Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2020

Danksagung

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

Projektleitung

RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte
Tomasz Lawicki - m3 management consulting GmbH

Autoren und mitwirkende Experten

Alsbih, Amir
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - Genua GmbH
Dehning, Oliver - Hornetsecurity GmbH
Dominkovic, Dennis - SEC Consult Unternehmensberatung GmbH
Dubbel, Sascha - CrowdStrike GmbH
Falkenthal, Oliver - CCVOSSEL GmbH
Fischer, Marco - procilon IT-Solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Jäger, Hubert - Digital Trust Innovations
Kerbl, Thomas - SEC Consult Unternehmensberatung GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Lawicki, Tomasz - m3 management consulting GmbH
Liedke-Deutscher, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line GmbH
Paulsen, Christian
Robin, Markus - SEC Consult Unternehmensberatung GmbH
Rost, Peter - secunet Security Networks AG
Schlensog, Alexander - secunet Security Networks AG
Wüpper, Werner - Wüpper Management Consulting GmbH

Impressum

Herausgeber:

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

V 1.7_2020-10 DE

Inhalt

Grundsätze der Handreichung 6

1 Einleitung 7
1.1 IT-Sicherheitsgesetz 7
1.2 Branchenspezifische Sicherheitsstandards des BSI für KRITIS-Betreiber 8
1.3 Europäische Implikationen 9
1.4 Datenschutz-Grundverordnung 9
1.5 Angemessenheit der Maßnahmen 10

2 Bestimmung des Technologiestandes 11
2.1 Begriffsklärung 11
2.2 Methode zur Bestimmung des Technologiestandes 12
2.3 Prozess zur Qualitätssicherung der Handreichung 13
2.4 Geforderte Schutzziele 14

3 Technische und organisatorische Maßnahmen (TOM) 16
3.1 Allgemeine Hinweise 16
3.2 Technische Maßnahmen 19
3.2.1 Bewertung der Passwortstärke 19
3.2.2 Durchsetzung starker Passwörter 21
3.2.3 Multifaktor-Authentifizierung 22
3.2.4 Kryptographische Verfahren 25
3.2.5 Verschlüsselung von Festplatten 26
3.2.6 Verschlüsselung von Dateien und Ordnern 28
3.2.7 Verschlüsselung von E-Mails 29
3.2.8 Sicherung des elektronischen Datenverkehrs mit PKI 31
3.2.9 Einsatz von VPN (Layer 3) 34
3.2.10 Verschlüsselung auf Layer 2 36
3.2.11 Cloudbasierter Datenaustausch 38
3.2.12 Datenablage in der Cloud 39
3.2.13 Nutzung von mobilen Sprach- und Datendiensten 41
3.2.14 Kommunikation mittels Instant-Messenger 42
3.2.15 Management mobiler Geräte 44
3.2.16 Routersicherheit 45
3.2.17 Netzwerküberwachung mittels Intrusion Detection System 47
3.2.18 Schutz des Web-Datenverkehrs 49
3.2.19 Schutz von Webanwendungen 50
3.2.20 Fernzugriff auf Netzwerke / Fernwartung 52
3.2.21 Server-Härtung 54
3.2.22 Endpoint Detection & Response Plattform 57
3.2.23 Internetnutzung mit Web-Isolation 59
3.2.24 Angriffserkennung und Auswertung (SIEM) 61
3.2.25 Vertrauliche Datenverarbeitung 62
3.2.26 Sandboxing zur Schadcode-Analyse 64
3.2.27 Cyber Threat Inteliigence 66
3.3 Organisatorische Maßnahmen 68
3.3.1 Standards und Normen 68
3.3.2 Prozesse 72
3.3.2.1 Sicherheitsorganisation 72
3.3.2.2 Anforderungsmanagement 74
3.3.2.3 Management des Geltungsbereichs 75
3.3.2.4 Management der Informationssicherheits-Leitlinie 75
3.3.2.5 Risikomanagement 75
3.3.2.6 Management der Erklärung zur Anwendbarkeit 76
3.3.2.7 Ressourcenmanagement 76
3.3.2.8 Wissens- und Kompetenzmanagement 76
3.3.2.9 Dokumentations- und Kommunikationsmanagement 76
3.3.2.10 IT-Servicemanagement 76
3.3.2.11 Management der Erfolgskontrolle 79
3.3.2.12 Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess) 80

3.3.3 Sichere Softwareentwicklung 81
3.3.4 Prozesszertifizierung 84
3.3.5 Schwachstellen- und Patchmanagement 88
3.3.6 Management von Informationssicherheitsrisiken 90

Abbildungsverzeichnis

Abbildung 1: Drei-Stufen-Theorie nach Kalkar-Entscheidung
Abbildung 3: Bewertungskriterien
Abbildung 4: Beispiel der Einordnung des Technologiestandes
Abbildung 6: Prozessskizze für die Bewertung der technischen Maßnahmen im Kapitel 3.2
Abbildung 7: Gliederungsebenen informationssicherheitsrelevanter Standards und Normen
Abbildung 8: PDCA-Modell

Tabellenverzeichnis

Tabelle 1: Übersicht der ISO/IEC 27000-Reihe
Tabelle 2: Abgrenzung ISO 27001 vs. BSI Grundschutz

Grundsätze der Handreichung

Als im Juli 2015 das IT-Sicherheitsgesetz in Kraft trat, hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) den Arbeitskreis "Stand der Technik" (im Folgenden auch "AK SdT") initiiert, um den Betroffenen Handlungsempfehlungen und Orientierung zum geforderten "Stand der Technik" von technischen und organisatorischen Maßnahmen zu geben. Um diesem hohen Anspruch gerecht zu werden, hat der Arbeitskreis die folgenden Grundsätze für die Entwicklung, Evaluierung und Fortschreibung der Handreichung festgelegt:

1. **Grundverständnis des Dokumentes**
   Diese Handreichung soll den anwendenden Unternehmen und Anbietern (Herstellern, Dienstleistern) gleichermaßen Hilfestellung zur Bestimmung des "Standes der Technik" im Sinne des IT-Sicherheitsgesetzes (IT-SiG) und der Datenschutz-Grundverordnung (DSGVO) geben. Das Dokument kann dabei als Referenz für vertragliche Vereinbarungen, Vergabeverfahren bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen.

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

2. **Verantwortung für die Entwicklung, Evaluierung und Fortschreibung**
   Der Arbeitskreis und die TeleTrusT-Arbeitsgruppe "Recht" widmen sich der Beantwortung der Frage, wie sich der jeweilige Stand der Technik im Sinne des Gesetzes in Bezug auf die technischen und organisatorischen Maßnahmen bestimmen lässt und wie rechtliche Anforderungen umzusetzen sind.

3. **Vorgehensverständnis**
   Der Arbeitskreis erarbeitet seine Ergebnisse in einem transparenten Verfahren und stellt die Handlungsempfehlungen und Orientierungen in einem regelmäßigen Fortschreibungsverfahren öffentlich zur Diskussion.

4. **Bewertungsverfahren**
   Der Arbeitskreis legt seiner Bewertung ein standardisiertes Schema zugrunde, das für die einzelnen betrachteten Maßnahmen ausgefüllt und veröffentlicht wird. Die Methode zur Bewertung des Technologiestandes der technischen Maßnahmen ist beschrieben im Kapitel 2.2.

5. **Fortschreibung**
   Um dem technologischen Fortschritt gerecht zu werden, ist es vorgesehen, diese Handreichung regelmäßig fortzuschreiben und zu publizieren. Gegenwärtig wird eine zweijährliche Publikation der Handreichung angestrebt.
   Kleine Anpassungen und Ergänzungen der Handreichung (z.B. neue Beiträge der technischen Maßnahmen) werden als sog. Revisionen der Handreichung unterjährlich erscheinen.

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.

1 Einleitung

1.1 IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz (ITSiG) ist seit dem 25.07.2015 in Kraft und soll zu einer Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland beitragen. Die dem Gesetz zugrunde liegenden Regelungen 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: Das Gesetz selbst diente lediglich zu einer Anpassung verschiedener bereichsspezifischer Gesetze. Durch das ITSiG 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) und Telekommunikationsgesetz (TKG) vorgenommen.

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

Die umfassendsten Änderungen sieht das ITSiG für KRITIS-Betreiber sowie Unternehmen, die Telemedienangebote bereithalten, vor. Betreiber Kritischer Infrastrukturen sollen gemäß § 8a Absatz 1 BSIG ein dem Stand der Technik entsprechendes Mindestniveau an IT-Sicherheit einhalten. 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, denen die KRITIS-Betreiber die betreffenden Pflichten vertraglich auferlegen.

Gemäß § 10 Absatz 1 des BSIG ist 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 stimmte am 13.04.2016 dem Erlass der vom Bundesinnenminister vorgelegten Ministerverordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) zu. Dieser erste Teil der KRITIS-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes ist in der Folge am 03.05.2016 in Kraft getreten. Am 31.05.2017 wurde zudem der zweite Teil der KRITIS-Verordnung beschlossen, der schließlich am 01.06.2017 in Kraft trat. Die Verordnung regelt die Einstufung von Unternehmen als Kritische Infrastrukturen für die Bereiche Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation (1. Korb) sowie die Sektoren Gesundheit, Finanzen und Transport und Verkehr (2. Korb).

Betreiber Kritischer Infrastrukturen haben gemäß § 8a Absatz 1 BSIG eine Frist von zwei Jahren nach Inkrafttreten der Rechtsverordnung, angemessene technische und organisatorische Vorkehrungen (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 gemäß § 13 Absatz 7 TMG zu gewährleisten, dass ihre technischen Einrichtungen im Rahmen ihrer technischen und wirtschaftlichen Möglichkeiten durch 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 Branchenspezifische Sicherheitsstandards des BSI für KRITIS-Betreiber

Das ITSiG fordert von den KRITIS-Betreibern die Einhaltung oder mindestens Berücksichtigung des "Standes der Technik" von IT-Sicherheitsmaßnahmen. Dieses Sicherheitsniveau wird im Gesetz allerdings nicht weitergehend konkretisiert. Jedoch ist es zulässig, für die KRITIS-Sektoren die sogenannten branchenspezifischen Sicherheitsstandards (im Folgenden "B3S" genannt) vorzuschlagen. Die Anerkennung der von den Branchenvertretern vorgeschlagenen branchenspezifischen Sicherheitsstandards obliegt dem BSI.

Erste Hinweise für die Erarbeitung eines solchen B3S finden die betroffenen KRITIS-Betreiber und Verbände in dem vom BSI veröffentlichten Entwurf einer "Orientierungshilfe zu Inhalten und Anforderungen an B3S gemäß § 8a Abs. 2 BSIG"[1]. Der Entwurf sieht folgende Vorgehensweise vor:

1. Definition des Geltungsbereichs sowie der Schutzziele des B3S.
2. Einschätzung der branchenspezifischen Gefährdungslage.
3. Risikoanalyse zur branchenspezifischen Gefährdungslage.
4. Ableitung geeigneter und angemessener Maßnahmen für die Branche im Fokus.

Der B3S soll demnach bei der Auswahl geeigneter Maßnahmen unterstützen, indem er auf Vorkehrungen und Maßnahmen nach dem branchenüblichen "Best Practice" verweist. Zudem soll der B3S bei Bedarf deren Grenzen aufzeigen, wenn beispielsweise ein "Mehr" an Schutz und somit ergänzende Maßnahmen benötigt wird und solche ergänzenden Vorkehrungen und Maßnahmen vorschlagen.

Bei der Frage der Angemessenheit ist vor allem der bei dem KRITIS-Betreiber erforderliche wirtschaftliche Aufwand, insbesondere die von ihm aufzuwendenden Realisierungskosten, zu berücksichtigen. Schließlich soll der für die Realisierung *"erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur*" stehen[2]. Ob eine Maßnahme angemessen, also wirtschaftlich ist, kann jedoch nur individuell unter Berücksichtigung des eigenen Schutzbedarfes und der Realisierungskosten für etwaige erforderliche Maßnahmen festgestellt werden.

Im Anschluss benennt die Orientierungshilfe eine Liste von Themen (z.B. Asset Management, Lieferanten, Dienstleister und Dritte), welche durch den B3S unbedingt abzudecken sind. Darauffolgend erhalten die betroffenen KRITIS-Betreiber und Verbände noch Hinweise, in welcher Detailtiefe Vorkehrungen im B3S zu beschreiben sind. Zuletzt nennt die Orientierungshilfe noch Optionen zur Nachweisbarkeit der Umsetzung.

Die Orientierungshilfe verdeutlicht nochmals, dass das Festlegen eines Mindeststandards für eine bestimmte Branche von vielen einzelnen Faktoren abhängig ist. Eine genaue Bestimmung des Mindeststandards muss mithin anhand der individuellen Voraussetzungen vorgenommen werden. Dies gilt insbesondere für regulierte Sektoren, welche spezialgesetzlichen Regelungen, wie beispielsweise dem Telekommunikationsgesetz, unterliegen.

Im Sektor Wasser für die Branchen Wasserversorgung und Abwasserbeseitigung ist seit dem 01.08.2017 erstmalig ein branchenspezifischer Standard (B3S WA) definiert und vom BSI anerkannt worden. Der B3S WA setzt sich aus einem Merkblatt und einem IT-Sicherheitsleitfaden zusammen,

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html.
[2] § 8a Abs. 1 Satz 3 BSIG

welcher jährlich aktualisiert werden soll. Als Grundlage nutzt der B3S WA den BSI-Grundschutzkatalog sowie branchenspezifische Sicherheitsanforderungen.

Unklar bleibt jedoch, nach welchen Kriterien die vorgeschlagenen Sicherheitsstandards vom Sektor Wasser ausgewählt und nach welchen Kriterien diese dann vom BSI als "B3S WA" im Sinne des "Standes der Technik" anerkannt wurden.

1.3 Europäische Implikationen

Das BSIG wird durch weitere europäische Vorgaben ergänzt. Die Kommission hat dazu die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie) verabschiedet, die in nationales Recht umzusetzen ist. Grundlegende Änderungen daraus ergeben sich nicht, da der nationale Gesetzgeber durch Verabschiedung des ITSiG bereits einen Großteil der vom europäischen Gesetzgeber beabsichtigten Anforderungen vorweggenommen hat. Das entsprechende, am 27.04.2017 verabschiedete, NIS-Richtlinien-Umsetzungsgesetz führt demnach lediglich zu einer Ergänzung des BSIG.

Auf Grundlage der Richtlinie wurde unter anderem der § 8c BSIG geschaffen, der zusätzliche Verpflichtung für Anbieter sogenannter digitaler Dienste schafft. Digitale Dienste sind danach Online-Marktplätze, Online-Suchmaschinen sowie Cloud-Computing-Dienste einer normierten Größe. Auch diese Dienste haben technische und organisatorische Maßnahmen (TOM) zum Schutze der IT Sicherheit umzusetzen, die den Stand der Technik zu berücksichtigen haben. Die Maßnahmen sollen ein dem Risiko entsprechendes angemessenes Schutzniveau gewährleisten und dabei unter anderem die Sicherheit der Systeme und Anlagen, den Umgang mit Sicherheitsvorfällen sowie das Betriebskontinuitätsmanagement berücksichtigen.

1.4 Datenschutz-Grundverordnung

Die europäische Datenschutz-Grundverordnung (DSGVO) wurde 2016 verabschiedet und entfaltete am 25.05.2018 endgültig Geltung. Primäres Ziel der DSGVO ist der Schutz personenbezogener Daten europäischer Bürger. Dabei liegt der Verordnung hinsichtlich ihrer Schutzziele ein risikobasierter Ansatz zugrunde. Im Bereich des technischen Datenschutzes sind zum Schutze der Rechte und Freiheiten natürlicher Personen entsprechende technische und organisatorische Maßnahmen zu treffen. Diese haben ebenfalls das Tatbestandsmerkmal "Standes der Technik" zu berücksichtigen. Insbesondere der die Sicherheit der Verarbeitung regelnde und zudem den § 9 Bundesdatenschutzgesetz (BDSG) zusammen mit seiner Anlage 1 ablösende Art. 32 DSGVO sieht vor, dass der Stand der Technik im Rahmen der Sicherheit der Datenverarbeitung zu berücksichtigen ist. Hierzu haben Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen. Wie auch das ITSiG, sieht die DSGVO keine Definition für das Tatbestandsmerkmal des Standes der Technik vor. Gleiches gilt ebenfalls für das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) sowie die daraus resultierende Neufassung des BDSG (BDSG-neu).

Darüber hinaus sind gemäß Art. 25 DSGVO die Grundsätze des Datenschutzes durch Technikgestaltung (privacy by design) sowie durch datenschutzfreundliche Voreinstellungen (privacy by default) zu beachten. Diese Grundsätze sind auch durch geeignete technische und organisatorische Maßnahmen umzusetzen.

Der Stand der Technik ist im Rahmen der Umsetzung der Vorgaben jedoch nicht nur zu berücksichtigen, sondern auch umfassend zu dokumentieren. Hierzu wurden umfassende und weit reichende Dokumentationspflichten, insbesondere durch die Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung sowie einer Rechenschaftspflicht, geschaffen. Die Verordnung statuiert diesbezüglich Dokumentationspflichten als eigene rechtliche Pflichten. Technische und organisatorischen Maß-

nahmen sind somit sowohl individuell festzustellen, als auch detailliert zu beschreiben bzw. zu dokumentieren.

1.5 Angemessenheit der Maßnahmen

Der in dieser Handreichung beschriebene "Stand der Technik" (im Folgenden auch SdT) fokussiert die durch das ITSiG und die DSGVO geforderten Inhalte. Es ist jedoch im Rahmen der IT-Sicherheits- und Datenschutzgesetze zulässig, bei der Auswahl der Schutzmaßnahmen unter anderem auch wirtschaftliche Aspekte zu berücksichtigen[3]. 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.

[3] Zu den Anforderungen des gesetzlichen "Berücksichtigens" siehe Bartels/Backer, Die Berücksichtigung des Standes der Technik in der DSGVO, DuD 4-2018, 214.

2 Bestimmung des Technologiestandes

2.1 Begriffsklärung

Der Technologiestand[4] "Stand der Technik" muss von den begrifflich ähnlich lautenden Technologieständen wie den "allgemein anerkannten Regeln der Technik" (im Folgenden "aaRdT" genannt) und dem "Stand der Wissenschaft und Forschung" (im Folgenden "SdWF" genannt) [5] inhaltlich und messbar voneinander abgegrenzt werden. Diese Unterscheidung ist die wesentliche Grundlage für die Bestimmung des geforderten Technologiestandes. Wie viele Beispiele aus der Praxis zeigen, werden diese drei Begriffe gleichermaßen in der Rechtsprechung und in der Öffentlichkeit vermischt oder gar verwechselt. [6]

Eingeführt wurden diese drei Begriffe mit der Kalkar-Entscheidung[7] des Bundesverfassungsgerichts im Jahr 1978 und der damit einhergehenden "Drei-Stufen-Theorie". Ausgehend von dieser Entscheidung lassen sich die drei Technologiestände in etwa so grafisch darstellen:

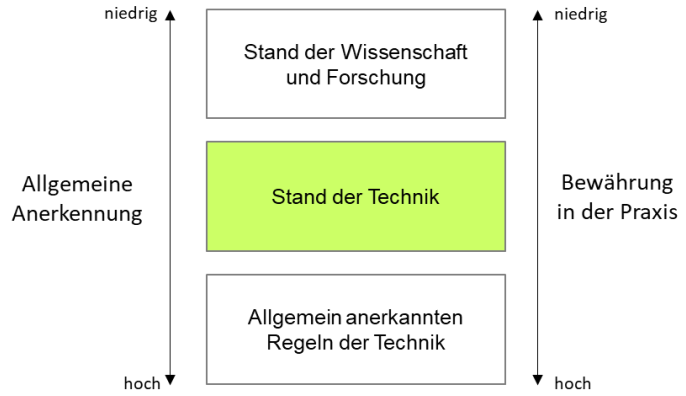


Abbildung 1: Drei-Stufen-Theorie nach Kalkar-Entscheidung

Das Technologieniveau "Stand der Technik" ist angesiedelt zwischen dem innovativeren Technologiestand "Stand der Wissenschaft und Forschung" und dem bewährten Technologiestand "allgemein anerkannten Regeln der Technik". Diese drei Technologiestände werden von den Kategorien "allgemeine Anerkennung" und "Bewährung in der Praxis" flankiert.

Aufgrund der Systematik der Gesetze ist eine eindeutige Unterscheidung zwischen subjektiven und objektiven Tatbestandsmerkmalen erforderlich. Das Merkmal "Stand der Technik" ist rein objektivtechnisch zu verstehen. Die subjektiven Aspekte berücksichtigen die Gesetze im konkreten Tatbestand; sie betreffen aber nicht den Definitionsgehalt des "Standes der Technik" selbst.

Somit kann der Stand der Technik als die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, bezeichnet werden.[8]

[4] Substitutiv für "Technologiestand" wird der Begriff "Technologieniveau" verwendet.
[5] Substitutiv kann "Stand der Wissenschaft und Technik" verwendet werden. Um eine begriffliche Unterscheidung vom "Stand der Technik" zu ermöglichen, wird in dieser Handreichung konsequent "Stand der Wissenschaft und Forschung" verwendet.
[6] Dr. Mark Seibel, Richter am OLG, https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[7] BVerfGE, 49, 89 [135 f]
[8] Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/ Schramm, Der "Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.

Verkürzt lässt sich sagen: Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung eines Subjekts zur Erreichung eines Objekts. Subjekt ist die IT-Sicherheitsmaßnahme; Objekt das gesetzliche IT-Sicherheitsziel.

Technische Maßnahmen im Stadium "Stand der Wissenschaft und Forschung" sind sehr dynamisch in ihrer Entwicklung und gehen mit der Erreichung der Marktreife (oder zumindest mit ihrer Markteinführung) in das Stadium "Stand der Technik" über. Dort nimmt die Dynamik z. B. durch die Standardisierung der Prozesse ab. Auch technische Maßnahmen im Stadium "allgemein anerkannte Regeln der Technik" sind am Markt verfügbar. Ihr Innovationsgrad nimmt ab, sie haben sich jedoch in der Praxis bewährt und werden oftmals in den entsprechenden Standards beschrieben.

Fortschrittsbedingt kann eine Verschiebung über die einzelnen Technologiestände beobachtet werden ("innovationsbedingte Verschiebung"):

1. Eine Maßnahme wird in ihrem Ursprung zunächst das Technologieniveau "Stand der Wissenschaft und Forschung" erreichen;
2. mit der Markteinführung geht sie den "Stand der Technik" über;
3. und mit zunehmender Verbreitung und Anerkennung am Markt wird sie irgendwann den "allgemein anerkannten Regeln der Technik" zugeordnet.

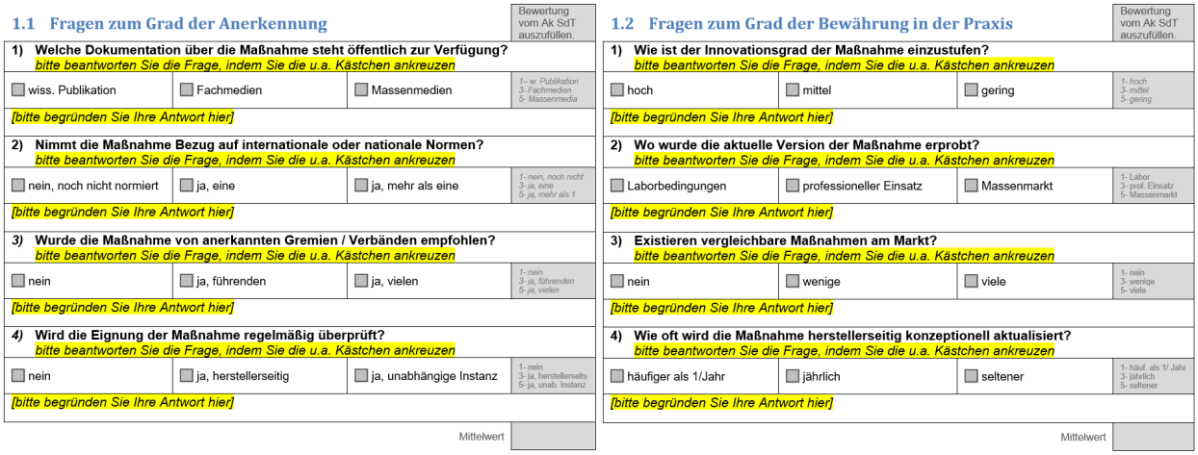
Um den geforderten Nachweis nach der Orientierung eigener Maßnahmen am Stand der Technik zu erbringen, reicht es nicht aus, die implementierten Maßnahmen einmalig zu bewerten und durch Installation von sogenannten Patches zu aktualisieren. Ein solcher Nachweis kann nur gelingen, indem die eingesetzte Maßnahme mittels einer transparenten Methode mit den am Markt verfügbaren Alternativen in regelmäßigen Abständen verglichen wird.

2.2 Methode zur Bestimmung des Technologiestandes

Die im Kapitel 3.2 dieser Handreichung beschriebenen technischen Maßnahmen wurden anhand einer praktikablen Methode bewertet, die auf einem einfachen Prinzip der Beantwortung von Leitfragen zu den Dimensionen "Grad der Anerkennung" und "Grad der Bewährung in der Praxis" basiert. Die verwendeten Leitfragen wurden bewusst einfach formuliert und ermöglichen eine detailliertere Sicht auf die beiden Untersuchungsdimensionen.

Zu jeder Leitfrage wurden drei mögliche Antworten vorgegeben. Die Antworten wurden so ausgewählt, dass sie die Einordnung in ein der drei Technologieniveaus ermöglichen. Jede Antwort muss zudem begründet sein. Die einzelnen Fragen ermöglichen zwar die Einordnung in ein der drei Technologieniveaus, jedoch decken sie jeweils nur Teilaspekte ab, weshalb der Technologiestand einer Maßnahme erst nach der Beantwortung aller Fragen beider Dimensionen bestimmt wird.

Die nachfolgende Abbildung zeigt die durch den Arbeitskreis "Stand der Technik" verwendete Vorlage samt Leitfragen für die Bewertung des Technologiestandes der technischen Maßnahmen:



1.1 Fragen zum Grad der Anerkennung

Bewertung vom Ak SdT auszufüllen.

1) Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ wiss. Publikation	☐ Fachmedien	☐ Massenmedien	1- w. Publikation 3- Fachmedien 5- Massenmedia

[bitte begründen Sie Ihre Antwort hier]

2) Nimmt die Maßnahme Bezug auf internationale oder nationale Normen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein, noch nicht normiert	☐ ja, eine	☐ ja, mehr als eine	1- nein, noch nicht 3- ja, eine 5- ja, mehr als 1

[bitte begründen Sie Ihre Antwort hier]

3) Wurde die Maßnahme von anerkannten Gremien / Verbänden empfohlen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, führenden	☐ ja, vielen	1- nein 3- ja, führenden 5- ja, vielen

[bitte begründen Sie Ihre Antwort hier]

4) Wird die Eignung der Maßnahme regelmäßig überprüft?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, herstellerseitig	☐ ja, unabhängige Instanz	1- nein 3- ja, herstellerseits 5- ja, unab. Instanz

[bitte begründen Sie Ihre Antwort hier]

Mittelwert

1.2 Fragen zum Grad der Bewährung in der Praxis

Bewertung vom Ak SdT auszufüllen.

1) Wie ist der Innovationsgrad der Maßnahme einzustufen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ hoch	☐ mittel	☐ gering	1- hoch 3- mittel 5- gering

[bitte begründen Sie Ihre Antwort hier]

2) Wo wurde die aktuelle Version der Maßnahme erprobt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ Laborbedingungen	☐ professioneller Einsatz	☐ Massenmarkt	1- Labor 3- prof. Einsatz 5- Massenmarkt

[bitte begründen Sie Ihre Antwort hier]

3) Existieren vergleichbare Maßnahmen am Markt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ wenige	☐ viele	1- nein 3- wenige 5- viele

[bitte begründen Sie Ihre Antwort hier]

4) Wie oft wird die Maßnahme herstellerseitig konzeptionell aktualisiert?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ häufiger als 1/Jahr	☐ jährlich	☐ seltener	1- häuf. als 1/ Jahr 3- jährlich 5- seltener

[bitte begründen Sie Ihre Antwort hier]

Mittelwert

Abbildung 2: Bewertungskriterien

Anhand eines Punktesystems wird ausgehend von den gemachten Antworten jeweils ein Mittelwert gebildet. Die ermittelten Werte ermöglichen die Einordnung der Maßnahme in das Diagramm:

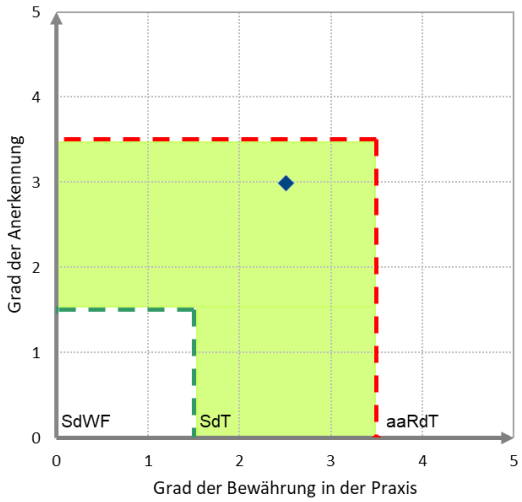


Abbildung 3: Beispiel der Einordnung des Technologiestandes

Aus der Grafik ist ersichtlich, dass eine Maßnahme dem Technologiestand "Stand der Technik" zuzuordnen ist, wenn sie sich ausgehend von der verwendeten Methode im grünen Feld befindet.

In dieser Handreichung werden Technologien und Methoden beschreiben und bewertet, also keine Sicherheitsprodukte im engeren Sinne. Daher wird beispielsweise die Eignung der hier beschriebenen Maßnahmen für den jeweiligen Zweck als erfüllt angenommen.

In der unternehmerischen Praxis sollte eine geeignete Methode (z.B. ähnlich der hier skizzierten) an die im Unternehmen vorhandenen Gegebenheiten angepasst werden, um die eingesetzten Maßnahmen objektiv zu bewerten, sie mit Alternativen zu vergleichen und zu Nachweiszwecken zu dokumentieren.[9]

2.3 Prozess zur Qualitätssicherung der Handreichung

Der Arbeitskreis "Stand der Technik" ist bemüht, eine hohe Qualität der Inhalte der Handreichung

[9] Lawicki, "Was bedeutet 'Stand der Technik?'", erschienen in der TeleTrusT-Sonderbeilage "Sicherheit & Datenschutz" der Zeitschrift iX 6/2018

sicherzustellen. Damit das gelingt, wurde im AK SdT ein Prozess etabliert, in dem die Beiträge mehrere Stufen erfolgreich bestehen müssen:

Abbildung 4: Prozessskizze für die Bewertung der technischen Maßnahmen im Kapitel 3.2

Nach Einreichung eines neuen oder geänderten Beitrags in einer standardisierten Vorlage (vgl. Abbildung 3) wird der Beitrag unter Wahrung der Anonymität durch IT-Sicherheitsexperten über eine Bewertungsplattform bewertet.

Die darin erzielten Ergebnisse werden durch das regelmäßig tagende Bewertungsgremium[10] des Arbeitskreises "Stand der Technik" diskutiert und final abgestimmt. Als Bewertungskriterien dienen u.a. die in der Vorlage definierten Leitfragen und ihre Antworten, aber auch fachliche Korrektheit und Aktualität der Inhalte.

Gelang das Bewertungsgremium zu der Erkenntnis, dass ein Beitrag die erforderliche Güte nicht erreicht, wird seine Übernahme in die Handreichung begründet abgelehnt und der Autor darüber informiert. Der Autor hat anschließend die Möglichkeit, seinen Beitrag zu aktualisieren bzw. zu ergänzen und zur erneuten Prüfung bereitstellen.

Beiträge, die diese umfassende Prozedur erfolgreich bestehen, werden in die Handreichung übernommen.

2.4 Geforderte Schutzziele

Mit den durch das ITSiG eingeführten Gesetzesänderungen werden die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität fokussiert:

- **Verfügbarkeit**
  Die Verfügbarkeit von informationstechnischen Systemen und Komponenten ist vorhanden, wenn diese stets gemäß ihrem Zweck und Funktionsumfang 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.

[10] Eine Liste der aktiv im Arbeitskreis agierenden Mitglieder (Bewertungsgremium) wird auf Seite des Arbeitskreises publiziert: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

Neben diesen durch das ITSiG fokussierten Schutzzielen der IT-Sicherheit, bestehen weitere Gewährleistungsziele aus Sicht des Datenschutzes, die insbesondere aufgrund hier der behandelten Datenschutzgrundverordnung erwähnt werden:[11]

- **Nichtverkettbarkeit (+ Datensparsamkeit)**
- **Transparenz**
- **Intervenierbarkeit**

Diese zusätzlichen Ziele stehen teilweise in Konkurrenz zu den zuvor erwähnten Schutzzielen der IT-Sicherheit. Da die gesetzlichen Vorgaben aus IT-SiG und DSGVO parallel gelten, ist in den Unternehmen eine gemeinsame tragfähige Lösung für ein hohes Niveau der IT-Sicherheit und des Datenschutzes anzustreben. Das kann nur durch eine Zusammenarbeit zwischen den Beauftragten für IT-Sicherheit und für den Datenschutz gelingen.

Während aus Sicht der IT-Sicherheit insbesondere der Schutz der Daten und der Infrastruktur angestrebt wird, geht es beim Datenschutz um den Schutz von Menschenrechten. Das Verständnis über diese unterschiedlichen Sichten ist wichtig, um Schutzmaßnahmen festzulegen und entsprechend zu implementieren.

[11] In Anlehnung an das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/

3 Technische und organisatorische Maßnahmen (TOM)

Das IT-SiG und die DSGVO fordern die Einhaltung oder mindestens die Berücksichtigung des Standes der Technik von technischen und organisatorischen Maßnahmen. Eine weitere Konkretisierung der relevanten Systeme und Komponenten erfolgt seitens des Gesetzgebers nicht. Daher muss von der Einhaltung des Standes der Technik alle relevanten Komponenten der Datenverarbeitung, einschließlich aller Datenübertragungs-, Datenspeicherungsmöglichkeiten, ausgegangen werden.

Da die IT-Infrastrukturen sehr anwendungs- und branchenabhängig sind, ist eine vollumfassende Auflistung der einzelnen Komponenten im Rahmen dieser Handreichung nicht möglich. Die Autoren haben sich daher auf die Beschreibung der wesentlichen Komponenten und Prozesse fokussiert.

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 der Betriebs- und Anwendungssysteme 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-Authentifizierung
- gegenseitige Authentisierung
- Verschlüsselung der Kommunikation während des Transports
- Verschlüsselung der Daten (z.B. bei der Speicherung)
- Sicherung des privaten Schlüssels vor unberechtigtem 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.

Darüber hinaus muss neben einzelnen technischen Anwendungsfunktionalitäten auch die gesamte Sicherheitsarchitektur betrachtet werden. 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 Investi-

tionssicherheit 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 eine 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 vertrauenswürdigem 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 Technische Maßnahmen

3.2.1 Bewertung der Passwortstärke

Die Maßnahme simuliert praxisnah Angriffe auf sicher gespeicherte/gehashte Anmeldedaten und misst die objektive Widerstandsfähigkeit auf Grundlage mathematischer Methoden, persönlicher Verhaltensweisen u.a. Die Maßnahme unternimmt eine umfassende Inventur und Bewertung aller, auch unbekannter, Passwörter. Die Maßnahme ermittelt den Erfüllungsgrad der Compliance zu unternehmensinternen Richtlinien und unterstützt bzw. ermöglicht die Durchführung weiterer sicherheitsrelevanter Maßnahmen, wie zum Beispiel die Notifikation von Mitarbeitern bei Verwendung unsicherer Passwörter unter Einhaltung der DSGVO.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Die Maßnahme soll das Risiko des Missbrauchs von Kontoinformationen (Zugangsdaten) verhindern.

80% der IT-Sicherheitsvorfälle die zur Offenlegung von Account-Informationen - privater, personenbezogener Daten und Geschäfts-Daten führen, gehen auf das Konto schwacher und oder gestohlener Passwörter (Verizon Report 2017).

Die Einhaltung statischer Passwort-Richtlinien für Benutzerkonten ist somit erwiesenermaßen keine geeignete Maßnahme für die Durchsetzung starker, sicherer Passwörter. Die Passwort-Richtlinie täuscht ein falsches Sicherheitsniveau vor.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Unternehmensnetzwerke verwenden in der Regel einen zentralen Speicher für Benutzer-Anmeldedaten, die eigesetzt werden um Benutzer zu authentifizieren, die auf Dienste und/oder Workstations zugreifen (z.B. Microsoft Active Directory).

Alle modernen Anmeldedaten-Speicher-Systeme verwenden Hashing-Funktionen für Passwörter, die verhindern sollen, dass ein Angreifer, mit Zugriff auf die zentrale Datenbank, in der Lage ist, Klartext-Passwörter wiederherzustellen.

Während diese Hashing-Funktionalität einen entscheidenden Schutz der Passwörter gegen unbefugten Zugriff darstellt, verhindert sie gleichermaßen, dass ein Unternehmen die Passwörter bewer-ten kann. Dies ist aber notwendig, um Maßnahmen gegen mögliche Angriffe - wie das Ausprobie-ren von Wörtern aus dem Wörterbuch als Passwort, die Verwendung von bekannten kompromittier-ten Passwörtern oder das Erraten der Passwörter aufgrund persönlicher Informationen über den anvisierten Benutzer - umzusetzen.

Das Passwort-Sicherheit-Assessment definiert die Widerstandsfähigkeit von Passwörtern, indem es einen realen Angriff simuliert, der verschiedene mögliche Schwachstellen, wie beispielsweise vorhersehbare / schwache, von mehreren Benutzern verwendete Passwörter, fehlerhafte kryptografische Implementierungen etc. ausnutzt und aufdeckt.

Auf diese Weise wiederhergestellte Passwörter werden entsprechend nationaler, regionaler und unternehmenseigener Datenschutzbestimmungen weiterverarbeitet, ohne Benutzer bzw. Passwort-spezifische Informationen offenzulegen oder zu speichern.

Die wiederhergestellten Passwörter werden dann auf Grundlage objektiver mathematischer und struktureller Entropie - und subjektiver - Passwort-Richtlinien Compliance - Kriterien beurteilt. Sobald die Beurteilung abgeschlossen ist, werden die Klartext-Passwörter verworfen und ein aussagefähiger Bericht generiert.

Die Ergebnisse der Passwortsicherheitsbeurteilung - der Auditbericht - ermöglichen dem Unternehmen, die exakten Sicherheitsrisiken der in den verschiedenen, multiplen und heterogenen Sys-temen verwendeten Passwörter zu messen. So können die besten Awareness- und Trainingsmaß-nahmen für die Benutzer definiert werden und zentrale Durchsetzungsmethoden für starke Passwörter ermittelt werden. Ebenso wird die Überprüfung und Optimierung der Effektivität bereits eingesetzter Maßnahmen ermöglicht.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

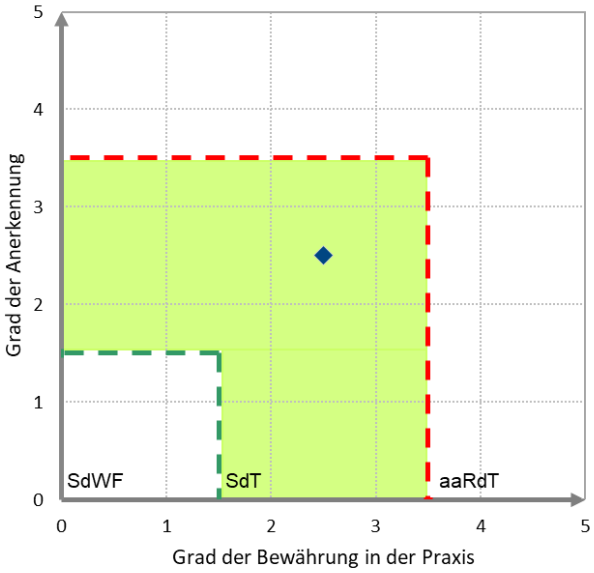
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.2 Durchsetzung starker Passwörter

Die Maßnahme erzwingt die Verwendung von starken und sicheren Passwörtern bei allen von einem Unternehmen eingesetzten technischen und organisatorischen Maßnahmen.

Die Stärke des Passwortes wird durch ein Regelungswerk an das Sicherheitslevel des jeweiligen Benutzerkontos angepasst. Das definierte Sicherheitslevel basiert auf den möglichen Auswirkungen einer Sicherheits-Kompromittierung dieses Accounts.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

80% der IT-Sicherheitsvorfälle die zur Offenlegung von Account-Informationen - privater, personenbezogener Daten und Geschäfts-Daten führen -, gehen auf das Konto schwacher und oder gestohlener Passwörter (Verizon Report 2017).

Die Einhaltung statischer Passwort-Richtlinien für Benutzerkonten ist somit erwiesenermaßen keine geeignete Maßnahme für die Durchsetzung starker, sicher Passwörter - Die Passwort-Richtlinie täuscht ein falsches Sicherheitsniveau vor.

Durch die beschriebene Maßnahme wird das Sicherheitsniveau verwendeter Passwörter auf ein dem Sicherheits-Risiko entsprechendes Maß (Steuerung und Nachweis) angehoben.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Neu gesetzte Passwörter werden gegen Set von Regeln geprüft, die jedem Account zugeordnet sind und individuell für verschiedene Kategorien parametrisiert werden.

Die Regeln beinhalten Maßgaben für: Komposition (Länge, Zeichensatz, Symbole, Buchstabenabfolgen und -wiederholungen), mathematische und strukturelle Entropie-Werte, Einzigartigkeit (das Passwort darf nicht von einem anderen Account auf dem gleichen System in der Organisation verwendet werden), die Verwendung von bekannten Standard-Passwörtern und der Wiederverwendung von Passwörtern (historisch). Die Regeln sind nicht auf Blacklisting beschränkt, sondern können individuell parametrisiert werden.

Die Lösung wird für alle Systeme in der Organisation von einer einzigen Schnittstelle zentral eingesetzt und verwaltet. Somit können kohärente, systemübergreifende Richtlinien effektiv greifen. Dadurch wird auch die Mehrfachbenutzung von Passwörtern in verschiedenen Systemen verhindert und eine zentrale Aufzeichnung über die Passwort-Historie ermöglicht.

Klartext-Daten werden zu keiner Zeit gespeichert oder angezeigt. Der Endnutzer erhält eine eindeutige Nachricht, wenn und weshalb das neue Passwort abgelehnt wird. Das entlastet das Call-Center und schützt die Privatsphäre des Benutzers.

Jegliche Kommunikation zwischen Servern und Systemen zur Durchsetzung starker Passwörter ist mithilfe von Verschlüsselung abgesichert.

Die beschriebene Maßnahme führt zur zentralen Durchsetzung der jeweilig angemessenen Passwortstärke und gibt der Organisation vollständige Kontrolle, Steuerung und Dokumentation über die verwendeten Passwörter im Unternehmen. Außerdem kann dadurch ein geeignetes Level an Sicherheit bei der Authentifizierung mithilfe von Passwörtern erreicht werden.

Das Enforcement/Durchsetzung ist durch eine Maßnahme zur Passwort Bewertung und Beurteilung zu evaluieren. Es ist die Widerstandsfähigkeit der verwendeten Passwörter gegen reale Angriffe zu messen und zu bestimmen und ob die Regeln wie erwartet greifen oder wie sie ggfs. korrigiert werden müssen, um die Verwendung von schwachen Passwörtern zu verhindern.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

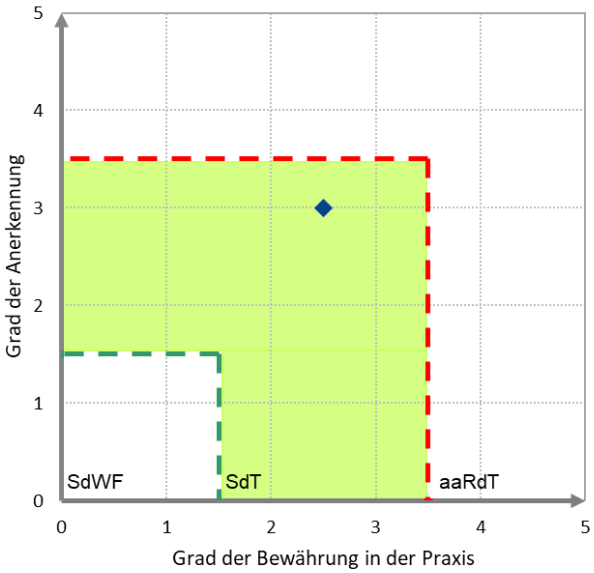
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.3 Multifaktor-Authentifizierung

Multifaktor-Authentifizierung (MFA) bzw. 2-Faktor Authentifizierung (2FA) bezeichnen Authentifizierungen, bei der mehr als ein Faktor wie z.B. das Passwort eingesetzt werden, um Subjekte an Objekten sicher zu authentifizieren. Durch eine MFA bzw. 2FA Lösung wird sichergestellt, dass es sich bei dem Subjekt auch wirklich um dieses handelt. In der vollvernetzen Welt und dem Anstieg der Bedeutung sowie der Zugangsmöglichkeiten von digitalen Identitäten wird diese Maßnahme immer wichtiger. Die Möglichkeiten moderner MFA-Systeme auch digitale Transaktionen abzusichern spielt in der zunehmenden Digitalisierung und der strengeren Regularien wie die EU-Zahlungsdiensterichtlinie 2 (Payment Service Directive 2, PSD2) eine weitere interessante Rolle.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

81% der Kompromittierungen basieren laut dem Verizon 2017 Data Breach Investigations Report[12] auf gestohlene und schwache Passwörter.

Gestohlene oder schwache Passwörter sind heute in über 80 Prozent aller Fälle die Ursache für eine Kompromittierung. Dies liegt daran, dass Passwörter empirisch keinen Schutz für digitale Identitäten darstellen. Dies ist wie folgt begründet:

[12] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

1. Angreifer können bereits mit 10 Rate-Versuchen pro Account - also innerhalb der typischen Rate-Limits - bereits ein Prozent[13] aller Benutzeraccounts übernehmen.
2. Die Einbeziehung von öffentlichen Informationen z.B. aus sozialen Medien (Targeted Guessing) ermöglicht es Angreifern digitale Identitäten mit einer Wahrscheinlichkeit von 32% (sehr sicherheitsaffine Benutzer) - 73% (normale Benutzer) zu übernehmen[14].
3. Desweiteren nutzen Benutzer in der Regel die gleichen Muster für die Bildung Ihrer Passwörter, was den tatsächlichen Passwort-Raum signifikant von dem möglichen theoretischen Passwort-Raum reduziert[15]. Muster sind beispielsweise:

    a. Großbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Ziffer Ziffer
    b. Großbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Ziffer Ziffer
    c. Großbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Kleinbuchstabe Ziffer Ziffer Ziffer Ziffer
    d. Vorherige Kombinationen mit einem "!" am Ende.

Dazu kommt, dass viele Nutzer ihre Passwörter mehrfach (5 Passwörter auf im Mittel 26 Accounts je Benutzer) für unterschiedliche Anwendungen verwenden. Die Kompromittierung eines dieser Dienste führt somit zur Kompromittierung aller Dienste. Angreifer probieren die erbeuteten Daten systematisch und automatisiert bei diversen anderen Diensten aus. Je länger die Angreifer dabei unerkannt bleiben, um so mehr Daten können diese erbeuten und damit weiteren Schaden anrichten bzw. Umsätze erzielen.

Mittels MFA bzw. 2FA Systemen sinkt das Risiko erheblich, dass ein Angreifer mit dem Passwort die digitalen Identitäten missbrauchen bzw. auf die damit zugänglichen Daten zugreifen kann.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Zwei-Faktor- oder Multi-Faktor-Authentifizierung erschweren den Identitätsdiebstahl erheblich. Durch diese Verfahren muss klassischerweise neben dem Passwort mindestens ein weiteres Authentifizierungskriterium erfüllt sein, bevor der Zugriff auf eine Seite, eine Anwendung oder bestimme Daten gewährt wird. Eine simple Zwei-Faktor-Authentifizierung erfordert also zwei von drei Merkmalen:

- Etwas, dass der Nutzer kennt (so wie ein Passwort)
- Etwas, dass der Nutzer mit sich führt (eine Bankkarte oder einen Authentifizierungs-Token - egal ob als Hardware oder digital)
- Etwas Nutzerspezifisches mit biometrischen Kennzeichen (z.B. der Fingerabdruck oder das Irismuster)
- Etwas, was das System über den Benutzer kennt. (Geolocation, Device-ID, Zeiträume, bisherige Transaktionen)

Moderne Multi-Faktor Systeme bieten dabei ein breites Spektrum von Einsatzmöglichkeiten:

1. Unterstützung diverser unterschiedlicher Tokenarten (Software, Hardware, SMS, Voice, mOTP) die je nach Einsatzzweck und Risiko für unterschiedliche Zielgruppen konfiguriert werden können.
2. Unterstützung von 3Party Szenarien mit der Möglichkeit zur Einschränkung der Gültigkeit jegliches Token-Typen in Hinblick auf Anzahl der Verwendungen oder in Hinblick auf Zeitdauer.
3. Unterstützung von Token mit Transaktionsbindung. Diese Token kommen lediglich bei modernen MFA / 2FA Lösungen zum Einsatz und erlauben die Absicherung von Prozessen

[13] http://www.jbonneau.com/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf
[14] http://www.comp.lancs.ac.uk/~yanj2/ccs16.pdf
[15] https://www.youtube.com/watch?v=5i_Im6JntPQ sowie https://youtu.be/zUM7i8fsf0g

durch die Berechnung des One Time Passwords (OTP) auf Basis der Transaktionsdetails wie z.B. bei PSD2 gefordert. Auf diese Art und Weise kann neben Vertraulichkeit, und Integrität auch Nichtabstreitbarkeit gewährleistet werden.

Moderne 2FA oder MFA Systeme lassen sich an sich einfach integrieren. Durch Standardanbindungen an ein Active Directory, LDAP, SQL oder JSON können Anwendungen schnell um eine MFA bzw. 2FA Komponente bereichert und die darin verwalteten Benutzer abgesichert werden. Durch moderne APIs lassen sich Eigenentwicklungen, Custom Software oder Portale sehr schnell und mit wenigen Zeilen Code absichern.

Die modernen Transaktionstoken ermöglichen es, eine hohe Benutzerfreundlichkeit zu realisieren und dabei auch Nichtabstreitbarkeit zu gewährleisten. Dabei erhält der Benutzer eine Nachricht auf sein Smartphone in der er seinen Login oder seine "kritische Aktion" im System noch einmal extra freigeben muss, in dem dieser auf seinem Smartphone auf OK drückt. Durch die Verwendung von Public-Key Mechanismen in Kombination mit QR Codes, können diese Verfahren auch zur Gerätetrennnung oder zur Offline-Authentifizierung verwendet werden.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

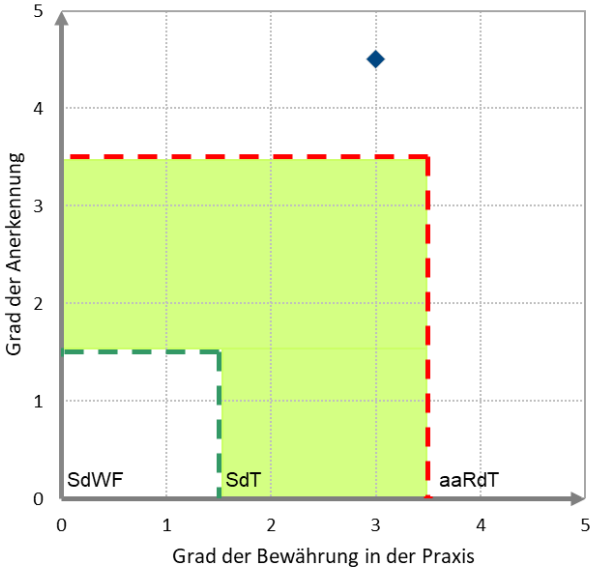
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



Anmerkung: Insbesondere aus dieser fortlaufenden Innovation und der hohen Wirksamkeit der Maßnahme gegen den Verlust digitaler Identitäten resultiert die hier vorgenommene Bewertung der Bewährung in der Praxis.

3.2.4 Kryptographische Verfahren

Kryptographische Verfahren, etwa Methoden zum Verschlüsseln und zum Signieren von Daten, hängen essentiell von der Konfiguration, den verwendeten Verfahren sowie der Schlüssellängen ab. Nur durch geeignete Kombination aller drei Faktoren lassen sich die Schutzziele im Hinblick auf Vertraulichkeit, die Integrität und die Authentizität realisieren. Dieses Kapitel gibt Empfehlungen für den Einsatz und die Auswahl von kryptographischen Verfahren.

Kryptographische Verfahren werden für vielfältige Zwecke eingesetzt und stellen die Grundlage für viele IT-Sicherheitsmaßnahmen dar. So kommt moderne Kryptographie in

- Authentisierungsverfahren
- Zur Gewährleistung der Authentizität
- Zugriffskontrolle
- Zur realisierung von Abstreitbarkeit und Nicht-Abstreitbarkeit (non-repudiation)
- Geheimnisteilung (Secret-Sharing)
- Realisierung von Anonymisierungsverfahren
- Wahlen und Abstimmungen (Commitment-Verfahren)
- Kryptowährungen
- Digitalem Rechtemanagement (DRM)

und vielen weiteren Szenarien zum Einsatz.

All diesen Verfahren ist gemein, dass diese primär dazu dienen, die Vertraulichkeit sowie die Authentizität zu gewährleisten. Also beispielsweise den Diebstahl vertraulicher Daten zu unterbinden oder die unbemerkte Manipulation von Daten zu verhindern.

Kryptographische Verfahren sollen das Kerckhoffs'sche Prinzip erfüllen. Offen gelegte Algorithmen können von einer breiten, weltweiten Experten-Community systematisch auf Schwachstellen evaluiert und optimiert werden. So entstand etwa der heutige Standard für symmetrische Verschlüsselung, AES, in einem öffentlichen Wettbewerbsverfahren. Er gilt als extrem sicher.

Das Sicherheitsniveau eines Verschlüsselungsverfahrens kennzeichnet den Aufwand, den ein Angreifer betreiben muss, um an den Klartext zu gelangen. Es wächst vereinfacht gesagt mit der Anzahl der Möglichkeiten, die für die Auswahl des Schlüssels zur Verfügung stehen (der Bit-Länge).

Durch die steigende Rechenleistung, analytische Fortschritte und technische Möglichkeiten besteht die Gefahr, dass ein Angriff auf ein Verfahren bekannt wird, der das Sicherheitsniveau auf ein praktisch durchführbares Niveau senkt. Auch ist es möglich, dass es gelingt, einen Quantencomputer zu bauen, der eine "brute force"-Schlüsselsuche in deutlich kürzerer Zeit durchführen kann, wodurch sich das Sicherheitsniveau symmetrischer Verfahren halbiert. Viele asymmetrische Verfahren würden durch praktisch verfügbare Quantencomputer gänzlich gebrochen.

Aus diesen Gründen müssen verwendete kryptographische Methoden etwa jährlich im Hinblick auf Ihre Wirksamkeit hin überprüft werden.

Die jeweils aktuellen Empfehlungen veröffentlicht das BSI als Technische Richtlinien TR-02102.[16] Weitere Empfehlung finden sich in Dokumenten des amerikanischen NIST, der ENISA und anderen Organisationen.[17,18,19,20,21,22]

[16] Vgl. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[17] BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2018-02
[18] NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General
[19] NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
[20] European Union Agency for Network and Information Security: Algorithms, key size and parameters report – 2014
[21] https://eprint.iacr.org/2015/1018.pdf
[22] https://safecurves.cr.yp.to/

Zum aktuellen Zeitpunkt können insbesondere die folgenden Empfehlungen gegeben werden:

- Symmetrische Verschlüsselungsverfahren: AES-128, AES-192, AES-256 im Idealfall mit GCM als Betriebsmodus. Auch der EAX Modus ist empfehlenswert, wenn aus Ressourcengründen eine Stromchiffre benötigt wird und etwas höhere Verzögerung durch Verschlüsselung akzeptabel ist. In modernen Systemen sollte Authenticated Encryption with Associated Data (AEAD) als Betriebsmodus verwendet werden. Generell gelten Betriebsmodi ohne zusätzliche Message Authentication Code (MAC) ohne weiteren Integritätsschutz als unsicher und sollten nicht verwendet werden.
- Asymmetrische Verschlüsselungsverfahren: mindestens ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 oder ECC-Brainpool. ECIES sollte mit 384 oder mehr Bit zum Einsatz kommen. Sofern DLIES oder RSA zum Einsatz kommen, sollten 3072 Bit oder mehr verwendet werden.
- Hashfunktionen: Achten Sie auf SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 sowie SHA3-512. Die SHA1 und MD5 Algorithmen sind nicht mehr Stand der Technik.
- Key derivation functions (KDF) bzw. Passwort-Hashes: Geeignete Verfahren sind nach heutigem Stand:[23] Argon2, PBKDF2, scrypt sowie bcrypt. Neue Systeme sollten das Argon2 Verfahren verwenden.
- Zufallszahlengeneratoren:
    - physikalischen Zufallsgeneratoren der Funktionalitätsklasse PTG.2 oder PTG.3[24]
    - Deterministische Zufallszahlengeneratoren der Funktionalitätsklasse DRG.3 sowie DRG.4
- TLS[25], [26]: TLS 1.3 in Kombination mit Forward Secrecy unter Verwendung von sicheren Algorithmen gemäß BSI TR-02102-2, Tabelle 1[27].Die Verwendung von Tools wie: https://www.owasp.org/index.php/O-Saft sowie https://www.ssllabs.com/ssltest/ hilft bei der Überprüfung der TLS-Konfiguration.

Anmerkung:

Seitenkanalangriffe sind ein relevantes Problem in der Kryptographie. Die Auswahl von "empfohlenen" Algorithmen schützt zwar vor analytischen Angriffen, nicht jedoch vor Seitenkanalangriffen. Diese Angriffe erfolgen in der Regel durch die Messung von physikalischen Parametern wie Laufzeiten, Stromverbrauch, Hitze und Schwingungen.

Die möglichen Seitenkanäle hängen insbesondere von der Implementation des Algorithmus sowie der eingesetzten Plattform ab. Die Seitenkanalresistenz von IT-Sicherheitsprodukten variiert von Anbieter zu Anbieter. Arbeiten Sie hier im Zweifel mit darauf spezialisierten Dienstleistern.

3.2.5 Verschlüsselung von Festplatten

Die Festplatten-Vollverschlüsselung oder auch "Full Disk Encryption" schützt die in einem System verbauten Datenträger, wie magnetische Festplatten oder Flash Memory-basierte SSDs, vor unbefugtem Zugriff (Auslesen, Modifikation) durch Dritte. Die dort gespeicherten Informationen werden erst nach Authentisierung des Nutzers vor dem Hochfahren des PC- oder Smartphone-Betriebssystems im Klartext zugänglich.

[23] https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

[25] Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS)

[26] NIST Special Publication 800-52 Revision 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

[27] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Diese Maßnahme schützt Daten auf Festspeichern unbeaufsichtigter, ausgeschalteter Endgeräte wie PCs, Laptops, Tablets oder Smartphones (Data at rest). Bei Verlust durch Unaufmerksamkeit oder Diebstahl, oder zeitweiliger Verfügbarkeit für unberechtigte Dritte (Hotelzimmer), können Angreifer keine inhaltliche Auswertung oder Manipulation der gespeicherten Informationen vornehmen. Das Kopieren der Festspeicher so geschützter Geräte liefert dann nur nutzlose, weil verschlüsselte Daten.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Der oder die in einem System verbauten Datenträger, wie magnetische Festplatten oder Flash Memory-basierte SSDs, auf denen sich das Betriebssystem und firmenvertrauliche Daten befinden, werden durch die Maßnahme derart verschlüsselt, dass ihr unberechtigtes Auslesen keinen Klartext liefert. Dies gilt sowohl für den Fall des Auslesens bei ausgeschaltetem System bzw. der ausgebauten Festplatte, als auch während des Betriebs für das Abgreifen der Daten an der festplattenseitigen internen Schnittstelle (eSATA etc.).

Als symmetrische Verschlüsselung sollte mindestens AES-256 im XTS-Modus gewählt werden. Ein zentrales Management-Tool erleichtert den Einsatz auf allen PCs einer Organisation erheblich. Die kryptografischen Schlüssel sollten niemals, auch nicht zu Backupzwecken, in die Cloud gesichert werden.

Bei der Wahl der Authentifikationsmerkmale sollte großer Wert auf schwer knackbare Passwörter sowie 2-Faktor-Authentisierung gelegt werden, idealerweise mittels "Wissen und Besitz", etwa mit zusätzlichem Token. Dies ermöglicht zusätzlich den Einsatz von hardware-gestützten Verzögerungsmechanismen bei mehrfacher Passwort-Falscheingabe. Ein Ausbau des Datenträgers zur Analyse in einem Angreifer-System wird damit zwecklos.

Soweit vom Gerät ermöglicht, etwa bei Windows 10 Systemen, sollte auch der sogenannte "Secure Boot" unterstützt werden. Dadurch wird der gesamte Bootprozess inklusive der 2-Faktor-Authentisierung gegen Manipulationen geschützt und die Integrität des Systems und der Verschlüsselungsmechanismen bleibt gewahrt.

Manche verfügbaren Lösungen unterstützen auch das volle oder ordnerbasierte Verschlüsseln von Wechseldatenträgern. Innerhalb von Organisationen ist hierbei eine automatische, nutzertransparente Verschlüsselung für Firmendaten vorzuziehen, um Klartext-Speicherung durch Bedienungsfehler vorzubeugen.

Vom BSI für den Behördengebrauch zugelassene, aber auch in kritischen Infrastrukturen sowie Unternehmen nutzbare Lösungen für Windows 7, 8 und 10 sind verfügbar.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

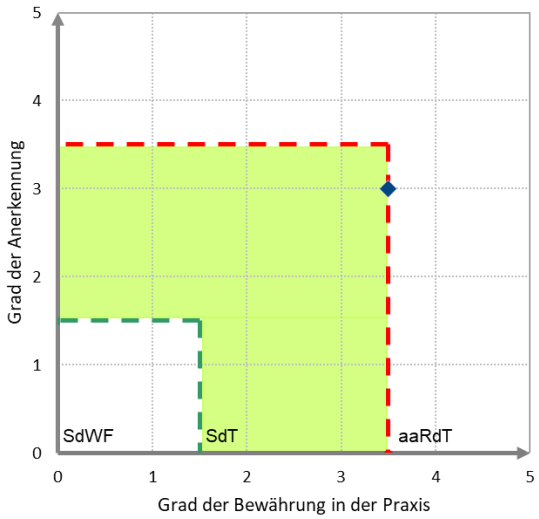
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☐ Authentizität

Einordnung des Technologiestandes



3.2.6 Verschlüsselung von Dateien und Ordnern

Datei und Ordner-Verschlüsselung umfasst 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.

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

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

1. Abfangen und Missbrauch von Daten beim Transport, bspw. per E-Mail
2. Verlust und Diebstahl von Wechseldatenträgern mit anschließendem unbefugtem Zugriff auf sensible Daten
3. Missbrauch von Daten, die in der Cloud abgelegt werden

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

File & Folder Encryption umfasst 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 zum anderen zu transportieren, an jedem Ort sicher zu speichern und dabei eine Einsichtnahme durch Unbefugte zu verhindern.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

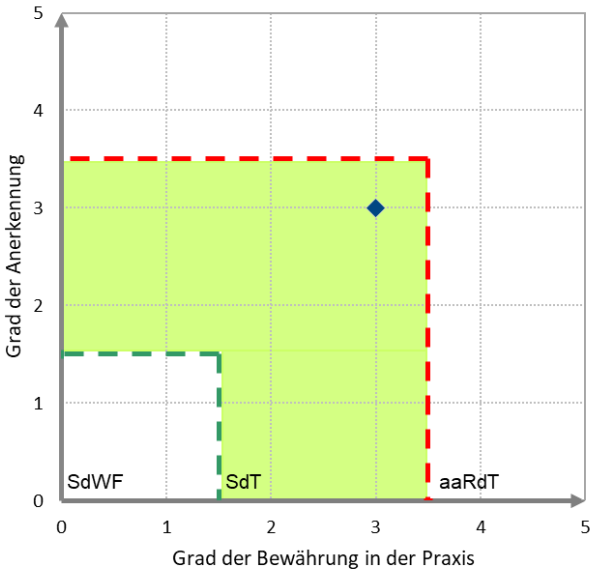
☐ Verfügbarkeit

☐ Integrität

☒ Vertraulichkeit

☐ Authentizität

Einordnung des Technologiestandes



3.2.7 Verschlüsselung von E-Mails

Geschäftliche E-Mails enthalten oft wichtige und schützenswerte Daten, zudem sind in der Regel schon E-Mail-Adressen personalisiert und E-Mails damit regelmäßig personenbezogene Daten, die gegen unbefugte Einsichtnahme oder Veränderung zu schützen sind. Die Schutzziele können generell durch Verschlüsselung der Übertragung von E-Mails und oder von E-Mail-Inhalten erreicht werden.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- *Ausspähung oder Manipulation von E-Mails im Transport*
- *Ausspähung oder Manipulation von gespeicherten E-Mails*

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Verschlüsselte Übertragung von E-Mails (Transportverschlüsselung); TLS

Verschlüsselung der Inhalte von E-Mails; S/MIME oder PGP

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 übermit-

telt 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) 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). Umfassende Empfehlungen zu TLS liefert die Technische Richtlinie TR-02102-2, Teil 2 des BSI.

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) und OpenPGP (Pretty Good Privacy, definiert in RFC 4880). 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 unternehmens-internen Inhaltsverschlüsselung.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

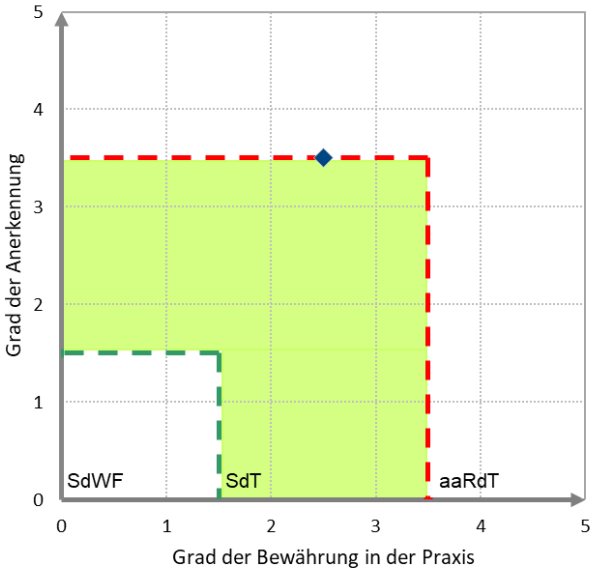
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.8 Sicherung des elektronischen Datenverkehrs mit PKI

Im elektronischen Datenverkehr ist es wichtig, dass die Identität der Kommunikationspartner und die Echtheit der übermittelten Inhalte sichergestellt sind. Der Nachweis von elektronischen Identitäten bei Personen, Organisationen oder Geräten lässt sich durch den Einsatz elektronischer Zertifikate sicherstellen. Für den Nachweis der Echtheit von übermittelten Dokumenten und Nachrichten sind elektronische Signaturen geeignet. Auch beim sicheren verschlüsselten Datentransport kommen zertifikatsbasierte Lösungen zum Einsatz. All diese Szenarien setzen eine Komponente zur Erzeugung, Management und Prüfung elektronischer Zertifikate voraus, welche den Nachweis von elektronischen Identitäten vertrauenswürdig sicherstellen: eine Public Key Infrastructure (PKI).

Auch die seit Sommer 2016 geltende eIDAS-Verordnung sieht die Verwendung und Nutzung einer PKI vor.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Diebstahl der Identität / Vortäuschung einer falschen Identität
- Manipulation der Inhalte von elektronischen Nachrichten oder Dateien
- Manipulation der zeitlichen Einordnung von Nachrichten oder Dateien

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Gegen die oben beschriebenen Bedrohungen sind die folgenden Maßnahmen sinnvoll:

- Einrichtung einer eigenen oder Nutzung einer externen PKI
- Nutzung elektronische Unterschriften (Signaturen, Zertifikate, Siegel) eines akkreditierten Trust-Centers
- Verwendung qualifizierter Zeitstempel für den Nachweis der Echtheit und zeitlicher Einordnung von Nachrichten und Dokumenten

Die elektronischen Zertifikate werden von der sogenannten Zertifizierungsstelle einer PKI-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.

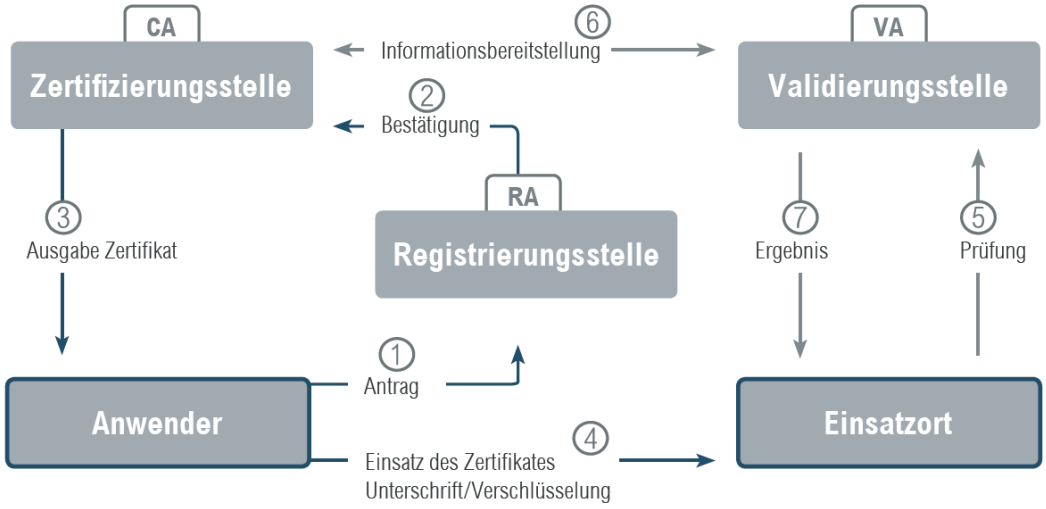
In Abhängigkeit des juristischen Status der PKI wird in den meisten Einsatzfällen die rechtlich verwertbare Protokollierung aller Transaktionen in einer PKI sinnvoll oder gar notwendig sein. Für einige Anwendungsgebiete sind auch zertifizierte CA-Produkte notwendig.

Die Einsatzmöglichkeiten von PKI-basierten Verfahren sind vielfältig. Folgende Einsatzverfahren werden beispielhaft genannt:

- Signatur und Verschlüsselung von E-Mails (S/MIME)
- Authentisierung und Verschlüsselung im "Internet der Dinge"
- Authentisierung und Verschlüsselung im Web (HTTPS)
- Authentisierung und Verschlüsselung bei VPN-Diensten
- Authentisierung und Integritätssicherung bei ausführbaren Code (Code-Signing)
- Authentisierung und Integritätssicherung bei Dokumenten (Digitale Signatur)
- Authentisierung von Clients/Nutzern im Internet

Je nach Status des Betreibers und des Sicherheitsstandards 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 Crosszertifizierung mit anderen PKI ist realisierbar.

Das folgende Schaubild zeigt den grundsätzlichen Aufbau und das Zusammenwirken von PKI-Komponenten in einem Workflow.



Die Anwendung von Zertifikaten ist in fast allen Bereichen sinnvoll und hilfreich. Neben Anwendungsbereichen der öffentlichen Hand findet man sie in der Energie- und Gasversorgung, dem Elektronischen Rechtsverkehr (mit beA, beN, beBPo), dem Gesundheitswesen aber auch im industriellen und Non-Profit-Umfeld (z.B. Verbände, Vereinigungen).

Speziell die eIDAS Verordnung sieht umfangreiche Nutzungsszenarien vor. So werden u.a. Identitätsnachweise und Vertrauensdienste durch PKI unterstützt (siehe nachfolgende Tabelle).

eIDAS Regelungen/Anwendungfälle	
Identitäten	Zertifikate
	elektronische Ausweise
Vertrauensdienste	elektronische Siegel
	elektronische Zeitstempel
	Website-Authentifizierung
	elektronische Zustelldienste
	Bewahrungsdienste

Ein Beispiel der Nutzung im öffentlichen Bereich ist: www.cio.bund.de/Web/DE/IT-Angebot/IT-Beratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html sowie im Energieversorgerbereich
www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html

oder auch bei TeleTrusT: https://www.ebca.de.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

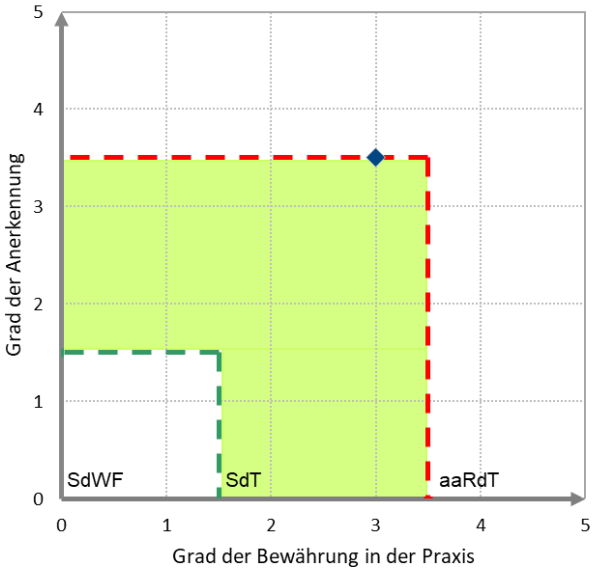
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.9 Einsatz von VPN (Layer 3)

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.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Der Einsatz von VPNs schützt gegen:

- Vertraulichkeitsverlust durch unverschlüsselte/schwach verschlüsselte Verbindungen
- Externe Angreifer
- Verbindungsmanipulation

Die eingesetzten VPNs unterliegen selbst auch weiteren Bedrohungen:

- Abfluss des Schlüsselmaterials
- Schwache Kryptographie
- Denial of Service: Durch Fehler oder Angriffe ist die Verfügbarkeit des VPNs gefährdet

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Ein Layer 3 VPN bezeichnet die Verbindung zweier oder mehrerer Netze oder die Anbindung eines Clients an ein Netzwerk auf Layer 3 des OSI Modells. Die dabei transportierten Daten werden verschlüsselt und die VPN-Endpunkte authentifizieren und autorisieren den jeweils anderen VPN-Endpunkt. Damit kann man zum Beispiel Firmenniederlassungen in verschiedenen Ländern über unsichere Leitungen Dritter, wie z.B. auch das Internet oder angemietete Leistungen bei einem Telekom-Dienstleister, sicher und vertraulich miteinander verbinden. Im Gegensatz zu einem Layer 2 VPN werden weniger Daten transportiert, da Layer 2 Daten, wie z.B. Broadcasts, nicht übertragen werden. Im Gegenzug ist ein Layer 3 VPN dadurch nicht für alle Anwendungen transparent nutzbar. 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 benötigt 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 zugutekommen. 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.

Ein Layer 3 VPN muss die Vertraulichkeit der durchgeleiteten Daten sicherstellen. Dazu muss das Gerät eine Verschlüsselung und Authentisierung mit als sicher geltenden Algorithmen und 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, in Hardware geschützte Authentisierungsinformationen), 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 werden über ein VPN schützenswerte Informationen transportiert.

Eine Layer 3 VPN, dessen Geräte Backdoors enthalten oder bei dem ein Softwarefehler zur Übernahme der Geräte selber führen kann, ist ein untragbares Risiko. Daher sind Produkte zu bevorzugen, die, beispielsweise durch unabhängige Prüfungen (Zertifizierungen oder auch Zulassungen) eine hohe Plattformsicherheit und einen hohen Selbstschutz nachweisen können. Durch Auflagen an die Einsatzumgebung muss weiterhin sichergestellt sein, dass physikalischer Zutritt zu den VPN-Geräten 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 die VPN-Geräte auf einer besonders gehärteten Plattform aufgebaut sind, einen ausgezeichneten Selbstschutz haben und frei von Backdoors sind. Die Sicherheitsprotokolle, die ein Layer 3 VPN nutzt, garantieren auch die Integrität und Authentizität der transportierten Daten. Eine besonders wichtige Rolle nimmt auch die Verwaltung und die sichere Nutzung von Schlüsselmaterial ein. Hierbei sind Hersteller zu bevorzugen, die nachweisen können, dass sie eine sichere Zufallszahlengenerierung, eine sichere Schlüsselhaltung der privaten Authentisierungsschlüssel (z.B. auf Chipkarten) ermöglichen und das Alter von verwendeten Verschlüsselungs-Schlüssel mitverfolgen.

Um die Verfügbarkeit des Layer 3 VPNs sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software des VPN-Endpunkten (z.B. VPN Konzentratoren) notwendig. Bei der Hardware muss der Hersteller nachweisen können, dass die Plattform entsprechend den Anforderungen hochverfügbar konzipiert und umgesetzt wurde. Das beinhaltet zum Beispiel redundante Netzteile, performante Ausführung der Rechenleistung, und eine Lüfterkonfiguration, bei der ein Ausfall eines Lüfters nicht zu einem Ausfall des gesamten 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 unterstützen. 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 Zutritt zu den Räumlichkeiten, in der die VPN-Endpunkte (VPN-Konzentratoren) im LAN betrieben werden.

Auf den Geräten eines Layer 3 VPN fallen Logdaten an. Diese sind eminent wichtig, um Angriffe auf das Netzwerk erkennen 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 eine Schnittstelle zu externen Logserver oder SIEM-Systeme.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

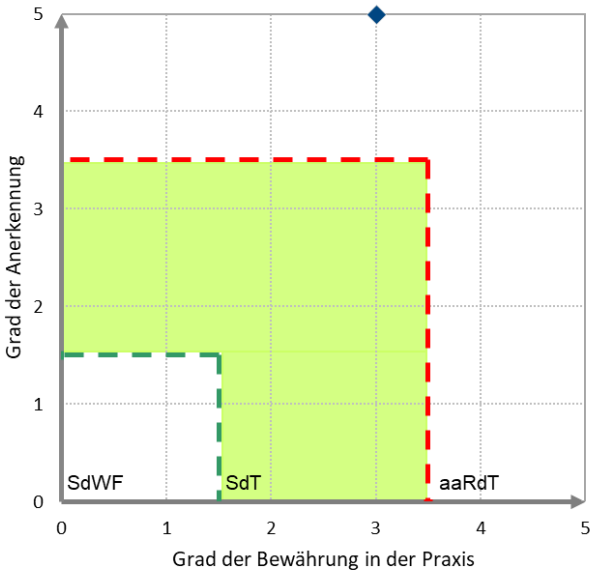
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



Anmerkung: Während die grundsätzliche Notwendigkeit des Einsatzes von VPNs nicht bezweifelt wird, liefern Hersteller regelmäßig Innovationen zur Steigerung ihres Sicherheitsniveaus, ihrer Benutzerfreundlichkeit und Betreibbarkeit. Der Stand der Technik bei VPNs definiert sich somit nicht allein über ihr Vorhandensein, sondern über die Ausprägung dieser Qualitäten.

3.2.10 Verschlüsselung auf Layer 2

Layer 2-Verschlüsselung ist eine Sicherheitslösung als Alternative zu Layer3-VPNs, die statt auf IP-Pakete auf die Payload von Ethernet-Frames angewandt wird. Die IP-Header müssen nicht verarbeitet werden (Zeitgewinn) und die Leitungskapazität wird deutlich geringerer durch Verschlüsselungs-Overhead belastet als bei Verschlüsselung über Layer 3 oder höher.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Mitschneiden und Auswertung massiver Datenmengen des standortverbindenden Verkehrs über das Corporate-Netzwerk-Backbone oder der Cloud-Anbindung durch Sicherheitslücken in der Netzwerkhardware, bei Netzwerkdienstleistern sowie nicht überwachte Erd- oder Seekabel und Richtfunk- oder Satellitenverbindungen sowie DDoS-Angriffe auf verschlüsselte Layer 3 - Verbindungen.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Sichern der WAN-Kommunikation zwischen Unternehmensstandorten und Rechenzentren mit Hilfe von Verschlüsselung. Einsatz verzögerungsarmer und bandbreitenneutraler Kryptolösungen für Layer2-WAN Backbones und direkte Links (z.B. dark fiber, Satcom).

Layer2-Verschlüsselung ist eine Sicherheitslösung, die in bestimmten Anwendungsszenarien eine zweckmäßige Alternative zu Layer3-VPNs ist. 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) oder von Netzwerkprovidern bereitgestellte Layer 2 Services (z.B. Carrier Ethernet-Dienste).

Typische Anwendungen für Layer 2 - Encryption sind der Schutz von WAN-Backbone-Leitungen (auch international) und Rechenzentrums-Anbindungen innerhalb des Corporate Networks oder zu vertrauenswürdigen Cloud bzw. Colocation Providern sowie für den Schutz von Campus-Backbone-Leitungen, die außerhalb von Gebäuden und über Drittgrundstücke verlaufen.

Insbesondere für die Einführung zentraler IT-Dienste, massive Desktop-Virtualisierungen, RZ-Konsolidierung, verteilte und redundante Speichersysteme (SAN/NAS), die einen hohen Anteil an kleinen und/oder echtzeit-relevanten IP-Paketen besitzen (z.B. VoIP, IoT, Smart Grid),

und bei denen IPsec-Overhead und Delay nicht akzeptabel sind, zahlen sich die Performance-Vorteile aus.

Beim Einsatz dieser Netzwerk-Verschlüsselungstechnologie ist eine Änderung an der bestehenden 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 messbaren Auswirkungen auf die Performance des Netzwerkes mit sich.

Die Synchronisation und Authentisierung der Krypto-Gegenstellen sowie 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.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

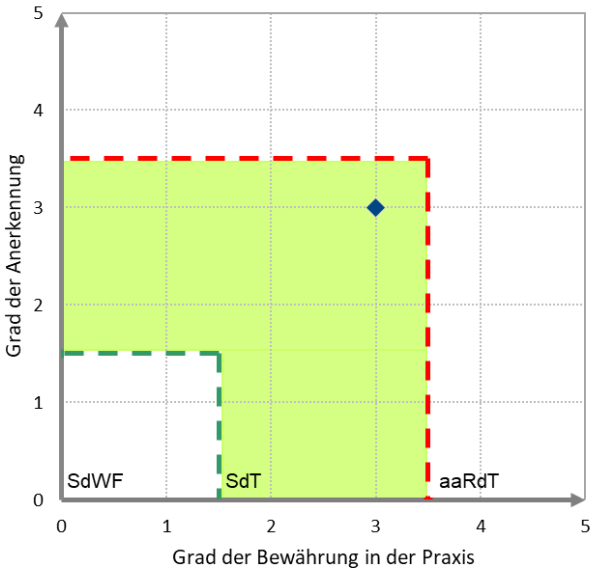
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.11 Cloudbasierter Datenaustausch

Mit fortschreitender Digitalisierung sowie geografisch verteilter Arbeitsweise haben sogenannte Dateiaustauschdienste auf Cloud-basis zunehmend Anwendung in der IT-Umgebung gefunden (Bsp. Dropbox, OneDrive, Google Drive) Um solche Dienste sicher zu nutzen und gegen die bekannten Bedrohungen zu schützen, müssen geeignete Maßnahmen eingesetzt werden.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Die in einem Cloud-basierten Dateiaustauschdienst gespeicherte Daten unterliegen den folgenden Bedrohungen:

- *Unbefugter Zugriff und Einsicht durch den Betreiber des Dienstes*
- *Ausspähung durch Dritte während des Transports der Daten durch das Internet*
- Diebstahl oder unberechtigte Nutzung der Identität, die gegenüber dem Cloud-Dienst vereinbart wurde

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Zum Schutz der gespeicherten Daten sind folgende Maßnahmen sinnvoll:

1. *Verschlüsselte Übertragung der Dateien von und zum Dateiaustauschdienst*
2. *Clientseitige Ende-zu-Ende-Verschlüsselung von Daten für den Empfänger vor der Übertragung in den Cloudspeicher*
   - *Durch in den Datenaustauschdienst integrierte Verschlüsselung im zum Cloudspeicher gehörender Client-Software*
   - *Durch separate Ende-zu-Ende-Verschlüsselungssoftware auf dem Client*

Dabei sind insbesondere die folgenden Fragen zu beachten:

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 Ende-zu-Ende-

Verschlüsselung der Daten selber unter Umständen verzichtet werden, sie ist aber grundsätzlich auch bei vertrauenswürdigen Betreibern sinnvoll.

Es sind Dateiaustauschdienste 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. Alternativ kann auf eine Client-seitige Verschlüsselungssoftware zurückgegriffen werden, die für eine Ende-zu-Ende-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 und Schlüsselhaltung geachtet werden.

Auf keinen Fall verzichtet werden darf auf die Verschlüsselung von Daten beim Transport von und zum Betreiber (Transportverschlüsselung, i.d.R. TLS).

Welche Schutzziele werden durch die Maßnahme abgedeckt?

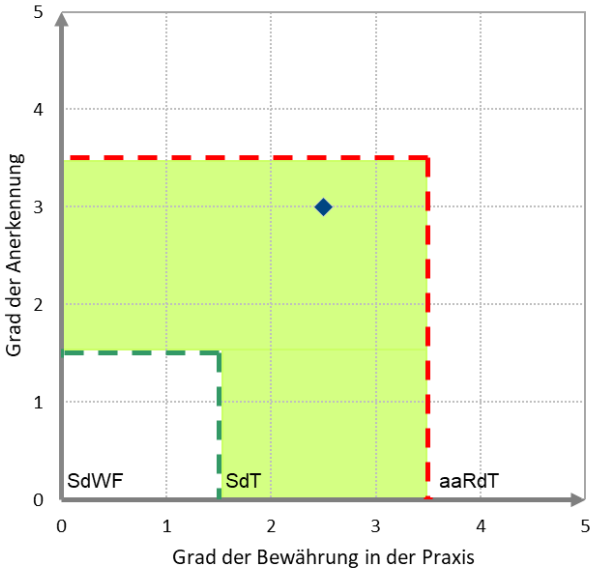
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.12 Datenablage in der Cloud

In dezentralen Cloud-Infrastrukturen reichen Schutzstrategien, die nur die IT-Infrastruktur an sich absichern, nicht mehr aus. Im Wettrüsten mit Angreifern ist die grundlegendste Maßnahme die sicherste: die Verschlüsselung von sensiblen Daten, sobald sie eine sichere, interne Umgebung verlassen, um in der Cloud verarbeitet oder gespeichert zu werden. Dabei sollten die kryptografischen Schlüssel ausschließlich im Besitz der Anwenderorganisation bleiben, um unberechtigte Datenzugriffe auch durch externe Administratoren auszuschließen. Eine Lösung nach Stand der Technik muss deshalb ein entsprechendes, vollständig internes Schlüsselmanagement erlauben. Eine interne Verteilung der admi-

nistrativen Aufgaben bei der Verwaltung der Schlüssel auf mehrere Personen erschwert das Kompromittieren sensibler Daten zusätzlich. Stand der Technik sind hierbei Lösungen, die wichtige Funktionalität, wie das Suchen oder Filtern von Daten, Reporting oder das automatisierte Verarbeiten der verschlüsselten Daten in Cloud-Anwendungen nicht einschränken.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Sensible Daten, die in der Cloud gespeichert oder verarbeitet werden, sind auf vielfache Weise kompromittierbar, unter anderem:

1. unbefugter Zugriff auf den Cloud-Speicher (durch externe wie interne Nutzer),
2. Zugriff durch externe Administratoren von Cloud-Anbietern oder Datenzentren,
3. Abfangen während der Übertragung zwischen Organisation und Cloud, und
4. Diebstahl vom Cloud-Speicher.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Ein Verschlüsselungsgateway ist eine Proxy-basierte Lösung, die zwischen Endnutzer-Anwendung und Cloud vermittelt. Es verschlüsselt alle Daten, die eine zuvor definierte, sichere interne Umgebung verlassen und entschlüsselt Informationen, die von autorisierten Endnutzern aus der Cloud angefragt werden. Die kryptografischen Schlüssel müssen bei einer solchen Lösung ausschließlich im Besitz der Anwenderorganisation bleiben, um die Datenhoheit zu gewährleisten und Lesezugriffsberechtigungen zentral zu steuern. Eine solche Lösung nach Stand der Technik sollte daher ein vollständig internes Schlüsselmanagement ermöglichen. Intern sollten die Aufgaben der Schlüsselverwaltung auf mehrere Verantwortliche aufgeteilt werden. So können Schlüsseldaten nicht von einer Einzelperson kompromittiert werden.

Das interne Schlüsselmanagement macht diese Lösung sicherer als die nativen Verschlüsselungslösungen dritter Cloud-Anbieter (Bring Your Own Key etc.). Im letzteren Fall kann nie völlig ausgeschlossen werden, dass Dritte (etwa Datenbankadministratoren) Lesezugriff auf sensible Informationen haben. Mit einem Verschlüsselungsgateway können dritte Datenverarbeiter auch weiterhin administrative Aufgaben durchführen, jedoch keine sensiblen Daten mehr im Klartext lesen. Die Lösung bietet zudem Schutz im Falle eines Datendiebstahls: Ohne die kryptografischen Schlüssel können Angreifer mit erbeuteten, verschlüsselten Daten nichts anfangen.

Zentrales Kriterium beim Einsatz eines Verschlüsselungsgateways sollte sein, das geschützte Daten weiterhin verarbeitbar sind. Dies kann durch Verfahren zur Teilverschlüsselung erreicht werden.

Mit Blick auf die Zukunft sollte ein Verschlüsselungsgateway gewählt werden, dass der Anwenderorganisation den freien Austausch der verwendeten Verschlüsselungsalgorithmen erlaubt. Mit der fortschreitenden Entwicklung extrem leistungsfähiger Quantencomputer können heute als sicher eingestufte Verfahren schon in naher Zukunft obsolet werden. Ideal ist deshalb eine Lösung, die schon heute kompatibel mit Algorithmen der Postquantenkryptografie (PQC) ist.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

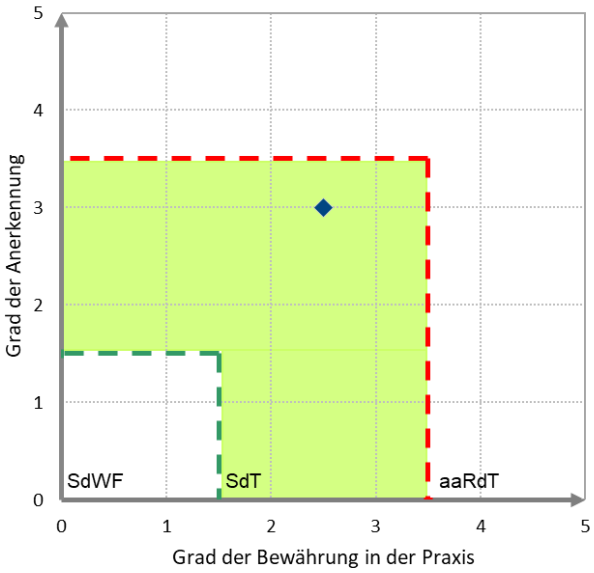
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.13 Nutzung von mobilen Sprach- und Datendiensten

Handy-Gespräche und Datentransfers können leichter abgehört werden als Festnetz-Telefonie. Davor schützen mobile Sprach- und Datentransfer-Verschlüsselung sowie geräteseitige Härtung und Konfiguration.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Die klassische Festnetz- und Mobiltelefonie ist auch heute, trotz Chat- und Webconference-Anwendungen, eines der direktesten und persönlichsten Kommunikationswerkzeuge. Sie birgt jedoch einige Gefahren und bietet potentielle Angriffsvektoren. Die überwiegende Zahl auch der von Festnetzapparaten ausgehenden Telefonate findet unter Beteiligung eines Mobiltelefons statt.

- *Ausspähen von Handy-Gesprächen und Datenverkehr im Festnetz der Mobilfunk- und Telefonie-Netzbetreiber, das die Basisstationen untereinander und den Festnetzanschlüssen verbindet, und das u.a. auf Internet-Technologie basiert*
- *Ausspähen von Handy-Gesprächen und Datenverkehr sowie deren Übertragung an Command & Control - Server der Angreifer durch im Handy installierte Schadsoftware, die Betriebssystem- und App-Schwachstellen ausnutzt, um direkten Zugang zu Mikrofon, Lautsprecher und Touchscreen-Tastatur und Bildschirm zu bekommen, und dadurch die Verschlüsselungs-App aushebelt*
- *Nicht verschlüsselte Handy-Gespräche und Datenverkehr können mit kostengünstiger Hardware auf der Luftschnittstelle abgehört werden. Dazu müssen Angreifer weder das Handy infizieren noch ins Kommunikationsnetz einbrechen. Sie müssen sich allerdings im Empfangsbereich des betreffenden Handys befinden. Angreifer täuschen beispielsweise vor, Teil des Mobilfunknetzes zu sein, um ein Einbuchen des Handys in ihre Abhöreinrichtung zu erreichen und dann Gespräche und Datenverkehr direkt mitzuschneiden und auszuwerten.*

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Die Vertraulichkeit von Gesprächen lässt sich mit Hilfe von Sprach- und Datenverschlüsselung auf OSI Layer 7 (in den Kommunikations-Apps) sicherstellen. Hier werden das gesprochene Wort sowie Chat-Daten und ggf. Dateitransfers in Echtzeit auf dem Gerät verschlüsselt und beim Empfänger wieder entschlüsselt und wiedergegeben.

Als Gegenmaßnahmen werden empfohlen:

- Verschlüsselung der Sprach- und Datenkommunikation durch geeignete und vertrauenswürdige Apps oder Hardware, die nach den aktuellen Verschlüsselungs-standards und den geltenden Datenschutzregeln eine Ende-zu-Ende-Verschlüsselung durchführen
- Ergänzend die zentrale Konfiguration der Endgeräte durch die ausgebende oder BYOD unterstützende Organisation mittels mobile device management (MDM/EMM) Systemen zur Vermeidung ungewollter Benutzeraktionen und App-Aktivitäten, die zu Handy-Infektionen führen können
- Für höheres Vertrauensniveau die Verwendung von Mobiltelefonen mit gehärtetem Betriebssystem, das die exklusive Nutzung von Mikrofon und Lautsprecher durch die Verschlüsselungs-App sicherstellt, sowie das Ausspähen der Kryptoschlüssel durch eventuell vorhandene Schadsoftware verhindert.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

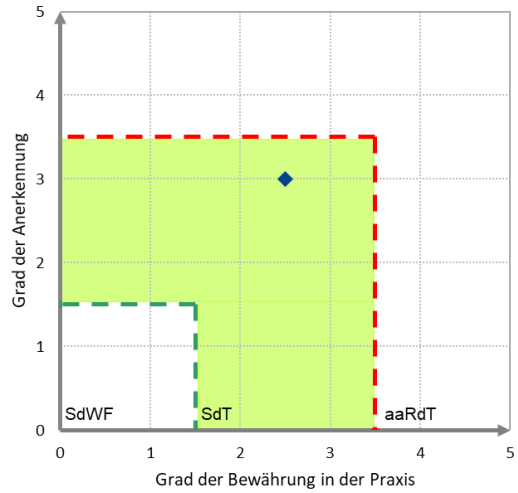
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.14 Kommunikation mittels Instant-Messenger

Instant Messaging nennt man eine Form der digitalen Kommunikation, bei der sich zwei oder mehrere Parteien mittels zügig übermittelter Text-, Bild und Sprachnachrichten unterhalten. Dazu nutzen die Gesprächspartner einen gemeinsamen Instant-Messenger für die Übertragung der Nachrichten über ein Netz. Falls ein Kommunikationspartner zum Zeitpunkt einer Nachrichtenübermittlung nicht online ist, erfolgt in der Regel eine spätere Auslieferung an den Empfänger. Secure Instant Messaging verfolgt das Ziel, Instant Messages vor unbefugten Zugriffen und Änderungen zu schützen.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Wenn Informationen mittels Instant Messaging ausgetauscht werden, sind die folgenden Bedrohungen zu beachten:

1. Mitschneiden, Auswerten und Verändern der Inhalte durch eine unbefugte dritte Partei (Man-in-the-Middle Angriff)
2. Identitätsdiebstahl innerhalb eines Kommunikationssystems
3. Diebstahl eines Geräts, um Instant Messaging Daten nachträglich unbefugt auswerten zu können

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

1. Secure Instant Messaging beinhaltet technische Sicherungsmaßnahmen zur Wahrung der Vertraulichkeit und Integrität der Kommunikationsinhalte:
   - Sicherung der Nachrichtenübermittlung mittels aktuellem TLS auf dem Transportweg
   - Einsatz asymmetrischer Ende-zu-Ende-Verschlüsselung mit einer mindestens zu RSA 2048 Bit vergleichbaren Sicherheit
   - Auch Forward Secrecy sollte Bestandteil der Architektur sein, um die Daten vor einer nachträglichen Entschlüsselung trotz Besitz des Langzeitschlüssels zu schützen.
2. Verlässliche Verifikation / Authentisierung von Identitäten
3. Sicherung der Zugriffsmöglichkeiten und Zugriffspfade auf die Inhalte:
   - Bildschirmsperre auf dem eingesetzten mobilen Gerät (starkes Passwort)
   - Eine aktivierte Geräteverschlüsselung
   - Die eingesetzte Kommunikations-App sollte eine eigenständige sichere Aufbewahrung der Daten anbieten und diese gegen Extraktion durch Unbefugte schützen.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

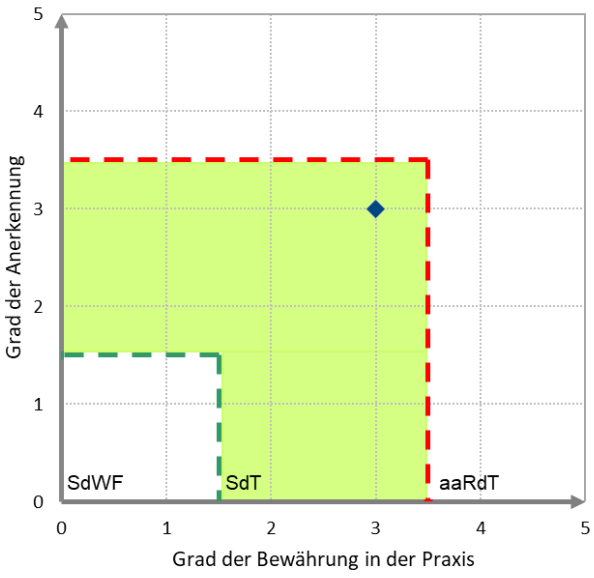
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.15 Management mobiler Geräte

Der Einsatz von Mobile Device Management (MDM)-Lösungen vermindert die Sicherheitsrisiken, die durch die unkontrollierte Nutzung mobiler Endgeräte zu dienstlichen Zwecken entstehen. MDM-Lösungen ermöglichen es, die eingesetzten mobilen Geräte zentral administrieren und konfigurieren zu können.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

1. Datenverlust: Wenn wichtige Daten auf den mobilen Geräten abgelegt werden und das Gerät verloren geht oder zerstört wird, muss das Unternehmen unter Umständen einen unwiederbringlichen Datenverlust hinnehmen.
2. Diebstahl: Wenn ein mobiles Endgerät gestohlen wird, kann der Dieb möglicherweise auf vertrauliche Unternehmensdaten zugreifen.
3. Schadsoftware: Durch die Verwendung von öffentlichen WLAN-Netzen, der Nichtinstallation verfügbarer Updates und durch die unkontrollierte Installation von Anwendungen aus teilweise fragwürdigen Quellen, werden mobile Geräte häufig mit Schadsoftware infiziert.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Mobile Device Management (MDM)-Lösungen ermöglichen den Administratoren auf unterschiedliche Art und Weise die Kontrolle über die Nutzung und den Zugriff auf dienstlich genutzte Mobilgeräte nach zuvor definierten Sicherheitsrichtlinien. MDM-Lösungen können den Patchstatus der Mobilgeräte ermitteln und das Einspielen von Updates auslösen, sobald diese verfügbar sind und getestet wurden. Außerdem kann zentral ein adäquater Passwortschutz, ein regelmäßiges Backup und eine Geräteverschlüsselung erzwungen werden. Im Falle eines Diebstahls oder eines Verlusts des Geräts kann zusätzlich eine Zwangslöschung erfolgen, um die Vertraulichkeit der Unternehmensdaten zu schützen. Dem Administrator wird es ermöglicht, die Nutzerrechte des Mobilgeräts dahingehend zu setzen, dass eine Installation von Anwendungen aus beliebigen und potentiell unsicheren Quellen nicht erlaubt ist.

Um den gestiegenen Funktionalitätsanforderungen bei der Verwendung von dienstlich genutzten Mobile Devices gerecht zu werden, haben einige Hersteller die bisherigen MDM-Features mit Mobile Application Management (MAM)- und Mobile Information Management (MIM)-Funktionen inklusive Cloudanbindung zu sogenannten Enterprise Mobility Management (EMM)-Lösungen erweitert.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

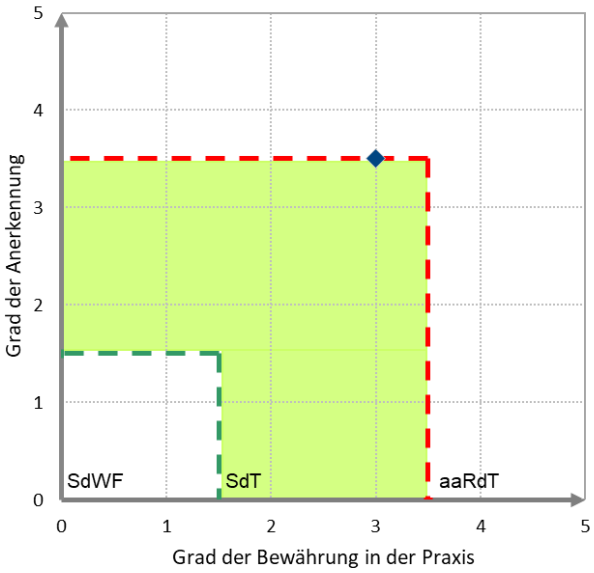
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☐ Authentizität

Einordnung des Technologiestandes



3.2.16 Routersicherheit

Router sind zentrale Infrastrukturkomponenten, die den Austausch von Netzwerkpaketen zwischen mehreren Netzwerken / Rechnern ermöglichen.

Im Geschäftskundenumfeld werden Router nicht nur als Internet-Zugangsgerät bzw. zum Routen von Daten eingesetzt. In den meisten Fällen bauen sie zugleich VPN-Netze auf. Im Zuge der Migration der Telefonieinfrastruktur (Ersatz der ISDN/Analog-Technik durch IP-Technik) werden die Router als ISDN-IP Gateway eingesetzt, um die noch bestehenden ISDN-Anlagen auch in den IP-Netzen weiter einsetzen zu können. Beide Anwendungen machen den Router zu einer unternehmenskritischen Komponente mit spezifischen Sicherheitsanforderungen.

Die weltweite Verbreitung sowohl in Firmen-, Organisations- und Privatnetzwerken macht die Router zur Zielscheibe verschiedener Angriffsmethoden, die durch geeignete Schutzmaßnahmen verhindert werden müssen. In diesem Abschnitt werden die Bedrohungen für Router genannt und aktuell vorhandene Schutzmaßnahmen beschrieben und bewertet.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Router sollen Daten verlässlich und sicher weiterleiten und dabei vor unberechtigten Zugriffen auf diese Daten schützen. Die folgenden Bedrohungen / Risiken gefährden diese Ziele:

1. Manipulation der Konfiguration
2. Angriffe unter Ausnutzung bekannter und nicht geschlossener Sicherheitslücken
3. Angriffe unter Ausnutzung von neu entdeckten Sicherheitslücken (Zero-Day Exploits)
4. Angriffe über IP-Telefonie-Verbindungen
5. Diebstahl (insbesondere auch Router im Außenbereich / Mobilfunk)
6. Verfügbarkeitsangriffe (DoS-Angriffe)
7. Zugriff durch undokumentierte Schnittstellen (s.g. Hintertüren/ Backdoors)
8. Ausführen von Fremdcode und Integration in Botnetze
9. Angriffe über unzureichend abgesicherte WLANs

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Für die oben genannten Bedrohungen existieren mehrere Sicherheitsmaßnahmen zur Risikominimierung, die im Folgenden als Maßnahmenbündel "Routersicherheit" zusammengefasst werden können:

1. Passwortschutz: Verwendung von sicheren,vor fremden Zugriff geschützten, Zugangsdaten sowie Vermeidung der Nutzung von Standardlogins
2. Regelmäßige Aktualisierung der Router-Firmware
3. Serviceverträge mit dem Hardwarehersteller und eine definierte maximale Reaktionszeit für den Fall, dass eine schwerwiegende Lücke bekannt wird.
4. Falls ein Routerhersteller nach Bekanntwerden einer Sicherheitslücke keine Updates bereitstellt, muss die Verwendung von Ausweichgeräten anderer Hersteller, die nicht von der Lücke betroffen sind, in Betracht gezogen werden.
5. Der Router sollte an einem zutrittsgeschützten Ort aufgestellt werden, z.B. ein abschließbarer Raum mit überwachtem Zugang von verantwortlichen Administratoren. Im Außenbereich ist es oft nicht möglich, den Router an einem zutrittsgeschützten Ort aufzustellen. Daher sollte der Router mit einer GPS-Funktion ausgestattet sein. Der Router sollte so konfiguriert werden, dass er z. B. nach einem Stromausfall überprüft, ob er sich noch am vorgesehenen Standort befinden. Sollte das nicht der Fall sein, muss er seinen Betrieb unterbrechen.
6. Zum Schutz vor DoS-Angriffen sollte nach ungültigen Adressen nach RFC 2267 gefiltert werden und Sperrlisten in der Firewall eingerichtet sein.
7. Alle offenen und nicht benötigten Ports und Schnittstellen sollten geschlossen werden.
8. Falls möglich, sollte der Router bei Inaktivität (z.B. über Nacht) automatisch deaktiviert werden, um das Angriffsfenster zu verkleinern. Das Einspielen von Updates sollte durch diese Maßnahme nicht eingeschränkt werden.
9. Um die Auswirkungen von erfolgreichen Angriffen auf Router zu minimieren, sollten unterschiedliche Netzwerkzonen eingerichtet werden (Netzwerksegmentierung).
10. WLAN-Router: Keine offenen Netze bzw. nur für Gastzugang (direkte Ausleitung), ansonsten Anwendung höchster Verschlüsselungsstandards
11. VPN-Router: Aufbau von VPN-Verbindungen nach Möglichkeit nicht über Pre-Shared Keys, sondern zertifikatbasiert
12. Router als All-IP/ISDN-Gateway: Einsatz von Geräten mit integriertem Session Border Controller. Firewalls sind nicht in der Lage, mit SIP-basierten Sprachpaketen umzugehen, so dass hierdurch die Gefahr eines Angriffs über Voice-over-IP-Verbindungen entsteht Der Routerbetrieb sollte zentral überwacht werden.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

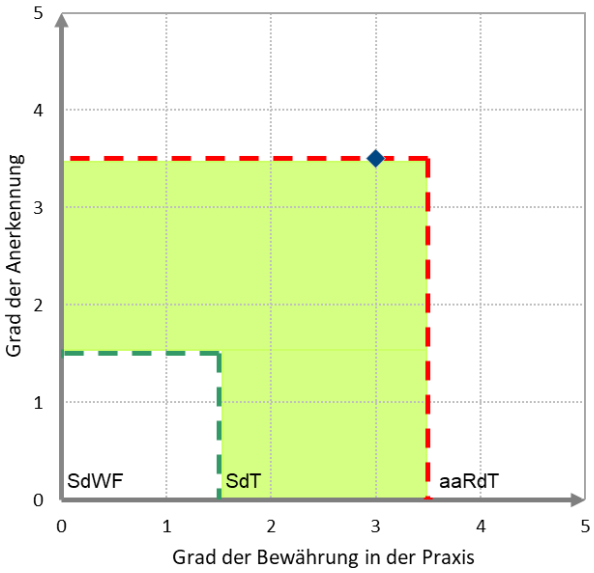
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.17 Netzwerküberwachung mittels Intrusion Detection System

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) erkennt und protokolliert Anomalien im IT-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

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

1. Informationsabfluss durch Abhören schutzbedürftiger Daten
2. Missbrauch von Diensten und Kommunikations-Protokollen
3. Zugang von Fremd-IT-Systemen zum IT-Netz
4. Ausnutzung von Zugangsmöglichkeiten zu vernetzten IT-Systemen
5. Manipulation an Informationen oder Software
6. Verbreitung von Schadsoftware im IT-Netz

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

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 Initiie-rung 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 übergreifen-den 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.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

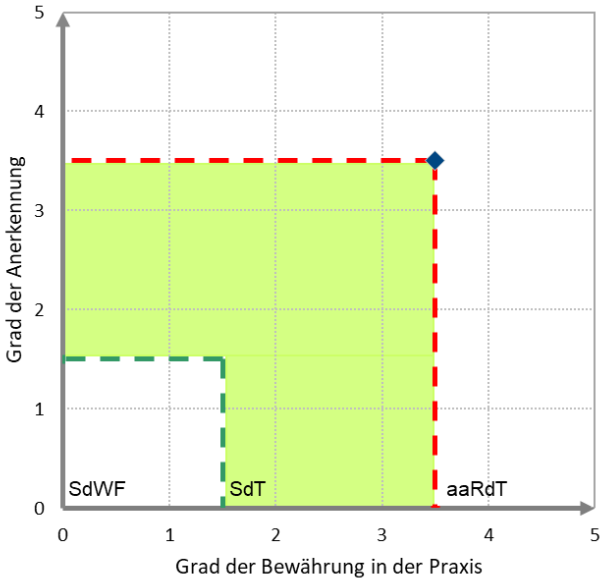
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.18 Schutz des Web-Datenverkehrs

Webserver sind einer der Hauptverbreitungswege für Malware. Benutzern wird durch infizierte Websites zumeist ohne, dass sie es bemerken, Malware auf das System geladen und zur Ausführung gebracht. Wird der Datenverkehr beim Surfen durch einen Webfilter geleitet, können solche Angriffe erkannt und gestoppt werden.

Gegen welche Bedrohung(en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Webserver sind einer der Hauptverbreitungswege für Malware. Zum Einsatz kommen dabei häufig infizierte Webserver, bei denen der Betreiber am Angriff nicht direkt beteiligt ist. 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.

Diese Websites werden vom Benutzer normal angesteuert. Beim Besuch einer infizierten Website wird dann Malware vom Benutzer unbemerkt auf das lokale System geladen und aktiviert (Drive-by-Downloads).

Zusätzlich werden von Angreifern speziell bereitgestellte Webserver eingesetzt, bei denen oft ein anderer Webserver imitiert wird. Beim sog. Phishing werden solche gefälschten Kopien bekannter 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.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Für den Schutz vor solchen Angriffen wird der Web-Datenverkehr durch Webfilter geleitet. 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 betriebe-ne Software.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

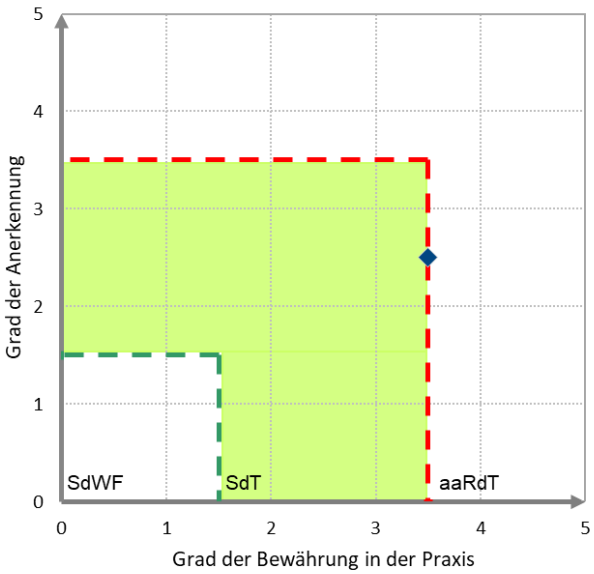
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.19 Schutz von Webanwendungen

Eine Web Application Firewall (WAF) schützt Webanwendungen (Homepages, Online-Shops, Home-banking-Portale etc.) vor Angriffen. Die WAF untersucht dazu die Kommunikation zwischen Benutzer und Webapplikation auf Anwendungsebene und blockiert potenziell schädlichen Datenverkehr, wie SQL Injections oder Cross-Site-Scripting. Für Machine-to-machine-Kommunikation ist auch die Bezeichnung Web Service Firewall (WSF) gebräuchlich.

Im Gegensatz zu einer Netzwerk-Firewall, die auf OSI Layer 3 und 4 arbeitet, behandeln WAFs den OSI Layer 7 - Datenverkehr und schützen damit vor Bedrohungen, die auf Ausnutzung von Sicherheits-Schwachstellen der Applikationen abzielen.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Angriffe auf Webanwendungen oder Web Service-Schnittstellen, wie z.B.

- SQL Injection
- Cross Site Scripting (XSS)
- Information Leakage

- Command Injection
- Weitere OWASP Bedrohungen

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Einsatz einer dem Web Server vorgeschalteten Web Application Firewall (WAF oder WSF).

Eine Web Application Firewall (WAF) schützt Webanwendungen (Homepages, Online-Shops, Homebanking-Portale etc.) vor Angriffen. Die WAF untersucht dazu die Kommunikation zwischen Benutzer und Webapplikation auf Anwendungsebene und blockiert potenziell schädlichen Datenverkehr. Im Fall kurzfristig zu schließender Sicherheitslücken der Webanwendung reicht meist eine Anpassung der WAF aus. Eine Anpassung bzw. Patchen der zu schützenden Webanwendung kann dann im Nachgang geplant und mit ausreichendem Vorlauf für Tests erfolgen. Für Angriffe wird oft eine Kombination von unterschiedlichen Schwachstellen ausgenutzt. Daher können durch das Blockieren einer zentralen Schwachstelle per WAF viele Angriffe schnell abgewehrt werden.

Die Web Services Firewall (WSF) ist ein Spezialfall der WAF für Maschine-zu-Maschine-Kommunikation und wird ebenfalls über http/https abgewickelt. Die Angriffsvektoren für WAF und WSF sind sehr ähnlich. Im Folgenden gilt für die WSF das gleiche wie für die WAF.

Moderne Web-Applikationen und Services bieten oft eine Programmierschnittstelle (API) an, die breite Funktionalität für flexible maschinelle Nutzung anbietet und dadurch selten optimal geschützt ist.

Die WAF terminiert den verschlüsselten benutzerseitigen Datenverkehr, analysiert seine Inhalte und leitet als ungefährlich eingestufte Requests verschlüsselt weiter an den Webserver. Schädliche Requests werden blockiert.

Der Betrieb von Web Applikationen ohne die Verwendung einer als Appliance oder virtuell vorgeschalteten WAF kann nicht mehr als Stand der Technik angesehen werden.

Eine WAF sollte folgende Leistungsmerkmale besitzen:

- Log-Daten-Übertragung an SIEM- und Anomalieerkennungs-Systeme mit Ausblendungsmöglichkeit für Passwörter, Kreditkarteninfos etc.
- Fähigkeit zum Cluster-Betrieb für Hochverfügbarkeit und Lastverteilung
- Schutz vor OWASP Top 10 Angriffen, wie SQL Injection, Cross-Site Scripting (XSS) und Directory Traversal über Blacklisting, Whitelisting und Mustererkennung
- Starke Authentisierung der Web-Applikations- bzw. Services-Nutzer
- Session-Management durch eine Prüfung sowie Manipulationsschutz der Session-Cookies
- Broken Access Control verhindert unerlaubten Zugriff auf Pfade (Path Traversal), Dateien oder API-Funktionen
- Filtern von unnötigen http-Headern
- Schutz vor Cross-Site Request Forgery (CSRF) durch Header-Auswertung der http-Requests, z.B. der referer-Information

Welche Schutzziele werden durch die Maßnahme abgedeckt?

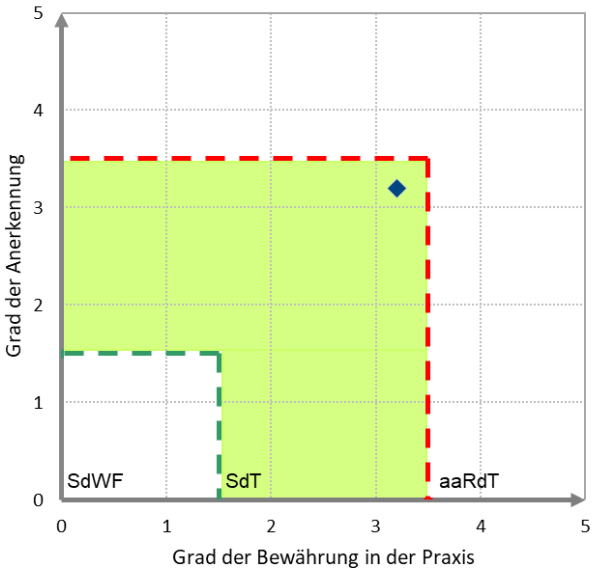
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.20 Fernzugriff auf Netzwerke / Fernwartung

Entfernte Netzwerke müssen zwecks Wartungs- oder Softwareaktualisierungsarbeiten über das Internet erreichbar sein.Im industriellen Umfeld sind diese Teilnehmer Maschinensteuerungskomponenten wie Z.B. SPS, Antriebs- oder Bediengeräte. Im Falle einer Wartung oder Softwareaktualisierung, muss der Fernwartende auf diese Systeme mit seinen Herstellerwerkzeugen (z.B. SPS-Programmiersoftware) online zugreifen.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Nicht autorisierte Zugriffe auf das Firmennetzwerk
- Nicht autorisierte Zugriffe auf die Zielsysteme
- Keine Nachvollziehbarkeit der Fernwartungszugriffe
- Datenabgriff oder Einwirkung während einer Fernwartungssitzung

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Um eine Fernwartung zu ermöglichen, werden typischerweise die Zielsysteme über Router mit dem Internet verbunden. Diese stellen dann darüber eine VPN-Verbindung zu einem so genannten Vermittlungsserver her. Diese Vermittlungsstelle ist Verknüpfungspunkt zwischen dem Zielsystem und dem Fernwartenden, welcher ebenfalls eine VPN-Verbindung zum Vermittlungsserver hergestellt hat. Da beide Stellen somit Ihre eigene Verbindung haben, hat jeder Teilnehmer die Möglichkeit diese jederzeit zu beenden. Die Aufgabe des Vermittlungsservers ist hierbei, nur die zugelassenen Zielsysteme für den jeweiligen Fernwartenden freizugeben. Idealerweise sollte die Einschränkung von Fernwartendem und Zielsystem bis auf Layer3 (IP, Port, Protokoll) erfolgen können. Damit ist die applikationsspezifische Verbindung bis zum Zielsystem gewährleistet. Je nach Anwendung können auch reine Terminalverbindungen über die Fernwartung hergestellt werden. Darunter zählen z.B. Web-, RDP, VNC oder SSH Zugriffe. Das ist abhängig von der Verfügbarkeit auf dem Zielsystem. Insbesondere sollte aber eine direkte 1:1 Netzkopplung vom Fernwarter zum Netzwerk des Zielsystems vermieden werden.

Durch verschlüsselte Verbindungen via VPN wird die Datenintegrität und der Schutz gegen Datenabgriff gewährleistet. Für die Autorisierung des Fernwartenden sollte eine 2-Faktor Authentifizierung zur Verfügung stehen.

Jede Fernwartungssitzung muss protokolliert werden. Diese ist notwendig, um bei einem Sicherheitsvorfall die letzten Zugriffe auf das Netzwerk bzw. Router erkennen zu können. In diesem Fall sollte die Kennung des Fernwartenden (IP-Adresse, Name), die Uhrzeit und Dauer der Verbindung protokolliert werden. Idealerweise wird das auf dem Vermittlungsserver gespeichert.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

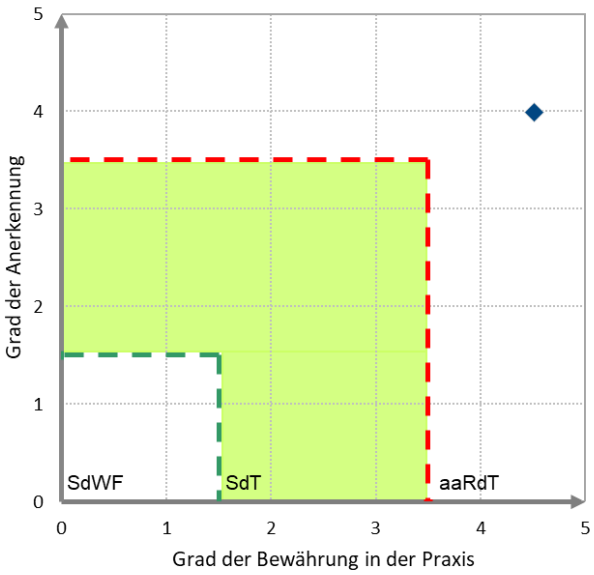
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.21 Serverhärtung

Da auf Serversystemen die wesentlichen (oftmals sensiblen) Daten des Unternehmens sowie personenbezogene Daten verarbeitet und gespeichert werden, müssen die verwendeten Systeme besonderen Schutzmaßnahmen unterzogen werden. Eine sehr wirkungsvolle Maßnahme zur Absicherung stellt die Serverhärtung dar. Sie sichert das Betriebssystem ab, unabhängig davon, ob es sich um einen physikalischen, virtuellen oder cloudbasierten Server handelt.

Gängige Serverbetriebssysteme (z.B. Microsoft Windows Server oder Linux Server) besitzen standardmäßig keine sehr restriktive Sicherheitskonfiguration und sind potentiell mit ungenutzten Komponenten ausgestattet. Gerade diese ungenutzten und nicht konfigurierten Funktionalitäten werden häufig als Einfallstor von Angreifern missbraucht.

Bei der Serverhärtung werden diese Funktionalitäten sowie deren Schnittstellen abgeschaltet und eine starke Sicherheitskonfiguration eingerichtet, was die Sicherheit der Serversysteme maßgeblich erhöht. Daher sollte die Serverhärtung ein fester Bestandteil der technischen Sicherheitsstrategie im Unternehmen sein.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Die wesentlichen Bedrohungen bei nicht gehärteten Serversystemen sind:

- Datenmanipulation von personenbezogenen Daten und sensiblen Unternehmensdaten
- Datenabfluss (z.B. Abzüge gesamter Datenbanken von Datenbanksystemen)
- Manipulation von Anwendungen auf dem Serversystem oder verbundenen Systemen
- Manipulation, Sabotage oder Spionage bei Betriebs- und Produktionsabläufen
- Diebstahl von Identitäten (z.B. bei Angriffen auf Domänencontroller)
- Einbringung von Malware jeglicher Art und Verteilung der Malware zu anderen Systemen
- Missbrauch der Server-Kapazität für Prozesse des Angreifers (z.B. Crypto-Mining)
- Sprungserver für Angreifer, um dann weitere Systeme anzugreifen

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Zur Härtung von Serversystemen sind vor allem folgende Maßnahmen zu berücksichtigen:

1. Deaktivierungen von Komponenten
    - Regelmäßige Überprüfung, ob aktivierte Dienste für den Betrieb noch notwendig sind
    - Deaktivierung oder Deinstallation von nicht notwendigen Betriebssystemkomponenten / Diensten inklusive Hintergrunddiensten
    - Deaktivierung von nicht notwendigen Autostart- oder zeitgesteuerten Prozessen
    - Deaktivierung von nicht benötigten, technisch veralteten oder als unsicher geltenden Schnittstellen oder Protokollen
    - Deaktivierung von Telemetriedaten-Übertragungen, soweit sie nicht für ein zentrales Monitoring mit abgestimmter Richtlinie benötigt werden.
    - Deaktivierung von ungenutzten Dateifreigaben
    - Deaktivierung bzw. Limitierung der Zugriffe auf administrative Webseiten

2. Aktivierung hardwarenaher Schutzfunktionen
    - Aktivierung von CPU-Sicherheitsfunktionen und Prüfung der ordnungsgemäßen Funktion der Anwendungen (z. B. Address Space Layout Randomization "ASLR“, Data Execution Prevention "DEP“)
    - Aktivierung des BIOS-Zugriffspassworts, Limitierung der Bootreihenfolge auf die notwendigen Devices
    - Ggfs. Aktivierung von Schutzverfahren gegen Seitenkanalangriffe
    - Ggfs. Aktivierung von sicheren Bootverfahren

3. Sicherheitskonfiguration
    - Einsatz von Kommunikationsprotokollen zur Sicherstellung, dass sensible Daten sowie Authentifizierungsinformationen verschlüsselt übertragen werden
    - Einsatz von Zertifikaten zum Austausch von kryptographischen Schlüsseln
    - Deaktivierung von Autostart-Mechanismen (z.B. für USB-Medien)
    - Aktivierung eines Bildschirmschoners mit Kennwortschutz
    - Aktivierung starker Benutzerkontensteuerung (User Account Control)
    - Aktivierung des Antivirenschutzes auf dem System bereits beim Bootvorgang
    - Entfernung von nicht notwendigen Zertifikaten aus Vertrauensspeichern
    - Unterbinden von Hinweisen auf installierte Services bzw. Versionsnummern
    - Deaktivierung von Fehler- oder Debug-Meldungen für Endbenutzer oder Ersatz dieser durch neutrale Fehlermeldungen
    - Betrieb der laufenden Dienste nur mit minimalen Rechten und mit einem eigenen Benutzer sowie Betrieb von Prozessen nach Möglichkeit in einer isolierten Umgebung
    - Aktivierung der Protokollierung

4. Minimale Vergabe von Berechtigungen (Need-to-know-Prinzip, Least-Privilege-Prinzip)
    - Regelmäßige Überprüfung der vergebenen Berechtigungen
    - Minimale Rechtevergabe für administrative Tätigkeiten
    - Minimale Rechtevergabe für Dateisystem und externe Datenschnittstellen
    - Minimale Rechtevergabe für Wartungsschnittstellen / -zugängen
    - Einschränkung des Zugriffs auf die Konfigurationsdateien des BetriebssystemsZugangsberechtigung zum physikalischen Server einschränken (insbesondere zur Vermeidung von Anschluss von unberechtigtem externen Datenträgerlaufwerken)
5. Konten und Kennwörter
    - Einsatz starker einheitlicher Kennwortrichtlinien für Benutzerpasswörter (z.B. Kennwortlänge, Komplexität, Sperrzähler, Änderungszyklus etc.) oder Verwendung von 2-Faktor-Authentifizierung (siehe Kap. 3.2.1 ff)
    - Schutz aller Konten mit zumindest einem Kennwort entsprechend der Kennwortrichtlinie
    - Änderung aller vorhandenen Standardkennwörter durch Kennwörter entsprechend der Kennwortrichtlinie
    - Sperre des lokalen Administrator-Kontos nach mehrmaliger Falscheingabe des Kennworts
    - Einsatz von eigenen personenbezogenen administrativen Konten für administrative Tätigkeiten
    - Deaktivierung oder Umbenennung von Standard-Benutzerkonten
    - Deaktivierung von lokalen Gast-Konten
    - Verwendung nicht privilegierter Benutzerkonten zur Ausführung von Prozessen
    - Sperre der Anmeldung von lokalen Benutzerkonten über das Netzwerk
    - Deaktivieren von Standard-, Test- und anonymer Konten für alle installierten Services / Softwarekomponenten

6. Netzwerkkomponenten
    - Einschränkungen bei den Netzwerkeinstellungen (z.B. TCP/IP-Konfiguration), Abschaltung von ungenutzten Netzwerkprotokollen
    - Beschränkung der über einen Dienst laufenden Verbindungen auf das erforderliche Minimum
    - Ggfs. Aktivierung von Paketfiltern/ Firewall und deren Öffnung der minimal benötigten Zugänge

Für gängige Serverbetriebssysteme sind detaillierte Härtungsrichtlinien im Internet öffentlich abrufbar:

- STIGs (Security Technical Implementation Guides): https://iase.disa.mil/stigs
- CIS Benchmarks ("Center for Internet Security, Inc."): https://www.cisecurity.org/cis-benchmarks
- Microsoft Security Guidance: https://blogs.technet.microsoft.com/secguide/

Eine Großzahl der aufgeführten Härtungsmaßnahmen ist durch technische Einstellungen realisierbar. Diese Einstellungen lassen sich über ein Härtungspaket (z.B. mittels Skripten) automatisiert auf alle Serversysteme des Unternehmens verteilen. Neue Serversysteme sollten direkt nach Abschluss der Installation mit dem Härtungspaket gehärtet werden. Bei der Härtung von bestehenden Systemen mit einem Härtungspaket könnte eine Härtung zum Ausfall von Funktionalitäten führen, daher muss eine Datensicherung erstellt und die Härtung ausgiebig getestet werden.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

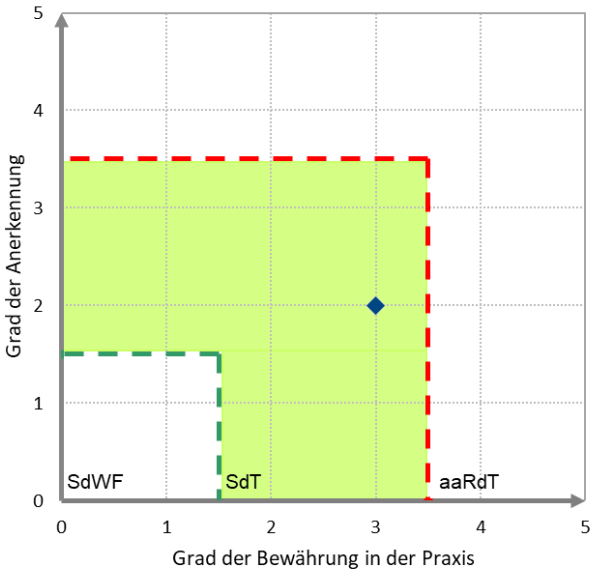
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

EDR-Plattformen kombinieren wirksame Detektions- und Präventionstechniken, um die Kompromittierung von Clients und Servern, auch über Computer und Betriebsystemgrenzen hinweg, zu verhindern und sogar aktive Angreifer in Computernetzen zu enttarnen.

Leichtgewichtige Agenten stellen die angriffsrelevanten Prozess-Telemetrie-Daten bereit, nutzen lokal wirksame Maschinen-Lern-Modelle (künstliche Intelligenz) und korrelieren und visualisieren ganzheitlich die Taktiken, Techniken und Prozeduren.

Aufgrund modernster Sensor-Architektur lasten Next Generation EPP-Lösungen einen Computer nur zu einem Bruchteil eines klassischen AV-Scanners aus und der regelmäßige Download von Signaturen entfällt. Das bedeutet:

- Signaturlose Erkennung und aktive Blockierung von Schadcode durch Maschinen-Lern-Modelle (vorzugsweise lokale Laufzeit),
- Prüfung und Aufzeichnung von Programm-Aktivitäten über Prozessketten hinweg und optionale Blockierung schädlichen Verhaltens,
- Schutz vor der Ausnutzung von Schwachstellen innerhalb legitimer Applikationen (Exploits und Speichermanipulation)
- Idealerweise werden Erkennungen korreliert dargestellt und die Technik und Taktik (inkl. Verwendeter Werkzeuge wie z.B. Malware, Trojaner, PowerShell-Scripting und das Ziel des Angreifers werden dargestellt (Exfiltration von Daten, Einrichten einer Backdoor, laterale Bewegung innerhalb der Organisation, Rechte-Eskalation etc.)
- Zusätzliche Threat Intelligence zeigt auf, wer der mutmaßliche Akteur/Gegner ist (Cybercrime oder nationalstaatlich motivierter Angriff) und welche Ziele und Branchen die Angreifer verfolgen.
- Eine vollintegrierte Sandbox-Anbindung erlaubt die sichere "Detonation“ von gefundenem Schadcode zur weiteren Analyse, ohne die Produktion zu gefährden

EDR-Plattformen adressieren den gesamten Lebenszyklus eines Angriffsversuches. Erst dadurch werden Rückschlüsse auf die Akteure und deren Motivation möglich, die idealerweise durch aktuelle Bedrohungsinformationen kontextuell vervollständigt wurden. Darüber hinaus können System-Telemetrie Daten durch externe Experten auf schädliche Indizien geprüft werden.

Darüber hinaus muss ergänzt werden, dass zu einer ganzheitlichen Absicherung von Endgeräten insbesondere die folgenden Punkte berücksichtigt werden müssen, sollten diese Aspekte nicht durch die jeweilige EDR-Lösung selbst bereitgestellt werden:

- Berechtigungen / Rollen (Stichwort: administrative Berechtigungen)
- Update-Mechanismen (Betriebssystem und Software)
- Einschränkungen / Kontrolle der installierten Software
- Verschlüsselung der Endgeräte
- Schutz gegen Bedrohungen / Malware wie oben beschrieben
- Regelungen / Richtlinien für den zulässigen Gebrauch (Privatnutzung, Nutzung in firmenfremden Netzwerken, Reisen, Verwendung von Datenträgern, Speicherung von Daten, Backup usw.); insb. wenn der User administrative Rechte besitzt
- Einsatz von Authentisierungsverfahren (Username/Passwort, PIN, Biometrie, usw.)

Welche Schutzziele werden durch die Maßnahme abgedeckt?

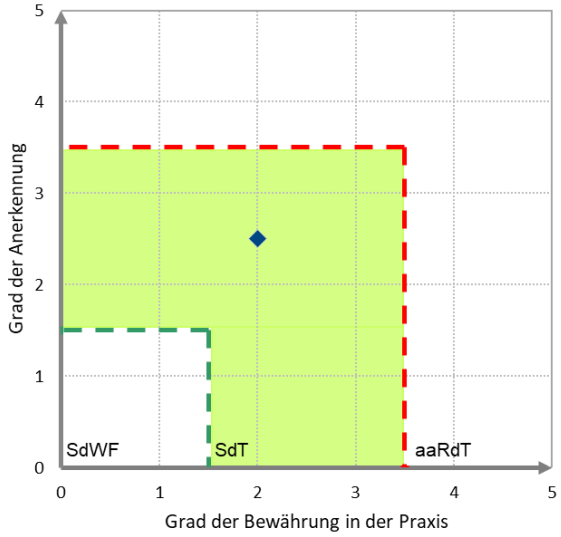
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.23 Internetnutzung mit Web-Isolation

Web-Isolation separiert den Arbeitsplatz des Anwenders von den Browser-Sessions und ermöglicht eine sichere Internetnutzung ohne Einschränkungen der Inhalte oder Funktionen. Browsergestützte Cyber-Angriffe, Datenabfluss/-verlust und damit einhergehende Produktivitätseinschränkungen und Image-Schäden werden wirksam verhindert.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Infektion des Arbeitsplatzrechners beispielsweise durch

- Browserschwachstellen, Drive-by-Downloads, Infektiöse Webseiten
- Ransomware, APT, Trojaner, Viren, Würmer
- Zero-Day-Exploits
- maliziöse Links in E-Mails

und dadurch Ausbreitung von Schadsoftware im unternehmenskritischen Netzwerk.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Die Isolation der Browser-Sessions kann auf mehrere Arten erfolgen. Ausschlaggebend sind dabei die eingesetzte Architektur und deren Sicherheitsmechanismen. Beispiele sind die sogenannten "Remote-Controlled“ Browser-Umgebungen oder mehrschichtige lokale Browser-Isolationen.

Eine simple Isolation der Browserumgebung (z.B. über einfache Virtualisierung auf Basis von Hyper-V oder das sogenannte Browser-Sandboxing) bietet keinen hinreichend hohen Schutz vor den genannten Bedrohungen, da sie z.B. standardmäßig kein sicheres gehärtetes Betriebssystem, in dem der Browser läuft, aufweist; keine zusätzliche abgesicherte Netzwerksegmentierung nutzt; kein sicheres Copy & Paste ermöglicht oder auch keine ergänzenden Sicherheitsfunktionen wie Datenschleusen nutzt. Deshalb ist diese Methode zur Abwehr der Bedrohungen nicht geeignet.

Remote-Controlled-Browser-Umgebungen auf Basis von ReCoBS

Das Remote-Controlled Browser System (ReCoBS) separiert auf physischer Ebene die Internetnutzung vom Endgerät des Anwenders. Jede Browsersession wird außerhalb des sensiblen Netzwerkbereichs in einer eigens abgeschotteten Umgebung innerhalb eines speziell gehärteten Systems auf separater Hardware in einem separierten Netzwerksegment (DMZ) ausgeführt.

Über einen technisch abgesicherten Kommunikationskanal wird der Browser vom Arbeitsplatz aus per Videostream auf dem Remote System ferngesteuert. Ein Großteil der Angriffe, die auf Windows-basierte Sicherheitslücken zielen, wird in der gehärteten Linux-Umgebung bereits erfolgreich abgewehrt. Weitere Sicherheitsmechanismen und -zonen in der Gesamtarchitektur schützen auch dann noch zuverlässig vor Angriffen, wenn der Browser kompromittiert wurde. Durch die physische Trennung von Arbeitsplatz und Browsersystem besteht zudem Schutz gegen Hardware-nahe Angriffe (Spectre, Meltdown, ZombieLoad oder Schwachstellen im Hypervisor).

In regelmäßigen Abständen (laut Standard einmal am Tag) sollte das Remote System über ein Systemimage in seinen Ursprungszustand zurückversetzt, so dass jeglicher Schadcode wirksam entfernt wird.Es muss sichergestellt werden, dass das Systemimage integer aufbewahrt wird.

Der Arbeitsplatz des Anwenders benötigt zu keinem Zeitpunkt direkten Zugang zum Internet und ist somit zusätzlich geschützt, z.B. gegen das Nachladen von Schadcode durch infektiöse Dokumente, die auf anderen Wegen - etwa per E-Mail oder USB-Stick - auf den Rechner gelangt sind.

Da durch die ReCoBS-Architektur gängige Standardfunktionen des Browsers prinzipbedingt auf dem Remote System ausgeführt werden, sind für die Akzeptanz der Anwender zusätzliche Entwicklungen

notwendig, damit der ferngesteuerte Browser sich unwesentlich von einer lokalen Browsernutzung unterscheidet und alle üblichen Funktionen wie persönliche Lesezeichen, Copy & Paste, Drucken oder Down- und Uploads prinzipiell angeboten werden.

Für die optionale Übertragung von Dateien (Browser Download/Upload) zwischen Remote System und Arbeitsplatz sind zusätzliche Prüfmechanismen vorzusehen, die auffällige Dateien in Quarantäne verschieben und Administratoren benachrichtigen. Als Beispiel eines solchen Prüfmechanismus ist der Virenschutz in der Datenschleuse.

Zudem empfiehlt sich ein zentrales Management der Gesamtlösung, so dass beispielswiese ein bestehender Verzeichnisdienst gekoppelt und zur Verwaltung der Benutzerrollen genutzt werden kann.

Web-Isolation basierend auf der lokalen Virtualisierung der Browser-Anwendung

Ein weiterer Ansatz zur Web-Isolation basiert auf der lokalen Kapselung der Browser-Anwendung durch sichere Virtualisierung in Kombination mit einem rechtebegrenzten Windows-Benutzer-Account, gehärtetem Gast-Betriebssystem sowie einer Internet-/Intranet-Trennung durch separaten VPN-Tunnel zum Internet-Gateway. Dadurch wird ein direkter Zugriff von der Browser-Session auf die PC-Hardware ausgeschlossen.

Ein Vorteil der lokalen Browser-Isolation ist die Möglichkeit einer Stand-alone-Verwendung auf mobilen Arbeitsplätzen. Die nicht vorhandene physische Trennung zwischen sensiblem Arbeitsplatz und Browsersystem könnte jedoch ermöglichen, dass über ein alle Schutzschichten umfassendes Exploit-Paket lokale Sicherheitslücken in der Prozessor-Hardware oder Software zum Einbruch in das Endgerät ausgenutzt werden könnten.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

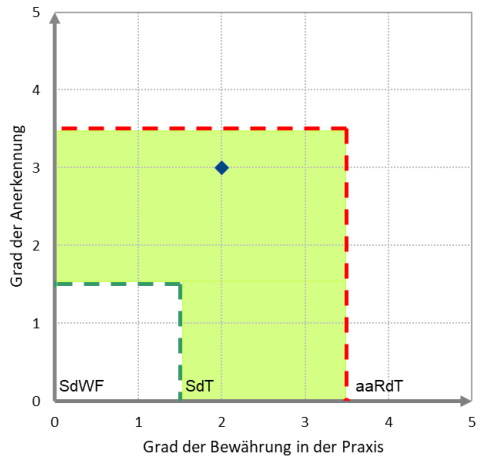
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.24 Angriffserkennung und Auswertung (SIEM)

Für die Auswertung von Anomalien und Erkennung von Angriffen der Unternehmensinfrastruktur werden sogenannte Security Information and Event Management Systeme (kurz: SIEM) eingesetzt. Sie ermöglichen ganzheitlich, sicherheitskritische Events der IT-Infrastruktur in Echtzeit zu erkennen und geeignete Maßnahmen (teilweise automatisiert) durchzuführen.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

SIEM kann gegen die folgenden Bedrohungen unterstützen:

- Angriffsaktivitäten durch Externe (Hacker-Angriffe)
- Bedrohungen durch Insider (z.B. wie der unberechtigte Zugriff auf Daten aus anderen Abteilungen, Computersabotage)
- Compliance-Verstöße

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Durch ein SIEM werden Log- und Eventdaten von Geräten, Netzkomponenten, Anwendungen und Security Systemen zentral gesammelt. Beispielsweise können im SIEM folgende Datenquellen abgebildet werden:

- Logfiles aus Betriebssystemen
- Firewall-Events von Netzwerkfirewalls
- Alarme von Intrusion Detection & Prevention Systemen (IDS/IPS)
- Intelligente Netzwerksensoren / Netzwerkmonitorsysteme mit Informationen über gefundene Assets/Geräte, Schwachstellen, Compliance-Verstößen oder anomalem Netzwerkverhalten
- Verzeichnisdiensten Authentication-Services (wie Single Sign on Systeme)
- Endpoint Detection & Response Systeme (EDR/XDR)
- Indikatoren zur Identifikation von Angreifern und Angriffen wie IP-Adressen, Hashes, Hostnamen etc. (Threat Intelligence Feeds) sowie z.B. Kontext-Informationen zu Angreifern zur Anreicherung

Das Sicherheitsteam im Unternehmen hat die Möglichkeit, durch gezielte Aggregation und Analyse sicherheitsrelevanter Event- und Systemprotokolle ein ganzheitliches Bild von den Vorgängen in seiner IT-Lösungs-/Infrastruktur in Echtzeit zu erhalten. Dadurch werden Angriffe, außergewöhnliche Muster und gefährliche Abläufe sichtbar. Auf Basis der gewonnenen Erkenntnisse sind Unternehmen in der Lage, schnell und präzise auf akute Bedrohungen zu reagieren. Auf Grundlage der verfügbaren Daten können im Nachgang eines Angriffs die Muster analysiert (Forensik) und die bestehenden Maßnahmen verbessert werden.

Moderne SIEM-Tools umfassen zuverlässige und sofort einsetzbare Erkennungsregeln, die an neue Bedrohungsfälle angepasst werden können. Der Betrieb einer SIEM-Lösung erfordert die Einbindung geeigneter Quellen aber auch die Bereitstellung signifikanter Systemressourcen (z.B. Graph-Datenbanken, Data Lakes und Server für den Betrieb und das Management). Durch den kontinuierlichen Datenaustausch wird gleichzeitig eine signifikante Bandbreitenauslastung erreicht. Die damit verbundene administrative Komplexität und die Anschaffungs- und Betriebskosten sind recht hoch, weshalb die klassischen SIEM-Lösungen in der Regel meist in großen und sehr großen Unternehmen zur Anwendung kommen.

Cloudbasierte und Drittanbieter-verwaltete Lösungsansätze wie SIEMaaS (SIEM as a Service) sind eine zeitgemäße Alternative mit gut kalkulierbaren Kosten. Sie ermöglichen den Einsatz der Technologie auch in kleineren und mittelständischen Unternehmen. Ebenso kann eine moderne Endpoint Detection & Response Plattformen (DER/XDR) mit seinen Schnittstellen zu Security Orchestration,

Automation and Response (kurz: SOAR), Netzwerk-Security Produkten wie Next-Generation Firewalls sowie integrierter Threat Intelligence eine sinnvolle Alternative darstellen.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

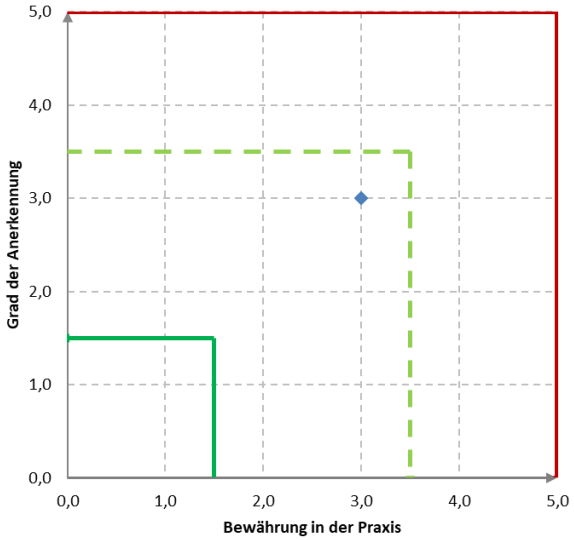
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.25 Vertrauliche Datenverarbeitung

Die privilegierten Zugriffe durch Administratoren auf Daten während der Verarbeitung sind herkömmlich lediglich mit organisatorischen oder reaktiven Maßnahmen gegen einen Missbrauch des Privilegs abgesichert. Mit Hilfe der vertraulichen Datenverarbeitung (eng. confidential computing) sind diese Daten manipulationssicher und präventiv gegen unberechtigten Zugriff geschützt. Dies ist insbesondere für Anwendungen im Bereich des Cloud-Computing wichtig. Vertrauliche Datenverarbeitung entspricht dem Schutzbedarf, wenn Cloud-Dienste für kritische Infrastrukturen oder für sensible Datenverarbeitungsvorgänge, etwa in der Medizin, der Industrie oder in regulierten Bereichen (e.g. regTech) eingesetzt werden.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Cloud-Administratoren sind für den störungsfreien Betrieb ihrer Systeme verantwortlich. Um diese Aufgabe erfüllen zu können, bekommen sie dafür zahlreiche Privilegien eingeräumt. Beispielsweise können sie die System-Konfiguration anpassen und Speicherinhalte auslesen. Somit können Daten auf dem Weg in die Cloud, im Cloud-Speicher liegend und während der Verarbeitung in der Cloud nicht nur durch Angriffe Dritter, sondern auch durch widerrechtlich handelnde Mitarbeiter von Cloud Service Providern kompromittiert werden.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Bisherige Ansätze zur Datensicherung beziehen sich auf Daten im Ruhezustand (Speicherung) und Daten im Transit (Netzwerk). Confidential computing fokussiert den Schutz der Daten während der Verarbeitung. Dabei handelt es sich um einen von der Außenwelt abgeschirmten Bereich oder Kapsel, in dem die komplette Datenverarbeitung im unverschlüsselten Zustand stattfindet. Diese Abschirmung kann entweder direkt auf dem Prozessorchip der Server und/oder gleich über mehrere Server umgesetzt werden. Damit die Daten verarbeitet werden können, muss der erforderliche Schlüssel innerhalb der Kapsel verfügbar sein. Würde ein Angreifer versuchen Zugriff zum gekapselten Bereich zu erlangen, würden zwangsläufig die dort unverschlüsselt verarbeiteten Daten vorsorglich gelöscht. Um eine erhöhte Sicherheit zu erreichen, können die Kapseln durch unabhängige Auditoren nach vorheriger Prüfung mittels bekannter kryptografischer Geheimnisse versiegelt werden.

Bei Datenverarbeitungsanlagen, die mit den unter dem Oberbegriff "Confidential Computing“ zusammengefassten Maßnahmen ausgestattet sind, kann ein einzelner Administrator keinen Zugriff auf die im Server verarbeiteten Daten erlangen. Nur durch ein arglistiges Zusammenwirken (malicious coalition) von mehreren unabhängigen Parteien (z.B. System-Administrator zusammen mit deren unabhängigen Auditoren) können die technischen Maßnahmen außer Kraft gesetzt werden. Dadurch verringert sich die Wahrscheinlichkeit eines missbräuchlichen Zugriffs um mehrere Größenordnungen.

Die vertrauliche Datenverarbeitung

- ermöglicht, Daten in zentralen Infrastrukturen zu verarbeiten, ohne sie der Möglichkeit der Kenntnisnahme durch die Betreiber dieser zentralen Infrastruktur auszusetzen,
- bietet den Benutzern mehr Kontrolle und je nach Audit auch Transparenz
- bietet neue Freiheitsgrade, denn es sind so neue Anwendungen denkbar, die unter herkömmlichen Datenschutz- und Sicherheitsbetrachtungen nicht rechtskonform implementierbar waren.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

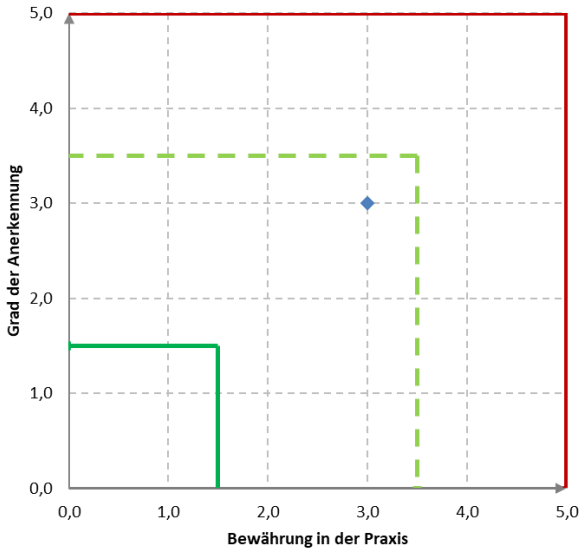
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung der Maßnahme



3.2.26 Sandboxing zur Schadcode-Analyse

Die Sandbox-Technologie wird genutzt, um potenziell gefährliche Dateien in einer isolierten Umgebung auszuführen und auf schädliches Verhalten hin zu überprüfen. Durch die Ausführung in einer separaten Umgebung wird eine mögliche Infektion verhindert.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- *Hacker Aktivitäten i.w.S.*
- *Malware (Viren, Trojaner etc.)*
- *Phishing*

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Die Nutzung der Sandboxing-Methode zur automatisierten Malware-Analyse ist in zwei Anwendungsfällen üblich.

Perimeter Sandboxing

Im Rahmen des Perimeter Sandboxing werden üblicherweise Dateianhänge (wie z.B. Dokumente aus der Wirkumgebung, aber auch eingebettete Inhalte wie Scripte) aus E-Mails automatisiert ausgeführt. Die Sandbox-Analyse am E-Mail Gateway erzeugt in der Regel eine Latenz im Zugriff auf den untersuchten Dateianhang durch den Anwender, die im Bereich von wenigen Sekunden bis Minuten liegt.

Auch am Web-Gateway (Next-Generation Firewall oder Proxy) lassen sich Sandboxen einsetzen, um z. B. heruntergeladene Programme zu prüfen. Auch hier wird eine Verzögerung bis zur Zustellung der Datei an den Anwender verursacht wird. Darüber hinaus beeinflusst der Einsatz ebenfalls das Verhalten des Browsers und einer Web-basierter Software. Daher wird neben der klassischen Funktionsweise des Sandboxing (erst prüfen, dass verzögert ausliefern) auch eine Zustellung der Datei an das Endgerät mit paralleler Prüfung praktiziert. Wird bei der letzteren Vorgehensweise Schadcode identifiziert, werden nachträgliche Maßnahmen ergriffen. Dazu zählen u.a. Netzwerk-Isolation, Sperrung von „Command und Control“ Adressen, die bei der Sandboxausführung ermittelt wurden.

Sandbox zur forensischen Untersuchung von Dateien die im Rahmen einer Detektion oder Ermittlung
Durch die Anbindung von Sandboxen an Next-Generation Antivirus-Produkte (Machine Learning-basiertes Antivirus) und EDR-Lösungen (Endpoint Detection und Response) lassen sich Dateien mit schädlicher Prognose oder aus erkannten und auch aktiv unterbundenen Angriffsketten außerhalb der

Wirkumgebung sicher zur Ausführung bringen. Die Ausführung ermöglicht dann die Extraktion weiterer relevanter Indikatoren (Dateien/Hashes, URLs, IP-Adressen, Registry-Aktivitäten etc.) die einem in der Untersuchung befindlichen Fall mehr Kontext und sogar die Attribution eines mutmaßlichen Angreifers ermöglicht.

Da Sandbox-Lösungen einen recht hohen Verbreitungsgrad aufweisen, versuchen Angreifer immer wieder die Erkennung in einer Sandbox zu verhindern. Beispielsweise versuchen sie bei der Ausführung ihres Schadcodes festzustellen, ob es sich um eine virtualisierte Laufzeitumgebung - wie bei Sandboxen üblich – oder einer Wirkumgebung mit bestimmten Programmen/Prozessen und anderen spezifischen Merkmalen handelt. Der Schadcode wird sich in der Regel dann harmlos verhalten, um seine Erkennung zu vermeiden. Allerdings kann auch dieses Verhalten in der Sandbox erkannt und zur Identifikation verdächtiger Inhalte genutzt werden (Katz- und Maus-Prinzip).

Auch die Ausnutzung von sogenannten „Day-0 Exploits“/ Zero-Day-Bedrohungen, also Schwachstellen, die der Öffentlichkeit bisher unbekannt sind, können zu Sandbox-Umgehungen führen. Ebenso kann es passieren, dass die emulierte Laufzeitumgebung nicht dem Opfersystem entspricht und somit das Verhalten bei der Ausführung in der Sandbox von dem auf den Zielsystem eines Angriffes abweicht. Es ist daher notwendig diese als „Sandbox-Evasion“ bekannten Taktiken zu beherrschen, indem beispielsweise statische und dynamische Analyse kombiniert wird.

Sandboxen bieten weiterhin aufgrund ihrer hohen Automatisierbarkeit einen großen Nutzen, um den Bedarf an manueller Analyse von Schadcode (s.g. Malware Reverse Engineering) durch einen Experten, massiv zu reduzieren.

Es gibt eine große Zahl von Opensource und kommerziellen Sandboxen. Diese werden als meist kostenintensive Hardware Lösungen angeboten, aber auch als öffentlich oder privat bereitgestellte Cloud-Lösungen. Seit längerem wird Sandbox-Technik auch in Browsern angewendet, um gängige Angriffsarten frühzeitig zu erkennen.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

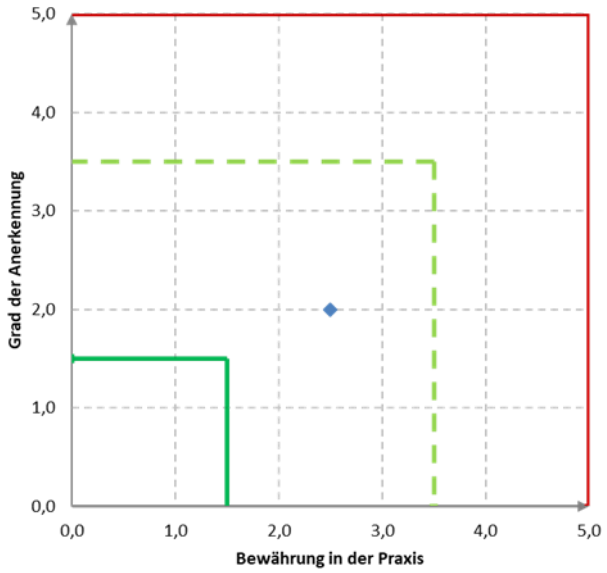
☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung der Maßnahme



3.2.27 Cyber Threat Intelligence

Cyber Threat Intelligence ist ein wichtiger Grundbaustein moderner Verteidigungsstrategien und liefert Indikatoren, Reports und Dienstleistungen, um sich über das aktuelle Angriffsgeschehen zu informieren, Cyberangriffe zu erkennen, deren mutmaßliche Urheber zu bestimmen und Gegenmaßnahmen abzuleiten.

Cyber Threat Intelligence gliedert sich in drei Anwendungsbereiche:

- Taktische Cyber Threat Intelligence umfasst Malware-Analyse und den Import von einzelnen, statischen und verhaltensrelevanten Bedrohungsindikatoren in defensive IT-Sicherheitslösungen wie Netzwerk-, Endpoint- und Applikationssicherheitslösungen, um deren Effektivität zu erhöhen. Durch Cyber Threat Intelligence gewonnene Indikatoren können bei Maßnahmen wie System-Patching eine wichtige Rolle spielen.
- Operative Cyber Threat Intelligence dient der Verbesserung des Wissens über einen Angreifer, seine Fähigkeiten, Infrastrukturen und Angriffstaktiken, sowie Techniken und Prozeduren (TTPs). Anhand dieser Informationen lassen sich deutlich zielgerichteter Cybersicherheitsmaßnahmen wie Vorfalls-Analysen, Incident Response und proaktives Threat Hunting umsetzen. Die Leistungsfähigkeit von Cybersicherheits-Mitarbeitern (z.B. aus dem Security Operation Center oder CERT) wie Threat Hunting Experten, Vulnerability Managern, Incident Response Analysten und Experten zur Abwehr von Insider-Bedrohungen wird dadurch verbessert.
- Strategische Threat Intelligence ermöglicht ein besseres Verständnis über die aktuelle Bedrohungslage (Threat Assessment), die Ableitung von Trends und die Motivation einzelner Angreifergruppen. Sie unterstützt bei strategischen Geschäftsentscheidungen zur Verbesserung der Cybersicherheit.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Cyber Threat Intelligence informiert über alle Arten von aktuellen und potentiellen Cyberbedrohungen und hilft bei deren Abwehr.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Taktische Cyber Threat Intelligence (TM)

Einbindung von Bedrohungsindikatoren (Feeds) in vorhandene Endpoint- und Netzwerk-Detection & Response-Systeme, System-Management-Lösungen, Firewalls, IDS/IPS und SIEM/SOAR Lösungen mit dem Ziel, reale Angriffe zu identifizieren und Analysen zu unterstützen (auch Retro Hunting), sowie präventiv Kompromittierungen zu verhindern. Für optimale Wirksamkeit sollten die Indikatoren automatisiert zur Detektion und Prävention von Cyberangriffen genutzt werden können. Die Quellen für Threat Intelligence Indikatoren ermöglichen ggf. Rückschlüsse auf deren Zuverlässigkeit und werden unterschieden in:

- Open-Source-Intelligence (OSINT),
- Events aus privaten Honeypot-Systemen,
- Erkenntnisse aus Angriffsanalysen aus echten Kundenumgebungen, oder der
- Ermittlungsarbeit von geheimdienstlich ausgebildeten Experten

Operative Cyber Threat Intelligence (TM/OM)

Organisationen, die ein Security Operation Center (SOC) betreiben und ggf. ein eigenes Computer Emergency Response Team (CERT) haben, nutzen Threat Intelligence operativ, um sich kontinuierlich über die Akteure und deren TTPs zu Informieren. Dazu bieten umfassende Threat Intelligence Plattformen neben dem Zugriff auf Indikatoren auch unterschiedliche Report-Formate (Kurzmeldungen, Lageberichte, Angreifer-Profile) sowie Zugriff auf Malware-Datenbanken, Sandbox-Technologie zur automatisierten Malware-Analyse sowie Malware-Reverse Engineering an. Kundenspezifische Bedürfnisse sollten vom Anbieter abgedeckt werden können. Weiterhin sollte es die Möglichkeit geben, direkt auf Analysten beim Anbieter zugreifen zu können und Nachforschungsanfragen (RFIs) zu stellen.

Strategische Threat Intelligence (OM)

Sowohl die Bereiche der Informationssicherheit als auch Gesamt/-Konzernsicherheit großer Unternehmen nutzen Threat Intelligence, um sich ein möglichst lückenloses Lagebild zu schaffen. Hierbei stehen die geopolitische Lage sowie branchenspezifische und globale Trends in der Bedrohungslandschaft im Vordergrund. Durch den Zugriff auf einen dedizierten Mitarbeiter beim Anbieter wird das eigene Team virtuell erweitert und sichergestellt, dass direkter Zugriff auf dessen Datenpool ermöglicht, sowie kundenspezifische Ermittlungsarbeit optimal geleistet wird.

Anbieter moderner IT-Sicherheitslösungen liefern, integrieren und automatisieren Threat Intelligence, so dass Bedrohungsindikatoren und relevante Angriffstelemetrie sinnvoll verknüpft, präventive Maßnahmen automatisiert und die Angreifer-Attribution ermöglicht werden, ohne dass der Anwender hierfür weitere Systeme und sogar Personalressourcen benötigt.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

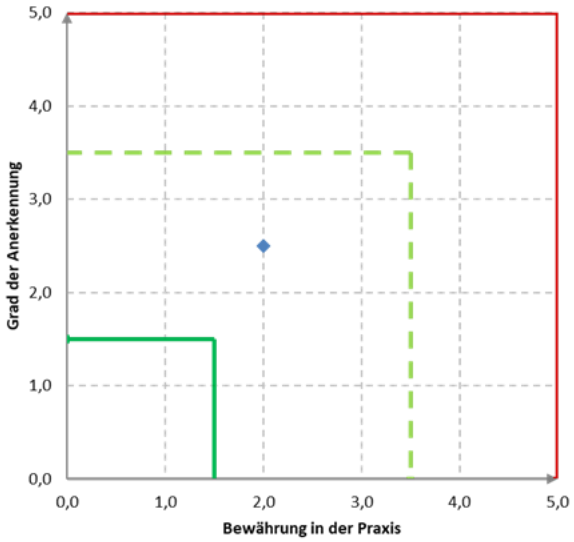
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☐ Authentizität

Einordnung der Maßnahme



3.3 Organisatorische Maßnahmen

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 wichtigen 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.

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 1: Übersicht der ISO/EC 27000-Reihe

Weitere 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:

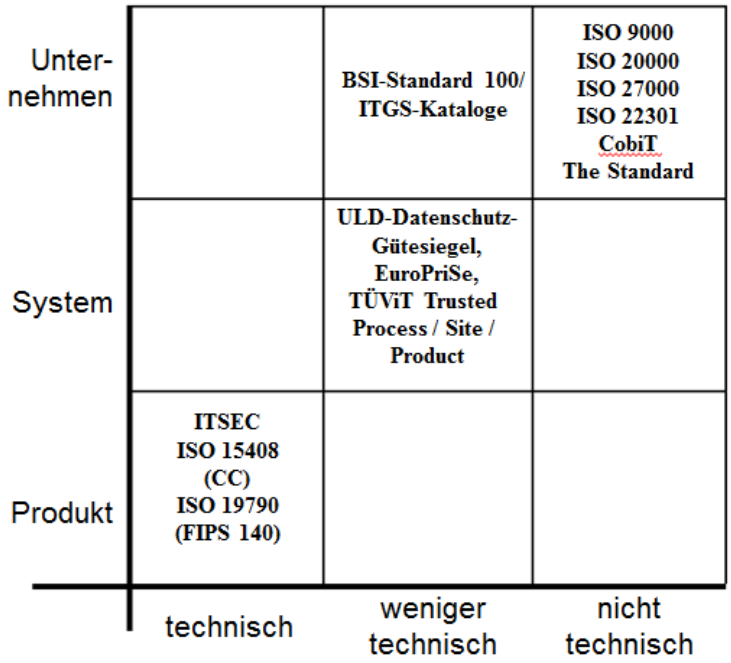


Abbildung 5: Gliederungsebenen informationssicherheitsrelevanter Standards und Normen

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 systematische 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 Rahmenbedingungen	Konkrete Vorgaben praktischer 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 2: Abgrenzung ISO 27001 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 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-Normen 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 "Standes 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 den aktuell gültigen Normen erfolgt. Für die Maßnahmen sind mindestens die Normen 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:

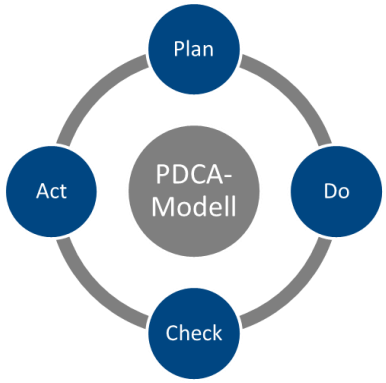


Abbildung 6: PDCA-Modell

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 "Standes 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. Desweiteren 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.

Weitere Details werden im Kapitel „Management von Informationssicherheitsrisiken“ erläutert.

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 TeleTrusT-Dokument "Informationssicherheitsmanagement - Praxisleitfaden für Manager" beschriebenen Schnittstellen und Prozessen, sind für die Einhaltung des "Standes 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 unberechtigte 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 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 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. (vgl. Kapitel 3.3.3)

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 "Standes 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 Organisationseinheit (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.

3.3.3 Sichere Softwareentwicklung

Die Sicherheit einer Anwendung muss im gesamten Softwareentwicklungsprozess berücksichtigt werden. Dabei sind Maßnahmen zur sicheren Anwendungsentwicklung unabhängig von der verwendeten Entwicklungsmethode zu berücksichtigen. Vorgehensmodelle und Best Practices für sichere Softwareentwicklung werden in u. a. in BSIMM, OWASP SAMM, OWASP ASVS, dem BSI Leitfaden "Leitfaden zur Entwicklung sicherer Webanwendungen“ oder ISO/IEC 27034 beschrieben und im TeleTrusT Professional for Secure Software Engineering T.P.S.S.E. gelehrt. Die wesentlichen Schutzmaßnahmen innerhalb des Softwareentwicklungsprozesses sind in den einzelnen Kapiteln aufgeführt.

3.3.3.1 Anforderungsanalyse

Sichere Anwendungsentwicklung beginnt bei der Anforderungsanalyse. Das Fundament der Anforderungsanalyse ist eine Bedrohungsanalyse. Hierbei müssen die zu schützenden (Unternehmens-) Werte definiert und die Bedrohungen beschrieben werden, die für diese Werte bestehen. Dabei müssen die Architektur der Anwendung - insbesondere die Datenhaltung und die Datenflüsse - sowie ihre Vertrauensgrenzen berücksichtigt werden. Anschließend müssen die Risiken dieser identifizierten Bedrohungen bewertet und daraus Gegenmaßnahmen und Sicherheitsanforderungen an die Anwendung abgeleitet werden. Eine hilfreiche Methode zur Identifikation konkreter Bedrohungen ist eine Definition sogenannter Abuse-Cases. Diese beschreiben konkrete Angriffe sowie das jeweilige gewünschte Verhalten der Anwendung im Angriffsfall. Weitere Sicherheitsanforderungen an die Anwendung ergeben sich bspw. aus Rechtsvorschriften oder vertraglichen Verpflichtungen. Diese Sicherheitsanforderungen fließen, wie die funktionalen Anforderungen, in die folgende Designphase des Softwareentwicklungsprozesses und auch in die Spezifikation der Testfälle für die späteren Tests der Anwendung mit ein.

Auch das oftmals als Standard der generellen Anforderungsspezifikation gesehene Volere-Template[28] definiert bereits eine Reihe von Security-Anforderungen, die berücksichtigt werden sollten:

- 15a. Access Requirements
- 15b. Integrity Requirements
- 15c. Privacy Requirements
- 15d. Audit Requirements
- 15e. Immunity Requirements

3.3.3.2 Softwaredesign

Ein sicheres Design muss alle Sicherheitsanforderungen berücksichtigen, um so den identifizierten Bedrohungen entgegenwirken zu können. Ergebnis des Designprozesses ist u. a. die Sicherheitsarchitektur inklusiver einer Datenbehandlungsstrategie. Ein sicheres Design berücksichtigt Aspekte wie Sichere Authentifizierung, Kryptografische Anforderungen, Fehlerbehandlung, Systemkonfiguration, Vertrauensbeziehung zwischen Anwendungskomponenten und die Geschäftslogik der Anwendung. Eine ungenügende Berücksichtigung der Sicherheit im Design einer Anwendung ist häufig die Ursache für Schwachstellen in der Anwendung, wie fehlende oder fehlerhafte Authentisierung und Autorisierung und ist im Nachhinein nur mit großen Aufwand zu beheben. Andere Ursachen sind im Code eingebaute Schlüssel oder Passwörter, falsche Behandlung sensitiver Daten oder eine unsichere Fehlerbehandlung, die dem Angreifer nützliche Informationen liefert. Die Einhaltung sogenannter Secure Design Principles verhilft einem Architekten zu einem robusten Design seiner Anwendung. Beispiele solcher bewährten Designprinzipien sind Least Privilege, Defense in Depth oder Secure by Default. Designprinzipien wie Privacy by Default gewinnen vor allem in Hinblick auf die EU-Datenschutzgrundverordnung vermehrt an Bedeutung. Zudem können sogenannte Design Patterns und Security

[28] https://www.volere.org/templates/volere-requirements-specification-template/

Best Practices von einem Architekten verwendet werden, die im Gegensatz zu Designprinzipien einen konkreteren, aber dennoch sprachunabhängigen Ansatz zur Lösung für wiederkehrende Problemstellungen bieten. Das Design oder zumindest die aus Sicherheitssicht relevanten Designaspekte müssen einem Design-Review unterzogen werden, bevor die Implementierung der Anwendung beginnt.

3.3.3.3 Implementierung

Typische Implementierungsfehler wie z. B. die ungeprüfte Verarbeitung von Eingaben einschließlich der Ausgabe dieser Daten oder die Vermengung von Code und Daten können zu Sicherheitsschwachstellen führen wie bspw. Injections, Cross-Site Scripting oder Buffer Overflows. Spezielle Programmierrichtlinien helfen Entwicklern, gezielt auf Sicherheit bei der Implementierung zu achten. Diese sollten individuell auf die eingesetzten Programmiersprachen, Bibliotheken und Frameworks zugeschnitten sein. Bei der Verwendung von Frameworks müssen diese korrekt verwendet werden, um ihre Sicherheitsfunktionen nicht auszuhebeln. So kann zum Beispiel festgelegt werden, dass nur bestimmte Funktionen und Objekte verwendet oder Softwaremodule erst nach erfolgreicher Prüfung mit einem Codeanalyse-Tool eingecheckt werden dürfen. Anhand von statischen Code-Prüfungen muss der Quellcode automatisiert auf typische Implementierungsfehler untersucht werden. Der Quellcode oder zumindest die aus Sicherheitssicht relevanten Teile des Quellcodes (gemäß der Ergebnisse der Bedrohungsanalyse) sollten zusätzlich einem manuellen Code-Review unterzogen werden.

Schwachstellen in der Anwendung können aber auch aus der Verwendung unsicherer Komponenten anderer Hersteller herrühren. Daher müssen solche Komponenten sorgfältig ausgewählt und die Veröffentlichungen von Sicherheits-Bulletins dieser Hersteller sowie die CVE Datenbank bekannter Sicherheitslücken kontinuierlich geprüft werden. Eine solche Überprüfung von Drittkomponenten sollte automatisch mit Hilfe eines Tools zur Abhängigkeitsprüfung stattfinden. Bei der Verwendung von Programmen zur Bereitstellung der Anwendung, wie zum Beispiel Containerlösungen, müssen diese ebenfalls auf bekannte Sicherheitslücken geprüft werden.

3.3.3.4 Softwaretests

Mit Hilfe von Blackbox-/Greybox-/Whitebox-Tests sowie statischen und dynamischen Sicherheitsscans werden Schwachstellen in der Anwendung gesucht. Sofern anwendbar ist hierbei eine Kombination aus Blackbox-/Greybox und Whitebox-Tests sowie statischen und dynamischen Sicherheitsscans zu bevorzugen, um eine möglichst hohe Effizienz zu erreichen. So lassen sich zum Beispiel verwendete Verschlüsselungsalgorithmen mittels statischer Analyse des Quellcodes leicht erkennen und auswerten, wohingegen Sicherheitslücken, die durch eine Integration verschiedener Komponenten oder erst zur Laufzeit entstehen (wie zum Beispiel in der Kommunikation mit einem Authentifizierungsservice), mittels dynamischen Scans des Systems gut erkannt werden. Im Gegensatz zu manuellen Penetrationstests können Sicherheitsscans im Rahmen des Softwareentwicklungsprozesses automatisiert durchgeführt werden, um eine Sicherheitsprüfung jeder Softwareversion zu gewährleisten. Darüber hinaus müssen in der Testphase die geforderten Sicherheitsmaßnahmen der Anwendung überprüft werden, d. h. inwiefern die Anwendung vor den in der Bedrohungsanalyse identifizierten Angriffen geschützt ist. Eine gute Quelle für die Testfallerstellung sind die definierten Abuse-Cases.

Diese Sicherheitstests liefern jedoch keine absolute Aussage über die Sicherheit der Anwendung. Sicherheit kann nicht - wie bei Funktionalitätstests - dadurch bewiesen werden, dass erwartetes Verhalten mit beobachtetem Verhalten übereinstimmt. Sicherheit ist ein negatives Kriterium, sie besteht meistens im Verhindern von unerwünschtem Verhalten. Hier ist die Kreativität eines Angreifers schier unendlich. So kann es immer noch weitere Bedrohungen und damit auch weitere Testfälle geben, die bislang noch nicht berücksichtigt wurden. Dennoch sind Sicherheitstests ein wichtiger Bestandteil im sicheren Softwareentwicklungsprozess.

3.3.3.5 Schutz von Quellcode und Resourcen

Um die Integrität von Code und Ressourcen zu bewahren und so die Anwendung vor Manipulationen wie Hintertüren, Trojanischen Pferden oder Veränderung der Ablauflogik zu schützen, sind Source Code Control Systeme einzusetzen und ggf. einzelne Code-Teile nur bestimmten Entwicklern zuzuweisen. Sensitive Informationen dürfen nicht in Source Code Control Systemen gespeichert sein, um zu verhindern, dass diese unbeabsichtigt an die Öffentlichkeit gelangen. Zudem muss eine sichere Entwicklungsumgebung gewährleistet werden, indem u. a. Zugriffsrechte beschränkt und Systeme gehärtet werden, Entwickler ausschließlich personalisierte Benutzerkonten verwenden, nicht mit Admin-Rechten arbeiten und in Bezug auf Sicherheit geschult sein müssen.

3.3.3.6 Zertifizierung der Software

Vor Auslieferung der Software ist eine vorherige Überprüfung und Zertifizierung durch eine neutrale Stelle sinnvoll. Während die Funktionalität der Software durch Tests sichergestellt wurde, stellt eine Zertifizierung sicher, dass die Architektur, das Anforderungsmanagement, das Konfigurationsmanagement und das Risikomanagement für einen sicheren Entwicklungs- und vor allem Fehlerbehebungsprozess geeignet sind.

Um später Schwachstellen beseitigen zu können, sollten Architektur und Design so gestaltet, dass nicht nur Bugs behoben, sondern fehlerhafte Komponenten im Notfall getauscht werden können.

Bei komplexerer Software ist ein Anforderungsmanagement unerlässlich. Die Anforderungen sollten vor der Auslieferung (nochmals) überprüft werden, ob sie nach IREB (International Requirements Engineering Board) klar definiert sind. Die Umsetzung von Anforderungen muss bis in den Quellcode verfolgbar sein. Im einfachsten Fall kann dies durch die Vergabe von Identifikatoren erfolgen, die dann auch in Codekommentaren verwendet werden. Hierdurch ist es möglich, auf bekannt werdende Schwachstellen schnell zu reagieren.

Eng verzahnt mit dem Anforderungsmanagement ist das Konfigurationsmanagement. Hier muss überprüft werden, ob eine Softwareversion mit Quellcode und all ihren dazugehörigen Dokumenten klar einem Versionsstand (und später einem Softwarerelease) zugeordnet werden kann. Bei Änderungen der Anforderungen muss klar sein, welche Dokumente schon auf einem neuen Stand sind und die Anforderungen berücksichtigen und welche nicht. Da Dokumente einzeln weiterentwickelt werden, haben die Dokumente in der Regel unterschiedliche Stände in der Versionierung. Daher muss neben der bloßen Versionierung der Dokumente auch eine sogenannte Baseline definiert sein, die festlegt, welche Dokumente in welcher Versionsnummer zusammengehören und damit einem Release entsprechen. Hierdurch ist es möglich zu sehen, welcher Softwarestand, welche Fehler und Schwachstellen schon behoben hat.

Ein Risikomanagement dient im ersten Schritt dazu, sich möglicher Risiken und Gefährdungen bewusst zu werden, die u.a. durch Schwachstellen eintreten könnten. Das Risikomanagement ist vor allem dann unerlässlich, wenn Menschenleben gefährdet werden können. Bei einer Softwarezertifizierung muss vor der Auslieferung überprüft werden, ob ein Risikomanagement vorliegt, das

- Risiken identifiziert,
- Risiken klassifiziert nach Eintrittswahrscheinlichkeit und Schwere,
- Maßnahmen zur Reduktion der Risiken definiert,
- die Risiken nach Durchführung der Maßnahmen erneut klassifiziert,
- in regelmäßigen Abständen und bei Änderungen weitergeführt wird.

Wenn die Software in einem Systemverbund läuft, sollte auch der Systemverbund zertifiziert werden.

3.3.3.7 Auslieferung der Software

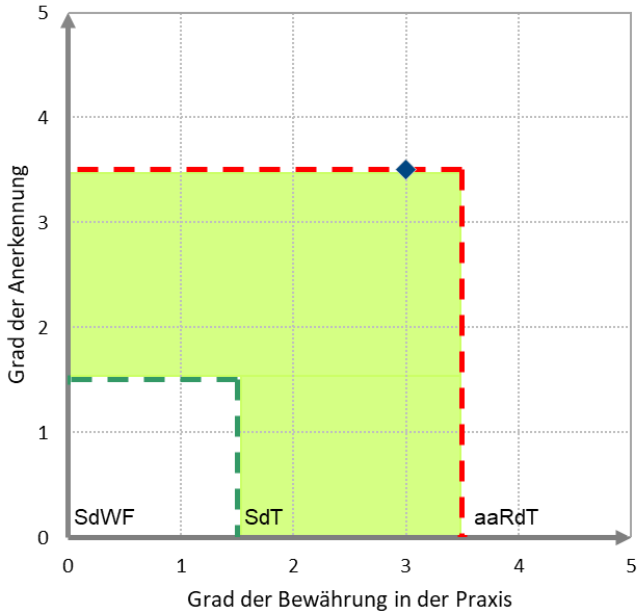
Eine Schwachstelle bei der Auslieferung und Einrichtung der Software macht das Ergebnis aller vorherigen Sicherheitsmaßnahmen im Softwareentwicklungsprozess zunichte. Daher muss ein sicherer

Auslieferungs- und Einrichtungsprozess die Integrität der ausgerollten Software sicherstellen, um zu verhindern, dass die produktive Anwendungsumgebung kompromittiert wird. Hierfür bietet sich die Verwendung von Code-Signaturen an. Angriffe auf die ausgerollte Anwendung können aber auch durch eine unsichere Konfiguration der Anwendung selbst möglich sein. Daher muss eine sichere Konfiguration der Software in der Produktiv-umgebung gewährleistet sein und dabei nicht-autorisierte Änderungen der Konfiguration verhindert werden. Als Sicherheitsmaßnahme bieten sich hier geeignete Standardeinstellungen (Secure by Default) und Handbücher für Administratoren an. Um den möglichen Schaden eines Angriffs gering zu halten, muss die Anwendung so wenig Berechtigungen wie möglich haben (Least Privilge). Vor allem in Containerumgebungen werden Anwendungen häufig unnötigerweise als root Benutzer ausgeführt, was unbedingt vermieden werden sollte. Essentiell für die Sicherheit der Anwendung ist zudem, dass diese hinsichtlich Sicherheits-Updates stets aktuell gehalten werden muss.

3.3.3.8 Security Response

Da Schwachstellen niemals völlig ausgeschlossen werden können, muss jeder Hersteller auf diesbezügliche Meldungen vorbereitet sein und schnell reagieren können. Der sogenannte Security Response Prozess eines Herstellers beschreibt seine Vorgehensweise im Umgang mit ihm bekannt gewordenen Sicherheitsproblemen. Sicherheits-Patches sind zeitkritisch und müssen daher zeitnah ausgeliefert werden. Dies beinhaltet sowohl selbst entwickelte Komponenten als auch bekannt gewordene Schwachstellen in verwendeter Standard-Software wie Bibliotheken und Frameworks. Um Sicherheitsforscher zu motivieren, die Sicherheitslücke zu melden bieten, sich Responsible Vulnerability Disclosure oder Bug-Bounty Programme an. Dabei ist es unerlässlich, dass gemeldete Schwachstellen so in den Softwareentwicklungsprozess zurück fließen, dass diese behoben werden.

Einordnung des Technologiestandes



3.3.4 Prozesszertifizierung

Um die Informationssicherheit und den Datenschutz in einem Unternehmen erfolgreich umzusetzen, müssen Prozesse identifiziert und entsprechende Maßnahmen implementiert werden. Die Umsetzung solcher Maßnahmen ist aber nur dann effektiv, wenn ihre Wirksamkeit regelmäßig überprüft wird. Diese Überprüfung kann durch interne oder externe Ressourcen erfolgen. Eine besondere Außenwir-

kung, aber nicht für alle Unternehmen verpflichtend, wird dabei durch eine Zertifizierung nach den gängigen Standards erzielt. In diesem Kapitel werden die Möglichkeiten der Prozesszertifizierung beschrieben.

Kontext Informationssicherheit

Im Kontext der Informationssicherheit kann ein ISMS gemäß ISO 27001ff oder (zumindest in Deutschland) auf der Basis von BSI IT-Grundschutz zertifiziert werden.

Dabei haben die ISMS-Zertifizierungsaudits die folgende Zielsetzung:

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

Interne Audits (sogenannte „First Party Audits“) innerhalb eines Geltungsbereichs des ISMS sollten grundsätzlich mindestens einmal pro Jahr durch die Organisation oder im Namen der Organisation durchgeführt werden. Diese Audits sind für eine ISMS-Zertifizierung verpflichtend vorgeschrieben. Jede Organisationseinheit (bzw. jeder Bestandteil des Geltungsbereichs wie Standort, Gebäude usw.) muss regelmäßig intern auditiert werden. Bei einem internen Audit ist unbedingt darauf zu achten, dass die Fachbereiche sich nicht selbst auditieren, sondern die Audits immer von einer unabhängigen Person durchgeführt werden.

Die sogenannten „Second Party Audits“ sind externe ISMS-Audits, die von Parteien durchgeführt werden, die an der Organisation interessiert sind (z. B. eigene Kunden). Werden die externen Audits durch unabhängige Auditorganisationen durchgeführt, werden sie als „Third Party Audits“ bezeichnet. Im Fall eines Outsourcing-Vertrages können entsprechende Lieferantenaudits erforderlich sein.

Der Lieferant (oder Outsourcing-Nehmer) kann die Erfüllung der Anforderungen an die Informationssicherheit jedoch auch durch ein geeignetes Zertifikat (z. B. ISO 27001 oder ISO 27001 auf der Basis von BSI IT-Grundschutz) nachweisen.

Soll ein ISMS zertifiziert werden, muss das Auditverfahren von einer akkreditierten Zertifizierungsstelle abgewickelt werden. 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. Für den IT-Grundschutz ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zuständige Zertifizierungsstelle.

Im Zertifizierungsaudit prüft das Auditteam die Erfüllung der Anforderungen aus der ISO 27001 bzw. des BSI IT-Grundschutz vom BSI. Die Audits müssen bei der ISO 27001 unter Berücksichtigung der Standards ISO 27002 und ISO 27005 realisiert sein (und ggf. weiterer branchenspezifischer Ergänzungen der Normen der 27-Reihe). Auditoren von Zertifizierungsstellen für ISO 27001 sind angehalten, im Rahmen des Auditverfahrens die Standards ISO 19011 und ISO 27007 zu berücksichtigen. Bei Audits gemäß BSI IT-Grundschutz muss das jeweils gültige Zertifizierungsschema des BSI beachtet werden.

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

Je nach Branche kann es sein, dass sog. sektorspezifische Anforderungen ebenfalls erfüllt werden müssen. Es ist zu prüfen, ob die relevanten sektorspezifischen Anforderungen den Nachweis eines

zertifizierten ISMS fordern. Darüber hinaus können weitere Anforderungen definiert werden, die entsprechend der Vorgabe umzusetzen und nachzuweisen sind. Eine Übersicht über die veröffentlichten sektorspezifischen Standards kann auf den Internetseiten des BSI abgerufen werden.

Darüber hinaus existieren andere, teilweise branchenspezifische Normen, Standards und Richtlinien, die auch einzelne Aspekte der Informationssicherheit abdecken (z. B. VdS10000, ISIS12, IDW980, HIPAA, EuroCloud Star Audit, CSA CCM, ITIL).

Weitere Vorteile, die für eine ISMS-Zertifizierung sprechen, sind:

- Nachweis über eine angemessene Risikobetrachtung und -behandlung
- Bestätigung der Funktionalität des ISMS durch unabhängige Dritte
- Nachweis über die kontinuierliche Verbesserung des ISMS
- Reduzierung der Haftbarkeit bei Vorfällen, weil die Erfüllung einer in der EU harmonierten Norm die Konformitätsvermutung mit den anerkannten Regeln der Technik (Normen) und dem Stand der Technik bewirkt.
- Außendarstellung im Rahmen eines Unternehmensmarketings/ für die Reputation gegenüber anderen

Kontext Datenschutz

Auch für die Überprüfung der Wirksamkeit von Maßnahmen im Zusammenhang mit den Anforderungen nach der Europäischen Datenschutzgrundverordnung (DSGVO) bietet sich die Implementierung eines Datenschutz-Managementsystems (DSMS) an. Zwar schreibt die DSGVO ein solches nicht ausdrücklich vor, sie lässt gleichwohl die Notwendigkeit eines solchen Systems an vielen Stellen erkennen. So verlangt beispielsweise[29] Art. 32 Abs. 1 lit. d) DSGVO ein „*Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung*".

Da ein solches Verfahren innerhalb der Organisation ein geplantes und strukturiertes Vorgehen erfordert, mithin also eine Umsetzung des klassischen PDCA-Modells bedingt, bietet sich hierfür die Einrichtung eines DSMS geradezu an. Wird dieses an den Elementen der ISO-High-Level-Structure ausgerichtet, kann es zudem in ein bereits vorhandenes ISMS auf Basis ISO 27001 integriert werden.

Genauso wie ein ISMS kann auch das DSMS auditiert und damit der Reifegrad eines solchen Systems festgestellt werden. Orientiert am Leitfaden ISO 19011 können, auf Basis eines Auditprogramms und eines Auditplans, Audits durchgeführt werden. Die Durchführung eines Audits kann grundsätzlich vom Datenschutzbeauftragten erfolgen. Bei größeren Organisationen können die Audits auch durch fachkundig geschulte Beschäftigte der Organisation oder auf Datenschutz spezialisierte Beratungsunternehmen wahrgenommen werden.

Im Rahmen der sog. Lieferantenaudits können zudem etwaige Auftragsverarbeiter der Organisation überwacht werden.

Unabhängig von vorstehenden Ausführungen besteht im Datenschutzkontext auch noch die Möglichkeit einer Zertifizierung zur Erlangung eines Nachweises über die Einhaltung der Bestimmungen der DSGVO (vgl. Art. 42 Abs. 1 DSGVO). Diesbezügliche „datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen" müssen gemäß Art. 42 Abs. 5 DSGVO aber zunächst von akkreditierten Zertifizierungsstellen nach Art. 43 DSGVO (in Deutschland etwa der DAkks) oder der zuständigen Aufsichtsbehörde freigegeben werden. Dies ist bislang nicht erfolgt.

Wie sich aus dem Wortlaut des Erwägungsgrundes 100 DSGVO entnehmen lässt, beziehen sich solche „datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen"

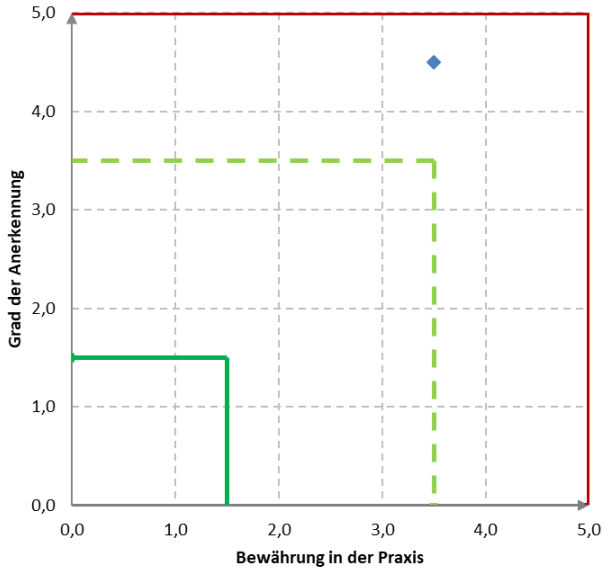
[29] Siehe ferner auch Art. 5 Abs. 2 DSGVO „*Der Verantwortliche (…) muss (…) Einhaltung nachweisen*" und Art. 24 Abs. 1 DSGVO „*(…) sicherzustellen und den Nachweis dafür erbringen (…), dass die Verarbeitung gemäß dieser Verordnung erfolgt*".

allerdings nur auf Produkt-, Prozess- und Dienstleistungszertifizierungen (vgl. ISO/IEC 17065). Die DSGVO selbst nennt in diesem Zusammenhang etwa

- den Nachweis über die Erfüllung der Pflichten eines Verantwortlichen (vgl. Art. 24 Abs. 3 DSGVO);
- den Nachweis über die Erfüllung an die Technikgestaltung und datenschutzfreundliche Voreinstellungen (vgl. Art. 25 Abs. 3 DSGVO);
- den Nachweis über hinreichende Garantien eines Auftragsverarbeiters (vgl. Art. 28 Abs. 5 und 6);
- den Nachweis betreffend die Sicherheit der Verarbeitung (vgl. Art. 32 Abs. 3 DSGVO);
- den Nachweis betreffend geeigneter Garantien im Zusammenhang mit Datenverarbeitungen in einem Drittland (vgl. Art. 46 Abs. 2 lit. f) DSGVO).

Mittels „datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen“ im Sinne der DSGVO kann zwar ein DSMS nicht zertifiziert werden. Nichtsdestotrotz sind diese zu einem DSMS komplementär und können grundsätzlich als Nachweis über die Einhaltung der Vorgaben der DSGVO bei der Auditierung eines DSMS flankierend berücksichtigt werden.

Einordnung des Technologiestandes



3.3.5 Schwachstellen- und Patchmanagement

Das Schwachstellen- und Patchmanagement haben den Zweck Sicherheits- und Funktionalitätsschwächen in Software und Firmware zu identifizieren und auszubessern. Patches[30] sollen identifizierte Schwachstellen beheben, um ihre Ausnutzung zu verhindern. Der Prozess zum Schwachstellen- und Patchmanagement umfasst die Beurteilung, Identifikation, Evaluierung sowie Bereitstellung für alle Produkte und Systeme eines Unternehmens. Für den Prozess zum Schwachstellen- und Patchmanagement sind die Verantwortlichkeiten für die Umsetzung und für die Prüfung der Wirksamkeit im Unternehmen festzulegen.

3.3.5.1 Beurteilung

Um Patches und Schwachstellen effizient zu managen, muss zuerst die IT-Landschaft des Unternehmens inventarisiert werden. Da diese sich im zeitlichen Verlauf verändern kann, muss eine solche Erhebung regelmäßig erfolgen und aktuell gehalten werden. Bestandteile, die nicht im internen Netz angesiedelt sind (z.B. Smartphones und Notebooks von Dienstleistern), müssen über spezielle Richtlinien gemanagt werden. Diese Richtlinien sollen die Besitzer dieser Bestandteile dazu auffordern, selbstständig für die Aktualisierung des Softwarestands auf ihren Geräten zu sorgen oder diese regelmäßig zur Aktualisierung mit dem Unternehmensnetzwerk zu verbinden.

3.3.5.2 Identifikation und Evaluierung

Um Schwachstellen, Softwarekorrekturen und Bedrohungen zu identifizieren, sind relevante Informationsquellen (Hersteller-Webseiten, CERTs, CVSS-Datenbanken, Mailing-Listen von Software- und Hardware-Herstellern, Newsgruppen von Drittanbietern, usw.) zu überwachen, aber auch professionelle Enterprise Patch Management Tools in Betracht zu ziehen. Alle Verantwortlichen von IT-Systemen, Anwendungen, Netzwerkkomponenten usw. müssen periodisch eine Übersicht / Zusammenfassung über den aktuellen Patch-Status bereitstellen. Daraus muss ein Report für die Bewertung der aktuellen Patch-Situation erstellt und dieser zur Beurteilung des aktuellen Risikos (z.B. CVSS Score) herangezogen werden. Als Behandlungsoptionen stehen folgende Lösungen bereit

- Übergabe an das Patchmanagement um identifizierte Schwachstelle mit einem passenden Patch (Update) zu schließen.
- Festlegen von Workarounds (Anpassung der Konfiguration, Code Analyse, etc.) um die Schwachstelle zu behandeln.
- Abschaltung oder Isolierung des betroffenen Systems.

Werden Patches zur Behebung der Schwachstelle manuell heruntergeladen, muss ihre Authentizität vor allem bei Downloads aus dem Internet mit standardisierten Methoden (kryptographische Checksummen, Signaturen oder digitale Zertifikate) geprüft werden. Paches sollten primär von Quellen der Hersteller direkt bezogen werden. Nur in Ausnahmefällen (z.B. bei integrierten Fremdprodukten, wie Run-Time-Libraries) sind Patches von anderer geprüfter vertrauenswürdiger Quelle zulässig.

3.3.5.3 Bereitstellung

3.3.5.3.1 Vorbereitung

[30] Die drei wichtigsten Bereiche sind:
- Bugfix: Unter Bugfix ist die Begebung von Fehlern zu verstehen, die sich im Programm-Quellcode ansiedeln.
- Hotfix: Mit Hotfix bezeichnet man die unaufschiebbare Behebung von Fehlern im Anwendungsprogramm.
- Update: Ein Update ist die klassische Form der Aktualisierung. Es beinhaltet Funktionserweiterungen, zum Teil auch die Behebung von Fehlern

Nachdem die Authentizität der Patches sichergestellt worden ist, sollten diese in Testsystemen überprüft werden. Die Testsysteme sollten nach Möglichkeit gleich oder vergleichbar wie das Produktionssystem ausgestattet und konfiguriert sein.

Vor der finalen Implementierung der Patches in der Produktivumgebung, sollte ein Backup der betroffenen Systeme erstellt werden, um eine Rückinstallation der Patches im Fehlerfall zu ermöglichen. Bei unerwünschter Leistung oder eingeschränkter Funktionalität sollten Maßnahmen zur Problembehebung ermittelt und umgesetzt werden.

3.3.5.3.2 Implementierung

Damit der Implementierungsprozess ordnungsgemäß verläuft, sollten entsprechende Vorbereitungen getroffen werden. Dazu gehören beispielsweise die Benachrichtigung aller Systemverantwortlichen und die Definition des Zeitraums für das Verteilen der Patches. Auch sollte die Installation bei den Anwendern angekündigt werden, damit sie ihre operativen Prozesse rechtzeitig vor dem angekündigten Installationszeitraum beenden können.

Im Normalfall sollte die Verteilung der Patches automatisch (z.B. mit einem Enterprise Patch Management Tool) erfolgen. Es kann jedoch passieren, dass die Administratoren einzelne Patches lokal installieren müssen. In diesem Fall sollte die Kommunikation sicher gehalten werden und der Austausch der Dateien mit einem Authentifizierungscheck erfolgen.

Sobald Patches ausgerollt werden, muss der Fortschritt überwacht und kommuniziert werden, um bspw. fehlgeschlagene Implementierungsversuche rechtzeitig zu erkennen. Hierfür müssen zeitnah geeignete Korrekturmaßnahmen durchgeführt werden.

3.3.5.4 Behandlung von Ausnahmen

3.3.5.4.1 Nicht-patchbare Systeme

Für Systeme oder Anwendungen, für die

- keine Updates seitens des Herstellers mehr verfügbar (sog. Legacy-Systeme) sind,
- noch keine Betriebssystem Updates vom Hersteller freigegeben sind,
- aus betrieblichen Gründen (z.B. Automatisierungen in der Prozesstechnik) kein Wartungsfenster kurzfristig zur Verfügung gestellt werden kann,
- bei einem Update eine Neuzertifizierung der Gesamtanlage notwendig wird,

müssen technische Maßnahmen identifiziert und umgesetzt werden. Da in der Regel eine Abschaltung oder einfache Neukonfiguration nicht mit den betrieblichen Erfordernissen vereinbar ist, sollten

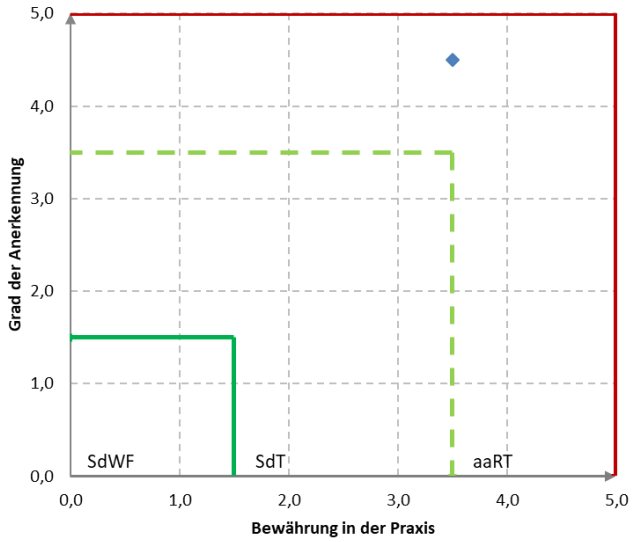
- Separierung, Zonierung, Kapselung oder Application Firewalls sowie
- Netzwerküberwachung mittels Intrusion Detection System

zum Schutz vor und zur Erkennung von Ausnutzung vorhandener Schwachstellen zum Einsatz kommen.

3.3.5.4.2 Hersteller-Freigaben

Ist für das Einspielen von Patches die Freigabe durch den Hersteller erforderlich (z.B. Freigaben für Patches von Datenbank- oder Betriebssystemen), können meist verfügbare Patches nicht eingespielt werden, da ein Funktionsverlust möglich wäre und durch den Hersteller keine Garantie übernommen würde. Aus diesem Grund sind mit dem Hersteller vertraglich Zeiträume zur Freigabe und Bereitstellung von Patches und Updates oder alternativen Workarounds für Schwachstellen festzulegen.

Einordnung des Technologiestandes



3.3.6 Management von Informationssicherheitsrisiken

Das Risikomanagement ist ein wesentliches Instrument zur Steuerung von Unternehmensrisiken und damit die Voraussetzung für die Auswahl angemessener risikoreduzierender Sicherheitsmaßnahmen. In der unternehmerischen Praxis wird der Einsatz von Sicherheitsmaßnahmen durch die Abwägung ihrer Kosten und dem Nutzen entschieden. Für die Ermittlung des Nutzens müssen Sicherheitsrisiken identifiziert und bewertet werden. Ein gutes und strukturiertes Management von Informationssicherheitsrisiken (kurz: ISRM) schafft die erforderliche Transparenz, die es der Leitungsebene ermöglicht, geeignete Entscheidungen in diesem Zusammenhang zu treffen. Darüber hinaus ist das Management von Informationssicherheitsrisiken[31] ein Kernelement bei der Umsetzung und wiederholten Aktualisierung von Informationssicherheitsmanagementsystemen (kurz: ISMS) bzw. Datenschutzmanagementsystemen (kurz: DSMS).

Standards

Der wichtigste internationale Standard zum Risikomanagement allgemein ist ISO 31000. Der speziell auf Informationssicherheitsrisiken anwendbare Standard ist ISO/IEC 27005[32]. Letzterer orientiert sich vom Prozess her sehr eng an ISO 31000, enthält aber zusätzliche (nicht-normative) Informationen zu Identifikation und Bewertung von Assets, Beispiele für Bedrohungen und Schwachstellen sowie Methoden der Risikobeurteilung im Kontext der Informationssicherheit. In Deutschland ist darüber hinaus der BSI-Grundschutz relevant, insbesondere BSI 200-3 (kurz: BSI-GS). Für industrielle Automatisierungssysteme steht ergänzend der Standard IEC 62443 Teil 3-2 zur "Sicherheitsrisikobeurteilung und Systemgestaltung" zur Verfügung.

Je nach regulativem Umfeld müssen Organisationen eventuell weitere Vorgaben erfüllen, wie beispielsweise die Europäische Datenschutz-Grundverordnung (kurz: DSGVO) oder den IT-Sicherheitskatalog der Bundesnetzagentur (kurz: IT-SiKat), die beide ergänzende Vorgaben zum Risikomanagement enthalten. Auch branchenspezifische Sicherheitsstandards, die sogenanntenB3S,

[31] Mit „IT-Risiken“ und „IT-Sicherheit“ sind in diesem Text Risiken und Sicherheit für alle Arten von Informationen gemeint, nicht allein elektronisch verarbeitete Daten.
[32] Der Standard ISO/IEC 27005 befindet sich aktuell in der Überarbeitung.

wurden für einzelne Branchen bezüglich des IT-Sicherheitsgesetzes definiert und geben Empfehlungen zur Umsetzung des Risikomanagements für KRITIS-Betreiber.

Prozess

Risikomanagement ist ein zyklischer Prozess (gemäß PDCA = Plan, Do, Check, Act). Da sich Bedingungen wie die Bedrohungslage, Systemschwachstellen oder das technologische Umfeld ändern, muss die Risikobetrachtung aktuell gehalten und ihre Wirksamkeit überwacht werden. Die Abbildung 1 zeigt den Risikoprozess nach ISO 31000.

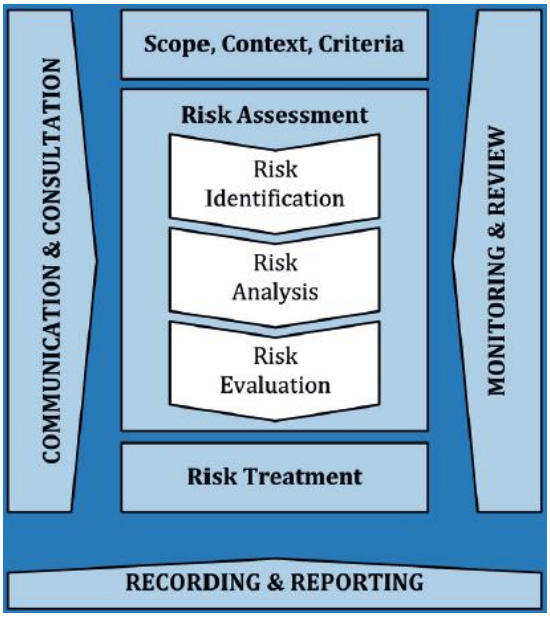


Abbildung 7: Risikoprozess nach [ISO 31000]

Im ersten Schritt (**Kontext herstellen**) werden die Grundvoraussetzungen für das ISRM geschaffen. Zunächst wird festgelegt, auf welche Teile der Organisation das ISRM überhaupt anwendbar ist; falls das ISRM im Rahmen eines ISMS eingeführt wird, ergibt sich dies i.a. aus dem Anwendungsbereich (Scope) des ISMS. Es sind die Geschäftsprozesse auszuwählen, die in das ISRM einzubeziehen sind. Von den Geschäftsprozessen ausgehend werden die zugehörigen Organisationseinheiten, IT- und OT-Systeme und -anwendungen, Einrichtungen für Daten- und Sprachkommunikation, Dienstleister und auch Liegenschaften bzw. Gebäude berücksichtigt. Es wird eine ISRM-Organisation mit entsprechender Aufgabenzuteilung geschaffen (z.B. unter Vorsitz eines Risikomanagers), sofern dies nicht ebenfalls innerhalb eines ISMS bzw. DSMS bereits geschehen ist. Es empfiehlt sich außerdem eine Definition von Schnittstellen zwischen dem ISRM und dem zentralen Unternehmens-Risikomanagement, soweit vorhanden.

Bei der **Risikoidentifikation** werden Gefährdungen ermittelt. Gefährdungen wirken gegen Werte (Assets). In einem ISRM sind die Werte in erster Linie Informationen, in zweiter Linie Systeme und Komponenten zu ihrer Verarbeitung und ihrem Schutz. Bei der Risikoidentifikation werden die Gefährdungen gegen die Assets ermittelt. Gefährdungen sind nach Definition des BSI [Glossar] das Zusammenwirken von Bedrohungen (z. B. Naturkatastrophen, Pandemien, Einbruch, Hacker, Innentäter) und Schwachstellen (z. B. Softwarefehler, organisatorische Mängel, technische Defekte). Die Herausforderung besteht darin, möglichst viele dieser Gefährdungen zu erkennen. Dabei leisten standardisierte Gefährdungskataloge wie in Anhang D von ISO/IEC 27005 oder die Gefährdungsübersicht aus dem BSI Grundschutzkompendium Unterstützung. Diese Kataloge müssen jedoch je nach dem gewählten Kontext und den vorhandenen Werten angepasst werden. Bei diesem Prozess ist die Zusammenwirkung von Informationssicherheitsverantwortlichen und Fachexperten – beispielsweise in einem Arbeitskreis – wichtig.

Risikoanalyse bedeutet, die Gefährdung hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihres Schadenspotenzials einzuschätzen. Wie bereits oben erwähnt, kann man für IT-Risiken selten auf solides Zahlenmaterial zurückgreifen. Auch hier sind die Einschätzungen von Fachexperten, möglichst aus mehreren Disziplinen – entscheidend. Schäden können unterschiedlicher Art sein (z. B. finanzielle Schäden, Gefährdung von Leib und Leben, Beeinträchtigungen der Versorgung bzw. der Erzeugung / Produktion, die Reputation betreffend etc.). Da Wahrscheinlichkeitsangaben mit hoher Unsicherheit behaftet und Schäden nicht immer klar zu beziffern sind, lassen sich IT-Risiken normalerweise nicht als eine konkrete Zahl (kardinal) ausdrücken, sondern eher innerhalb einer Ordinalskala, beispielsweise „hoch", „mittel", „niedrig". Zu dieser Art von Einstufung gibt Anhang E in ISO/IEC 27005 eine hilfreiche Anleitung. Eine derart eingestufte Gefährdung wird als „Risiko" bezeichnet.

Risiken müssen **ausgewertet** und angemessen **behandelt** werden, wofür es mehrere Optionen gibt. Man kann sie z. B. bewusst tragen (akzeptieren), sich dagegen versichern oder Gegenmaßnahmen einführen (siehe hierzu Kap. 6.4.4 in ISO 31000), jedoch sollte man sie nicht „ignorieren". Auf diese Weise wird eine bewusste Entscheidung herbeigeführt. Diese Entscheidung muss von einer Person getroffen werden, die entsprechende Verantwortung übernimmt, sei es für Kosten von Maßnahmen oder Schäden bei Eintritt eines Risikos. Diese Person wird üblicherweise als „Risikoeigentümer"[33] bezeichnet. Falls das Risiko reduziert werden soll, schlagen Fachexperten Gegenmaßnahmen vor, deren Kosten und die Reduzierung des Risikos die Entscheidungsgrundlage bilden, ob die Maßnahmen umgesetzt werden. Der „Risikoeigentümer" trifft anschließend die Entscheidung über ihre Durchführung und die Akzeptanz des Restrisikos, das nach der Umsetzung der Maßnahmen noch verbleibt. Aufgrund gesetzlicher Vorgaben bei KRITIS-Betreibern oder im Umfeld der DSGVO ist der „Risikoeigentümer" nicht gänzlich frei darin, Risiken ohne weitere Behandlung zu akzeptieren oder zu transferieren.

Kommunikation, **Berichtswesen** (vor allem in Richtung Management) und **Überwachung** sind unterstützende Prozesse. Innerhalb eines ISMS bzw. DSMS sind sie ohnehin etabliert und müssen auf das ISRM entsprechend angewendet werden. Bei Vorhandensein eines zentralen Unternehmens-Risikomanagements kommt es auf eine effiziente Kommunikation und gegenseitige Ergänzung zwischen diesem und dem ISRM an, und dass Kriterien zur Eskalation von Informationssicherheitsrisiken an das zentrale Unternehmens-Risikomanagement festgelegt werden, die für beide Seiten verständlich und akzeptabel sind.

Praktische Tipps

Die komplette Neueinführung eines ISRM ist für Unternehmen häufig eine umfassende Aufgabe (zeitlich und kostenseitig). Wie andere Prozesse unterliegt auch das ISRM einem kontinuierlichen Verbesserungsprozess, was gleichzeitig bedeutet, dass man nicht erwarten kann, im ersten Anlauf einen perfekten Prozess zu etablieren. Vielmehr kann sich ein zu schwergewichtiges Vorgehen für die Zukunft als Belastung erweisen: Es besteht dann die Gefahr, dass der Prozess auf Dauer „einschläft" oder nur als formal notwendiges Relikt ohne erkennbaren Nutzen umgesetzt wird. Insofern empfiehlt es sich, zu Beginn einen pragmatischen Ansatz zu wählen, bei dem weniger auf Vollständigkeit als auf Qualität geachtet wird. Wichtig ist dabei, dass die Risiken hoher Priorität ermittelt, analysiert und angemessen behandelt werden, und dass bei den entscheidenden Parteien darüber größtmöglicher Konsens besteht.

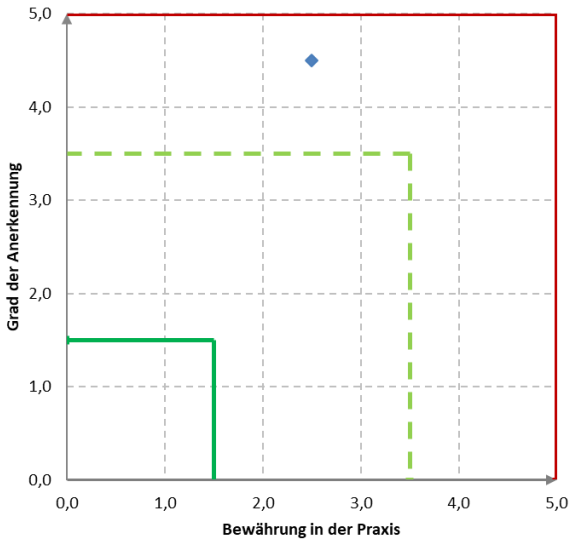
Anspruchsvoll sind zu Beginn besonders die Ermittlung von Bedrohungen und ihre geeignete Kategorisierung. Man kann sich dabei an Standardbedrohungskataloge wie in ISO/IEC 27005 halten. Trotzdem gibt es zum Beispiel auf die Frage, ob man die Bedrohung „Blitzschlag" unter „höhere Gewalt" einordnen und als ein großes Gesamtrisiko behandeln soll, selten eine eindeutige Antwort, ebenso ob man Risiken voneinander unabhängig behandeln kann, also ob beispielsweise „Blitzschlag" nicht zusammen mit dem Risiko „Stromausfall" behandelt werden muss. Die Zusammenhänge können beliebig komplex werden, so dass man gewisse Ungenauigkeiten in Kauf nehmen muss. Ungenauigkeiten

[33] Der Begriff „risk owner" aus der ISO 27001 wird je nach den Verantwortlichkeiten der betreffenden Person auch mit „Risikoverantwortlicher" oder „Risikoträger" übersetzt.

kommen ohnehin über Schätzungen von Eintrittswahrscheinlichkeiten ins Spiel. Wichtig ist hierbei, das Ziel nicht aus den Augen zu verlieren, nämlich dass man aufgrund der Ergebnisse der Risikoanalyse nachvollziehbar entscheiden kann, ob Handlungsbedarf besteht oder nicht.

Kaum weniger schwierig ist die Einschätzung von Eintrittswahrscheinlichkeiten. Es empfiehlt sich, möglichst viele externe und interne Informationsquellen zu nutzen. Zu ersteren gehören unter anderem CVE[34]-Listen, Herstellerinformationen, CERT-Dienste (z.B. des BSI), zu letzteren die Auswertung von Informationssicherheitsvorfällen, Penetrationstests, Audits oder Awareness-Maßnahmen. Die Werte sollten regelmäßig, z.B. mindestens einmal im Jahr, der aktuellen Situation angepasst werden.

Einordnung des Technologiestandes



[34] Bei den Common Vulnerabilities and Exposures (CVE) handelt es sich um eine standardisierte Liste über Schwachstellen und Sicherheitsrisiken von Computersystemen.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
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.