbeiters) muss jedoch als relativ unsicher angesehen werden, da hier in der Regel ungesicherte Hardware und Software eingesetzt wird und das Gerät im Normalfall mit Internetzugriff genutzt wird. Es muss also Aufwand getrieben werden, um das VPN-Schlüsselmaterial besonders zu schützen. Ebenso muss Aufwand getrieben werden, um eine direkte Verbindung zwischen Internet und Firmennetz zu verhindern. Daher sind an dieser Stelle Lösungen zu bevorzugen, die eine entsprechende Sicherheitsarchitektur aufweisen. Das kann beispielsweise ein Separationssystem sein, welches VPN-Schlüssel bzw. den VPN-Zugang vom Rest des Systems abschottet. Eine andere Möglichkeit ist, Schlüsselmaterial und Kryptooperationen auf eine Smartcard auszulagern. In diesem Fall sollte aus Sicherheitsgründen der Internetzugang des Geräts durch den VPN-Tunnel und das Firmennetzwerk erfolgen, damit eine ungewollte Verbindung über das Gerät zwischen Internet und Firmennetzwerk ausgeschlossen bleibt. Hersteller, die keine Sicherheitsarchitektur zur Trennung vorsehen, sollten für erhöhten Sicherheitsbedarf von der Betrachtung ausgeschlossen werden.

Für das VPN muss eine Verschlüsselung mit starken Algorithmen und sicheren Parametern durchgeführt werden. Der Hersteller muss nachweisen können, dass er aktiv an der Sicherheit der eingesetzten Kryptographie arbeitet, sei es durch die Ablösung von unsicher gewordenen Algorithmen oder die Wahl passender Parameter. Sichere Mechanismen zur Authentifizierung müssen überall eingesetzt werden, wo es technisch möglich ist. Es sind Produkte zu bevorzugen, die, beispielsweise durch unabhängige Nachweise, eine hohe Sicherheit nachweisen können. Die starke Verschlüsselung, die im VPN vorliegen muss, garantiert die Integrität und Authentizität der durchgeleiteten Daten. Eine besonders wichtige Rolle nimmt hier jedoch die Verwaltung von Schlüsselmaterial ein. Hierbei sind Hersteller zu bevorzugen, die nachweisen können, dass sie einen einfachen und sicheren Schlüsseltausch ermöglichen und das Alter von eingesetzten Schlüsseln mitverfolgen. Auch hier gilt weiterhin, dass ein physikalischer Zugriff nur für autorisierte Personen möglich sein darf.

Bedrohung	Gegenmaßnahme	Stand der Technik
Unerwünschte Kopplung zwischen Firmennetz und Internet	Sichere Konfiguration des mobilen Geräts	Das mobile Gerät muss seine Konfiguration von einem Mobile Device Management System entgegen nehmen können und auf sichere Art verwalten.
Abfluss sensitiver Daten vom Mobilgerät	Sichere Architektur des Systems	Die kryptographischen Daten und Operationen finden auf einer Smartcard statt, so dass der direkte Zugriff vom mobilen Gerät ausgeschlossen ist. Zusätzlich gibt es eine abgeschottete Arbeitsumgebung auf dem Gerät, wo sensible Firmendaten sicher abgelegt werden können.

Tabelle 2: SdT für Sichere Anbindung mobiler User / Telearbeiter

3.2.1.2 VPN-Gateway

Ein VPN-Gateway ist ein Gerät, welches mehrere Netzwerke auf Schicht 2 oder 3 des OSI-Modells miteinander verbindet. Dabei verschlüsselt es die weitergeleiteten Daten und stellt damit einen sicheren Tunnel eines Netzwerks durch ein anderes Netz dar.

Als zentraler Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb dieser Geräte besondere Aufmerksamkeit zugute kommen. VPN-Gateways sollten nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Im besten Fall sind die Geräte ohne Umweg direkt vom Hersteller zu beschaffen. Vom Hersteller von sicheren VPN-Gateways erwartet man ein aktives Patchmanagement und schnelle Reaktion auf Sicherheitsprobleme, so dass man zu jedem Zeitpunkt bestmöglich geschützt ist. Ein Hersteller ohne ein entsprechendes Patchmanagement kann nicht als professionell angesehen werden und sollte von der Auswahl ausgeschlossen sein.

Die Schutzziele eines VPN-Gateways sind:

- Vertraulichkeit der durchgeleiteten Daten sicherstellen
- Integrität der durchgeleiteten Daten sicherstellen
- Authentizität der durchgeleiteten Daten sicherstellen
- Verfügbarkeit des Systems sicherstellen
- Verbindlichkeit der vom System generierten Logdaten garantieren
- Zurechenbarkeit der vom System generierten Accounting-Daten.

Ein VPN-Gateway muss die Vertraulichkeit der durchgeleiteten Daten sicherstellen. Dazu muss das Gateway eine Verschlüsselung mit starken Algorithmen und sicheren Parametern durchführen. Der Hersteller muss nachweisen können, dass er aktiv an der Sicherheit der eingesetzten Kryptographie arbeitet, sei es durch die Ablösung von unsicher gewordenen Algorithmen oder die Wahl passender Parameter. Sichere Mechanismen zur Authentifizierung müssen überall eingesetzt werden, wo es technisch möglich ist. Der Zugang zur Administration des VPN-Gateways muss durch verschiedene Maßnahmen besonders geschützt werden. Das beinhaltet einen verschlüsselten Zugang mit einer sicheren Authentifizierung (z.B. HTTPS bei einer Web-GUI, SSH für Konsolenzugang), aber auch ein besonderes Augenmerk des Herstellers auf die Sicherheit der Plattform selber, damit unbefugter Zugriff wegen technischer Schwächen ausgeschlossen ist. In der Regel behandelt ein VPN-Gateway sensiblen Datenverkehr an kritischen Stellen im Netzwerk. Eine VPN-Gateway, welches Backdoors enthält oder bei dem ein Softwarefehler zur Übernahme des VPN-Gateways selber führen kann, ist ein untragbares Risiko. Daher sind hier Produkte zu bevorzugen, die, beispielsweise durch unabhängige Nachweise, eine hohe Plattformsicherheit und einen hohen Selbstschutz nachweisen können. Durch Auflagen an die Einsatzumgebung muss weiterhin sichergestellt sein, dass physikalischer Zugriff zum VPN-Gateway nur für berechtigte Personen möglich ist.

Ebenso wie beim Schutzziel Vertraulichkeit ist zur Wahrung der Integrität und Authentizität der durchgeleiteten Daten die Integrität der Plattform entscheidend. Auch hier ist es wichtig, dass das VPN-Gateway auf einer besonders gehärteten Plattform aufgebaut ist, einen ausgezeichneten Selbstschutz hat und frei von Backdoors ist. Die starke Verschlüsselung, die ein VPN-Gateway vornimmt, garantiert die Integrität und Authentizität der durchgeleiteten Daten. Eine besonders wichtige Rolle nimmt hier jedoch die Verwaltung von Schlüsselmaterial ein. Hierbei sind Hersteller zu bevorzugen, die nachweisen können, dass sie einen einfachen und sicheren Schlüsseltausch ermöglichen und das Alter von eingesetzten Schlüsseln mitverfolgen. Auch hier gilt weiterhin, dass ein physikalischer Zugriff nur für autorisierte Personen möglich sein darf.

Um die Verfügbarkeit des VPN-Gateways sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software notwendig. Bei der Hardware muss der Hersteller nachweisen können, dass die Plattform entsprechend konzipiert wurde. Das beinhaltet zum Beispiel redundante Netzteile, RAID für Massenspeicher und eine Lüfterkonfiguration, bei der ein einzelner Ausfall nicht zu einem Ausfall des Systems führt. Da diese Maßnahmen alleine in der Praxis noch nicht ausreichen, um einen Ausfall der Hardware zu verhindern, muss die Möglichkeit des redundanten Betriebs gegeben sein (High Availability Konfiguration). Die Überwachung spielt ebenfalls eine zentrale Rolle, damit defekte Hardware rechtzeitig erkannt wird. Hier muss der Hersteller ein entsprechendes Monitoring, z.B. mittels SNMP anbieten. Auf der Softwareseite ist zum einen ein besonderes Augenmerk auf korrekte Implementierung notwendig, um eine Fehlfunktion auszuschließen. Hier sollten Hersteller bevorzugt werden, die besonderen Aufwand bei der Entwicklung in Form von Code-Reviews betreiben. Weiterhin sollte ein besonderer Augenmerk auf einem Schutz vor Denial-of-Service-Angriffen gelegt werden. Natürlich ist auch hier wieder eine besonders sichere Plattform eine wichtige Voraussetzung, sowie auch der kontrollierte physikalische Zugang.

Ein VPN-Gateway erzeugt Logdaten. Diese sind eminent wichtig, um Bedrohungen im eigenen Netzwerk zu erkennen und um Problemen nachgehen zu können. Dazu müssen diese Daten jedoch verbindlich sein. Ebenso ist eine Nachvollziehbarkeit von administrativen Änderungen und eine entsprechende Verbindlichkeit und Zurechenbarkeit dieser Logdaten wichtig. Dazu muss das VPN-Gateway Möglichkeiten bieten, solche Logdaten manipulationssicher abzulegen. Dies kann z.B. durch lokale append-only Logs gewährleistet werden, oder durch Support für externe Logserver oder SIEM-Systeme.

Bedrohung	Gegenmaßnahme	Stand der Technik
Abfluss des Schlüsselmaterials	Die Firewall muss Schlüsselmaterial besonders sicher verwalten.	Firewalls, die Schlüsselmaterial mit einer Smartcard verwalten, wobei die Schlüssel selber immer auf der Smartcard verbleiben.
Schwache Kryptographie	Ausschließliche Unterstützung starker Kryptoalgorithmen und Parameter	Ein modernes VPN-Gateway unterstützt Verfahren, die beim Schlüsseltausch Perfect Forward Secrecy (PFS) garantieren. Weiterhin bieten sie Unterstützung für Kryptographie mit elliptischen Kurven. Veraltete Algorithmen wie zum Beispiel RC4 werden nicht unterstützt.
Denial of Service: Durch Fehler oder Angriffe ist die Verfügbarkeit der Firewall gefährdet.	Die Firewall muss sich selbst durch technische Maßnahmen soweit möglich gegen Denial-of-Service-Angriffe schützen.	Eine moderne Firewall beinhaltet Mechanismen um sich gegen klassische Syn-Flood-Attacken zu schützen.
Angriff auf Firewall selbst.	Die Firewall muss nachweisbar mit einem besonderen Augenmerk auf Eigensicherheit entwickelt werden.	Eine Firewall, die einen besonders hohen Selbstschutz durch unabhängige Zertifizierungen nachweist.
Unberechtigter Login.	Die Firewall stellt sicher, dass nur berechtigte Administratoren sich einloggen dürfen, beziehungsweise dass nur berechtigte Clients sich verbinden dürfen.	Eine kryptographisch sichere Client-Authentifizierung an der Firewall wird unterstützt. Die Authentisierung der Administratoren an der Firewall findet nicht durch einfache Passworte statt, sondern durch Verfahren mit kryptographischen Schlüsseln. Alle externen Schnittstellen der Firewall sind besonders getestet und abgesichert, um unauthentifizierten Zugang auszuschließen.

Tabelle 3: SdT für VPN-Gateway

3.2.1.3 Router

Die Anforderungen an einen Router als zentrale Aufgabe sind das verlässliche Weiterleiten von Daten zwischen verschiedenen Punkten und der Zugriffsschutz durch unbefugte Dritte auf das Gerät selbst. Dabei gibt es verschiedene Angriffsvektoren, die berücksichtigt werden müssen. Als Rückgrat heutiger Infrastrukturen müssen hierbei verschiedene Aspekte berücksichtigt werden, um die Verlässlichkeit dieser Geräte zu keinem Zeitpunkt bewusst zu gefährden.

Die wichtigsten Gesamtziele für Router sind die Sicherstellung von verlässlichem Weiterleiten von Daten und der Zugriffschutz vor Unbefugten.

Bedrohung	Gegenmaßnahme	Stand der Technik
Manipulation der Konfiguration	Passwortschutz	Ausreichend sichere Zugangsdaten, die sicher aufzubewahren und nur durch befugte einsehbar sind. Vermeidung der Nutzung von Standardlogins, sowohl bei Benutzern als auch Passwörtern.
Angriff durch Exploits/Lücken	Installation neuer Software	Servicevertrag mit dem Hardwarehersteller und eine definierte minimale Reaktionszeit im Fall, dass eine schwerwiegende Lücke bekannt wird.
Verwundbarkeit aufgrund fehlender Updates	Austausch der Komponente gegen eine nicht verwundbare	Ausweichgräte anderer Hersteller, die nicht von diesen Sicherheitsproblemen betroffen sind.
Schutz vor Diebstahl	Gesicherter Aufstellungsort	Abschließbarer Raum mit überwachtem Zugang von verantwortlichen Administratoren
Angriff auf die Verfügbarkeit (DDoS)	Maßnahmen gegen Dienstblockaden	Filtern ungültiger Adressen nach RFC 2267, Einrichten von Sperrlisten in der Firewall
Zugriff durch Hintertüren und ungesicherte Schnittstellen	Schließen von offenen Ports und Schnittstellen	Schließen von bekannten und nicht erforderlichen Ports wie z.B. Telnet

Tabelle 4: SdT für Router

3.2.1.4 Layer3-VPN

Ein Layer 3 VPN bezeichnet die Verbindung zweier oder mehrerer Netze auf Layer 3 des OSI Modells. Die weitergeleiteten Daten werden verschlüsselt. Damit kann man zum Beispiel Firmenniederlassungen in verschiedenen Ländern über das Internet sicher und vertraulich miteinander verbinden. Im Gegensatz zu einem Layer 2 VPN werden hier weniger Daten übertragen, da Layer 2 Daten, wie z.B. Broadcasts, nicht übertragen werden. Im Gegenzug ist ein Layer 3 VPN dadurch nicht für alle Anwendungen transparent. Komplexe Topologien, wie z.B. On-Demand VPN-Verbindungen, sind teilweise nur, oder erheblich einfacher mit einem Layer 3 VPN umsetzbar. Dasselbe gilt für VPN-Konfigurationen mit sehr vielen Endpunkten. Ein Layer 3 VPN bentigt für jeden Teilnehmer einen VPN-Zugang. Oft wird eine Hub-and-Spoke VPN-Architektur eingesetzt, der zentrale Knoten wird in diesem Fall VPN-Konzentrator genannt. Es empfiehlt sich, ein Layer 3 VPN als Lösung vom Hersteller zu beziehen.

Als zentraler Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb eines Layer 3 VPN besondere Aufmerksamkeit zugute kommen. Eine Layer 3 VPN-Lösung sollte nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Vom Hersteller von sicheren VPN-Lösungen erwartet man ein aktives Patchmanagement und schnelle Reaktion auf Sicherheitsprobleme, so dass man zu jedem Zeitpunkt bestmöglich geschützt ist. Ein Hersteller ohne ein entsprechendes Patchmanagement kann nicht als professionell angesehen werden und sollte von der Auswahl ausgeschlossen sein.

Die Schutzziele eines Layer 3 VPNs sind:

- Vertraulichkeit der durchgeleiteten Daten sicherstellen
- Integrität der durchgeleiteten Daten sicherstellen
- Authentizität der durchgeleiteten Daten sicherstellen
- Verfügbarkeit des Systems sicherstellen
- Verbindlichkeit der vom System generierten Logdaten garantieren
- Zurechenbarkeit der vom System generierten Accounting-Daten.

Ein Layer 3 VPN muss die Vertraulichkeit der durchgeleiteten Daten sicherstellen. Dazu muss das Gerät eine Verschlüsselung mit starken Algorithmen und sicheren Parametern durchführen. Der Hersteller muss nachweisen können, dass er aktiv an der Sicherheit der eingesetzten Kryptographie arbeitet, sei es durch die Ablösung von unsicher gewordenen Algorithmen oder die Wahl passender Parameter. Sichere Mechanismen zur Authentifizierung müssen überall eingesetzt werden, wo es technisch möglich ist. Der Zugang zur Administration des Layer 3 VPNs muss durch verschiedene Maßnahmen besonders geschützt werden. Das beinhaltet einen verschlüsselten Zugang mit einer sicheren Authentifizierung (z.B. HTTPS bei einer Web-GUI, SSH für Konsolenzugang), aber auch ein besonderes Augenmerk des Herstellers auf die Sicherheit der Plattform der VPN-Geräte selber, damit unbefugter Zugriff wegen technischer Schwächen ausgeschlossen ist. In der Regel behandelt ein Layer 3 VPN sensiblen Datenverkehr.

Eine Layer 3 VPN, dessen Geräte Backdoors enthalten oder bei dem ein Softwarefehler zur Ãœbernahme der Geräte selber führen kann, ist ein untragbares Risiko. Daher sind hier Produkte zu bevorzugen, die, beispielsweise durch unabhängige Nachweise, eine hohe Plattformsicherheit und einen hohen Selbstschutz nachweisen können. Durch Auflagen an die Einsatzumgebung muss weiterhin sichergestellt sein, dass physikalischer Zugriff zu den VPN-Geräten nur für berechtigte Personen möglich ist.

Ebenso wie beim Schutzziel Vertraulichkeit ist zur Wahrung der Integrität und Aunthentizität der durchgeleiteten Daten die Integrität der Plattform entscheidend. Auch hier ist es wichtig, dass die VPN-Geräte auf einer besonders gehärteten Plattform aufgebaut sind, einen ausgezeichneten Selbstschutz haben und frei von Backdoors sind. Die starke Verschlüsselung, die ein Layer 3 VPN vornimmt, garantiert die Integrität und Authentizität der durchgeleiteten Daten. Eine besonders wichtige Rolle nimmt hier jedoch die Verwaltung von Schlüsselmaterial ein. Hierbei sind Hersteller zu bevorzugen, die nachweisen können, dass sie einen einfachen und sicheren Schlüsseltausch ermöglichen und das Alter von eingesetzten Schlüsseln mitverfolgen. Auch hier gilt weiterhin, dass ein physikalischer Zugriff nur für autorisierte Personen möglich sein darf.

Um die Verfügbarkeit des Layer 3 VPNs sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software notwendig. Bei der Hardware muss der Hersteller nachweisen können, dass die Plattform entsprechend konzipiert wurde. Das beinhaltet zum Beispiel redundante Netzteile, RAID für Massenspeicher und eine Lüfterkonfiguration, bei der ein einzelner Ausfall nicht zu einem Ausfall des Systems führt. Da diese Maßnahmen alleine in der Praxis noch nicht ausreichen, um einen Ausfall der Hardware zu verhindern, muss die Möglichkeit des redundanten Betriebs gegeben sein (High Availability Konfiguration). Die Überwachung spielt ebenfalls eine zentrale Rolle, damit defekte Hardware rechtzeitig erkannt wird. Hier muss der Hersteller ein entsprechendes Monitoring, z.B. mittels SNMP anbieten. Auf der Softwareseite ist zum einen ein besonderes Augenmerk auf korrekte Implementierung notwendig, um eine Fehlfunktion auszuschließen. Hier sollten Hersteller bevorzugt werden, die besonderen Aufwand bei der Entwicklung in Form von Code-Reviews betreiben. Weiterhin sollte ein besonderer Augenmerk auf einem Schutz vor Denial-of-Service Angriffen gelegt werden. Natürlich ist auch hier wieder eine besonders sichere Plattform eine wichtige Voraussetzung, sowie auch der kontrollierte physikalische Zugang.

Auf den Geräten eines Layer 3 VPN fallen Logdaten an. Diese sind eminent wichtig, um Bedrohungen im eigenen Netzwerk zu erkennen und um Problemen nachgehen zu können. Dazu müssen diese Daten jedoch verbindlich sein. Ebenso ist eine Nachvollziehbarkeit von administrativen Änderungen und eine entsprechende Verbindlichkeit und Zurechenbarkeit dieser Logdaten wichtig. Dazu müssen Möglichkeiten existieren, solche Logdaten manipulationssicher abzulegen. Dies kann z.B. durch lokale append-only Logs gewährleistet werden, oder durch Support für externe Logserver oder SIEM-Systeme.

Bedrohung	Gegenmaßnahme	Stand der Technik
Abfluss des Schlüsselmaterials	Die Geräte müssen Schlüsselmaterial besonders sicher verwalten.	Geräte, die Schlüsselmaterial mit einer Smartcard verwalten, wobei die Schlüssel selber immer auf der Smartcard verbleiben.
Schwache Kryptographie	Ausschließliche Unterstützung starker Kryptoalgorithmen und Parameter	Ein modernes Layer 3 VPN unterstützt Verfahren, die beim Schlüsseltausch Perfect Forward Secrecy (PFS) garantieren. Weiterhin bieten sie Unterstützung für Kryptographie mit elliptischen Kurven. Veraltete Algorithmen wie zum Beispiel RC4 werden nicht unterstützt.
Denial of Service: Durch Fehler oder Angriffe ist die Verfügbarkeit des VPNs gefährdet.	Die Geräte müssen sich selbst durch technische Maßnahmen soweit möglich gegen Denial of Service Angriffe schützen.	Eine modernes VPN-Gerät beinhaltet Mechanismen um sich gegen klassische Syn-Flood-Attacken zu schützen.
Angriff auf das VPN-Gerät selbst.	Ein VPN-Gerät muss nachweisbar mit einem besonderen Augenmerk auf Eigensicherheit entwickelt werden.	Ein VPN-Gerät, welches einen besonders hohen Selbstschutz durch unabhängige Zertifizierungen nachweist.
Unberechtigter Login.	Ein VPN-Gerät stellt sicher, dass nur berechtigte Administratoren sich einloggen dürfen, beziehungsweise dass nur berechtigte Clients sich verbinden dürfen.	Eine kryptographisch sichere Client-Authentifizierung wird unterstützt. Die Authentisierung der Administratoren am VPN-Gerät findet nicht durch einfache Passworte statt, sondern durch Verfahren mit kryptographischen Schlüsseln. Alle externen Schnittstellen des Geräts sind besonders getestet und abgesichert, um unauthentifizierten Zugang auszuschließen.

Tabelle 5: Stand der Technik für Layer3-VPN

3.2.1.5 Layer2-Encryption

Layer2-Verschlüsselung ist eine Sicherheitslösung, welche in bestimmten Anwendungsszenarien als Alternative zu Layer3-VPNs existiert. Sie wird statt auf IP-Pakete auf die Payload von Ethernet-Frames angewandt. Die IP-Header müssen nicht verarbeitet werden (Zeitgewinn) und es entsteht kein Verschlüsselungs-Overhead (Leitungsbandbreite steht voll zur Verfügung). Voraussetzung für den Einsatz ist ein Ethernet-basiertes Netzwerk (Punkt-zu-Punkt, Hub-Spoke oder vollvermascht) über eigene Kabel (Kupfer/Glasfaser) und sowie bei vermaschten Netzen WAN-Switches, oder von Netzwerkprovidern bereitgestellte Layer 2 Services (z.B. Carrier Ethernet-Dienste). Beim Einsatz dieser Netzwerk-Verschlüsselungstechnologie ist eine Änderung an der bestehenden Infrastruktur, insbesondere der IP-Routing-Konfiguration, nicht notwendig. Diese Art der Verschlüsselung ist für praktisch alle Netzwerk-Dienste und Anwendungen der OSI Schichten 3 und höher transparent und bringt keine Auswirkungen auf die Performance des Netzwerkes mit sich.

Typische Anwendungen für Layer 2 - Encryption sind

- Schutz von WAN-Backbone-Leitungen (auch international) und RZ-Anbindungen innerhalb des Corporate Networks oder zu vertrauenswürdigen Cloud Providern bzw. Colocation Providern
- Schutz von Campus-Backbone-Leitungen, die außerhalb von Gebäuden und über Drittgrundstücke verlaufen

- Einführung zentraler IT-Dienste, massive Desktop-Virtualisierungen, RZ-Konsolidierung, verteilte und redundante Speichersysteme (SAN/NAS)
- Hoher Anteil an kleinen und/oder echtzeit-relevanten IP-Paketen (z.B. VoIP, IoT, Smart Grid), bei denen IPsec-Overhead und Delay nicht akzeptabel sind

Bedrohung	Gegenmaßnahme	Stand der Technik
Mitschneiden und Auswertung massiver Datenmengen vom Netzwerk-Backbone oder der Cloud-Anbindung durch Sicherheitslücken in der Netzwerkhardware oder bei Netzwerkdienstleistern sowie nicht überwachte Erd- oder Seekabel und Richtfunk- oder Satellitenverbindungen	Sichern der WAN-Kommunikation mit Hilfe von Verschlüsselung. Einsatz verzögerungsarmer und bandbreitenneutraler Kryptolösungen für Layer2-WAN-Backbones und direkte Links (z.B. dark fiber, Satcom).	Synchronisation und Authentisierung der Krypto-Gegenstellen erfolgt automatisch. Der periodische Wechsel der kryptographischen Schlüssel erfolgt automatisch. Die Schlüsselerzeugung und -verteilung in den Layer 2 - Kryptogeräten erfolgt dezentral, vermeidet Schlüsselserver als single point of failure und erhöht damit die Verfügbarkeit des Netzes. BSI-zugelassene Lösungen sind verfügbar.

Tabelle 6: SdT für Layer2-Encryption

3.2.1.6 Datendiode

Eine Datendiode oder Guard ist ein Gerät, das ein sicheres mit einem weniger sicheren Netzwerk verbinden soll, so dass Daten nur in eine Richtung zwischen beiden Netzen fließen können. Das sichere Netz kann ein eingestuftes Netz sein im Sinne der Geheimschutzordnung. In diesem Fall ist in der Regel der Abfluss von Informationen aus dem Netz zu verhindern. Es kann aber auch ein Netzwerk an einem besonders schützenswerten Gerät sein. In diesem Fall soll nur der Abfluss von Daten möglich sein, aber keine Einflussnahme von außen. Dioden sind so konzipiert, dass es entweder gar keinen Rückkanal gibt, oder einen klar definierten und begrenzten Rückkanal. Das ist häufig wichtig, damit eine erfolgreiche Übertragung signalisiert werden kann.

Datendioden kommen in der Regel an Stellen zum Einsatz, wo ein Verlust der Eigenschaft, Daten unidirektional weiterzuleiten, eine große Gefährdung bedeutet. Daher muss dem Betrieb dieser Geräte besondere Aufmerksamkeit zugute kommen. Datendioden sollten nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Im besten Fall sind die Geräte ohne Umweg direkt vom Hersteller zu beschaffen. Vom Hersteller erwartet man einen Nachweis der konzeptionellen Sicherheit der Diode, zum Beispiel durch entsprechende Common Criteria Zertifizierung oder andere entsprechende Zertifizierung.

Die Schutzziele einer Datendiode sind:

- Vertraulichkeit, Integrität und Authentizität von Daten im sicheren Netz nicht gefährden
- Integrität der durchgeleiteten Daten sicherstellen
- Verfügbarkeit des Systems sicherstellen
- Verbindlichkeit der vom System generierten Logdaten garantieren

Um Vertraulichkeit, Integrität und Authentizität von Daten im sicheren Netz nicht zu gefährden muss die Datendiode nicht nur unidirektionalen Datenfluss sicherstellen, sondern auch eine Fehlkonfiguration ausschließen. Hier sind Dioden mit wenig Konfigurationsmöglichkeiten und einfacher Verkabelung zu bevorzugen. Der Zugang zur Administration der Datendiode soll im Betrieb gar nicht möglich sein. Um die Integrität der durchgeleiteten Daten sicherzustellen, bietet es sich an, eine Diode mit begrenztem Rückkanal in Erwägung zu ziehen, da Probleme bei der Datenübertragung hier auffallen. Bei Dioden muss es ein besonderes Augenmerk des Herstellers auf die Sicherheit der Plattform selber geben, damit unbefugter Zugriff wegen technischer Schwächen ausgeschlossen ist. In der Regel behandelt eine Datendiode sensiblen Datenverkehr an kritischen Stellen im Netzwerk. Eine Datendiode, welche Backdoors enthält oder bei der ein Softwarefehler zur Übernahme der Datendiode selber füh-

ren kann, ist ein untragbares Risiko. Daher sind hier Produkte zu bevorzugen, die, durch unabhängige Nachweise, eine hohe Plattformsicherheit und einen hohen Selbstschutz nachweisen können. Durch Auflagen an die Einsatzumgebung muss weiterhin sichergestellt sein, dass physikalischer Zugriff zur Datendiode nur für berechtigte Personen möglich ist.

Um die Verfügbarkeit der Datendiode sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software notwendig. Bei der Hardware muss der Hersteller nachweisen können, dass die Plattform entsprechend konzipiert wurde. Das beinhaltet zum Beispiel redundante Netzteile, RAID für Massenspeicher und eine Lüfterkonfiguration, bei der ein einzelner Ausfall nicht zu einem Ausfall des Systems führt. Da diese Maßnahmen alleine in der Praxis noch nicht ausreichen, um einen Ausfall der Hardware zu verhindern, muss die Möglichkeit des redundanten Betriebs gegeben sein (High Availability Konfiguration).

Die Überwachung spielt ebenfalls eine zentrale Rolle, damit defekte Hardware rechtzeitig erkannt wird. Hier muss der Hersteller ein entsprechendes Monitoring, z.B. mittels SNMP anbieten. Auf der Softwareseite ist zum einen ein besonderes Augenmerk auf korrekte Implementierung notwendig, um eine Fehlfunktion auszuschließen. Hier sollten Hersteller bevorzugt werden, die besonderen Aufwand bei der Entwicklung in Form von Code-Reviews betreiben. Natürlich ist auch hier wieder eine besonders sichere Plattform eine wichtige Voraussetzung, sowie auch der kontrollierte physikalische Zugang.

Eine Datendiode erzeugt Logdaten. Diese sind wichtig, um Bedrohungen im eigenen Netzwerk zu erkennen und um Problemen nachgehen zu können. Die Datendiode muss die Möglichkeiten bieten, die Logdaten manipulationssicher abzulegen. Dies kann z.B. durch lokale append-only Logs gewährleistet werden, oder durch Support für externe Logserver oder SIEM-Systeme.

Bedrohung	Gegenmaßnahme	Stand der Technik
Datenfluss in die falsche Richtung	Die Diode muss dies durch technische Maßnahmen verhindern.	Moderne Implementierungen haben eine Isolation zwischen Hardware und Software, zum Beispiel durch ein Mikrokernsystem. Die Architektur muss so sein, dass die Diodeneigenschaft durch kompakten, leicht reviewbaren Code erreicht wird.

Tabelle 7: SdT für Datendiode

3.2.2 Sicherer Internetzugang

3.2.2.1 Firewall

Eine Paketfilter-Firewall ist wie ein Router ein Gerät, welches mehrere Netzwerke auf der Netzwerkschicht des OSI-Modells miteinander verbindet. Zusätzlich bietet es Sicherheit vor schädlichem Netzwerkverkehr, indem es diesen analysiert und filtert. Es arbeitet auf Paketebene. Ein Application Level Gateway (ALG) leistet dasselbe, es arbeitet dabei jedoch auf der Anwendungsschicht des OSI-Modells und somit auf vollständigen Datenströmen. Eine Umgehung der Analyse ist nicht möglich. Ein ALG sollte für erhöhten Schutzbedarf immer in Erwägung gezogen werden.

Als zentraler Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb dieser Geräte besondere Aufmerksamkeit zugute kommen. Firewalls sollten nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Im besten Fall sind die Geräte ohne Umweg direkt vom Hersteller zu beschaffen. Vom Hersteller einer sicheren Firewalllösung erwartet man ein aktives Patchmanagement und schnelle Reaktion auf Sicherheitsprobleme, so dass man zu jedem Zeitpunkt bestmöglich geschätzt ist. Ein Hersteller ohne ein entsprechendes Patchmanagement kann nicht als professionell angesehen werden und sollte von der Auswahl ausgeschlossen sein.

Die Schutzziele einer Firewall sind:

- Vertraulichkeit der durchgeleiteten Daten sicherstellen
- Vertraulichkeit von auf der Firewall gespeicherten Daten sicherstellen
- Integrität der durchgeleiteten Daten sicherstellen
- Integrität der Firewallplattform sicherstellen
- Authentizität der durchgeleiteten Daten sicherstellen
- Verfügbarkeit des Firewallsystems sicherstellen
- Verbindlichkeit der von der Firewall generierten Logdaten garantieren
- Zurechenbarkeit der von der Firewall generierten Accounting-Daten gewährleisten

Eine Firewall muss die Möglichkeit bieten, die Vertraulichkeit der durchgeleiteten Daten sicherzustellen. Dazu muss sie Verschlüsselung mit starken Algorithmen und sicheren Parametern nicht nur ermöglichen, sondern forcieren. Sie muss die Möglichkeit bieten, dass Netzwerkzugriff nur nach einer kryptographisch sicheren Authentifizierung des Nutzers gestattet wird. Sichere Mechanismen zur Authentifizierung müssen überall eingesetzt werden, wo es technisch möglich ist. Der Zugang zur Administration der Firewall muss durch verschiedene Maßnahmen besonders geschätzt werden. Das beinhaltet einen verschlüsselten Zugang mit einer sicheren Authentifizierung (z.B. HTTPS bei einer Web-GUI, SSH für Konsolenzugang), aber auch ein besonderes Augenmerk des Herstellers auf die Sicherheit der Plattform selber, damit unbefugter Zugriff wegen technischer Schwächen ausgeschlossen ist. In der Regel kontrolliert eine Firewall sensiblen Datenverkehr an kritischen Stellen im Netzwerk. Eine Firewall, die Backdoors enthält oder bei der ein Softwarefehler zur Übernahme der Firewall selber führen kann, ist ein untragbares Risiko. Daher sind hier Produkte zu bevorzugen, die, beispielsweise durch unabhängige Nachweise, eine hohe Plattformsicherheit und einen hohen Selbstschutz nachweisen können. Ebenfalls wichtig ist die Möglichkeit, vertrauliche Daten die auf der Firewall anfallen, beispielsweise Logdaten mit Personenbezug, gezielt nur ausgewählten Personen zugänglich machen zu können. Das erfordert ein ausreichend mächtiges Rollenkonzept auf der Firewall. Durch Auflagen an die Einsatzumgebung muss weiterhin sichergestellt sein, dass physikalischer Zugriff zur Firewall nur für berechtigte Personen möglich ist.

Ebenso wie beim Schutzziel Vertraulichkeit ist zur Wahrung der Integrität und Authentizität der durchgeleiteten als auch lokal gespeicherten Daten die Integrität der Plattform entscheidend. Auch hier ist es wichtig, dass die Firewall auf einer besonders gehärteten Plattform aufgebaut ist, einen ausgezeichneten Selbstschutz hat und frei von Backdoors ist. Weitere Mechanismen sollten zum Einsatz kommen, um Datenintegrität und -authentizität sicherzustellen. Bei den meisten Protokollen bietet eine Verschlüsselung automatisch eine zugesicherte Integrität und Authentizität. Zusätzlich ist beim Einsatz von SSL eine gründliche Prüfung von SSL-Zertifikaten notwendig um Man-in-the-Middle Angriffe auszuschließen. Hierbei sind Hersteller zu bevorzugen, die Nachweisen können, dass sie oft und regelmäßig Pflegeaufwand für ihre SSL-Implementierung und die zugehörigen Zertifikate erbringen. Auch der Support für moderne Technologien wie z.B. Perfect Forward Secrecy oder OCSP ist hier wichtig. Das gilt für alle Stellen, wo Zertifikate eingesetzt werden können, nicht nur für den klassischen Web-Zugang. Ähnliches gilt für DNS, hier ist die Unterstützung von DNSSec besonders wichtig, um beide Schutzziele erfüllen zu können. Auch hier gilt weiterhin, dass ein physikalischer Zugriff nur für autorisierte Personen möglich sein darf.

Um die Verfügbarkeit der Firewall sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software notwendig. Bei der Hardware muss der Hersteller nachweisen können, dass die Plattform entsprechend konzipiert wurde. Das beinhaltet zum Beispiel redundante Netzteile, RAID für Massenspeicher und eine Lüfterkonfiguration, bei der ein einzelner Ausfall nicht zu einem Ausfall des Systems führt. Da diese Maßnahmen alleine in der Praxis noch nicht ausreichen, um einen Ausfall der Hardware zu verhindern, muss die Möglichkeit des redundanten Betriebs gegeben sein (High Availability Konfiguration). Die Überwachung spielt ebenfalls eine zentrale Rolle, damit defekte Hardware rechtzeitig erkannt wird. Hier muss der Hersteller ein entsprechendes Monitoring, z.B. mittels SNMP anbieten. Auf der Softwareseite ist zum einen ein besonderes Augenmerk auf korrekte Implementierung notwendig, um eine Fehlfunktion auszuschließen. Hier sollten Hersteller bevorzugt werden, die besonderen Aufwand bei der Entwicklung in Form von Code-Reviews betreiben. Weiterhin sollte ein besonderes Augenmerk auf einem Schutz vor Denial-of-Service Angriffen gelegt werden. Natürlich ist auch hier wieder eine besonders sichere Plattform eine wichtige Voraussetzung, sowie auch der kontrollierte physikalische Zugang.

Eine Firewall erzeugt Logdaten. Diese sind eminent wichtig, um Bedrohungen im eigenen Netzwerk zu erkennen und um Problemen nachgehen zu können. Dazu müssen diese Daten jedoch verbindlich sein. Ebenso ist eine Nachvollziehbarkeit von administrativen Änderungen und eine entsprechende Verbindlichkeit und Zurechenbarkeit dieser Logdaten wichtig. Dazu muss die Firewall Möglichkeiten bieten, solche Logdaten manipulationssicher abzulegen. Dies kann z.B. durch lokale append-only Logs gewährleistet werden, oder durch Support für externe Logserver oder SIEM-Systeme.

Applikationserkennung und Nutzerbezug: Next Generation Firewalls

Hoch vertrauenswürdige Paketfilter sind unverzichtbarer Bestandteil von Firewalls. Angesichts der verschwimmenden Grenzen zwischen Intranet und Internet, Web 2.0 Anwendungen und dem Internet der Dinge ist es erforderlich, Firewalls auch auf höheren OSI-Layern einzusetzen. APT-Angriffe arbeiten nicht mit statischen IP-Adressen und Portnummer-Protokoll-Zuordnungen, sondern suchen sich offene Ports, nutzen zunächst unverdächtige Protokolle, um sich nach Überwindung der stateful Inspection in verschlüsselten Tunneln zu verbergen. Firewalls, die jedes ein- und ausgehende IP-Paket mittels Deep Packet Inspection einem Stream zuordnen, das Anwendungsprotokoll verifizieren, den menschlichen oder maschinellen User bestimmen und darauf ihre Regeln anwenden, sind im Markt verfügbar und können bei gezieltem Einsatz von Whitelisting kritische Bereiche sehr effektiv schützen. Um Datenabfluss über verschlüsselte Tunnel von infizierten Endpoints ins Internet zu vermeiden, ist die Fähigkeit des Aufbrechens von TLS/SSL-Verbindungen durch die Firewall mit anschließender Regelanwendung unverzichtbar.

So können Next Generation Firewalls beispielsweise verschlüsselten Dateitransfer und VoIP-Telefonie vom Vertrieb zum Kunden über bestimmte Dienste erlauben, die gleiche Anwendung jedoch der LDAP-Gruppe der Kopier/Scan/Faxgeräte untersagen - unabhängig von IP-Adressen, benutzten Rechnern bzw. Servern und Ports. Energieversorger können damit sicherstellen, dass in ihren Steuernetzen nur ausdrücklich erlaubte IoT-Steuerungsinformationen ausgetauscht werden können und selbst von eventuell infizierten Netzelementen und Endpoints keine Gefahr für ihre angeschlossene Office-IT ausgeht.

Bedrohung	**Gegenmaßnahme**	**Stand der Technik**
Datenabfluß von infizierten Endpoints aus dem internen Netz an externe C&C-Server der Angreifer	Einsatz von Firewalls mit Anwendungs- und User-Erkennung und ggf. Whitelisting	Deep Packet Inspection, vollständige und permanente Protokollvalidierung, User-bezogene Firewall-Regeln, Aufbrechen aller TLS/SSL-Verbindungen und Regelanwendung auf den unverschlüsselten Datenverkehr
Infektion von Arbeitsplatzrechnern und internen Servern durch Malware, die über verschlüsselte Verbindungen (z.B. HTTPS) heruntergeladen wird	Firewall bricht verschlüsselte Tunnel auf, und überprüft die Inhalte mittels Virenscanner, IDS/IPS usw.	Die Firewall verifiziert zuerst die Internet-Serverzertifikate über Trust Center. Sie rollt ihr eigenes HTTPS-Proxy-Zertifikat auf die Browser der Endpoints aus und baut sowohl zum Internet-Server als auch zum internen Endpoint je einen Tunnel mit gleichem Zertifikat auf. Innerhalb der Firewall liegt der Datenstrom im Klartext vor und kann auf Malware überprüft werden.
Netzkopplung: Trotz korrekter Konfiguration gibt es eine ungewollte Verbindung zwischen getrennten Netzen	Die Firewall muss eine ungewollte Netzkopplung durch technische Maßnahmen verhindern.	Ein Application Level Gateway terminiert Verbindungen und bietet hier den höchsten Schutz.
Tunnel: Durch fehlende Protokollanalyse kann leicht ein Tunnel durch die Firewall hergestellt werden.	Die Firewall muss durch gründliche Protokollanalyse eine hohe Hürde für die Erstellung eines Tunnels darstellen	Ein Application Level Gateway analysiert Daten auf Applikationsebene. Viele Möglichkeiten, einen Tunnel aufzubauen werden damit verhindert.

Fehlkonfiguration: Durch falsche Konfiguration wird die Firewall unsicher.	Die Firewall muss dem Administrator Hilfen anbieten, die eine Fehlkonfiguration unwahrscheinlich machen und ihm eine klare Sicht auf die aktive Konfiguration bieten.	Die Firewall bietet umfangreiche Syntax- und Semantikprüfungen, sowie teilautomatisierte Vorgänge (Wizards) um einfach korrekte Einstellungen vornehmen zu können. Die aktive Konfiguration ist einfach ersichtlich. Es existiert die Möglichkeit, einen read-only Account zur Prüfung der Konfiguration zu haben (Revisor). Konfigurationsänderungen werden nachvollziehbar und auf sichere Art geloggt.
Durchlassen von Malware: Die Firewall lässt durch mangelnde Analyse oder durch Umgehung der Analyse bösartige Daten durch.	Die Firewall muss durch gründliche Protokollanalyse eine Umgehung unmöglich machen. Die Firewall muss durch Normalisierung von Daten eine Interpretationshoheit herstellen. Die Firewall muss gründliche Analysen durchführen.	Application Level Gateways zeichnen sich durch besonders gründliche Protokollanalyse aus. Eine Firewall muss immer der Sicherheit Vorzug vor anderen Eigenschaften bieten. Wenn die Firewall bei mehrdeutigen Daten keine Interpretationshoheit herstellen kann, muss die Verbindung geschlossen werden. Firewalls, die Daten normalisieren, bieten besonders hohe Sicherheit.
Verlust der Vertraulichkeit: Daten, die vertraulich sind, können von Unberechtigten gelesen werden.	Die Firewall muss besondere technische Maßnahmen beinhalten, um Man-in-the-Middle-Angriffe und Umgehung oder Schwächung von Kryptographie (zum Beispiel SSL Downgrade, SSL Strip) zu verhindern. Es dürfen nur moderne, sichere Kryptoalgorithmen und Kryptosysteme eingesetzt werden. Es müssen zeitgemäße Parameter gewählt werden. Schlüsselmaterial muss besonders geschützt werden.	Eine Firewall muss alles genannte Umsetzen. Sie muss besonders gründlich bei der Zertifikatsprüfung sein und häufig durch Updates auf den neuesten Stand gebracht werden, was den Bereich Kryptographie betrifft.
Kommunikation mit falschem Partner: Durch gefälschte Zertifikate, DNS Poisoning, Man in the Middle Angriffen oder anderen Angriffen wird eine Kommunikationsbeziehung zum falschen Partner aufgebaut.	Die Firewall muss durch moderne technische Mechanismen sicherstellen, dass mit dem richtigen Partner kommuniziert wird.	Die Firewall bietet Unterstützung für eine gründliche Zertifikatsvalidierung, bei der Fehler zum Abbruch der Verbindung führen. Problematische CA-Zertifikate werden nach kurzer Zeit von der Firewall entfernt. Die Firewall bietet Möglichkeiten, die DNS-Auflösung präzise zu konfigurieren und bietet Unterstützung für DNSSec.
Denial of Service: Durch Fehler oder Angriffe ist die Verfügbarkeit der Firewall gefährdet.	Die Firewall muss sich selbst durch technische Maßnahmen soweit möglich gegen Denial-of- Service-Angriffe schützen.	Eine moderne Firewall beinhaltet Mechanismen um sich gegen klassische Syn-Flood-Attacken zu schützen. Darüber hinaus enthält sie Mechanismen, um auf andere Angriffsformen (zum Beispiel Resource Exhaustion Attacken) zu reagieren. Insbesondere

		gegen DDoS braucht es jedoch zusätzliche Mechanismen, die den Traffic vor der Firewall aufteilen und so Angriffe abpuffern.
Angriff auf Firewall selbst.	Die Firewall muss nachweisbar mit einem besonderen Augenmerk auf Eigensicherheit entwickelt werden.	Eine Firewall, die einen besonders hohen Selbstschutz durch unabhängige Zertifizierungen nachweist.
Keine Nachvollziehbarkeit von Netzereignissen.	Die Firewall stellt eine Nachvollziehbarkeit sicher.	Die Firewall hat ein umfassendes Loggingkonzept und unterstützt Logserver und SIEM-Systeme. Alle wichtigen Netzereignisse werden protokolliert und bei Problemen oder Bedrohungen geeignet gewarnt.
Falsche Zuordnung von Logdaten zu Verursachern.	Die Firewall stellt sicher, dass eine Zuordnung möglich ist.	Die Firewall hat ein revisionssicheres Logging und unterstützt Logserver und SIEM-Systeme. Eine Client-Authentifizierung an der Firewall wird unterstützt. Eine Remote-Authentisierung der Administratoren der Firewall wird unterstützt. Entsprechende Authentisierungen werden durchgängig aufgezeichnet.
Unberechtigter Login.	Die Firewall stellt sicher, dass nur berechtigte Administratoren sich einloggen dürfen, beziehungsweise dass nur berechtigte Clients sich verbinden dürfen	Eine kryptographisch sichere Client-Authentifizierung an der Firewall wird unterstützt. Die Authentisierung der Administratoren an der Firewall findet nicht durch einfache Passworte statt, sondern durch Verfahren mit kryptographischen Schlüsseln. Alle externen Schnittstellen der Firewall sind besonders getestet und abgesichert, um unauthentifizierten Zugang auszuschließen.
Unberechtigte Änderungen an der Konfiguration.	Die Firewall verhindert unberechtigte Änderungen an der Konfiguration.	Die Firewall unterstützt verschiedene Rollen mit entsprechenden Rechten für die Administration. Die Konfiguration ist nur mit enstprechenden Rechten zu ändern. Konfigurationsänderungen werden durchgängig und nachvollziehbar aufgezeichnet.

Tabelle 8: SdT für Firewall

3.2.2.2 Intrusion Detection System/ Intrusion Prevention System

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) ist ein IT-System zur Erkennung und Protokollierung von Anomalien im Netz. Das Ziel beider Systeme ist es das Eindringen und Verteilen von Schadsoftware möglichst vor Schadenseintritt zu erkennen. Im Gegensatz zum IDS, welches ausschließlich Informationen von anomalem Verhalten anzeigt und Alarme generiert, kann ein IPS auch selbsttätig eingreifen. Damit soll die weitere Ausbreitung von Schadsoftware über das

Netz verhindert werden. Dabei ist zu beachten das z.B. bei Industrie- und Produktionsanlagen oder vollautomatisierten Bestell-/Lieferprozessen sowie Meldungs- und Sicherheitsprozessen (u. a. Brandschutz) ein direkter Eingriff durch ein IPS die Verfügbarkeit unmittelbar beeinflusst.

Eine Unterscheidung besteht zwischen Netz- und Host-basierten IDS / IPS. Netz-basierte IDS / IPS nutzen eigene Komponenten und/oder die Netzinfrastruktur, um die Kommunikationen zu überwachen. Host-basierte IDS und IPS nutzen Informationen von IT-Systemen (über Software-Agenten, Logfile-Auswertungen usw.). In der verteilten Systemarchitektur müssen die Daten verschlüsselt und signiert ausgetauscht und gespeichert werden.

Das Erkennen basiert auf zwei unterschiedlichen Verfahren. Beim sogenannten "Pattern Matching" wird bereits bekannte Schadsoftware auf Basis von Mustern (Signaturen) erkannt. Neue Angriffsmuster müssen schnellstmöglich analysiert und deren Signaturen sofort manipulationssicher eingepflegt werden, weil darauf basierende Angriffe ansonsten unerkannt bleiben.

Die zweite Methode basiert auf dem Erkennen von Änderungen im Kommunikationsmuster von Netzkomponenten durch einen Angriff. Jede Kommunikation, die sich außerhalb eines erwarteten Datenverkehrsprofils bewegt, wird als Anomalie bewertet. Dadurch können auch neue Angriffe erkannt werden. Eine Pflege von Angriffsmuster in einer Datenbank entfällt. Jedoch muss definiert sein, welche Kommunikationsmuster zum normalen Datenverkehr gehören.

Ein IDS muss im Falle der Erkennung einer Schadsoftware bzw. bei Abweichungen des validen Sollzustandes der Kommunikation entsprechende Ereignismeldungen automatisiert erzeugen. Alle Ereignismeldungen sollen zu Analysezwecken in einem ausreichend langen Zeitraum im System vorgehalten werden und bei Bedarf in einem offenen bzw. standardisierten Format exportierbar sein. Die Ereignismeldungen müssen alle relevanten Informationen zur Ereignisanalyse und Initiierung von Gegenmaßnahmen wie z.B. erkannte Signatur bzw. auffällige Kommunikationsverbindung enthalten. Die Alarmmeldungen sollen auf der Managementkonsole vordergründig erkennbar sein, als Mail an definierte Accounts gesendet sowie über eine Export-Schnittstelle einem übergreifenden Alarmierungssystem (siehe SIEM) zur Verfügung gestellt werden können.

Ein IPS muss zusätzlich selbsttätig jede Kommunikation im Netzwerk blockieren, die einem Angriffsversuch zugrunde liegt. Dabei ist zu gewährleisten, dass möglichst keine Kommunikation verhindert wird, die keinem Angriffsverhalten eindeutig zuzuordnen ist.

Ein IDS/IPS muss Komponenten zur Verfügung stellen, um die gesamte Kommunikation an Netzübergängen und/oder innerhalb von IT-Systemen (Hosts) zu analysieren, die sich für einen stabilen Betrieb nach einem temporären Ausfall selbsttätig resynchronisieren. Es darf keine unerwünschte Kommunikation der IDS / IPS-Komponenten zu Dritten zugelassen werden. Außerdem sollten alle IDS und IPS Komponenten nicht erkennbar sein, den Datenverkehr nicht beeinflussen, keine Dienste anbieten sowie selbst geschützt sein.

Es sollen symmetrische und asymmetrische Algorithmen sowie Signaturen- und Schlüssellänge der genutzten Zertifikate nach den aktuellen Empfehlungen des BSI zum Einsatz kommen.

Bedrohung	**Gegenmaßnahme**	**Stand der Technik**
Ausbreitung von Schadsoftware (z.B. Advanced Persistent Threats)	• Kontinuierliche Überwachung der Netzkommunikation und / oder Verhalten der IT-Systeme. • Alarmierung bei Anomalien • Unterbrechung von Verbindungen und Systemprozessen.	Kontinuierliches Scannen (aktiv und/oder passiv) von Kommunikation und IT-Systemen (z.B. über SNMP, Syslog, NetFlow_IPFIX oder herstellerspezifische Agenten) Erkennen von Abweichung zum statistischen Normalverhalten Protokoll Inspektion (u.a. TCP/IP, UDP, IPsec, ICMP, ARP, HTTP, FTP) Dynamische Änderung von

		Zugriffsrechten (nur IPS), direkt im System oder indirekt über Onlineschnittstellen in anderer Netzinfrastruktur- und IT-Systemen (z.B. TCP reset, DNS, FW Regeln) Alarmierungen per Mail oder direkter Schnittstellenkopplung
Unberechtigter Zugang zu IT-Systeme	Hier insbesondere Unterbrechung von Verbindungs- und Login-Versuchen	Erkennen von wiederholten nicht-erfolgreichen Verbindungsaufbauten • in den Protokollheadern, • durch Schlüsselworte (Login, User, Account) • neue Verbindungen zu weiteren IT-Systemen
Manipulation über externe Kommunikation (z.B.zu Command & Control Servern)	…hier insbesondere Unterbrechung von Verbindungen zu externen blackgelisteten Services und Systemen.	Trennen der externen Verbindungen (IPS). Initiierung von Konfigurationsänderungen in Netz- und IT-Komponenten (online)
Unberechtigter Informationsabfluss	… hier insbesondere Unterbrechung von erhöhtem Datenvolumen nach extern.	Überwachung des externen Datenaufkommens Speicherung und Analyse von Statistiken des Datenaufkommens Konfigurierbare Schwellwerte

Tabelle 9: SdT für Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)

Quellen:
1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile
2. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05071.html

3.2.2.3 Sicherer Browser/Exploit Protection

Die Verwendung des Internets ist aus dem heutigen Arbeitsalltag - allein schon zur Informationsgewinnung - kaum mehr wegzudenken. Gleichzeitig wird der PC zur Verarbeitung von vertraulichen Informationen verwendet, seien dies personenbezogene oder betriebsinterne, unternehmenskritische Daten. Dem immensen Nutzen des Internet stehen seine sich fortwährend wandelnden Gefahren gegenüber. Die Browser-Entwicklung der letzten Jahre kann neben allen funktionalen und Komfortfortschritten vor allem auch als ein beständiger Wettlauf im Kampf gegen unterschiedliche Angriffsszenarien verstanden werden.

Spätestens seit das Internet mit "Web 2.0" aktiv wurde, ist die Gefahren - Nutzen Balance verloren gegangen. "Aktive Inhalte" sind aus heutigen Webseiten nicht mehr wegzudenken, moderne Webseiten sind von vollwertigen nativen Anwendungen kaum noch zu unterscheiden. Programmierschnittstellen wie JavaScript, Java, ActiveX oder Flash erlauben auch den Zugriff auf den PC des Benutzers, etwa auf das Dateisystem oder eine angeschlossene Kamera oder Mikrophone. Trojaner und Viren können damit diese neuen mächtigen Werkzeuge zum Zugriff auf vertrauliche Daten missbrauchen.

Technisch bedeuten Aktive Inhalte, dass Programmcode, welcher in die Webseiten integriert ist, heruntergeladen und im Browser ausgeführt wird. Fremder, externer Programmcode wird also auf dem Arbeitsplatz PC mitten in der internen Infrastruktur ausgeführt. Enthält dieser Programmcode Schadsoftware, so gelangt diese ebenfalls zur Ausführung. Dabei ist die Ausführung der Aktiven Inhalte

völlig transparent für den Benutzer und geschieht bereits beim Laden der Webseite ohne weitere Interaktion (wie beispielsweise das Öffnen von Anhängen in Emails). Somit besteht schon beim Ansehen von Webseiten die Gefahr der Infektion mit Schadcode. Dies wird mit "Drive By Download" bezeichnet und ist heute eines der größten Einfallstore für die Infektion mit Schadsoftware.

Wichtig ist hier, dass Schadsoftware nicht nur von nicht vertrauenswürdigen Webportalen verbreitet wird, sondern oftmals ohne Wissen der Betreiber auf die Webserver von vertrauenswürdigen Seiten gelangen, beispielsweise über vermietete Reklameflächen oder Sicherheitslücken in den Webservern. Es ist nicht unüblich, dass beim Anzeigen der Startseite eines Nachrichtenportales mehr als 50 Webserver kontaktiert werden, welche alle gegebenenfalls offene Sicherheitslücken haben könnten.

Bekannte gewordene Sicherheitslücken werden üblicherweise im Laufe der Zeit durch Patches geschlossen, die aber zunächst entwickelt und dann auch von den Betreibern der Webseite eingespielt werden müssen.

Dies gilt ebenso für Sicherheitslücken in Browsern und Betriebssystemen. Auch Schutzprogramme wie Virenchecker müssen regelmäßig aktualisiert werden, um wirksam gegen bekannte Schadsoftware zu sein. Im besten Falle, wenn alle Webserver und Arbeitsplatzrechner auf dem aktuellen Patchlevel sind, ist man vor bereits bekannter Schadsoftware geschützt. Gegen neuartige Angriffe, sogenannte "Zero Day Exploits" ist man aber auch in diesem Falle ungeschützt.

Der Gefahr, die durch Aktive Inhalte ausgeht, sind sich auch die Browserhersteller bewusst. Immer wieder versuchen sie durch neue Schutzmechanismen die möglichen negativen Auswirkungen von Schadsoftware einzudämmen. Sowohl die im Browser und im Betriebssystem eingebauten Schutzkonzepte als auch klassische Sicherheitslösungen greifen aber dauerhaft zu kurz. Beispielsweise basiert die Abwehr in Virenscannern auf der Erkennung von bekanntem Code bzw. bei moderner verhaltensbasierter Schadsoftware-Erkennung auf Code mit bekannten auffälligen Verhaltensmustern. Die jüngere Vergangenheit hat deutlich bewiesen dass solche Techniken wirkungslos gegenüber Angriffen auf neue Sicherheitslücken in den Systemen sind. Derartige Sicherheitslösungen hinken also systematisch bekannten Angriffen hinterher.

Unternehmen und Behörden stehen deshalb heute vor einem Dilemma. Aus dem heutigen Arbeitsalltag ist die Nutzung des Internet nicht mehr wegzudenken. Da aber die eingebauten Sicherheitskonzepte zu kurz greifen, ist die Nutzung des Internet gleichzeitig eine große Gefahr für den operativen Betrieb des Unternehmens oder Behörde.

Um dieses Dilemma grundsätzlich zu lösen bedarf es neuer Innovativer Sicherheitskonzepte mit einer neuen Grundstrategie: Nicht der Browser wird abgesichert, sondern der Arbeitsplatz PC und das Intranet wird vor dem Browser geschützt. Auch im Falle eines erfolgreichen Angriffs auf den Browser sorgen Isolationsmechanismen dafür, dass die Schutzziele nach wie vor erfüllt werden. Die zentralen Schutzziele sind dabei der Schutz von vertraulichen Daten und der Schutz der internen Infrastruktur (Intranet). Beide Systeme adressieren das Problem mit der gleichen Grundstrategie:

Bedrohung	Gegenmaßnahme	Stand der Technik
Infektion des Arbeitsplatzrechners durch das Surfen auf manipulierten Webseiten mit maliziösen aktiven Inhalten	Trennung der Ausführungsumgebung des Browsers von der Anzeige am Arbeitsplatz-PC. Entweder durch zentrales Ausführen aller Browser-Instanzen einer Organisation auf vorgelagerten Servern in der DMZ, oder durch lokale Ausführung in einer virtuellen Maschine gekapselter und auf gehärtetem Gast-Betriebssystem laufender Browser.	Einsatz eines zentralen ReCoBS-Systems oder einer dezentralen Lösung, die den Browser in einer lokalen virtuellen Maschine und einem darin laufenden gehärteten Betriebssystem ausführt

Tabelle 10: SdT für Sicherer Browser / Exploit Protection

Quellen:
1. Bundesamt für Sicherheit in der Informationstechnik. (2008). Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS). Bonn.
2. Bundesamt für Sicherheit in der Informationstechnik. (2006). Remote-Controlled Browsers System (ReCoBS) - Grundlagen und Anforderungen. Bonn.

3.2.2.4 Webfilter

Webserver sind einer der Hauptverbreitungswege für Malware. Zum Einsatz kommen dabei infizierte Webserver, bei denen der Betreiber am Angriff nicht direkt beteiligt ist. Diese Websites werden vom Benutzer normal angesurft. Ein großer Prozentsatz von Webservern weist permanent Sicherheitslöcher auf und kann darüber durch Hacker angegriffen werden, die dann Malware, meist sog. Root-Kits auf dem System hinterlegen.

Zusätzlich werden von Angreifern speziell bereitgestellte Webserver eingesetzt, bei denen oft ein anderer Webserver imitiert wird. In jedem Fall wird Malware beim Besuch einer infizierten Website vom Benutzer unbemerkt auf das lokale System geladen und aktiviert (Drive-by-Downloads).
Beim sog. Phishing werden gefälschte Kopien bekannte Webseiten mit dem Ziel bereitgestellt, sensible Informationen vom Benutzer abzugreifen, meist Benutzername und Kennwort, zusätzlich z.B. Bankdaten, Kreditkartendaten, Adressdaten usw.

Oft wird die eigentliche Zieladresse (URL mit Schadcode bzw. die URL der infizierten oder gefälschten Seite) durch automatische Weiterleitungen verschleiert, gerne auch mehrfach und über sog. URL-Verkürzer (Bit.ly, Tiny URL u.a.) - diese sind aber am eigentlichen Angriff nicht beteiligt. Benutzer werden durch gezielt platzierte Links in E-Mails, sozialen Medien u.ä. auf die speziell bereitgestellten Websites gelenkt.

Für den Schutz vor solchen Angriffen werden u.a. Webfilter eingesetzt. Webfilter schützen vor diesen Angriffen durch Sperre der betroffenen Websites und Analyse der von Websites geladenen Daten auf Schadcode. Webfilter können zentral betrieben werden, als Webfilter in der Cloud oder als Appliance on Premise, oder als lokal auf dem System des Endnutzers betriebene Software.

Webfilter sollten mindestens folgende Anforderungen erfüllen:

- Blockieren von potentiell oder tatsächlich gefährlichen URLs, z.B. an Hand von Datenbanken
- Scannen des Datenverkehrs auf Schadcode; dazu auch Möglichkeit zum Aufbrechen verschlüsselter Verbindungen (https)
- Für mobile Systeme (Laptops usw.) muss die Funktion unabhängig vom Standort und Netzanschluss gegeben sein.

In größeren Organisationen ist die Erfüllung folgender Anforderungen sinnvoll:

- Zentrale Einrichtung und Verwaltung benutzer- oder gruppenspezifischer Policies (unterschiedliche Profile für unterschiedliche Benutzer)
- Benutzererkennung und Umsetzung der Policies.

Bedrohung	Gegenmaßnahme	Stand der Technik
Infizierung des lokalen Systems durch Malware über einen infizierten Webserver (Drive-by Downloads)	Sperrung des Zugriffs auf als gefährlich erkannte Websites. Analyse übertragener Daten auf Malware.	Einsatz eines Webfilters in aktueller Version
Abgreifen sensibler Informationen von Benutzern über gefälschte Webserver (Phishing)	Sperrung des Zugriffs auf als gefährlich erkannte Websites.	Einsatz eines Webfilters in aktueller Version

Tabelle 11: SdT für Webfilter

3.2.2.5 Virtuelle Schleuse

IT-Sicherheit wird durch die Einschränkungen der Handlungsmöglichkeiten oft als Business-Verhinderer wahrgenommen - "von zu Hause" bekannte Funktionen stehen im Büro aus Sicherheitsgründen nicht zur Verfügung. Häufig werden für diese nicht erlaubten Funktionen dann Schleusenrechner zur Verfügung gestellt, die bewusst "entnetzt" sind. So gibt es dann Internet-Schleusenrechner, USB-Schleusen, Medien-Schleusen für Kameras usw. Die Entnetzung hat aus Sicht der IT-Sicherheit Vorteile, praktisch benötigt der Anwender häufig aber Daten aus den entnetzten Schleusenumgebungen in seiner Arbeitsumgebung.

Die Virtualisierung von potentiell schädlichen Inhalten und unbekanntem Code alleine ist als Lösung jedoch zu kurz gegriffen. Erst wenn die Arbeitsergebnisse aus der virtualisierten Umgebung sicher in die Prozesse der Produktionsumgebung eingebunden werden und die Aktivitäten in der virtualisierten Welt nahtlos und barrierefrei automatisch für den Anwender eingebunden sind, schafft das effiziente sichere Arbeitsumgebungen, die gleichzeitig prüfbar geschützt sind. Dazu müssen Virtualisierung, Applikations- und Contentkontrolle sowie Verschlüsselung geeignet kombiniert werden und können dann die sichere und flexible Alternative zu rigiden Verboten oder physikalisch getrennten Systemen darstellen. Durch ein Remote-Controlled-Application-System (kurz ReCAppS) werden sicherheitskritische Aktionen in der produktiven Umgebung sicher erkannt und dann automatisch in eine virtualisierte Umgebung ausgelagert.

Effiziente Arbeitsumgebungen benötigen aus Sicht des Anwenders die Möglichkeit, auch kritische Aktionen sofort durchzuführen. In einer "Remote Controlled Session" der ReCAppS Umgebung kann der Anwender alle aktiven Inhalte nutzen und beliebige z.B. Makro-behaftete Dateien einsehen, sowie kritische Aktionen durchführen, ohne die produktive Umgebung zu gefährden. Kritisch ist etwa das Anklicken einer problematischen URL, das Herunterladen von ausführbaren Elementen aus dem Internet, das Anstecken eines fremden nicht in Echtzeit geprüften Peripheriegerätes oder das Installieren einer unbekannten Anwendung von einem fremden Datenträger. Inhalte werden sowohl auf dem Remote Controlled System als auch auf dem produktiven Client-System des Anwenders nach den zentralen Vorgaben kontrolliert, so dass kein Schadcode ins interne Netz gerät. Wesentlich ist hier, dass eine Prüfung auf Schadcode wie sie von Anti Viren Programmen durchgeführt wird, nicht ausreicht, da jeder potentielle Code der fremd und nicht positiv authentisiert ist erkannt werden muss und in der virtuellen Schleuse auszuführen ist.

Für den sicheren Betrieb von Browsern hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit ReCoBS ein Konzept vorgestellt, welche das sichere Surfen durch Auslagern des Browsers in die sogenannte demilitarisierte Zone (DMZ) über eine Trennung von Anzeige und Ausführung. ermöglicht. Die ReCAppS Lösungen nutzen dieses Verfahren nicht nur zum sicheren Betrieb des Browsers sondern für alle ungeplanten, sicherheitskritischen Aktionen.

Ein Remote-Controlled-Application-System ergänzt damit das BSI-Verfahren ReCoBS und kann also für alle unbekannten oder ungeplanten sicherheitskritischen Aktionen verwendet werden. Dieses Verfahren erweitert ReCoBS auch um einige in der Praxis wesentliche Elemente. Arbeitsergebnisse, die der Anwender in der virtuellen Schleuse erstellt hat, können über spezielle abgesicherte Kanäle ausgedruckt werden, ohne dass der Ausdruck selbst wieder eine Angriffsmöglichkeit darstellt. Neben dem Drucken unterstützen ReCAppS auch den Datentransport für den Anwender vollautomatisch. Der Datentransport wird durch eine automatische Datenkonversion abgesichert, so dass nur sichere "Bilder" aber keine ungeprüften Makros oder Ähnliches transportiert werden. Gegenüber Standardschleusen wie z.B. Janus und physikalisch getrennten Netzen, die mittels einer "Drehstuhlschnittstelle" gekoppelt sind hat diese Lösung einen entscheidenden Vorteil. Der an der Drehstuhlschnittstelle verwendete oder in dem Schleusensystem als "geprüft" markierte Datenträger kann selbst von Schadcode wie BadUSB befallen sein. Dadurch, dass es in ReCAppS keinen Kontakt des Datenträgers zum produktiven System gibt fällt ein wesentlicher Angriffsvektor weg. Auch Angriffe wie .lnk oder ähnliche sind dadurch eliminiert.

In der virtuellen Umgebung hat der Anwender alle nötigen Rechte - sogar administrative Rechte sind problemlos möglich, ohne die produktive Umgebung zu gefährden. Nur dann ist das Benutzererlebnis wie gewünscht. Natürlich kann der Anwender auch mit lokalen Admin-Privilegien die Sicherheitseinstellungen nicht nachhaltig verändern, da beim nächsten Start zurückgesetzt wird.

Die virtualisierte Umgebung muss in Echtzeit automatisch geeignet ausgewählt werden und ohne Benutzerinteraktion muss die Benutzeraktivität nahtlos weitergeführt werden. Optionen der Lokation der virtuellen Umgebung sind:

- hinter einer Firewall im Backbone,
- in der DMZ,
- lokal für Fremdanwendungen unterwegs bei geringer Bandbreite

Gut ist es, wenn alle Virtualisierungsumgebungen unterstützt werden, da dadurch das Unternehmen seine Lizenzen und Expertise weiter nutzen kann.

Quellen: BSI-Standards zur Internet-Sicherheit: Remote-Controlled Browsers System (ReCoBS). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf;jsessionid=83B213ABBA67FF2026B1994EEFF2A974.2_cid286?__blob=publicationFile&v=1 (abgerufen am 11.01.2016)

3.2.3 Digital Enterprise Security

3.2.3.1 Authentifikation

Die Prüfung einer Identität und der dazu erforderliche Prozess zum Nachweis einer Identität wird als Authentisierung bezeichnet. Im Allgemeinen geht es darum eine Person oder eine Sache (Internet of Things) zu authentisieren. Manchmal ist es auch sinnvoll eine Umgebung oder eine Situation zu bestätigen - auch dazu sagt man Authentisierung z.B. eines Netzes.

Authentisiert wird meist mittels bestimmter Eigenschaften der zu authentisierenden Entität oder einem Geheimnis, welches dieser Entität bekannt ist, oder eines konkreten Gegenstandes, welcher im Besitz ist. Bei Personen werden als Eigenschaften gerne biometrische Erkennungsmerkmale (Handvenen, Iris, Fingerabdruck, Stimme …) oder auch Fähigkeiten (Tippcharakteristik auf einer bestimmten Tastatur) verwendet. Personen können sich auch Geheimnisse merken, wenn diese nicht zu kompliziert sind. Die Authentisierung von "Dingen" oder Maschinen im Bereich Industrie 4.0 und Internet of Things (IoT) auf Basis von Eigenschaften ist leicht kopierbar und deshalb nicht besonders robust gegen Angriffe. Geheimnisse können in den Maschinen zwar gelagert werden dürfen aber von der Maschine nicht an jeden weiter gegeben werden. Im Umfeld der Maschinen ist deshalb auch eine gegenseitige Authentisierung wichtig, da die Geheimnisse nicht an jeden weiter gegeben werden sollten. Optimal ist es, wenn statt das Geheimnis weiter zu geben nur der Beweis erbracht wird, dass man das Geheimnis besitzt - asymmetrische Kryptographie beruht darauf. Besitz und Geheimnis können z.B. in Form einer Smartcard mit Schlüsseln im Speicher kombiniert werden.

Die Angriffe auf Authentisierungen - also der Diebstahl digitaler Identitäten - sind vielfältig. Hier sind nur die gängigsten aufgeführt. Dazu ist auch zu verstehen, dass als Ergebnis einer Authentisierung eine Aussage "das ist die Person xy" nicht sinnvoll weitergegeben werden kann. Wie in der analogen Welt braucht man etwas in der Hand, wenn man Dritten gegenüber beglaubigen will wer oder was man ist. In der Analogen Welt wird mit Stempeln, Dokumenten, besonderem Papier oder auch Diensten zur Nachfrage gearbeitet. In der digitalen Welt ist die Authentisierung meist eine Anwendung, die mehr oder weniger komplexe Algorithmen ausführt und als Ergebnis ein Datenpaket, meist Ticket oder Token genannt, erstellt. Dieses Ticket hat dann eine gewisse Gültigkeit und kann von den Anwendungen auf einem System verwendet werden, um zu beweisen für welchen Anwender die Prozesse der Anwendung arbeiten.

Die Angriffe:

1. Die Rohdaten des Anwenders (sein Passwort, sein Fingerabdruck …) können gestohlen werden und dem echten System (oder einer Kopie des echten Systems) übergeben werden.

2. Das System kann so manipuliert werden, dass echte Daten multipliziert werden

- Keylogger lesen die Tastatureingabe mit und greifen dadurch Passworte im Klartext ab
- Jede Anwendung auf dem System, welches die Authentisierung vornimmt und unter bestimmten Voraussetzungen auch Remote-Anwendungen können die Authentisierungsdaten unberechtigt abgreifen oder - falls Smartcards eingesetzt werden - eine neue Smartcard-Signatur erstellen lassen.

3. Das Ticket (das Ergebnis der Authentisierung) kann gestohlen werden und als Benutzerrepräsentanz verwendet werden. Natürlich können digitale Elemente einfach kopiert/multipliziert und von überall in der Welt wieder eingespielt werden.

4. Der Authentisierungsdienst kann von Dritten unberechtigt angeboten werden und die so erhaltenen Authentisierungsdaten können an den echten Authentisierungsdienst weiter gegeben werden. Der unechte Dienst erhält dabei ein echtes Ticket. Angriffe dieser Form werden als Man-in-the-middle bezeichnet

5. Bei Passwortauthentisierung kann die Datenbasis mit den im Normalfall einfach oder doppelt verschlüsselten bzw. gehashten Passworten gestohlen werden. Dictionary Attacs prüfen alle möglichen Tastenkombinationen gegen diese Datenbasis und können dadurch Klartextpasswort ermitteln. In sogenannten Rainbow-Tabellen sind die Werte schon vorberechnet, so dass die Zeiten zur Berechnung eines Klartextpasswortes kurz werden.

3.2.3.2 Hardware-Sicherheitsmodul

Um ein hohes Maß an Sicherheit in unternehmens- oder gesellschaftskritischen Bereichen zu gewährleisten, werden kryptographische Verfahren verwendet, die bei verschiedenen Anwendungen zum Einsatz kommen. Diese werden im Falle von Massendatenverarbeitung durch Hardware-Sicherheitsmodule (HSMs) realisiert. Hierzu zählen beispielsweise:

- Die Verschlüsselung personenbezogener Daten, wie etwa von Kreditkarten-Daten, in Kundendatenbanken zur Erfüllung der Anforderungen des PCI Data Security Standard (PCI DSS)
- Die Erzeugung von Signaturen für Zertifikate (Certification Authority) von PKIs
- Die Kommunikation über Web-Portale von Behörden und Banken (eID für eGovernment und online-Banking)
- Die Erzeugung elektronischer Tickets
- Signaturen in Zeitstempeldiensten
- Die Verarbeitung verschlüsselter Daten innerhalb der Cloud ohne Einsichtnahme-Möglichkeit des Betreibers

All diese Anwendungen sind essentiell und bilden das Fundament wichtiger und teils kritischer Systeme. Umso wichtiger ist, dass HSM sicher vor Manipulationen und Einflussnahme durch unbefugte Dritte betrieben werden können.

Bedrohung	**Gegenmaßnahme**	**Stand der Technik**
Manipulation von Zeitstempeln	Erzeugen von Zeitstempeln mit Hilfe eines sicheren HSM	Unterstützung aller gängigen Kryptoalgorithmen
Angreifer erraten kryptografische Schlüssel, die von schwachen Zufallsgeneratoren stammen oder Ausspähen von schlecht gesicherten Schlüsseln für Datenbanken, Root-Zertifikaten von PKIs (z.B. für	Erzeugen kryptografischer Schlüssel und deren sichere und hochverfügbare Speicherung in HSMs	Physikalischer Hochgeschwindigkeits-Zufallszahlengenerator für Massen-Zufallszahlen, Implementierungen von z.B. AES256, ECDSA und SHA-2, Mechanischer und sensorbasierter Schutz vor Auslesen der

Mitarbeiterausweise und Berechtigungen)		im HSM gespeicherten Schlüssel durch Ätz-, Bohr-, Kratz und Kryoangriffe, Unterstützung von Standard-Schnittstellen zu Anwendungen wie PKCS#11, OpenSSL, SQLEKM oder eID für den nPA, Unterstützung von HSM-Redundanz für Hochverfügbarkeits-Anforderungen durch Schlüssel-Backup/Restore

Tabelle 12: SdT für Hardware-Sicherheitsmodul (HSM)

3.2.3.3 Public-Key-Infrastruktur

Der Nachweis von elektronischen Identitäten - egal ob Personen, Organisationen oder Geräten - läßt sich vertrauenswürdig nur durch den Einsatz elektronischer Zertifikate sicherstellen. Dies gilt abgeleitet ebenso für die Integrität elektronischer Dokumente und Nachrichten durch den Einsatz von elektronischen Signaturen. Auch beim sicheren verschlüsselten Datentransport kommen zertifikatsbasierte Lösungen zum Einsatz. All diese Szenarien setzen eine Komponente zur Erzeugung, Management und Prüfung voraus - eine Public Key Infrastrucutre (PKI).

Ähnlich wie in anderen Bereichen werden elektronische Zertifikate von der sog. Zertifizierungsstelle einer Organisation herausgegeben. Verwendet wird hier der Begriff Certification Authority oder CA. Die Gültigkeit von öffentlichen Schlüsseln wird hier durch digitale Signaturen der CA bestätigt. Neben dem Schlüssel selbst enthält das digitale Zertifikat weitere Informationen, wie Gültigkeitsdauer usw. Als verantwortliche Instanz ist die CA die zentrale Komponente in der Public-Key-Infrastructure.
Zur Wahrung der Vertrauenswürdigkeit der CA ist vor Erteilung des elektronischen Zertifikates eine eindeutige Prüfung der Identität der beantragenden Person oder Organisation notwendig. Dies wird von der Registrierungsstelle oder Registration Authority (RA) geleistet.

Zur Überprüfung der Gültigkeit elektronischer Zertifikate wird ein Validierungsdienst oder Validation Authority (VA) benötigt. Generell unterscheidet man die Prüfung gegen eine veröffentlichte Zertifikatssperrliste (CRL) oder die Echtzeitprüfung durch einen Online Certificate Status Protocol (OCSP) Dienst. Die Wahl der Prüfungsvariante ergibt sich meist aus dem jeweiligen Einsatzszenario.

In Abhängigkeit des juristischen Status der PKI wird in den meisten Einsatzfällen die rechtlich verwertbare Protokollierung aller Transaktionen in einer PKI sinnvoll oder gar notwendig sein. Grundlage dafür bietet die Archivierung dieser Transaktionen nach BSI TR-ESOR. Die Einsatzmöglichkeiten reichen dabei von Signatur und Verschlüsselung von E-Mails (S/MIME) über Authentisierungsprozesse bis zur schnellen Erzeugung von Zertifikaten im "Internet der Dinge". Optimal sind alle Komponenten auch für mobile Anwendungen geeignet. Die Anbringung einer elektronischen Signatur an Dokumente ist ebenfalls abgedeckt.

Je nach Status des Betreibers und des Sicherheitsstandard des zugehörigen Rechenzentrums können unterschiedlichste Lösungen aufgebaut werden. Dies reicht von einer Root-CA als sogenannter Vertrauensanker bis zu streng hierarchischen PKI mit mehreren Sub-CA's. Auch eine Cross-Zertifizierung mit an- deren PKI ist realisierbar.

Eine PKI unterstützt somit die Schutzziele Vertraulichkeit, Integrität, Authentizität.
Die Auswahl und Nutzung der kryptographischen Algorithmen und relevanter Parameter orientiert sich dabei an den vom BSI stetig aktuell gehaltenen Vorgaben und Empfehlungen.

Ein Beispiel der Nutzung im öffentlichen Bereich:
www.cio.bund.de/Web/DE/IT-Angebot/IT-Beratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html

Ein Beispiel der Nutzung im Energieversorgerbereich:
www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html

Bedrohung	Gegenmaßnahme	Stand der Technik
Diebstahl von Identitäten	Verwendung von elektronischen IDs (eIDs)	Nutzung einer eigenen oder externen PKI, um Zertifikate bzw. eIDs auszustellen und zu nutzen
Vorspiegelung einer falschen Identität	Starke Authentisierung für Intra-/Extra-/Internet-Ressourcen	Nutzung einer eigenen oder externen PKI, um Zertifikate bzw. eIDs auszustellen und zu nutzen bzw. Identitäten zu prüfen
Echtheit und zeitliche Einordnung von Daten und Vorgängen ist nicht gewährleistet	Nachweisbarkeit über das Anbringen von Zeitstempels sicherstellen	Elektronische Zeitstempel (Qualifiziert - Akkreditiert) von einem akkreditierten Trustcenter beziehen
Integrität: Unbefugte Manipulationen an der Nachricht bzw. Datei (z.B. Einfügen, Weglassen, Ersetzung von Teilen) sollen entdeckt werden können.	Nutzung von fortgeschrittenen oder qualifizierten Signaturen (elektronische Unterschriften)	Signaturkarten über ein oder von einem akkreditierten Trust-Center beziehen und einsetzen

Tabelle 13: SdT für Public-Key-Infrastruktur (PKI)

3.2.4 Client- und Serversicherheit

3.2.4.1 Antivirus

Die Antivirus-Lösungen bilden einen heute immer noch wichtigen Faktor auf der Client- und Serverseite. Diese Schutzschicht wird als Grundschutz bezeichnet und sollte nicht vernachlässigt werden, da er einen bedeutenden Baustein innerhalb eines IT-Sicherheitskonzeptes bildet. Die Sicherheit steht und fällt mit der Erkennungsrate und Aktualität der Signaturen. Hierbei gibt es sehr große qualitative Unterschiede, wie unabhängige Tests von AV-TEST zeigen (1).

Bedrohung	Gegenmaßnahme	Stand der Technik
Angriffe durch infizierte Webseiten, Diebstahl lokaler persönlicher Daten, Befall durch Trojaner und Ransomware	Verwendung einer Antivirensoftware mit den neusten Signaturen.	Verwendung einer Antivirensoftware mit einer hohen Erkennungsrate. Bei den Signaturupdates sind möglichst kurze Intervalle zu wählen. (z.B. 1 Stunde)

Tabelle 14: SdT für Antivirus

Quelle: (1) Die besten Antivirus Programme für Windows Client Unternehmensanwender - https://www.av-test.org/de/antivirus/unternehmen-windows-client/, letzter Aufruf: 27.03.2016

3.2.4.2 Device und Portkontrolle

Über USB, PCMCIA, Bluetooth, Firewire usw. an einen PC angeschlossene Geräte beginnen sofort mit dem Betriebssystem zu kommunizieren. D.h. schon lange bevor die ersten Funktionen eines Peripheriegerätes für Anwendungen oder den Nutzer sichtbar sind findet ein Austausch mit dem Device statt. Dadurch entstehen vielfältige Sicherheitslücken. Wechseldatenträger sind dabei nicht das höchste Risiko. Über Funktastaturen ausgetauschte Passwörter oder ohne Kenntnis der Netzwerkabteilung unsicher konfigurierte Funknetze sind beispielsweise noch kritischer, da man als Außentäter Angriffe erfolgreich durchführen kann ohne physikalischen Zugriff auf IT-Systeme eines Unternehmens zu bekommen.

Häufig beginnen Anti Virus Programme beim Verbinden mit größeren mobilen Datenträgern den ganzen Datenträger zu Scannen, während der Nutzer aber schon auf alle - also auch die nicht geprüften - Dateien Zugriff bekommt. Hier gilt es entweder Quarantäne, bzw. Schleusen Umgebungen einzurichten oder über Device Control Verfahren auf Treiber Ebene sicherzustellen, dass jede gelesene Datei vor Nutzung durch das Anti Virus Programm geprüft wird.

Die Device und Portkontrolle zerfällt in zwei Teile:

1. Sicherstellen dass über den Port und das verbundene Device nur die dafür prinzipiell in der Nutzerebene vorgesehenen Funktionen ausgeführt werden können. Dafür muss das Betriebssystem im Kernel-mode von bestimmten Automatismen abgehalten werden, wie z.B. lnk-Angriffe, BadUSB und bestimmte DMA-Angriffe zeigen.

2. Auf den freigegebenen Funktionen des Ports und des Devices sicherstellen, dass die Firmenrichtlinie zwangsweise eingehalten wird.

Einige Device Control Lösungen im Markt schützen die Kommunikation mit dem Device nur zeitverzögert. D.h. der Anwender kann ein vorbereitetes Skript, z.B. mit automatischen Copy-Kommandos starten bevor das Device verbunden wird und hat dadurch die Sicherheitsrichtlinie für einen kurzen Zeitslot umgangen.

3.2.4.3 Full Disk Encryption

Mit der "Full Disk Encryption" ist die Festplattenvollverschlüsselung gemeint, welche alle verbauten Datenträger in einem System betrifft. Hierbei soll der unbefugte Zugriff durch Dritte unterbunden werden. Diese Technologie bietet Schutz bei Verlust von Geräten durch Unaufmerksamkeit oder Diebstahl. Der sogenannte "Evil Maid Angriff", bezieht sich auf Geräte, die unbeaufsichtigt bleiben, beispielsweise in einem Hotelzimmer.

Die eingesetzte Software sollte starke Verschlüsselung bereitstellen und die kryptografischen Schlüssel sollten niemals, auch nicht zu "Backupzwecken", "in die Cloud gesichert" werden.

Bei der Wahl der Authentifikationsmerkmale sollte großer Wert auf lange Passwörter und einen zusätzlichen "Token" gelegt werden als 2-Faktor-System.

Bedrohung	Gegenmaßnahme	Stand der Technik
Einsehen von Daten auf verlorenen oder gestohlenen Geräten durch Unbefugte	Vollverschlüsselung des gesamten Laufwerks, auf dem sich das Betriebssystem befindet	Mindestens AES-256 mit einem starken Kennwort und einem 2. Faktor als zusätzliches Merkmal (2-Faktor-Mechanismus) oder vergleichbar. Optimal ist die Kapselung mehrerer Verschlüsselungsalgorithmen ineinander, wie z.B. Serpent(Two Fisch(AES)). Ein zentrales Management-Tool erleichtert den Einsatz auf allen PCs der Organisation erheblich. Vom BSI zugelassene Lösungen für Win 7, 8 und 10 sind verfügbar.

Tabelle 15: SdT für Full Disk Encryption

3.2.4.4 File & Folder Encryption

Die folgende Kategorie beschreibt die Verschlüsselung einzelner Objekte, wie z.B. Container, Ordner oder einzelne Dateien, daher ist diese Art der Verschlüsselung auch als Objektverschlüsselung bekannt. Die hierfür verfügbaren Programme arbeiten oft transparent, d.h. der Nutzer kann mit den Objekten arbeiten, als wären sie unverschlüsselt.

Objektverschlüsselung bietet die Möglichkeit Dateien und Ordner sicher von einem Ort zu einem anderen zu transportieren und eine Einsichtnahme durch unbefugte zu verhindern. Es muss also sichergestellt werden, dass niemand außer den autorisierten Personen Zugriff auf die geschützten Informationen erhält. Dies kann persönliche Daten einzelner oder im schlimmsten Fall die Existenzgrundlage eines Unternehmens gefährden.

Des Weiteren bietet sich die Objektverschlüsselung bei der Verwendung von Clouddiensten an, denn damit lässt sich die Einsichtnahme der Daten durch den Betreiber wirkungsvoll verhindern.

Bedrohung	Gegenmaßnahme	Stand der Technik
Diebstahl von Wechseldatenträgern und Extraktion sensibler Daten	Verschlüsselung der Ordner und Dateien, die sich auf dem Datenträger befinden	AES-256 und RSA Verschlüsselung mit einer Mindestschlüssellänge von 4096 Bit oder z.B. ECC 256 (Curve 25519)
Abfangen und Missbrauch versendeter Daten per Post oder E-Mail	Verschlüsselung der Ordner und Dateien, die sich auf dem Datenträger befinden	
Missbrauch von Daten, die in der Cloud abgelegt wurden	Lokale Verschlüsselung der Ordner und Dateien vor dem Upload in die Cloud	

Tabelle 16: SdT für File & Folder Encryption

3.2.4.5 Data Loss Prevention (DLP)

Klassisch gesehen gehört Data Loss Prevention (DLP) zu den Schutzmaßnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützt und je nach Ausprägung direkt oder indirekt die Integrität und Zuordenbarkeit. Der unerwünschte Abfluss von Daten, der Schaden verursacht soll vermieden bzw. wenn erfolgt mindestens bemerkt werden.

Inzwischen bezeichnet DLP ein umfangreiches Sammelsurium unterschiedlichster IT-Sicherheitstechniken und Maßnahmen. Je nach verwendeter Technik sind mehr oder weniger flankierende Maßnahmen erforderlich, um einen vollständigen Schutz der Vertraulichkeit herzustellen. Vorhandenen Systeme wie Identitätsmanagement, Verschlüsselung, Monitoring und Zugriffskontrolle müssen um den DLP-Ansatz und um ein einheitliches Management ergänzt werden, das auf DLP-Zwecke ausgerichtet ist. Bei der Einführung und Umsetzung von Data Loss Prevention im Unternehmen muss eine sorgfältige Abstimmung und Abwägung mit Datenschutzvorschriften und den Persönlichkeitsrechten der Mitarbeiter erfolgen, damit Verletzungen dieser Regeln und Rechte vermieden werden. Data Loss Prevention Lösungen sind somit in Einklang mit der Unternehmenspolicy zur Identifizierung der unerlaubten Weitergabe von sensitiven Informationen via E-Mail, Web, IM, P2P und sonstigen Kanälen zu implementieren.

3.2.4.5.1 Datendiebstahl von außen

Datendiebe versuchen über mehrere Wege Daten eines Unternehmens nach "außen" zu transportieren:

1) Manipulierte Anwendungen (Malware)
   a) Botnetze - siehe "Botnetze"
   b) Remote Desktop Steuerungsprogramme (RDP)
      i) Tatsächlich im Unternehmen verwendete RDP
      ii) Fremde RDP - siehe "Applikationskontrolle"
   c) Modifizierte bekannte Anwendungen - siehe "Applikationskontrolle"

d) Makros, Skripte … - siehe "aktive Inhalte"
e) In RAM Modifikationen

2) Manipulierte Hardware (diese muss zuerst in das Netzwerk gebracht werden, z.B. durch die Modifikation einer Original-Maus während des Urlaubs des Besitzers)

3) Diebstahl von Kennungen - siehe "Sicheres Login"

4) Ungewollte Netzverbindungen oder erfolgreiche Angriffe auf die Netze
   a) Direkt aus dem Internet -. Siehe "Firewall"
   b) Über ungeschützte Verbindungen vom Client

5) Hintertüren, Covert Channels … - undokumentierte Kommunikationskanäle

Im einfachsten Fall werden die Diebstahlvorrichtungen unter dem Account eines Anwenders in das System eingeschleust und arbeiten dort unentdeckt im Namen des Anwenders. Gegen diese Angriffe wirken also alle Maßnahmen, die auch gegen den Datendiebstahl von Innen wirken (siehe 3.2.4.5.2). Diese sollten zusätzlich zu den Maßnahmen gegen Datendiebstahl von außen umgesetzt werden. Hier sind noch zusätzliche Maßnahmen angegeben, die davor schützen, dass die Anwenderumgebung infiltriert wird. Wichtig ist, dass man alle Maßnahmen jeweils in verschiedenen Stärken umsetzen kann:

- Verdachtsmomente monitoren und
  - in einem Echtzeit-SIEM alarmieren - auf dieser Stufe wird keine Modifikation der Businessabläufe notwendig und es gibt keine Restriktionen, aber höheres Bedrohungspotential
  - die zugehörige Aktion in einer virtuellen Schleuse (siehe virtuelle Schleuse) ausführen. Wichtig ist hierbei, dass die Aktion nahtlos in den Benutzerablauf eingebunden wird
- Benutzerinteraktion als Nachfrage, ob die konkrete Aktivität, die als kritisch erkannt wurde, auch intendiert ist. Hier sind gruppenspezifische Interaktionen zwingend, denn ein Administrator wird verstehen, was es bedeutet, wenn sein Browser ohne seine Kenntnis versucht ein ausführbares Programm zu verändern, wohingegen ein Endanwender dazu evtl. weniger qualifizierte Kenntnis hat. Dementsprechend sind die Dialoge nur für die adäquat geschulten Anwendergruppen. Für alle anderen ist die Blockade oder virtuelle Schleuse die richtige Lösung
- Aktion blockieren und ggf. Anwender über die Blockade und Handlungsalternativen informieren, da sonst zum einen die User Experience leidet und zum anderen der Anwender mit Kollegen versucht die Blockade zu umgehen (z.B. wird das Objekt auf privaten Mailaccount geschickt und dort weiter verarbeitet, verlässt aber dadurch den Unternehmensschutz ist für die DLP Richtlinien nicht mehr greifbar)
- Stärke des Schutzes: Gegen Angriffe von außen ist es sinnvoll eine zweite Sicherheitsbastion aufzubauen. Da bei mobilen Arbeitsplätzen das Betriebssystem den Angriffen fast direkt ausgesetzt ist, da die Firewall auf den Clients meist nicht als separate Hardware mit eigenem Betriebssystem ausgeführt ist , gilt es das Betriebssystem geeignet zu schützen. Vorzuziehen sind auf mobilen Clients Schutzvorrichtungen, die im Kernel Mode im Betriebssystem verankert sind gegenüber solchen, die die Schutzmaßnahmen des Betreibsystems selbst nutzen oder auf Applikationsebene oder Dienstebene arbeiten.

3.2.4.5.2 Datendiebstahl von innen

Gegen den Datendiebstahl durch Innentäter gibt es verschiedenen Strategien, die z.T. auch parallel verwendet werden können.

1. Zum einen ist Datenklassifikation und (virtuelle) Trennung der Kronjuwelen (extrem sensible Daten) von den weniger kritischen Daten eine plausible Strategie, die darunter leidet, dass der Schutz der Kronjuwelen mit stärksten Mitteln durchgesetzt werden muss, aber die Durchmischung der Kronjuwelen mit Standarddaten immer wieder aus praktischen Gründen notwendig ist.

2. Zum anderen kann man den an potentiellen Datenabflussstellen (Leckagepunkten) prinzipiell auftretenden Datenfluss monitoren, um dann die aus Unternehmenssicht notwendigen suk-

zessive von den unerwünschten Daten zu trennen und Maßnahmen gegen den unerwünschten Datenabfluss einzuleiten.

Der Nachteil der ersten Vorgehensweise besteht darin, dass es relativ lange dauert bis alle Daten klassifiziert sind und während dieser Zeit kein Nutzen für das Unternehmen entsteht. Das Vorgehensmodell unter 2 bringt von Anfang an einen Nutzen. Es erlaubt beispielsweise von Anfang an die Verstöße gegen die Firmenrichtlinien und den gesamten Datenabfluss statistisch zu erfassen. In vordefinierten Intervallen, z.B. jährlich, werden dann die statistischen Daten mit dem letzten Intervall verglichen und dadurch die Fortschritte im Projekt auch in Zahlen statistisch dokumentiert. Bei der zweiten Vorgehensweise kann zu einem beliebigen Zeitpunkt als Teilprojekt dann eine zwangsweise Datenklassifikation bestimmter Datenströme (z.B. Attachments an Mail-Ausgang, Auf mobile Datenträger exportierte Daten) eingerichtet werden und dadurch die Qualität der Information über die Kronjuwelen erhöht werden.

Sind die Kronjuwelen durch ein vollständig getrenntes Netz ohne eigenen Internet Zugang geschützt, so wird immer ein Datenübergang des Kronjuwelen Netzes, allgemein als rotes Netz bezeichnet, zu dem am Internet angebundenen Netz, allgemein als schwarzes Netz bezeichnet, notwendig. Dieser Datenübergang ist entweder als "Drehstuhlschnittstelle" mit einem mobilen Datenträger, mit einem Fileserver mit zwei Netzwerkkarten und unterschiedlichen Schutzprofilen (z.B. Write up - no read down), einem rot-schwarz-Gateway oder einer virtuellen Schleusen (siehe 3.2.2.5) Lösung ausgestattet.

Im Folgenden sind alle potentiellen Leckagepunkte über welche ein Abfluss stattfinden kann gelistet:

1. Mobile Datenträger - als Lösungen gegen Datenabfluss gibt es:
   a. Verschlüsselung aller abgehenden Informationen mit einem Unternehmensschlüssel, dessen Verschlüsselung nur auf Unternehmenseigenen IT-Systemen wieder entschlüsselt werden kann
   b. Verhinderung des Abflusses von kritischer / sensibler Information

2. Kommunizierende Peripheriegeräte mit direktem Kontakt oder einer Anbindung über Funkstrekken wie Bluetooth wie Netzwerkkarten, Modems, Mobiltelefone usw.

3. Peer to Peer Kommunikation unter Umgehung von Rechtestrukturen kabelgebunden (z.B. über Druckerkabel) oder über Funk wie z.B. Bluetooth

4. Anwendungen, die zur Kommunikation mit Dritten intendiert sind (z.B. ftp, Browser, E-Mail), und Anwendungen, die zur Kommunikation missbraucht werden können.

5. Netzwerkkontakte - Vorsicht, denn ein Innentäter kann die gesamte Struktur eines Unternehmensnetzes "zu Hause" nachbauen und so Daten auf einen nachgebauten Fileserver auslagern, der so aussieht als wäre es der firmeneigene Fileserver

6. Druckoutput - da das Ausdrucken nicht generell verhindert werden kann müssen Anwenderdialoge (Zweck, Weitergabe an?, …) mit geeigneten individuellen Wasserzeichen auf den Ausdrucken, die sich aus sichtbaren und unsichtbaren Elementen zusammen setzen, und revisionssicheren Archiven, die mit mindestens 4-Auf´gen geschützt sind, kombiniert werden

7. Hintertüren, covert Channels … durch den Anwender

   a. Für den normalen Endanwender ist die Nutzung von steganographischen Verschleierungstechniken nur mit Hilfe von geeigneten Programmen möglich. Deshalb ist mit guter Applikationskontrolle auch der nutzergesteuerte steganographische Datenverkehr sicher zu verhindern

   b. Einfache nutzergesteuerte Verfahren, die vielen DLP Systemen entgehen, sind mehrfach geschachtelte Objekte. Benutzer reichern erlaubte Objekte (z.B. Word-Dokumente) durch das Einbetten von weiteren z.T. mehrfach geschachtelten Objekten an und versuchen so den eigentlichen Inhalt zu verschleiern.

Wichtig ist, dass bei dem Schutz vor Innentätern auch die Serversysteme identisch zu schützen sind, falls potentielle Innentäter auch Zugang zu den Serversystemen oder deren Funkverbindungen haben können.

Für DLP Projekte gibt es auch den Motivationspunkt der Compliance / Governance. Gilt es bestimmte Regularien bei der Datenweitergabe einzuhalten, wie das z.B. bei den Landeskrankenhausdatenschutzgesetzen in Deutschland häufig der Fall ist, so muss zum einen der Anwender über die Inhalte der Regularien aufgeklärt sein (am besten über E-Learning mit Lernzielkontrolle), zum anderen muss der Anwender auf die Regularien individuell verpflichtet werden (am besten durch elektronische Willenserklärungen, welche einen Individualvertrag ersetzen können) und zu guter Letzt muss der Anwender technisch auf die konkrete Situation hingewiesen werden.

3.2.4.6 E-Mail-Verschlüsselung

Die Sicherheitsanforderungen an E-Mail werden u.a. bestimmt durch die Art der übermittelten und im Mail-System gespeicherten Daten. Im Geschäftsverkehr kann man grundsätzlich davon ausgehen, dass E-Mails für das Unternehmen zumindest wichtige Informationen enthalten. Weiterhin werden schon E-Mail-Adressen, wenn personalisiert, als personenbezogene Daten betrachtet; es kann also davon ausgegangen werden, dass mit E-Mails personenbezogene Daten übermittelt und gespeichert werden. In Einzelfällen und abhängig vom jeweiligen Einsatz von E-Mail können auch Daten übermittelt werden, die besonderen Schutzbedarf haben, so z.B. Gesundheitsdaten, Daten von Mandanten z.B. von Rechtsanwälten oder besonders wertvolle Firmengeheimnisse, wie z.B. Konstruktionsdaten.

Daraus ergeben sich folgende Sicherheitsanforderungen an E-Mail:

- Schutz vor unbefugter Einsichtnahme oder Veränderung im Transport und bei gespeicherten E-Mails (Schutzziel: Vertraulichkeit),
- Schutz vor nachträglicher Veränderung von E-Mails bei langfristig archivierten E-Mails (Schutzziel: Integrität).

Diese Schutzziele können generell durch Verschlüsselung erreicht werden. Bei der Verschlüsselung von E-Mails ist zu unterscheiden zwischen der Verschlüsselung bei der Übertragung (Transportverschlüsselung) und der Verschlüsselung der E-Mail an sich (auch "Ende-zu-Ende Verschlüsselung"). Die Schutzziele bedingen zwingend zumindest den Einsatz von Transportverschlüsselung bei der Übertragung von E-Mails durch öffentliche Netze. Die bei der Übermittlung von E-Mails durch das Internet genutzten Protokolle, namentlich SMTP, POP3 und IMAP sehen in Ihrer Grundform allerdings eine unverschlüsselte Datenübertragung vor. Wahrscheinlich werden deshalb große Teile des E-Mail-Verkehrs unverschlüsselt übertragen, obwohl schon lange ausreichend Werkzeuge zur Verschlüsselung von E-Mails zur Verfügung stehen.

Im E Mail-Verkehr sollte zur Transportverschlüsselung TLS (Transport Layer Security) in der aktuellen Version 1.2 (definiert in RFC 5246 [1]) oder alternativ ein verschlüsseltes VPN eingesetzt werden. Zum Einsatz kommen müssen sichere Verschlüsselungsverfahren (aktuell z.B. AES-256), die Verwendung unsicherer Verschlüsselungsverfahren (z.B. RC4) muss ausgeschlossen werden. Forward Secrecy sollte generell aktiviert werden. Zusätzlich ist es sinnvoll, die bei TLS genutzten Zertifikate der jeweiligen Gegenseite auf Authentizität und Gültigkeit zu überprüfen, z.B. mittels DANE (RFC 7671 [2]). Umfassende Empfehlungen zu TLS liefert die Technische Richtlinie TR-02102-2, Teil 2 des BSI [3].

Ende-zu-Ende Verschlüsselung empfiehlt sich zum Schutz besonders schützenswerter Daten. Dazu haben sich zwei Standards etabliert: S/MIME (Secure/Multipurpose Internet Mail Extensions, definiert in RFC 5751 [4]) und OpenPGP (Pretty Good Privacy, definiert in RFC 4880 [5]). Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel und damit in den Vertrauensmodellen und sind zueinander nicht kompatibel.

Beim Einsatz von Ende-zu-Ende-Verschlüsselung kann kein System im Übertragungsweg auf die Inhalte der E Mail zugreifen. Dies bedeutet allerdings den kompletten Verzicht auf Content-Filter, Antivirus, Antispam, Data Loss Prevention und Archivierung. Deshalb kann alternativ der Einsatz von Inhaltverschlüsselung nur zwischen Organisationen sinnvoll sein; d.h. E-Mails werden im Übergang vom öffentlichen Internet zum privaten Netz der Organisation (Gateway) verschlüsselt bzw. entschlüsselt

(Organisations-Ende-zu-Ende-Verschlüsselung), ggf. kombiniert mit einer unternehmensinternen Inhaltsverschlüsselung.

Bedrohung	Gegenmaßnahme	Stand der Technik
Ausspähung oder Manipulation von E-Mails im Transport	Verschlüsselung der E-Mail selber oder des Übertragungsweges	TLS auf allen Transportwegen; alternativ / zusätzlich VPN ggf. Prüfung der Gegenstelle (DANE usw.) je nach Schutzbedarf der übermittelten Daten Inhaltsverschlüsselung per S/MIME oder PGP Verwendung sicherer Schlüssellängen und Verschlüsselungsverfahren gemäß BIS Empfehlungen
Ausspähung oder Manipulation von gespeicherten E-Mails	Zugangsschutz Verschlüsselung der E-Mail-Inhalte Langzeitarchivierung (Schutz gegen Manipulation)	Kennwortschutz mit starkem Kennwort; idealerweise 2-Faktor-Authentisierung Zugang nur über verschlüsselte Verbindungen (TLS und/oder VPN) Inhaltsverschlüsselung per S/MIME oder PGP Revisionssicheres Langzeitarchiv

Tabelle 17: SdT für E-Mail-Verschlüsselung

Quellen:
1. https://www.ietf.org/rfc/rfc5246.txt
2. https://tools.ietf.org/txt/rfc7671.txt
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile
4. https://tools.ietf.org/rfc/rfc5751.txt
5. https://www.ietf.org/rfc/rfc4880.txt

3.2.4.7 Sicheres Logon

Jedes handelsübliche Anmeldeverfahren, das eine Tastatur zur Eingabe benötigt und dafür keine Spezialhardware einsetzt, setzt auf Infrastrukturen des Betriebssystems wie Message bzw. Keyboard Queue, die für alle laufenden Anwendungen öffentlich zugänglich sind und daher sehr leicht mitgelesen werden können. Keylogger in Hardware und Software stellen ebenfalls solche Bedrohungen dar. Danach kann diese Identität von jedem anderen Rechner aus übernommen werden, da Netzwerkadressen, Hardwareidentitäten, Anmeldename und Passwort mitgelesen wurden. Die Anmeldung findet zum einen lokal zum anderen aber im Fall eines Netzwerkbetriebes auch zentral statt. Die Anmeldung resultiert dann in einem technischen Datenelement (meist Token genannt), welches eine Anwendung im Netz gegenüber dem Service präsentiert, um die Identität zu beglaubigen. Dieses Token kann ebenfalls gestohlen werden, lokal auf dem Client auf dem Weg im Netz oder auf dem Server - dafür gibt es im Internet auch spezielle Angriffssoftware (Mimikatz, PassTheHash …). Eine Sicherheit gegen Wiedereinspielen bieten diese Token meist nicht.

Angriffe auf Tastaturen sind seit langem bekannt. Identitätsdiebstahl ist eines der massivsten Risiken, denn es bleibt nach einem gelungenen Identitätsdiebstahl keine Vertrauenskette mehr erhalten. Mit diesen Angriffsmustern kann jede Passwort und PIN gebundene Authentisierung gebrochen werden - auch wenn Hardwareelemente beteiligt sind, wenn die Eingabe der Passworte und PINs nicht gegenüber Soft- und Hardware-Keyloggern geschützt ist.

Effektiven Schutz bietet eine durchgehende Vertrauenskette, die mit einer "sicheren Tastatur" beginnt und alle an der Anmeldung beteiligten Vertrauenselemente sowie das Ergebnis der Anmeldung geeignet beschützt. Dazu gehören: die starke Authentisierung von Eingabegeräten, der Schutz vor dop-

pelten Eingabegeräten, das Einfrieren eines Hardwaresets beim Auslieferungszustand, das Verbot von unbekannten Prozessen und die sichere Weiterleitung von Passworten und Token an den Schwachstellen des Betriebssystems vorbei direkt in die Anwendung bzw. das Login, so dass Hardware und Software-Keylogger keine Chance haben.

3.2.4.8 Fernwartung / Remote Access

Bei einem Fernwartungszugang erhält ein Mitarbeiter einer Fremdfirma zu Wartungszwecken Zugang zum Firmennetz. Hierbei wird zum Beispiel die Software einer Maschine aktualisiert. Der Zugang ist in der Regel temporär, bis die Wartungsarbeiten abgeschlossen sind. Bisher war es hier üblich, dem Mitarbeiter der Fremdfirma per VPN Zugang zum eigenen Netz zu geben. Das stellt ein unnötiges Sicherheitsrisiko dar und ist nicht mehr zeitgemäß. Eine moderne Fernwartungslösung sieht hier ein Rendezvouskonzept vor. Hier verbindet sich der Mitarbeiter der Fremdfirma auf einen Rendezvousserver, der in der Regel in der DMZ steht. Die Verbindung vom Wartungsobjekt zum Rendezvousserver wird von einem Mitarbeiter der eigenen Firma aufgebaut. Der Rendezvousserver übernimmt Monitoring- und Logging-Aufgaben. Eine Netzkopplung ist hier in der Regel nicht mehr nötig. Es kann überwacht oder später nachvollzogen werden, was im Rahmen der Fernwartung genau passiert ist.

Als kritischer Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb einer Fernwartungslösung besondere Aufmerksamkeit zugute kommen. Entsprechende Lösungen sollten nur von autorisierten und vertrauenswürdigen Lieferanten geliefert werden. Im besten Fall ist die Lösung ohne Umweg direkt vom Hersteller zu beschaffen.

Die Schutzziele für solche Lösungen sind:

- Vertraulichkeit und Integrität der Firmendaten schützen
- Authentizität und Verbindlichkeit der vom System generierten Logdaten garantieren
- Zurechenbarkeit von Eingaben sicherstellen.

Moderne Maschinen haben eine hohe Komplexität erreicht. Sie enthalten oft große Mengen an Software zur Steuerung und zur Erhebung von Analysedaten. Es ist oft der Fall, dass nur der Hersteller der Maschine bestimmte Fehleranalysen oder bestimmte Wartungsaufgaben durchführen kann. Für Hersteller, die ihre Maschinen international vertreiben, ist es aber im Allgemeinen nicht möglich, für diese Aufgaben mit einem Mitarbeiter vor Ort zu sein. Stattdessen wird dem Mitarbeiter des Herstellers Zugang zum Steuerrechner der Maschine gegeben.

Klassisch wurde hier ein VPN zwischen Hersteller und dem eigenen Produktionsnetz aufgebaut. Dies birgt große Risiken. Statt zu genau einer Maschine hat der Hersteller potentiell Zugang zu allen Maschinen. Die Vertraulichkeit und Integrität der dort vorhandenen Daten ist gefährdet. Eine gute Fernwartungslösung schützt die Daten, indem sie eine Eins-zu-Eins-Beziehung aufbaut. Hierbei wird im Normalfall keine Kopplung der zwei beteiligten Netze vorgenommen. Stattdessen stellt der Rendezvousserver Zugriffsmöglichkeiten bereit, die keine Netzkopplung erfordern.

Um auch für die Daten zwischen Hersteller und Wartungsobjekt Vertraulichkeit und insbesondere Integrität zu garantieren, muss zwischen Rendezvousserver und Hersteller eine kryptographisch abgesicherte Verbindung bestehen. Hierbei sind ausschließlich moderne und sicher konfigurierte kryptographische Verfahren anzuwenden.

Der Rendezvousserver dient nicht nur der Kopplung, sondern insbesondere auch der Überwachung der Fernwartung. Es sollten Systeme bevorzugt werden, die revisionssichere, verbindliche Aufzeichnungen der Fernwartung anlegen. Es muss zurechenbar sein, welche Person welche Aktion zu welchem Zeitpunkt ausgeführt hat. Die Authentizität des Mitarbeiters des Herstellers sowie der eigenen Firma muss durch sichere Authentifizierungsmechanismen sichergestellt werden.

Bedrohung	**Gegenmaßnahme**	**Stand der Technik**
Zugriff externen Personen auf das Firmennetzwerk	Keine Kopplung der Netze	Die Fernwartungslösung stellt dem Fernwarter zum Beispiel nur ein Terminal zur Verfügung oder sorgt durch andere Maßnahmen dafür, dass keine

		Netzkopplung nötig ist. Die Lösung erzwingt eine Eins zu Eins-Zuordnung zwischen Fernwarter und dem Zielsystem.
Keine Nachvollziehbarkeit der vorgenommenen Aktionen	Die Fernwartungslösung stellt die Nachvollziehbarkeit sicher.	Die Fernwartungslösung stellt eine komplette Aufzeichnung der Fernwartung sowohl Live wie auch zur späteren Ansicht zur Verfügung. Es kann in eine laufende Fernwartung eingegriffen werden um dem Fernwarter Eingabemöglichkeiten zu entziehen oder die Fernwartung zu beenden.

Tabelle 18: SdT für Fernwartung / Remote Access

3.2.4.9 Austausch von Dateien

Für den Austausch von Dateien werden in der Praxis sehr viele verschiedene Wege und Verfahren genutzt, u.a.:

- per Wechselmedium (off-line); z.B. USB-Stick,
- per Fileserver (in der Regel innerhalb einer Organisation, innerhalb eines internen Netzwerks),
- über Online-Speicherdienste (FTP-Server, Web-DAV u.ä.),
- über Browser-orientierte Lösungen, z.B. für Projektzusammenarbeit oder geschützte Datenräume,
- via "File Share & Sync" Services (meist in Verbindung mit Online-Speicherdiensten),
- via E-Mail (als Anhang).

Welche Sicherheitsmaßnahmen beim Austausch von Dateien notwendig sind, hängt einerseits vom Inhalt der Dateien ab, andererseits davon, welche Wege zum Datenaustausch genutzt werden. Sofern der Austausch über Online-Dienste erfolgt (FTP-Server, Browser-orientierte Lösungen, File Share & Sync), sind zwei Fragen zu beantworten:

1. Wer betreibt den Dienst und hat der Betreiber ggf. Zugriff auf die Daten?
2. Wie sind die Daten beim Transport vom und zum Betreiber geschützt?

Wird der Dienst von einer vertrauenswürdigen Instanz betrieben, dann kann auf eine Verschlüsselung der Daten selber unter Umständen verzichtet werden. Ob ein Betreiber als vertrauenswürdig angesehen werden darf, ist dabei abhängig von der Sensibilität der Daten: Für bestimmte Daten (z.B. Gesundheitsdaten, Daten von Mandanten) sind besondere Anforderungen an den Betreiber zu stellen, sofern dieser technisch Einblick in die Daten nehmen könnte.

Ungeachtet dessen ist eine Verschlüsselung der Daten selber auch bei vertrauenswürdigen Betreibern sinnvoll. Ob das in der Praxis umsetzbar ist, hängt von der Art der Anwendung ab. Es sind z.B. Share & Sync Services verfügbar, bei denen Daten vor dem Upload transparent, d.h. ohne besondere Aktion des Benutzers verschlüsselt und nach dem Download wieder entschlüsselt werden. Der Betreiber sieht dann nur verschlüsselte Daten. Bei reinen Online-Speicherdiensten (FTP, Web-DAV usw.) kann auf eine Client-seitige Verschlüsselungssoftware zurückgegriffen werden, die für eine Verschlüsselung der Daten vor dem Upload bzw. nach dem Download sorgt. Diese Lösungen erfordern allerdings in der Regel zusätzlichen Aufwand für den Anwender. Bei der Verschlüsselung sollte auf den Einsatz sicherer Verfahren zur Verschlüsselung und bei der Schlüsselerzeugung geachtet werden.

Auf keinen Fall verzichtet werden darf auf die Verschlüsselung von Daten beim Transport von und zum Betreiber. Zum Einsatz kommt in der Regel TLS (Transport Layer Security), es sollte die Version 1.2 (definiert in RFC 5246 1) eingesetzt werden, in Verbindung mit sicheren Verschlüsselungsverfah-

ren (aktuell z.B. AES-256) und Forward Secrecy (PFS). Umfassende Empfehlungen zu TLS liefert die Technische Richtlinie TR-02102-2, Teil 2 des BSI [2] .

Erfolgt der Datenaustausch innerhalb einer kontrollierten und geschützten Umgebung, d.h. kann hinreichend sichergestellt werden, dass nur befugte Personen Zugriff auf die Dateien bekommen, dann ist auch bei sensiblen Informationen ein unverschlüsselter Austausch von Dateien hinreichend sicher. Beispiele dafür sind der Austausch via USB-Stick, sofern der Stick persönlich übergeben wird und sichergestellt ist, dass der Stick nicht in die Hände Dritter gelangen kann, oder der Austausch via Fileserver innerhalb eines gesicherten Unternehmensnetzes. Dessen ungeachtet ist auch hier der zusätzliche Einsatz von Verschlüsselung sinnvoll - etwa durch Verschlüsselung der Dateien selber, durch Verschlüsselung der genutzten Dateisysteme oder durch Nutzung verschlüsselter Festplatten bzw. USB-Sticks. Diese Verschlüsselungen sind oft einfach einzurichten und transparent für den Nutzer, d.h. erfordern nur geringen Aufwand und kaum oder nur geringe spezielle Kenntnisse des Nutzers.

Für den Austausch von Daten via E-Mail wird auf den Abschnitt "E-Mail-Verschlüsselung" verwiesen.

Bedrohung	Gegenmaßnahme	Stand der Technik
Ausspähung oder Manipulation von Inhalten durch Unberechtigte	Zugrifsschutzmaßnahmen: Authentisierung Verschlüsselung von Daten im Transport und von gespeicherten Daten	Kennwortschutz mit starkem Kennwort, idealerweise 2-Faktor-Authentisierung, starke Verschlüsselung mindestens im Transport; Schlüssellänge und Verfahren gemäß BSI Empfehlungen (z.B. AES-128)
Nichtverfügbarkeit von Daten	Backup Versionierung Redundante Speicherung	Regelmäßiges Backup; je nach Bedeutung der Daten und Häufigkeit von Änderungen wöchentlich oder täglich, Automatische Versionierung und längere Speicherung zurückliegender Versionen, Je nach Verfügbarkeitsanforderungen redundante Datenhaltung mit automatischer Synchronisierung, Speicherung mindestens einer Kopie / aktuelles Backup / letzte Version räumlich vom Original getrennt / in einer anderen Feuerschutzzone

Tabelle 19: SdT für Austausch von Dateien

Quellen:
1. https://www.ietf.org/rfc/rfc5246.txt
2. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile

3.2.5 Mobile Security

3.2.5.1 Applikationssicherheit

Unter dem Begriff "Applikationen" werden alle gängigen IT-Anwendungen zusammengefasst. Diese reichen von klassischen Anwendungen am Host über Fat-Clients bis hin zu modernen Webanwendungen. Abhängig vom Schutzbedarf der jeweiligen Applikation sind unterschiedliche Aktivitäten notwendig, um diese angemessen abzusichern.

Um einen Grundschutz zu erreichen, sind mindestens folgende Aktivitäten durchzuführen.

- Schutzbedarfsbestimmung und Bedrohungsanalyse
- Definition und Verifikation von Security-Anforderungen im Rahmen der Beschaffung
- Definition und Verifikation von Security-Anforderungen im Rahmen der Software-Entwicklung
- Sichere Konfiguration und sicherer Betrieb aller relevanten Komponenten
- Regelmäßige Kontroll-Audits im laufenden Betrieb

Für Anwendungen mit hohem Schutzbedarf müssen weiterführende Aktivitäten umgesetzt werden, die jedoch nicht im vorliegenden Dokument erläutert werden. Details können dem BSI-Leitfaden "Leitfaden zur Entwicklung sicherer Webanwendungen" [1] entnommen werden.

Bedrohung	Gegenmaßnahme	Stand der Technik
Beschaffung unsicherer Softwarekomponenten	Definition von Security-Anforderungen als Entscheidungskriterium im Beschaffungsprozess	Anforderungen gemäß dem BSI-Leitfaden für die Beschaffung sicherer Anwendungen [2]
Kompromittierung der Anwendung aufgrund von Applikationsschwachstellen	Implementierung einer sicheren Architektur basierend auf einer Bedrohungsanalyse Sichere Software-Entwicklung basierend auf etablierten Standards Verifikation des Security Niveaus durch Quality Gates	Bedrohungsmodellierung im Rahmen des Applikationsdesigns OpenSAMM [3] und BSIMM [4] werden als Reifegradmodelle für SSD eingesetzt Durchführung von Security Audits im Whitebox-Ansatz basierend auf dem Standard ASVS [5] als Abnahmetest vor Go-Live
Kompromittierung der Anwendung aufgrund von System- bzw. Infrastruktur-Schwachstellen	Etablieren von Patch- und Vulnerability-Management Laufende Qualitätskontrollen im laufenden Betrieb	Umsetzung der Controls A.12.6 aus ISO 27002 Mindestens jährliche Whitebox-Audits basierend auf dem Standard ASVS [5]

Tabelle 20: SdT für Applikationssicherheit

Quellen:

1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer_pdf.pdf
2. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftraggeber_pdf.pdf
3. http://www.opensamm.org/
4. https://www.bsimm.com/
5. https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

3.2.5.2 Cloud-Daten-Verschlüsselung (Cloud Encryption)

Cloud-Produkte ermöglichen es Anwendern, ihre Daten dezentral zu lagern und über einen Browser oder eine Anwendung von vielen verschiedenen Endgeräten darauf zuzugreifen. Sie erlauben dadurch den mobilen Zugriff auf Daten zu jeder Zeit und von jedem Ort der Welt, was die Flexibilität von Unternehmen erheblich erhöht.

Das bringt aber auch neue Risiken mit sich: Das Auslagern der Daten auf nicht-unternehmenseigene Server und der Zugriff darauf über Third-Party-Software macht Unternehmensdaten anfälliger für Angriffe. In Deutschland sind Unternehmen nach dem Datenschutzgesetz verpflichtet, jederzeit Verfügungsgewalt über alle von ihnen erhobenen und verarbeiteten personenbeziehbaren Daten ausüben zu können (Datenhoheit). Insbesondere muss ein angemessenes Datenschutzniveau (§ 4b Abs. 2 BDSG) gewährleistet werden, wenn personenbeziehbare Daten an Server im nicht-europäischen Ausland gesendet, dort gespeichert und verarbeitet werden.

Datenhoheit ist gegeben, wenn:

- die Daten des Cloud-Nutzers jederzeit verfügbar sind,
- der Nutzer die Verfügungsbefugnis über die Daten hat,
- die Daten im jeweils genutzten System durchgängig verschlüsselt werden, und
- das genutzte System geschützt ist vor Überwachung, Missbrauch oder Veränderung.

Der effektivste Weg, um diese Anforderungen zu erfüllen, ist die Verschlüsselung von Daten vor dem Senden an nicht-unternehmenseigene Server. Damit ist gewährleistet, dass auch bei Datenverlust - etwa durch Diebstahl oder Spionage - die entwendeten personenbeziehbaren Daten nicht genutzt werden können. Stand der Technik ist hier die Verschlüsselung mit AES-256 oder andere durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene Verschlüsselungs-Algorithmen. Das IT-Sicherheitsgesetz (ITSiG) von 2015 schreibt Diensteanbietern zudem vor, bei der Verarbeitung personenbeziehbarer Daten eine als sicher anerkannte, also nachprüfbare Verschlüsselungslösung einzusetzen. Hier bieten Open-Source-Lösungen und austauschbare Algorithmen die beste Transparenz: Sie sind jederzeit und von jedermann auf Sicherheitslücken überprüfbar. Unternehmen sollten zudem nach flexiblen Verschlüsselungslösungen Ausschau halten, die sowohl eine Vielzahl an Anwendungen, Datenbanken und Dateiformaten unterstützen als auch ohne substantielle Veränderung der IT-Struktur zu installieren sind. So kann eine Abhängigkeit von einem einzigen Hersteller über eine längere Zeit (Vendor Lock) vermieden werden.

Um den Zugriff auf Cloud-Anwendungen zu steuern, bieten sich Cloud Access Security Broker (CASB) an. Sie befinden sich zwischen dem Cloud-Nutzer und dem Cloud-Anbieter und regeln den Datenzugriff von außen. So steuern sie etwa, welcher Benutzer Zugang zu welchen Apps hat und seine Berechtigungen in diesen. Momentan werden für CASBs drei Verfahrensweisen verwendet:

1) ein Proxy-artiges, On-Premise-Gateway,
2) ein hostbasiertes Agentenmodell, oder
3) eine API-basierte, Cloud-eigene SaaS-Lösung.

CASB unterstützen Unternehmen in vierfacher Hinsicht bei der Cloud-Datenverschlüsselung:

- Besseres Monitoring von genutzten Cloud-Apps im Unternehmen
- Sichern der IT-Compliance führt zu höherer Rechtssicherheit
- Verbesserte Krisenprävention durch genauere Kontrolle des Datenflusses
- Zusätzlicher Sicherheits-Layer für sensitive Firmendaten.

Bedrohung	Gegenmaßnahme	Stand der Technik
Diebstahl von ganzen Datenbanken, Diebstahl von Daten aus Datenbanken	Externe Datenverschlüsselung zusätzlich zur Standard-Datenbanksicherheit innerhalb der Datenbank	AES-256-Verschlüsselung von personenbeziehbaren Daten vor dem Senden an und Verarbeiten in der Cloud
Spionage durch externe Datenbankadministratoren	Externe Datenverschlüsselung zusätzlich zur Standard-Datenbanksicherheit innerhalb der Datenbank	AES-256-Verschlüsselung von personenbeziehbaren Daten vor dem Senden an und Verarbeiten in der Cloud
Abfangen von Daten beim Transport	Verschlüsselte Verbindung nutzen Datenverschlüsselung	TLS 1.2 AES-256-Verschlüsselung von personenbeziehbaren Daten vor dem Senden an und Verarbeiten in der Cloud

Tabelle 21: SdT für Cloud-Daten-Verschlüsselung

3.2.5.3 Voice Encryption

Die klassische Telefonie ist heute nach wie vor eines der direktesten und persönlichsten Kommunikationswerkzeuge. Sie birgt jedoch einige Gefahren und bietet potentielle Angriffsvektoren.

Bei Sprachübertragungen besteht heute die Gefahr, dass Gespräche mit relativ kostengünstiger Hardware und entsprechendem Wissen abgehört werden können. So täuschen beispielsweise IMSI-Catcher (1) vor, Teil des Mobilfunknetzes zu sein, um dann Gespräche belauschen zu können.
Unabhängig von der Motivation lässt sich die Vertraulichkeit von Gesprächen mit Hilfe von Sprachverschlüsselung sicherstellen. Hier wird das gesprochene Wort in Echtzeit auf dem Gerät verschlüsselt und beim Empfänger wieder entschlüsselt und wiedergegeben.

Bedrohung	Gegenmaßnahme	Stand der Technik
Ausspähen von Gesprächen durch IMSI-Catcher	Verschlüsselung der Sprachkommunikation durch Apps	Verwendung einer hierfür geeigneten Applikation, die nach den aktuellen Verschlüsselungsstandards Ende-zu-Ende-Verschlüsselung durchführt.
Ausspähen von Gesprächen durch Schadsoftware im Mobiltelefon oder ein modifiziertes Handy-Betriebssystem	Härtung des Mobiltelefon-Betriebssystems und Einsatz einer Krypto-App	Verwendung eines Mobiltelefons mit gehärtetem Betriebssystem, das die ausschließliche Nutzung von Mikrofon und Lautsprecher durch die Verschlüsselungs-App sicherstellen kann
	Verwendung eines vom Mobiltelefon unabhängigen Krypto-Zusatzgerätes	Separates mobiles Verschlüsselungsgerät (Kryptohörer), das die Sprache außerhalb des Mobiltelefons ver- und entschlüsselt, so dass kein Auslesen des Schlüssels über das Mobiltelefon erfolgen kann, selbst wenn es infiziert oder manipuliert wurde

Tabelle 22: SdT für Voice Encryption

Quellen:
1. Digitale Selbstverteidigung mit dem IMSI-Catcher-Catcher : http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html, letzter Aufruf: 27.03.2016

2. Hochsichere mobile Endgeräte: http://www.it-zoom.de/it-director/e/hochsichere-mobile-endgeraete-13109/ , letzter Aufruf: 4.4.2016

3.2.5.4 Secure Instant Messaging

Kommunikation ist ein essentieller Bestandteil jeder Unternehmenskultur, durchdringt alle Ebenen und Bereiche und kann auf verschiedene Arten ablaufen, unterschiedlich organisiert sein und muss geschützt stattfinden, damit sie nicht abgehört und manipuliert werden kann. Dieser Schutz kann technisch mit Hilfe der Ende-zu-Ende-Verschlüsselung stattfinden und sich nicht lediglich auf einen Transportschutz (https mit TLS) für die Datenverbindung begrenzen.

Technisch bedeutet in diesem Fall nicht nur, ein robustes Protokoll und die dazugehörigen "stabilen Apps zu implementieren", sondern legt ein deutlich größeres Maß an, welches weit über diese Eigenschaften hinausgeht. Im Mittelpunkt stehen hier ebenso eine einfache Bedienung (Nutzerakzeptanz) und angemessene Sicherheit. Zudem ist es heute wichtiger denn je, die eigenen Daten nicht an Dritte abzugeben, sondern diese unter der eigenen Hoheit behalten zu können. Hier muss unter anderem die Forderung nach eigener durchsetzbarer Selbstbestimmung und einem hohen Grad an Datenschutz gestellt werden.

Unabhängig von der eingesetzten Plattform sollte die Sicherheit und Vertraulichkeit der Kommunikation gewährleistet sein.

Bedrohung	Gegenmaßnahme	Stand der Technik
Mitschneiden und Auswerten aller Inhalte textueller Kommunikation	Technische Sicherungsmaßnahmen zur Wahrung der Vertraulichkeit und Integrität und Einsatz von Verschlüsselungsmechanismen	Sicherung der Übermittlung mittels TLS 1.2 auf dem Transportweg Einsatz von Asymmetrische Ende-zu-Ende-Verschlüsselung mit einer mindestens zu RSA 2048 Bit vergleichbaren Sicherheit Auch Forward Secrecy sollte Bestandteil der Architektur sein.
Manipulation versendeter Nachrichten zwischen zwei Kommunikationspartnern		
Identitätsdiebstahl innerhalb eines Kommunikationssystems	Verlässliche Verifikation von Identitäten	Möglichkeit der sicheren Prüfung von teilenehmenden Identitäten
Entwenden des Geräts um die Kommunikation nachträglich unbefugt auszuwerten	Sicherung der Zugriffsmöglichkeiten und Zugriffspfade auf die Inhalte	Bildschirmsperre auf dem eingesetzten mobilen Gerät (starkes Passwort) und eine aktivierte Geräteverschlüsselung. Die eingesetzte Kommunikation-App sollte eine eigenständige sichere Aufbewahrung der Daten anbieten und diese gegen Extraktion durch unbefugte schützen.

Tabelle 23: SdT für Secure Instant Messaging

3.2.5.5 Mobile Device Management

Mobile Endgeräte bergen die Gefahr, dass ihre Nutzung innerhalb eines Unternehmers mangels Überblick durch den Verantwortlichen, außer Kontrolle gerät. Sie können so zur Gefahrenquelle oder einem Einfallstor für Angreifer werden. Angriffsvektoren und Stolperfallen bei der Nutzung wären beispielsweise: Geräte gehen verloren, es wird versucht bedenkliche Apps zu installieren und Geräte werden teilweise weder verschlüsselt noch wird eine Bildschirmsperre verwendet. So kann der einfache Mitarbeiter durch die falsche Nutzung seines mobilen Endgerätes eine Gefährdung für die Datensicherheit des gesamten Unternehmens darstellen. Mobile Device Management-Anwendungen (MDM)

greifen hier auf Schnittstellen zu, die durch das mobile Betriebssystem zur Verfügung gestellt werden und erlauben, es die eingesetzten mobilen Geräte zentral administrieren und konfigurieren zu können.

Bedrohung	Gegenmaßnahme	Stand der Technik
Angriffe auf mobile Geräte aufgrund von Schwachstellen durch mangelnde Wartung oder Diebstahl	Durchsetzung von Sicherheitsrichtlinien und Wartungsvorgängen	Definition von verschiedenen Profilen und Richtlinien, die gegenüber dem Nutzer durchgesetzt werden. (z.B. Verschlüsselung des Gerätes und Passwortschutz, Blacklisting von Apps, usw.)
Installation von gefährlichen Apps mittels Sideloading durch den Benutzer	Verbieten der Option Apps aus unsicheren beliebigen Quellen zu beziehen und sie auf dem Gerät zu installieren	Richtlinie für Verhinderung von Installation aus unseren Quellen, Einsatz von Mobile Device Management - Lösungen
Sicherheitslücken durch Nichtinstallation von verfügbaren Updates	Erzwingen von Installationen verfügbarer Updates, um stets das aktuellste Patchlevel zu erreichen	Erzwingen von Updateinstallationen, sobald verfügbar und getestet

Tabelle 24: SdT für Mobile Device Management

3.3 Prozesse

Da Informations- und Kommunikationseinrichtungen nicht immer grundsätzlich auf Sicherheit hin ausgelegt sind und die technische Sicherheit nur dann wirkt, wenn sie mit organisatorischen und personellen Maßnahmen entsprechend flankiert wird, benötigt jede Organisation ein System von Verfahren, Prozeduren und Regeln zum Management der betrieblichen Informationssicherheit, d.h. ein sogenanntes Informationssicherheits-Managementsystem (ISMS).

Durch ein Informationssicherheitsmanagementsystem (ISMS) werden Regeln für die Einordnung von und den Umgang mit schützenswerten Informationen aufgestellt und umgesetzt. Das ISMS ist ein wichtiger Bestandteil des Managementsystems und zieht sich durch alle wichtigen Bereiche des Unternehmens. Zum ISMS gehören Verfahren zur regelmäßigen Überprüfung und Dokumentation organisatorischer und technischer Änderungen.

Ein wichtiger Schwerpunkt des ISMS ist die Berücksichtigung der Anforderungen der Informationssicherheit bei geplanten Veränderungen und Wartungen der wichtiger Elemente der IT-Infrastruktur. Ein weiterer Aspekt ist die regelmäßige Schulung und Sensibilisierung der Mitarbeiter. Außerdem werden im Informationssicherheitsmanagementsystem festgelegt, wie die Notfallvorsorge erfolgt und wie auf eventuelle Sicherheitsvorfälle reagiert werden soll. Ziel des ISMS ist die permanente Einhaltung und Gewährleistung eines effizienten und stets angemessenen Sicherheitsniveaus.

TeleTrusT hat in seinem Dokument "Informationssicherheitsmanagement - Praxisleitfaden für Manager" eine umsetzbare Anleitung für das Management der Informationssicherheit zur Verfügung gestellt. Das Dokument zeigt, dass mit dem Informationssicherheitsmanagement und der damit verbundenen Compliance- und Risikokultur ein strategisches Steuerungsinstrument vorhanden sein kann, das die Sicherheitslage auf einen Blick veranschaulicht.

3.3.1 Standards und Normen

Es existieren eine Reihe von internationalen Standards und Normen, die als Grundlage für die Einführung eines ISMS dienen können. Anders als bei den technischen Maßnahmen kommt, ist der kontinuierliche Wandel der organisatorischen Maßnahmen eine langfristige Erscheinung, so dass ein Referenzieren auf Standards und Normen auch im Zusammenhang mit dem "Stand der Technik" möglich ist. Die ISO/IEC 27000-Reihe wird dabei als Orientierungspunkt für weitere Standards und Normen genutzt. Es kommt zum Teil zu Überschneidungen, jedoch lassen sich die Überschneidungen in der Regel als Synergien nutzen, so dass es im Sinne der Informationssicherheit zu einer positiven Beein-

flussung der eingesetzten Standards kommt. Sofern zusätzliche Standards oder Normen zum Management von IT-Services, Prozessen oder Risiken umgesetzt werden, sollten die angesprochenen Überschneidungen identifiziert und genutzt werden.

3.3.1.1 Die ISO 27000er-Normenwelt

Bei der ISO/IEC 27000-Reihe (manchmal auch nur kurz ISO27k genannt) handelt es sich um eine Reihe von Standards der IT-Sicherheit. Herausgegeben werden diese Normen von der International Organization for Standardization (kurz ISO) und der International Electrotechnical Commission (kurz IEC).

Die ISO/IEC 27001 ist die bekannteste Norm in der ISO/IEC 27000 Reihe. Sie formuliert die zu erfüllenden Anforderungen an ein ISMS. Ergänzend dazu finden sich weitere Normen und Leitfäden für die konkrete Umsetzung.

Die ISO/IEC 27000-Reihe enthält u.a. die folgenden wesentlichen Inhalte, die jeweils als eigenständige Norm geführt werden und als Normen-Reihe zusammengefasst sind.

ISO/IEC Norm	Inhalt
ISO/IEC 27000	Begriffe und Definitionen, welche in der Normenserie ISO/IEC 27000 verwendet werden
ISO/IEC 27001	Anforderungen an ein ISMS
ISO/IEC 27002	Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit
ISO/IEC 27003	Leitfaden zur Umsetzung der ISO/IEC 27001
ISO/IEC 27004	Bewertung der ISMS Effektivität
ISO/IEC 27005	Entwicklung und Betrieb eines Informationssicherheits-Risikomanagementsystems
ISO/IEC TR 27019	Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002
ISO/IEC 27031	Leitfaden zu Konzepten und Prinzipien hinsichtlich der IT-seitigen Unterstützung der Business Continuity in einer Organisation
ISO/IEC 27034	Application Security
ISO/IEC 27035	Information Security Incident Management

Tabelle 25: Übersicht der ISO/EC 27000-Reihe

3.3.1.2 Weitere informationssicherheitsrelevanten Standards und Normen

Informationssicherheitsstandards und -kriterien können nach ihrer Betrachtungsebene als Unternehmen-, System- und Produktstandards klassifiziert werden. Nach ihrer Formulierung lassen sich diese in technische, weniger technische und nicht-technische Standards gliedern.

Angelehnt an eine frühere Darstellung der Initiative D21 ließen sich die o.a. Gliederungsebenen wie folgt darstellen:

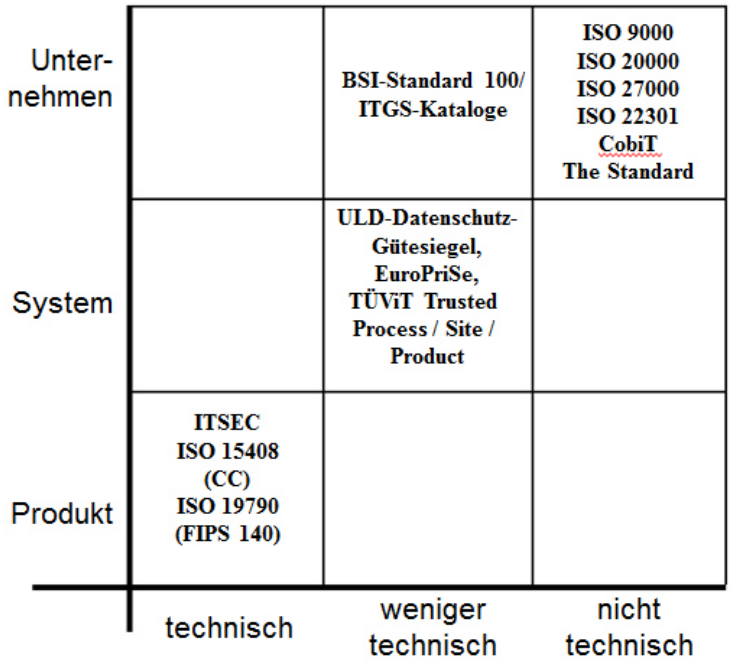

Abbildung 2: Gliederungsebenen informationssicherheitsrelevanten Standards und Normen

Als Standard für Unternehmen und öffentliche Institutionen (Organisationen), der in einer nicht technischen Sprache formuliert ist, entsteht insbesondere der Bedarf der Abgrenzung der ISO 27001 von ISO 9001, ISO 20000-1, ISO 22301, CoBIT und The Standard.

ISO 27000 ff.
Die Normenreihe ISO 27000ff. umfasst mehrere Normen zu ISMS. Kernstück der Normenreihe ist ISO/IEC 27001, welche Andorderungen an ein funktionierendes Informationssicherheits-Managementsystem im Kontext einer Organisation beschreibt (siehe 3.3.1.1).

ISO 27001 auf der Basis von IT-Grundschutz
Hierbei handelt es sich um die Umsetzung der ISO 27001 mit Hilfe der IT-Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik (dokumentiert in BSI-Standard 100-2) und der IT-Grundschutz-Kataloge.

Der BSI-Standard 100-1 definiert allgemeine Anforderungen an ein ISMS. Er ist grundsätzlich kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der anderen ISO-Standards der ISO 2700x-Familie wie beispielsweise ISO 27002. Er bietet Interessierten eine leicht verständliche und syste-matische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

BSI-Standard 100-2 liefert mit der Vorgehensweise nach IT-Grundschutz:

- Konkrete und methodische Hilfestellungen zur schrittweisen Einführung eines Managementsystems für Informationssicherheit
- Betrachtung der einzelnen Phasen des Informationssicherheitsprozesses
- Lösungen aus der Praxis, sogenannte "best practice"-Ansätze
- Möglichkeit zur Zertifizierung

Die Abgrenzung der "nativen" ISO 27001-Umsetzung vom Grundschutz-Ansatz des BSI ist der u.a. Tabelle zu entnehmen:

Kategorie	ISO27001	BSI Grundschutz
Regulatorischer Umfang	Relevante Normen < 100 Seiten	Grundschutz-Kataloge > 4.000 Seiten
Anforderungen	Abstrakte und generische	Konkrete Vorgaben praktischer

	Rahmenbedingungen	Maßnahmen
Risikoanalyse	Vollständige Analyse jedes Zielobjektes	Vereinfachte Analyse bei erhöhtem Schutzbedarf
Maßnahmen	ca. 150 konzeptionelle Anforderungen	> 1.100 konkrete Maßnahmen
Zertifizierung	Zertifizierung	Auditor-Testate + Zertifizierung
Gültigkeit	3 Jahre, jährliche Überwachungsaudits	3 Jahre, jährliche Überwachungsaudits

Tabelle 26: Abgrenzung ISO27001 vs. BSI Grundschutz

ISO 20000-1
Diese Norm spezifiziert Anforderungen an (interne oder externe IT-) Organisationen hinsichtlich der Erbringung von prozessorientierten Dienstleistungen. Ein Teil der dort angeforderten Prozesse (vor allem Information Security Management, Incident & Event Management und Service Continuity Management) haben Überschneidungen mit ISO 27001. Klassischerweise wird ISO 20000-1 auf IT-Organisationen angewandt, während der Geltungsbereich der ISO 27001 aller Arten von Organisationen umfassen kann.

ISO 22301
Die Norm beschäftigt sich mit der Sicherstellung der geschäftlichen Kontinuität (Business Continuity Management, kurz BCM) und spezifiziert Anforderungen an Business Continuity Managementsysteme in Organisationen. BCM Systeme nach ISO 22301 haben auch (aber nicht nur) einen IT-Bezug. Mit dem Thema BCM beschäftigt sich auch ein Themenbereich der ISO 27001, allerdings nur aus der Perspektive der Informationssicherheit (d.h. inwiefern die Geschäftskontinuität durch Informationssicherheitsvorfälle gefährdet werden kann).

ISO 9001
Diese Norm spezifiziert Anforderungen an Qualitätsmanagementsysteme, enthält aber auch erstaunlich viele Informationssicherheitsaspekte, beispielsweise hinsichtlich der Pflichten zur/zum

- Sicherstellung der Verfügbarkeit von Ressourcen und Informationen zur Durchführung und Überwachung der Prozesse
- Kennzeichnung, Aufbewahrung, Schutz und Wiederauffindbarkeit von Aufzeichnungen
- Ermittlung, Bereitstellung und Aufrechterhaltung der Infrastruktur wie Gebäude, Arbeitsort und zugehörige Versorgungseinrichtungen, Prozessausrüstungen (u.a. Hardware und Software) und unterstützende Dienstleistungen (u.a. Kommunikations- und Informationssysteme)
- Schutz des Kundeneigentums, wie geistiges Eigentum, personenbezogene Daten usw.

CobiT
CobiT ist eine Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben. Es ist eine auf Revision und Controlling orientierte "tool box" für das Management, die Ergebnis- und Leistungsmessungen für alle IT-Prozesse definiert. CobiT beschreibt mehrere Prozessbereiche, jeweils mit definierten Kontrollzielen, Reifegradmodell und Messgrößen. CobiT bezieht sich auf alle IT-Prozesse, während ISO 27001 auf die Steuerung des Informationssicherheitsprozesses fokussiert.

The Standard
ISF's Standard of Good Practice for Information Security ist ein "good practice" Ansatz für die betriebliche Informationssicherheit, der auch "Security Benchmarking" erlaubt. The Standard behandelt mehrere Themenbereiche der Informationssicherheit (z.B. IT-Sicherheitsmanagement, geschäftskritische Anwendungen, Informationsverarbeitung, Kommunikation/Netze, Systementwicklung) aus geschäftlicher Perspektive und bietet eine alternative, z.T. ergänzende bzw. komplementäre Sicht zu ISO 27001.

3.3.2 "Stand der Technik" der Prozesse

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt fest, dass es nicht möglich ist, den "Stand der Technik" allgemeingültig und abschließend zu beschreiben. Er lasse sich jedoch "anhand existierender nationaler oder internationaler Standards wie DIN oder ISO-Standards oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln".

Für die vom ITSiG direkt und indirekt betroffenen Unternehmen bedeutet dies, dass eine Vielzahl von allgemeinen und branchenspezifischen Normen und Standards einzuhalten, geprüft und ggf. zertifiziert werden müssen.

In den folgenden Abschnitten findet sich eine kurze Beschreibung der notwendigen organisatorischen Maßnahmen, sowie eine Einschätzung, welche Normen der ISO/IEC 27000-Reihe umzusetzen sind, um dem Stand der Technik zu entsprechen. Die Inhalte dieses Kapitels dienen dabei als Anhaltspunkt. Der konstante technologische Fortschritt sorgt jedoch dafür, dass auch offizielle Rahmenwerke, Normen und Standards einer regelmäßigen Aktualisierung unterliegen.

Einer Betrachtung des "Stands der Technik" bedarf daher eine individuelle Untersuchung, inwieweit eine einzelne Maßnahme oder ein Bündel an Maßnahmen zu einem bestimmten Zeitpunkt sowohl geeignet, erforderlich und angemessen ist.

Im Gegensatz zu den technischen Maßnahmen, bei denen Systeme oder technische Verfahren für den Schutz der Informationen sorgen, beschreiben organisatorische Maßnahmen z.B. Prozesse, Arbeitsanweisungen, Richtlinien oder ähnliches, mit denen sich Unternehmen "selbst verpflichten", die Sicherheit zu erhöhen. Die Umsetzung und Einhaltung obliegt dabei in der Regel den beteiligten Personen und wird bestenfalls durch technische Maßnahmen unterstützt. Regelmäßige Kontrollen und Schulungen sorgen für eine korrekte Implementierung der geplanten Maßnahmen.

Die aktive Unterstützung des Managements und die Mitarbeit der Fachbereiche ist bei der Einführung eines Informationssicherheitsmanagementsystems zwingend erforderlich. Betrachtet werden müssen die Risiken identifiziert und bewertet werden, die auf die Unternehmenswerte Infrastruktur, Personal, IT, Prozesse, Informationen wirken und hierbei einen oder mehrere der Grundwerte von Informationssicherheit (z.B. Vertraulich, Integrität, Verfügbarkeit) beeinträchtigen.

Es lassen sich im Wesentlichen die nachfolgenden organisatorischen Prozesse und Maßnahmen zum Stand der Technik ableiten.

3.3.2.1 Sicherheitsorganisation

Die Sicherheitsorganisation hat die Etablierung eines Management-Frameworks zum Ziel. Die Beschreibung einer Sicherheitsorganisation umfasst die Aufgaben und Verantwortlichkeiten, um die Implementierung und den Betrieb der Informationssicherheit innerhalb der Organisation zu initiieren und kontrollieren.

Damit ein ISMS erfolgreich eingeführt und betrieben werden kann, muss die oberste Leitung

- die Gesamtverantwortung für das ISMS und die Informationssicherheit in der Organisation übernehmen
- sensibilisiert sein und alle relevanten Verantwortungsträger und Mitarbeiter auf mögliche Risiken, persönliche Haftungen bei nicht Einhaltung der Vorgaben sowie auf die Chancen eines ISMS für die eigene Organisation hinweisen und auf die Informationssicherheit verpflichten
- eine effektive Sicherheitsorganisation in Form von Rollen, Verantwortungen und Befugnisse definieren, umsetzen und fortlaufend verbessern
- Dabei sind die folgenden Festlegungen mit Blick auf das Management der Informationssicherheit zu treffen: Organisationsstrukturen (z.B. Abteilungen, Gruppen, Kompetenzzentren), Rollen und Aufgaben.

Als Mindestanforderungen an eine Sicherheitsorganisation gelten:

- die Benennung eines verantwortlichen Managers (Welcher Vorstand oder Geschäftsführer verantwortet das Thema Informationssicherheit unmittelbar/direkt?) und
- die Benennung eines Informationssicherheitsbeauftragten (CISO) als zentrale Rolle innerhalb einer IS-Organisation.

Dabei sind die folgenden Grundregeln unbedingt zu beachten:

- Gesamtverantwortung verbleibt bei der Leitungsebene
- Jeder Mitarbeiter ist verantwortlich für die Informationssicherheit in seinem Arbeitsumfeld

Die wesentlichen Rollen und Zuständigkeiten innerhalb einer Sicherheitsorganisation sind:

Oberste Leitung (Geschäftsführung, Vorstand)

- Strategische Verantwortung (dediziert), jedoch in letzter Instanz auch die Gesamtverantwortung für die Informationssicherheit
- Verantwortung für alle Risikoentscheidungen

Chief Information Security Officer (CISO) / IS-Beauftragter / IT-Sicherheitsbeauftragter

- Taktische bzw. (in Teilen) operative Steuerung der Informationssicherheit
- Unterstützung der Geschäftsführung bei der Wahrnehmung ihrer IS-Aufgaben
- Stabsstelle mit direktem Berichtsrecht und -pflicht an die oberste Leitung

Information Security Officer (ISO)

- Operative Steuerung der Informationssicherheit, ggf. taktische Aufgaben für einzelne Geschäftsbereiche
- Organisatorisch dem CISO direkt zugeordnet

IS-Management-Team / IS Management Forum / Security Steering Committee

- Ständiges Gremium zur Koordinierung der Planung und Umsetzung von Maßnahmen zur Informationssicherheit
- Bestehend aus CISO, ISO(s), Anwendungsvertretern, Fachverantwortlichen, Datenschutzbeauftragten, Vertretern der obersten Leitung
- Beratungs- und Kontrollfunktion für den CISO

Datenschutzbeauftragter /Data Protection Officer

- Nicht zwingend als Teil des IS-Managements anzusehen, aber als wichtiger Ansprechpartner beim Thema Compliance idealerweise regelmäßig in den IS-Management-Prozess mit eingebunden

Auditbeauftragter / Audit Manager

- Zentraler Ansprechpartner für interne und externe Audits
- Koordiniert und steuert die Planung und Durchführung von Audits
- Unterstützung des CISO in dessen Auftrag

Organisatorische Maßnahmen entsprechen dem Stand der Technik, wenn ihre Umsetzung gemäß der aktuell gültigen Normen erfolgt. Für die Maßnahmen sind mindestens die Standards ISO/IEC 27000 bis ISO/IEC 27005 der ISO/IEC 27000er Reihe zu beachten. Sofern weitere anwendbare Anforderungen, Standards oder Ergebnisse von Risikoanalysen es erfordern, können auch weitere organisatorische Maßnahmen erforderlich sein.

3.3.2.2 Anforderungsmanagement

Ein zielgerichtetes und effektives ISMS kann nur im Kontext der Organisation und der Anforderungen an die Informationssicherheit in der Organisation stattfinden. Daher sind die sicherheitsrelevanten Anforderungen festzustellen, deren Umsetzung zu planen, zu realisieren, zu überprüfen und fortlaufend zu verbessern.

Das Anforderungsmanagement bildet die Basis für die Ausrichtung der Informationssicherheit als Prozess und Zustand innerhalb einer Organisation.

Die kontinuierliche Erfüllung von Anforderungen ist der Garant für die Zufriedenheit der interessierten Parteien (Stakeholder) eines ISMS. Aufgrund der Komplexität empfiehlt sich die Etablierung eines Anforderungsmanagementprozesses.

Anforderungen an eine Organisation können unterteilt werden in:

- gesetzliche Anforderungen,
- vertragliche Anforderungen und
- sonstige Anforderungen.

Gesetzliche Anforderungen entstehen aus verschiedenen Rechtsgebieten, wie Datenschutzrecht, Arbeitsrecht, IT-Recht, Strafrecht u.v.a.m. (kein einheitliches "Recht der Informationssicherheit"). Anforderungen (und Erwartungen), zunehmend hinsichtlich einer nachweisbaren Informationssicherheit, können aber auch durch verschiedene Geschäftspartner der Organisation (z.B. durch Kunden, Lieferanten, Dienstleister, Outsourcing-Partner, Kooperationspartner, Versicherungen gestellt werden. Gesetzliche und vertragliche Anforderungen werden oft auch "primäre" oder "grundsätzliche" Anforderungen genannt, da sie an der Basis des IS-Prozesses stehen.

Sonstige Anforderungen (und/oder Erwartungen bzw. Einschränkungen) können sich typischerweise durch die folgenden Instanzen ergeben:

- Markt
- Öffentlichkeit
- Konzern, Zentrale
- Shareholder
- Mitarbeiter
- Geschäftsprozesse (einschl. der intern definierten Regelwerke)
- Technik.

Ein Anforderungsmanagementprozess nach dem "Stand der Technik" ließe sich in einem P-D-C-A-Modell folgendermaßen darstellen:

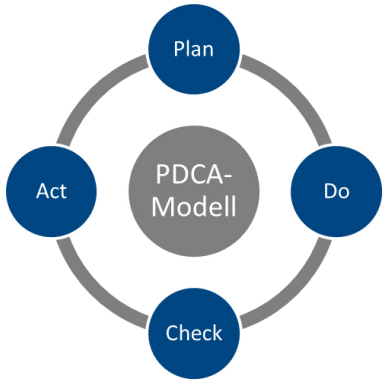

Abbildung 3: PDCA-Modell

PLAN: Anforderungen und Erwartungen aller Art an die Institution

- erfassen,
- analysieren,
- bewerten und
- in interne (Sicherheits-)Vorgaben für die Institution umwandeln

DO: Informationssicherheitsvorgaben der Institution (und damit implizit auch die Anforderungen und Erwartungen an die Institution) erfüllen, bspw. in Form von:

- organisatorischen Maßnahmen: Policies, Regelungen, Richtlinien…
- personellen Maßnahmen Personalüberprüfung, Sensibilisierung, Weiterbildung…
- technischen Maßnahmen Zugangs- und Zugriffskontrolle, Verschlüsselung usw.
- infrastrukturellen Maßnahmen Zutrittskontrolle, Sicherheitszonen…

CHECK: Erfüllungsgrad der Informationssicherheits-Vorgaben der Institution (und damit implizit auch der Anforderungen und Erwartungen an die Institution) überwachen und überprüfen:

- Indikatoren und Parameter abfragen
- Defizite (in Interaktion mit den Stakeholdern) erkennen
- Korrekturmaßnahmen definieren

ACT: Erfüllungsgrad der Informationssicherheits-Vorgaben der Institution (und damit implizit auch der Anforderungen und Erwartungen an die Institution) kontinuierlich verbessern:

- Korrekturmaßnahmen umsetzen und ihre Wirksamkeit überprüfen
- Verbesserung kommunizieren

Ein effektives Anforderungsmanagement garantiert Compliance mit gesetzlichen, vertraglichen und sonstigen Anforderungen und stellt sicher, dass Verstöße gegen gesetzliche, regulatorische, vertragliche und sonstige Verpflichtungen bezüglich Informationssicherheit vermieden werden.

Durch positive Bewertungen des ISMS und der erreichten Informationssicherheit wird gewährleistet, dass diese angemessen implementiert sind und im Einklang mit den Unternehmensrichtlinien, -verfahren und den relevanten Anforderungen betrieben werden.

3.3.2.3 Management des Geltungsbereichs

Der Anwendungs- und Geltungsbereich eines ISMS sollte stets den Anforderungen an die Informationssicherheit der Organisation Rechnung tragen. Der Geltungsbereich entwickelt sich dementsprechend. Entsprechende Veränderungen sind sorgfältig zu planen und umzusetzen.
Eine Dokumentation und Begründung des Geltungsbereichs ist für den Nachweis des "Stands der Technik" vorzuhalten.

3.3.2.4 Management der Informationssicherheits-Leitlinie

Als Grundlage für ein Informationssicherheits-Management-System muss die Ausrichtung der Unternehmensführung auf Informationssicherheit bestimmt werden. Ziel ist, dass die Unternehmensführung eine Richtung vorgibt und die Schutzziele im Einklang mit Geschäftsanforderungen und relevanten Gesetzen und Vorschriften stehen.

Um dem "Stand der Technik" zu entsprechen müssen die Informationssicherheitspolitik und Informationssicherheitsziele in Form einer Leitlinie definiert und verpflichtend innerhalb der Organisation bekanntgemacht werden. Des Weiteren sollten ausreichend Ressourcen zur Verfügung gestellt und Wichtigkeit der Erfüllung der Anforderungen vermittelt werden. Die Leitlinie (einschl. der Informationssicherheitsziele) sollte mindestens einmal jährlich inhaltlich auf ihre Aktualität und Relevanz geprüft und bei Bedarf verbessert werden.

3.3.2.5 Risikomanagement

Das Risikomanagement besteht aus einer systematischen Risikoanalyse und Identifikation, Überwachung und Handhabung der Risikogebiete. Ziel ist die systematische Identifizierung von Chancen und Risiken für ein Unternehmen, sowie die Bewertung der Risiken in Bezug auf die Eintrittswahrscheinlichkeit und quantitative Auswirkungen auf die Unternehmenswerte.

Für das Risikomanagement nach dem "Stand der Technik" müssen Regeln zur Ermittlung der organisationseigenen Werte, Schwachstellen, Bedrohungen, Auswirkungen und Eintrittswahrscheinlichkeiten bestimmt und die zulässige Höhe des Restrisikos definiert werden. Ebenso die Methodik zur Durchführung einer Risikoeinschätzung- und Behandlung sowie zur Übernahme der Restrisiken durch die oberste Leitung.

Bestehende Risiken müssen auf dieser Basis analysiert, bewertet und behandelt werden. Die Restrisiken müssen von der obersten Leitung nachweislich übernommen und die Risikolage der Organisation fortlaufend optimiert werden.

3.3.2.6 Management der Erklärung zur Anwendbarkeit

In einer Erklärung zur Anwendbarkeit muss stets aktuell dokumentiert sein, welche Controls aus der Anlage A der ISO 27001 (ggf. auch sonstige Sicherheitsmaßnahmen) anwendbar sind und welche nicht, die Gründe für diese Entscheidung sowie eine Beschreibung, wie diese Maßnahmen umzusetzen sind. Die Erklärung zur Anwendbarkeit vermittelt nach dem "Stand der Technik" im jeweiligen Überprüfungszyklus ein aktuelles Bild über den Soll- und den Ist-Zustand der Informationssicherheit in einer Organisation

3.3.2.7 Ressourcenmanagement

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung des ISMS bestimmen, bereitstellen und dem tatsächlichen Bedarf fortlaufend anpassen.
Der "Stand der Technik" erfordert, dass die bereitgestellten Ressourcen den Erfordernissen mindestens entsprechen.

3.3.2.8 Wissens- und Kompetenzmanagement

Damit ein ISMS professionell gelebt werden kann, sollten die handelnden Personen entsprechende Kompetenzen aufweisen bzw. durch Weiterbildungen dahingehend geschult werden. Um dem "Stand der Technik" zu entsprechen, ist der Wissens- und Kompetenzbedarf zu bestimmen, die Kompetenz anzueignen und dem tatsächlichen Bedarf fortlaufend anzupassen.

3.3.2.9 Dokumentations- und Kommunikationsmanagement

Hierbei geht es darum, sowohl die Festlegungen, als auch den tatsächlichen Zustand des ISMS und der Informationssicherheit, einschl. der Erreichung der Ziele, Behandlung der Risiken und Erfüllung der Anforderungen zu dokumentieren und zielgruppengerecht an die interessierten Parteien zu kommunizieren.

Um dem "Stand der Technik" zu entsprechen, müssen für alle zu überprüfenden Controls die notwendigen Dokumentationen erstellt und nachweislich kommuniziert worden sein.

3.3.2.10 IT-Servicemanagement

Ein IT-Servicemanagement liefert eine Vorgehensweise auf allen Management-Ebenen der IT sowie auf allen Sachebenen beginnend bei der Geschäftsausrichtung, über die Servicegestaltung und Gewährleistung der Informationssicherheit bis hin zum Betrieb von Anwendungen und Infrastruktur und

dem hiermit verbundenen Technologieeinsatz. Wichtig ist die Einbettung des Sicherheitsprozesses in die Prozesslandschaft des Unternehmens.

Neben den im Dokument "Informationssicherheitsmanagement - Praxisleitfaden für Manager" beschriebenen Schnittstellen und Prozessen, sind für die Einhaltung des "Stands der Technik" insbesondere die folgenden Prozesse zu beachten:

Asset Management
Das Asset Management beschreibt drei wesentliche Aspekte für die Unternehmenswerte und stellt die Basis für die Analyse und Bewertung der Risiken (siehe auch 3.3.2.5). Die Verantwortlichkeiten, die Klassifizierung und die Handhabung von Medien. Zur Bestimmung der Verantwortlichkeiten werden die Unternehmenswerte identifiziert und eine geeignete Schutzverantwortung definiert. Sind die Werte und verantwortlichen Rollen definiert, wird anhand einer Klassifizierung gewährleistet, dass die Information ein angemessenes Schutzniveau im Einklang mit seiner Bedeutung für die Organisation erhalten. Eine Richtlinie zur Handhabung von Medien sorgt dafür, dass die unberechtigten Weitergabe, Veränderung, Beseitigung oder Zerstörung von auf Medien gespeicherten Informationen vermieden wird.

Schulungen & Awareness
Die Sensibilisierung der Mitarbeiter ist eine wesentliche Voraussetzung für die Umsetzung des gewünschten Sicherheitsniveaus. Mitarbeiter sollten wissen, welchen Stellenwert die Informationssicherheit im Unternehmen hat und wie sie persönlich dazu beitragen können, dieses Ziel zu erreichen. Auch sollten sie das Verhalten bei Verdacht oder Feststellung von Sicherheitsvorfällen kennen. Für die Erfüllung ihrer Aufgaben sollten die Mitarbeiter im Interesse der Informationssicherheit periodisch geschult werden, um alle für sie relevanten organisatorischen und technischen Rahmenbedingungen beherrschen zu können. Die Schulungen und Belehrungen helfen den Mitarbeitern, die (IT-)Technik ordnungsgemäß zu bedienen und alle erforderlichen Regelungen einzuhalten. Diese Aspekte sind ggf. im Rahmen des Prozesses Ressourcenmanagement (siehe 3.3.2.7) zu regeln.

Betrieb
Der Betrieb einer Sicherheits-Organisation und -Umgebung dient dazu, alles zu unternehmen, um das Netzwerk, Computer- und Server-Systeme, Anwendungen und Lösungen in einem sicheren und geschützten Zustand zu halten. Er stellt sicher, dass Mitarbeiter, Anwendungen und Server die richtigen Zugriffsrechte auf ihnen erlaubte Ressourcen haben und dass eine Überwachung über Monitoring, Audits und Reporting eingerichtet ist. Der Betrieb findet nach der Implementierung und dem Test eines Systems statt und stellt kontinuierliche Wartung, Updates und Kontrollen sicher.

Referenzmodelle zum IT-Servicemanagement (z.B. ITIL) geben einen Rahmen für den erfolgreichen Betrieb. So können die Prozesse des Informationssicherheitsmanagements eng an die übrigen IT-Prozesse angekoppelt werden.

Incident Management
Im Rahmen des Incident Managements werden technische und organisatorische Maßnahmen als Reaktion auf erkannte oder potentielle Sicherheitsvorfälle zusammengefasst. Neben der Erfassung, Analyse und Verwaltung von Problemen, Schwachstellen oder gezielten Angriffen, wird auch beschrieben und geplant, wie mit solchen Vorfällen umgegangen wird, was auch organisatorische und juristische Fragestellungen mit einschließt.

Ziel des Incident Managements ist es, Planung voranzutreiben, Voraussetzungen zu identifizieren und umzusetzen, um im Falle eines Vorfalls ohne zeitliche Verzögerung effektive und effiziente Maßnahmen zum Schutz der Organisation durchführen zu können.

Continuity Management
Im Rahmen des Continuity Managements werden technische und organisatorischen Maßnahmen zur Vermeidung von Betriebsausfällen zusammengefasst. Neben der Erfassung, Analyse und Management der Ausfallrisiken und deren Auswirkungen entlang der Zeitachse, wird auch beschrieben und geplant, wie mit der Eskalation von Incidents auf Notfälle umgegangen wird, was auch organisatorische und juristische Fragestellungen mit einschließt.
Ziel des Continuity Managements ist es, Planung voranzutreiben, Voraussetzungen zu identifizieren und umzusetzen, um im Falle eines Notfalls ohne zeitliche Verzögerung effektive und effiziente Maßnahmen zum Schutz der Organisation durchführen zu können.

Beschaffung
Vor der eigentlichen Beschaffung von IT-Systemen oder Leistungen sollten einige vorbereitende Schritte unternommen werden, um sicherzustellen, dass das Resultat den Anforderungen des Unternehmens entspricht. Dies gilt sowohl für inhaltliche, wie für sicherheitsrelevante Aspekte. Diese Punkte beinhalten z.B.:

- Anforderungsanalyse
- Risikoanalyse
- Sicherheitsanalyse (Anforderungen zu Funktionen und zur Zuverlässigkeit)
- Test- und Abnahmeplan.

Sind Lieferanten längerfristig in der Bereitstellung von Software, Lösungen oder Dienstleistungen involviert, so ist sicherzustellen, dass der Schutz der Unternehmenswerte, die Lieferanten zugänglich sind, gewährleistet ist. Dies beinhaltet insbesondere Service Level und ein Sicherheitsniveau, die in einer Lieferantenvereinbarung abgebildet sind.

Softwareentwicklung und IT-Projekte
IT-Projekte müssen das Thema Informationssicherheit von Beginn an transparent und messbar behandeln. Projektorganisationen in Unternehmen müssen zu einem strengeren, wiederholbaren Prozess übergehen, der das Thema Sicherheit als elementaren Baustein in jeder Phase einschließt und verbindliche Verantwortlichkeiten für den Security Manager in jeder Projektphase festlegt. Diese Vorgaben müssen durch die Unternehmensleitung bekräftigt und legitimiert sein. Insbesondere bei den Phasenübergängen muss eine formelle Freigabe-Regelung getroffen werden, um den obligatorischen Aspekt von "Secure by Design" im IT-Prozess zu unterstreichen.

Erfahrungen zeigen, dass das Sicherheitsteam, insbesondere in der Planungs- und Realisierungsphase, in enger Abstimmung mit dem Projektteam stehen sollte. Das Sicherheitsteam sollte zusätzliche Sicherheitsanforderungen und eine verbindliche Sicherheitsarchitektur definieren sowie eine Bedrohungsanalyse durchführen. Die Ergebnisse fließen dann in die Gesamtkonzeption ein und verhindern so aufwändige Korrekturen in späteren Projektphasen.

3.3.2.11 Management der Erfolgskontrolle

Dieser Prozess beinhaltet sämtliche Überwachungs-, Messungs-, Analyse- und Bewertungsaktivitäten zum ISMS und der in diesem Rahmen erzeugten Informationssicherheit. Diese müssen für die Einhaltung des "Stands der Technik" überwacht und überprüft werden. So müssen u.a. Protokolle aufgezeichnet und regelmäßig ausgewertet, aber auch interne Audits und technische Systemaudits in regelmäßigen Abständen durchgeführt werden, um Informationen darüber zu erhalten, ob das ISMS und die damit erzeugte Informationssicherheit (immer noch) den Anforderungen genügt, wirksam umgesetzt und aufrechterhalten werden. Die oberste Leitung muss das ISMS mindestens einmal jährlich daraufhin bewerten, ob und inwiefern es seinen definierten Zweck erfüllt und zur Umsetzung der Informationssicherheitsziele beiträgt. Dies stellt die Grundlage für weitere Entscheidungen dar.

Technische Systemaudits, interne und externe Audits können als Unterprozesse(s.u.) des hier angesprochenen Prozesses angesehen werden. Ebenso auch alle weiteren Kategorien von Überwachungs-, Messungs-, Analyse- und Bewertungsaktivitäten.

3.3.2.11.1 Technische Systemaudits

Technische Systemaudits (Prüfungen auf Netzwerk-, System- und Applikationsebene) müssen regelmäßig durch die oder im Namen der Organisation durchgeführt werden. Typischerweise werden diese als Penetrationstests oder Webchecks durchgeführt.

- Bei einem kleinen IS-Penetrationstest werden in Form eines technischen Audits stichprobenartig sicherheitsrelevante Konfigurationen und Regelwerke der eingesetzten IT-Systeme untersucht und Empfehlungen für das Schließen möglicher Schwachstellen gegeben. Die Sichtung der IT-Systeme wird gemeinsam mit den Administratoren durchgeführt.

- Bei einem umfangreichen IS-Penetrationstest werden, über das technische Audit hinaus, durch technische Untersuchungen u.a. mit Hilfe von speziellen Sicherheitstools Schwachstellen in den getesteten IT-Systemen aufgespürt. Hierbei greifen die Tester vor Ort unter Aufsicht der Fachadministratoren auf die zu untersuchenden IT-Systeme zu.
- Mit einem IS-Webcheck wird der Sicherheitsstand der Internet-, Intranet- und/oder Extranetpräsenz der Organisation geprüft. Hierbei werden die Tests größtenteils durch den Einsatz automatisierter Methoden über das Internet und ggf. auch aus dem internen Netz (bei Intranet und Extranet) durchgeführt.

3.3.2.11.2 Interne und externe Audits, ISMS-Zertifizierung

ISMS-Audits verfolgen die folgende Zielsetzung:

- Prüfung des Fortschritts der Implementierung des ISMS
- Feststellung der Übereinstimmung des ISMS mit den Auditkriterien der Organisation
- Feststellung der Fähigkeit des ISMS, die rechtlichen, behördlichen und mit Verträgen verbundenen Anforderungen zu erfüllen
- Prüfung der Anwendung und Wirksamkeit des ISMS
- Identifikation von Schwachstellen / Verbesserungspotenzial des ISMS

Interne Audits müssen innerhalb eines Geltungsbereichs des ISMS grundsätzlich mindestens einmal pro Jahr durch die Organisation oder im Namen der Organisation durchgeführt werden. Zum Stand der Technik entspricht, dass jede Organisationseinheiten (bzw. jeder Bestandteil des Geltungsbereichs wie Standort, Gebäude usw.) mindestens alle drei Jahre intern auditiert wird.

Externe ISMS-Audits werden von Parteien durchgeführt, die an der Organisation interessiert sind (z.B. Kunden) [Second Party Audit] oder aber von externen, unabhängigen Auditorganisationen durchgeführt [Third Party Audit].

Im Rahmen der Durchführung von Zertifizierungsaudits prüft das Auditteam die Erfüllung der Anforderungen aus der ISO 27001, welche unter Berücksichtigung der Standards ISO 27002 und ISO 27005 realisiert sein muss. Auditoren von Zertifizierungsstellen werden angehalten, im Rahmen des Auditverfahrens die Standards ISO 19011 und ISO 27007 zu berücksichtigen. ISO/IEC TR 27008 enthält einen Leitfaden zur Auditierung der ISMS-Controls und findet ebenfalls Anwendung.
Im Rahmen eines Zertifizierungsverfahrens übernimmt die Zertifizierungsstelle die folgenden Aufgaben:

- Prüfung der Auditergebnisse inkl. Auditschlussfolgerungen
- Dokumentierung der Prüfung der Auditergebnisse inkl. Auditschlussfolgerungen
- Zertifizierungsbericht mit Zertifikatfreigabe
- Ausstellung des Zertifikates.

Qualifizierte Zertifizierungsstellen für ISO 27001 besitzen eine Akkreditierung nach ISO 17021 und ISO 27006.Eine Übersicht in Deutschland akkreditierter Stellen zur ISMS-Zertifizierung kann auf der Internetseite der Deutschen Akkreditierungsstelle (DAkkS) abgerufen werden.

Zertifizierungen nach ISO 27001 haben eine Gültigkeitsdauer von 3 Jahren und werden mindestens jährlich im Rahmen sogenannter Überwachungsaudits überwacht. Sollte das Zertifikat nach 3 Jahren erneuert werden, muss die Organisation vor Ablauf der dreijährigen Frist ein Re-Zertifizierungsaudit erfolgreich bestanden haben.

3.3.2.12 Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess)

Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit ihres ISMS fortlaufend verbessern.

Die wesentlichen Aktivitäten hinsichtlich der Aufrechterhaltung und fortlaufenden Verbesserung eines ISMS zielen auf Bewertung und fortlaufende Optimierung der Leistung des ISMS. Im Einzelnen sind hier die nachfolgenden Aspekte zu regeln:

- Umgang mit Nichtkonformitäten, die aus der Überwachung, Messung, Analyse und Bewertung des ISMS und der in diesem Rahmen erzeugten Informationssicherheit resultieren
- Definition und Umsetzung von Korrekturmaßnahmen zur Beseitigung der Ursache von Nichtkonformitäten
- Fortlaufende Verbesserung der Eignung, Angemessenheit und Wirksamkeit des ISMS sowie der damit erzeugten Informationssicherheit.

4 Anhang

4.1 Tabellenverzeichnis

4.2 Abbildungsverzeichnis

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.), "TeleTrusT Engineer for System Security" (T.E.S.S.) und "Certified Professional for Secure Software Engineering" (CPSSE) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.