Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Handreichung
Stand der Technik in der IT-Sicherheit

Technische und organisatorische Maßnahmen

2025

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

Tomasz Lawicki - Capgemini
RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte

Autoren und mitwirkende Experten

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - genua
Bausewein, Christoph - CrowdStrike
Benzmüller, Ralf - G DATA
Bernhardt, Ulf - valantic
Dehning, Oliver - eco
Dominkovic, Dennis - SEC Consult
Dubbel, Sascha
Falkenthal, Oliver - CCVOSSEL
Fischer, Marco - procilon
Föllmer, Nancy - heinzl
Glemser, Tobias - secuvera
Gremeyer, Erik - ATM Consulting
Heyde, Steffen - secunet
Jäger, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX
Kissling, Kristian - DCSO
Kohn, Ulrich - Adva Network Security
Kolmhofer, Robert - FH Oberösterreich
Kowol, Dominik - eperi
Krosta-Hartl, Pamela - LANCOM
Kynast, Michael - DCSO
Lang, Thomas - valantic
Lawicki, Tomasz - Capgemini
Leitner, Alexander - UNINET
Liedke-Deutscher, Bernd - TÜV Informationstechnik
Maier, Janosch - Crashtest Security
Martin, Karl-Ulrich - Detack
Menge, Stefan - Achtwerk
Mielke, Tobias - TÜV Informationstechnik
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried
Pfister, Benjamin - VAF
Rechberg, Johanna - UNINET
Rost, Peter - secunet
Schlensog, Alexander - secunet
Weigmann, Matthias - ANMATHO
Wilke, Klaus - CCVOSSEL
Zingsheim, André - TÜV TRUST IT

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Desweiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1_2025-06 DE

ISBN 978-3-9825553-0-0

Inhaltsverzeichnis

Grundsätze der Handreichung 5

1 Einleitung 6
1.1 Gesetzliche und regulatorische Grundlagen 6
1.2 Branchenspezifische Sicherheitsstandards (B3S) 12
1.3 Angemessenheit der Maßnahmen 12

2 Bestimmung des Technologiestandes 13
2.1 Begriffsklärung 13
2.2 Methode zur Einordnung des Technologiestandes 15
2.3 Prozess zur Qualitätssicherung der Handreichung 17
2.4 Geforderte Schutzziele 18

3 Technische und organisatorische Maßnahmen (TOM) 19
3.1 Allgemeine Hinweise 19
3.2 Technische Maßnahmen 22
3.2.1 Authentisierung 22
3.2.2 Bewertung und Durchsetzung starker Passwörter 23
3.2.3 Multifaktor-Authentifizierung 25
3.2.4 Kryptographische Verfahren 27
3.2.5 Verschlüsselung von Datenträgern 30
3.2.6 Verschlüsselung von Dateien und Ordnern 31
3.2.7 Verschlüsselung von E-Mails 32
3.2.8 Schutz des elektronischen Datenverkehrs mit PKI 34
3.2.9 Einsatz von verschlüsselten VPN-Lösungen (Layer 3) 36
3.2.10 Verschlüsselung auf Layer 2 39
3.2.11 Schutz in der Cloud gespeicherter Dateien 40
3.2.12 Datenverarbeitung in der Cloud 41
3.2.13 Schutz mobiler Sprach- und Datendienste 43
3.2.14 Schutz der Kommunikation mittels Instant Messenger 44
3.2.15 Schutz mobiler Geräte 46
3.2.16 Routersicherheit 47
3.2.17 Netzwerküberwachung mit IDS 49
3.2.18 Schutz des Web-Datenverkehrs 51
3.2.19 Schutz von Web-Anwendungen 52
3.2.20 Schutz des Fernzugriffs auf Netzwerke 54
3.2.21 Systemhärtung 55
3.2.22 Endpoint Detection & Response Platform 58
3.2.23 Web-Isolation der Internetnutzung 60
3.2.24 Angriffserkennung und Auswertung (SIEM) 61
3.2.25 Vertrauliche Datenverarbeitung in der Cloud 63
3.2.26 Sandboxing zur Schadcode-Analyse 64
3.2.27 Cyber Threat Intelligence 66
3.2.28 Absicherung administrativer IT-Systeme 68
3.2.29 Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung 69
3.2.30 Netzwerksegmentierung und Separierung 71
3.2.31 Cloud-Sicherheitsplattform 74
3.2.32 Tokenisierung 75
3.2.33 VOIP-Verschlüsselung mit SIPS/SRTP 77
3.2.34 Verschlüsselung (Layer 1) 79
3.3 Organisatorische Maßnahmen 81
3.3.1 Standards und Normen 81
3.3.2 Sicherheitsorganisation 84
3.3.3 Informationssicherheitsmanagementsystem (ISMS) 86
3.3.4 Sichere Softwareentwicklung 88
3.3.5 Prozesszertifizierung 92
3.3.6 Schwachstellen- und Patchmanagement 95
3.3.7 Risikomanagement 97
3.3.8 Personenzertifizierung 100
3.3.9 Absicherung privilegierter Benutzerkonten 103

3.3.10 Dark Web Monitoring ... 106
3.3.11 Umgang mit Dienstleistern ... 108
3.3.12 Software Bill of Materials (SBOM) ... 109
3.3.13 Geo-Redundanzen ... 111
3.3.14 Sensibilisierung der Anwender ... 112
3.3.15 Asset Management ... 115
3.3.16 Incident Management ... 116
3.3.17 Geschäftskontinuitäts-Management (BCM) ... 118
3.3.18 Notfall- und Krisenmanagement ... 119
3.3.19 Notfallübungen ... 122
3.3.20 Technische Sicherheitsüberprüfung ... 123

4 Exkurse ... 127
4.1 Maßnahmen gegen Ransomware-Angriffe ... 127
4.2 Einordnung der Maßnahmen in ISO/IEC 27001:2022 ... 129
4.3 Einordnung der Maßnahmen in das NIST-Rahmenwerk ... 132
4.4 Auswirkung von KI auf Informationssicherheit ... 134
4.5 Absicherung der Lieferkette ... 138

Abbildungsverzeichnis

Abbildung 1: Drei-Stufen-Theorie nach Kalkar-Entscheidung ... 13
Abbildung 2: Beispiel der Einordnung des Technologiestandes ... 16
Abbildung 3: Prozessskizze für die Bewertung der Maßnahmen im Arbeitskreis ... 17
Abbildung 4: Aufbau und das Zusammenwirken von PKI-Komponenten ... 35
Abbildung 5: Gliederungsebenen informationssicherheitsrelevanter Standards und Normen ... 83
Abbildung 6: Risikoprozess nach ISO/IEC 31000 ... 98
Abbildung 7: Ransomware-kill-chain und Schutzmaßnahmen (Beispiel) ... 127

Tabellenverzeichnis

Tabelle 1: Übersicht der ISO/IEC 27000-Reihe ... 82
Tabelle 2: Abgrenzung ISO/IEC 27001 vs. BSI-Grundschutz ... 83
Tabelle 3: Rollen und Zuständigkeiten innerhalb einer Sicherheitsorganisation ... 85
Tabelle 4: Abgrenzung BCM vs. Notfall- und Krisenmanagement ... 120
Tabelle 5: Zusammensetzung des Krisenstabs ... 120
Tabelle 6: Beispielhafte Fragestellungen bei Konfigurationsanalysen ... 124
Tabelle 7: Beispielhafte Fragestellungen bei Härtungsüberprüfungen ... 125
Tabelle 8: Maßnahmen gegen Ransomware-Angriffe ... 129
Tabelle 9: Einordnung der Maßnahmen in ISO/IEC 27001:2022 ... 131
Tabelle 10: Einordnung der Maßnahmen in das NIST-Rahmenwerk ... 133
Tabelle 11: Sicherheitsrisiken von KI-Modellen und Schutzmaßnahmen ... 137

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 der gültigen Gesetzgebung 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 gesetzlich geforderten IT-Sicherheitsmaßnahmen. Sie ersetzt eine technische, organisatorische oder rechtliche Beratung oder Bewertung im Einzelfall nicht. Gleichwohl kann sie bei der Identifikation von IT-Sicherheitsmaßnahmen zur Stärkung der Systemimmunität gegen laufende Bedrohungen dienen.

2. **Verantwortung für die Entwicklung, Evaluierung und Fortschreibung**
   Der TeleTrusT Arbeitskreis "Stand der Technik" 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 Einordnung des Technologiestandes der hier beschriebenen Sicherheitsmaßnahmen ist im Abschnitt 2 dieses Dokumentes erläutert.

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

6. **Haftungsausschluss und rechtlicher Hinweis**
   Diese Handreichung stellt keine rechtsverbindliche Auslegung oder technische Norm dar. Sie kann jedoch als anerkannter Branchenkonsens in Fachkreisen, im Rahmen von Audits oder bei der Auslegung unbestimmter Rechtsbegriffe herangezogen werden. Sie ersetzt keine individuelle rechtliche, technische oder organisatorische Beratung. Ihre Inhalte beruhen auf dem aktuellen Stand von Technik, Wissenschaft und Praxis zum Zeitpunkt der Veröffentlichung. Änderungen gesetzlicher Grundlagen oder technischer Entwicklungen können eine Aktualisierung erforderlich machen. Die Anwendung der in dieser Handreichung enthaltenen Empfehlungen erfolgt auf eigene Verantwortung.

1 Einleitung

1.1 Gesetzliche und regulatorische Grundlagen

Die Frage, was unter dem "Stand der Technik" im Bereich der IT-Sicherheit konkret zu verstehen ist, zählt zu den anspruchsvollsten Herausforderungen bei der rechtskonformen Gestaltung und Umsetzung technischer und organisatorischer Maßnahmen zum Schutz von Netzwerk- und Informationssystemen oder verarbeiteter Daten oder der Dienste, die über diese Netzwerk- und Informationssysteme angeboten werden bzw. zugänglich sind.

Lange blieb die IT-Sicherheit in der Gesetzgebung unberücksichtigt. Im Laufe der vergangenen Dekade begannen der nationale sowie der europäische Gesetzgeber jedoch, der zunehmenden Digitalisierung aller Lebens- und Wirtschaftsbereiche auch auf regulatorischer Ebene zu begegnen. Die Gesetzgebung im IT-Sicherheitsrecht ist seitdem von einer besonderen Dynamik geprägt, die kaum ein anderes Rechtsgebiet aufweisen kann. Das Zusammenspiel von nationaler (Umsetzungs-)Gesetzgebung und europäischer Vorgaben, das mitunter parallele Vorliegen sektorspezifischer sowie sektorübergreifender Vorschriften und der dauerhafte Regulierungsdruck aufgrund technischer Entwicklungen und sich fortwährend verändernden Bedrohungslagen machen das IT-Sicherheitsrecht zu einer komplizierten Herausforderung für Unternehmen, Behörden und Rechtsanwender gleichermaßen.

Um der Dynamik zu begegnen, ist der Gebrauch des "Stands der Technik" als Verweisungsbegriff und Technologieniveau in einem Großteil der Rechtsakte vorgesehen. Auch zur Konkretisierung unbestimmter Rechtsbegriffe wie bei der "Erforderlichkeit" oder "Angemessenheit" von Maßnahmen kann der Stand der Technik Bedeutung erlangen. Nachfolgend sollen die wichtigsten Gesetze und Vorschriften des IT-Sicherheitsrechts, die einen Bezug zum Stand der Technik aufweisen, kurz vorgestellt werden.

1.1.1 Die IT-Sicherheitsgesetze und europäische Harmonisierung

Als "Herzstück" des IT-Sicherheitsrechts können die europäischen NIS-Richtlinien sowie die nationalen IT-Sicherheitsgesetze ausgemacht werden, die insbesondere weitreichende Änderungen des BSIG herbeiführten. Ziel dieser Regelwerke ist es, sektorübergreifend ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme zu gewährleisten, das nationale wie auch grenzüberschreitende Risiken angemessen adressiert. Die europäische Überformung verfolgt das Ziel, einen einheitlichen Rahmen mit Mindestanforderungen an die IT-Sicherheit von Netz- und Informationssystemen innerhalb der gesamten Europäischen Union zu kreieren.

1.1.1.1 2015 ITSiG

Das IT-Sicherheitsgesetz (ITSiG) trat am 25.07.2015 in Kraft und kann als "Startschuss" zu einer Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland angesehen werden.

Bei dem IT-Sicherheitsgesetz handelte es sich um ein sogenanntes Artikelgesetz, mit dem eine Anpassung verschiedener bereichsspezifischer Gesetze erfolgte. Durch das ITSiG wurden insbesondere Regelungen für kritische Infrastrukturen (KRITIS) im Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG) geschaffen. Darüber hinaus erfolgten IT-sicherheitsspezifische Gesetzesänderungen im Atomgesetz (AtomG), Energiewirtschaftsgesetz (EnWG), Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG).

Die umfassendsten Änderungen sah das ITSiG für das BSIG vor. KRITIS-Betreiber wurden hiermit erstmals gesondert adressiert und ihnen IT-Sicherheitspflichten auferlegt. Dies betraf Unternehmen, die im Zusammenhang mit der Versorgung der Gesellschaft mit Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung und dem Finanzwesen standen. Dabei verfolgte das BSIG einen risikobasierten Ansatz: nur solche Unternehmen wurden adressiert, die derart bedeutsam waren, dass ihr Ausfall eine erhebliche Gefahr für die Versorgungs- und öffentliche Sicherheit darstellte. Dies wurde anhand von Schwellenwerten in den einzelnen Sektoren durch eine Rechtsverordnung (KRITIS-Verordnung) festgelegt.

Diese KRITIS-Betreiber wurden nach § 8a Abs. 1 BSIG a. F. dazu verpflichtet, angemessene technische und organisatorische Vorkehrungen zum Schutz der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme zu treffen. Hierbei kam dem "Stand der Technik" als einzuhaltender Mindestmaßstab bereits eine elementare Bedeutung zu. Weitere Vorschriften enthielten unter anderem eine

Nachweispflicht dieser Anforderungen (§ 8a Abs. 3 BSIG a.F.) und eine Meldepflicht bei bestimmten IT-Sicherheitsvorfällen (§ 8b Abs. 4 BSIG a.F.)
Die TeleTrusT-Kommentierung zum IT-Sicherheitsgesetz sowie dessen Gesetzesbegründung sind unter folgendem Link abrufbar: www.teletrust.de/it-sicherheitsgesetz.

1.1.1.2 NIS-Richtlinie

Die Europäische Kommission hat im Jahr 2016 die "Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen" (NIS-Richtlinie) verabschiedet, die in nationales Recht umzusetzen war. Grundlegende Änderungen daraus ergaben sich jedoch nicht, da der nationale Gesetzgeber durch Verabschiedung des ITSiG im Jahr 2015 bereits einen Großteil, der vom europäischen Gesetzgeber beabsichtigten Anforderungen vorweggenommen hat. Das entsprechende, am 27.04.2017 verabschiedete NIS-Richtlinien-Umsetzungsgesetz führte demnach lediglich zu einer Ergänzung des BSIG.

Auf Grundlage der Richtlinie wurde unter anderem der § 8c BSIG a.F. geschaffen, der zusätzliche Verpflichtungen für Anbieter digitaler Dienste schuf. 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 und dabei den Stand der Technik zu berücksichtigen. Die Maßnahmen sollen ein dem Risiko angemessenes Schutzniveau gewährleisten und dabei unter anderem die Sicherheit der Systeme und Anlagen, den Umgang mit Sicherheitsvorfällen sowie das Betriebskontinuitätsmanagement sicherstellen. Ferner wurden mit dem NIS-Umsetzungsgesetz die Befugnisse des Bundesamts für Sicherheit in der Informationstechnik im BSIG erweitert. Auch die entsprechenden Vorschriften im AtomG, EnWG, SGB V und TKG wurden durch das NIS-Umsetzungsgesetz als Artikelgesetz geändert.

1.1.1.3 2021 ITSiG 2.0

Das IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) trat im Mai 2021 in Kraft und erweiterte die bestehenden Regelungen zur Informationssicherheit in Deutschland erheblich.

Neben den bisher definierten Sektoren wie Energie, Wasser, Ernährung, Gesundheit, Informationstechnik und Telekommunikation, Transport und Verkehr sowie Finanz- und Versicherungswesen wurden durch das ITSiG 2.0 zwei weitere Bereiche adressiert:

- Zum einen wurde die **Siedlungsabfallentsorgung** als neuer Sektor der kritischen Infrastrukturen hinzugefügt. Dieser Sektor umfasst die Sammlung, Beförderung, Verwertung und Beseitigung von Siedlungsabfällen.
- Zum anderen wurden **Unternehmen im besonderen öffentlichen Interesse (UBI)** als neue Adressatengruppe neben den KRITIS-Betreibern und Anbietern digitaler Dienste hinzugefügt. Hierzu zählen Unternehmen, die aufgrund ihrer Bedeutung für das Gemeinwesen als besonders schützenswert gelten. Die UBIs haben ein eigenes Pflichtenprogramm nach § 8f BSIG.

Diese Erweiterung führte dazu, dass nun deutlich mehr Organisationen verpflichtet wurden, wirksame Maßnahmen zur Erhöhung ihrer IT-Sicherheit zu implementieren.

Das IT-SiG 2.0 brachte für KRITIS-Betreiber und Unternehmen im besonderen öffentlichen Interesse (UBI) erweiterte Verpflichtungen mit sich, wie beispielsweise:

- **Systeme zur Angriffserkennung:** Betreiber sind verpflichtet, technische Werkzeuge und unterstützende Prozesse zur kontinuierlichen Erkennung von Bedrohungen im laufenden Betrieb einzusetzen, § 8a Abs. 1a BSIG. Diese Systeme müssen spätestens ab dem 1. Mai 2023 implementiert und in Prüfungen nachgewiesen werden.

- **Unmittelbare Registrierung:** Betreiber müssen sich nach Feststellung ihrer KRITIS-Eigenschaft unverzüglich beim BSI registrieren und eine Kontaktstelle benennen, § 8b Abs. 3 BSIG. Das BSI hat zudem die Befugnis, Betreiber eigenständig als Kritische Infrastruktur zu identifizieren und entsprechende Unterlagen einzusehen.

Darüber hinaus wurden mit dem ITSiG 2.0 erstmals "kritische Komponenten" reguliert. Der Einsatz von besonderen IT-Komponenten in KRITIS-Anlagen ist nach § 9b Abs. 1 BSIG dem Bundesinnenministerium anzuzeigen, welches den Einsatz daraufhin untersagen kann. Zudem sieht das ITSiG 2.0 höhere Bußgelder bei Verstößen vor und stärkt die Befugnisse des BSI. So kann das BSI bei Verstößen vertieften Einblick in die IT-Systeme der Betreiber verlangen und gegebenenfalls Maßnahmen anordnen.

Der Stand der Technik hat auch bei den Pflichten für UBIs Eingang gefunden. Die nach § 8f Abs. 1 BSIG vorzulegende Selbsterklärung des UBI muss u.a. enthalten, wie sichergestellt wird, dass die IT-Systeme des Unternehmens angemessen geschützt werden und ob dabei der Stand der Technik eingehalten wird. Eine direkte Pflicht zum Einhalten des Stands der Technik besteht für UBIs, anders als für KRITIS-Betreiber, jedoch nicht.

1.1.1.4 NIS-2-Richtlinie

Die NIS-2-Richtlinie ("Richtlinie über Maßnahmen für ein hohes gemeinsames Cyber-Sicherheitsniveau in der Union") vom 14. Dezember 2022 ist eine EU-Richtlinie, die darauf abzielt, ein hohes gemeinsames Niveau der Cyber-Sicherheit innerhalb der Europäischen Union sicherzustellen und die damit die NIS-Richtlinie aus 2016 ablöst. Das Fristende für die mitgliedstaatliche Umsetzung war der 17. Oktober 2024. Der deutsche Gesetzgeber hat die Umsetzungsfrist nicht eingehalten. Zum Zeitpunkt der Erstellung der Handreichung lag noch kein Umsetzungsgesetz vor.

Die NIS-2-Richtlinie erweitert den Anwendungsbereich, überarbeitet die Regelungssystematik der ursprünglichen NIS-Richtlinie und führt strengere Sicherheitsanforderungen sowie Meldepflichten für ein breites Spektrum von Sektoren und Unternehmen ein.

Infolge der Neustrukturierung des Anwendungsbereichs, der Herabsenkung von Schwellenwerten und der Aufnahme neuer Sektoren unterliegen der NIS-2-Richtlinie deutlich mehr Unternehmen als der NIS-Richtlinie. Jedes Unternehmen, das kritische Dienstleistungen erbringt oder eine wesentliche gesellschaftliche Bedeutung hat, unterliegt den neuen, strengeren Anforderungen der NIS-2-Richtlinie.

Um eine einheitliche Definition zu gewährleisten und Unterschiede in der Auslegung durch die Mitgliedstaaten zu vermeiden, legt die NIS-2-Richtlinie klare Kriterien für die Einstufung von Organisationen fest. Sie unterteilt betroffene Unternehmen in **wesentliche Einrichtungen** und **wichtige Einrichtungen**.

Unter die wesentlichen Einrichtungen fallen nach Art. 3 Abs. 1 NIS-2-Richtlinie u.a. mittlere bis große Unternehmen, die einem in Anhang 1 zur NIS-2-Richtlinie aufgeführten Sektor zugeordnet werden können (neu hinzugefügte Sektoren sind beispielsweise Abwasser, Verwaltung von IKT-Diensten und Weltraum). Unabhängig von der Unternehmensgröße werden u.a. qualifizierte Vertrauensdienstanbieter und DNS-Diensteanbieter erfasst. Auch Einrichtungen der öffentlichen Verwaltung werden als wesentliche Einrichtungen reguliert. Ferner umfasst der Anwendungsbereich der NIS-2-Richtlinie auch Betreiber besonders kritischer Dienstleistungen, sofern sie durch die Mitgliedstaaten als wesentliche Einrichtung eingeordnet werden (vgl. Art. 2 Abs. 2 lit. b-e NIS-2-Richtlinie).

Als wichtige Einrichtung umfasst die NIS-2-Richtlinie nach Art. 3 Abs. 2 sonstige Unternehmen, die in einem der in Anhang 1 oder Anhang 2 der NIS-2-Richtlinie aufgeführten Sektoren tätig sind. Anhang 2 enthält u.a. die Sektoren Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren und Forschung. Auch hier besteht die Möglichkeit der Qualifizierung als wichtige Einrichtung durch den Mitgliedstaat.

Wie bei der NIS-Richtlinie findet sich die Pflicht zum Ergreifen von technischen und organisatorischen Maßnahmen auch in der NIS-2-Richtlinie. Diese müssen geeignet und verhältnismäßig sein und neben einschlägigen europäischen und internationalen Normen und den Kosten der Umsetzung auch den Stand der Technik berücksichtigen, um ein risikoadäquates Sicherheitsniveau zu gewährleisten, Art. 21 Abs. 1 NIS-2-Richtlinie.

Mindestanforderungen an die Risikomanagementmaßnahmen werden in der NIS-2-Richtlinie erstmals ausführlich konkretisiert, Art. 21 Abs. 2 NIS-2-Richtlinie. Hierbei wird ein verstärkter Fokus auch auf die Sicherheit in der Lieferkette gelegt, um potenzielle Schwachstellen bei Drittanbietern zu minimieren.

Darüber hinaus müssen Sicherheitsvorfälle mit erheblichen Auswirkungen unverzüglich an die zuständigen Behörden gemeldet werden, Art. 23 NIS-2-Richtlinie.

Für einen konkreten Pflichtenkatalog ist auf das Umsetzungsgesetz abzustellen.

1.1.1.5 NIS2UmsuCG

Das erforderliche Gesetz zur Umsetzung der NIS-2-Richtlinie besteht gegenwärtig nicht. Im Juli 2024 veröffentlichte das Bundesinnenministerium einen Gesetzentwurf für das "NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG).

Im Kern sah das NIS2UmsuCG eine vollständige Erneuerung des BSIG vor, der eine neue Regelungsstruktur sowie eine beachtliche Ausdehnung des Umfangs erfahren sollte.

Die Termini der NIS-2-Richtlinie übernahm der Entwurf des neuen BSIG (BSIG-E) nicht, der stattdessen zwischen **besonders wichtigen Einrichtungen** und **wichtigen Einrichtungen** unterschied. Darüber hinaus wurden auch **Einrichtungen der Bundesverwaltung** durch den BSIG-E adressiert. Insgesamt wird die Zahl der von dem Umsetzungsentwurf betroffenen Unternehmen in Deutschland auf über 30.000 geschätzt.

Neben einer bedeutsamen Ausweitung des Anwendungsbereichs sah der BSIG-E auch ein umfangreiches Pflichtenprogramm für die adressierten Unternehmen vor: In Umsetzung der NIS-2-Richtlinie sind Unternehmen zu den o. g. Risikomanagementmaßnahmen verpflichtet und sollen hierbei den Stand der Technik einhalten. Betreiber kritischer Anlagen als Untergruppe der besonders wichtigen Einrichtungen haben nach dem BSIG-E sogar gesteigerte Anforderungen an die Risikomanagementmaßnahmen zu erfüllen. Weiterhin sieht der BSIG-E ein ausführliches Meldesystem vor, Registrierungspflichten, Unterrichtungspflichten, Nachweispflichten sowie Umsetzungs-, Überwachungs- und Schulungspflichten für Geschäftsleitungen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) übernimmt eine zentrale Rolle als Aufsichtsbehörde und wird für eine Vielzahl neuer Unternehmen zuständig sein. Der BSIG-E stärkt die Befugnisse des BSI insbesondere im Hinblick auf Registrierungs- und Meldepflichten sowie die Durchsetzung von Sicherheitsstandards.

Zusätzlich zum NIS2UmsuCG ist die Einführung eines KRITIS-Dachgesetzes geplant, das die Resilienz und das Business Continuity Management (BCM) für Betreiber kritischer Anlagen regeln soll. Dieses Gesetz zielt darauf ab, die physische Sicherheit und die Widerstandsfähigkeit kritischer Infrastrukturen zu erhöhen.

Weder das NIS2UmsuCG noch das KRITIS-Dachgesetz wurden letztendlich durch die Ampel-Regierung umgesetzt. Es bleibt zum Zeitpunkt der Veröffentlichung dieser Handreichung abzuwarten, ob und welche Veränderungen kommende Umsetzungsgesetze an den vergangenen Entwürfen vornehmen werden.

1.1.2 Sonstige europäische Rechtsquellen

1.1.2.1 DSGVO

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 Bürgerinnen und Bürger. Dabei liegt der Verordnung hinsichtlich ihrer Schutzziele ein risikobasierter Ansatz zugrunde.

Dem Stand der Technik kommt dabei an mehreren Stellen der DSGVO eine besondere Bedeutung zu.

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

Im Bereich des technischen Datenschutzes sind zum Schutze der Rechte und Freiheiten natürlicher Personen nach Art. 32 Abs. 1 DSGVO risikoangemessene und geeignete technische und organisatorische Maßnahmen zu treffen.

Sowohl im Rahmen von Art. 25 Abs. 1 DSGVO als auch bei Art. 32 Abs. 1 DSGVO müssen die zu ergreifenden technischen und organisatorischen Maßnahmen verschiedene Aspekte berücksichtigen:

- Eintrittswahrscheinlichkeit und Schwere des Risikos einer Rechtsverletzung des Betroffenen
- Art, Umfang, Umstände und Zweck der Verarbeitung
- Implementierungskosten
- Stand der Technik

Wie auch die IT-Sicherheitsgesetze, sieht die DSGVO keine Definition vor, was unter "Stand der Technik" zu verstehen ist. Gleiches gilt ebenfalls für das Datenschutz-Anpassungs- und -Umsetzungsgesetz

EU (DSAnpUG-EU) sowie die daraus resultierende Neufassung des Bundesdatenschutzgesetzes (BDSG).

Der Stand der Technik ist im Rahmen der Umsetzung der Vorgaben jedoch nicht nur zu berücksichtigen, sondern auch umfassend zu dokumentieren. Hierzu wurden weitreichende Dokumentationspflichten, insbesondere durch die Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung sowie einer Rechenschaftspflicht, geschaffen. Die Verordnung statuiert diesbezüglich Dokumentationspflichten als eigene rechtliche Pflichten. Technische und organisatorische Maßnahmen sind somit sowohl individuell festzustellen als auch detailliert zu beschreiben bzw. zu dokumentieren.

1.1.2.2 DORA

Der Digital Operational Resilience Act (DORA) vom 14. Dezember 2022 ist eine Verordnung der Europäischen Union, die darauf abzielt, die digitale operationelle Resilienz im Finanzsektor zu stärken. Sie betrifft neben den in Art. 2 Abs. 1 DORA aufgeführten "Finanzunternehmen" (Kreditinstitute, Zahlungsinstitute, Handelsplätze, Versicherungsunternehmen etc.) auch IKT-Drittdienstleister für diese Finanzunternehmen. Die vom DORA betroffenen Unternehmen mussten die Anforderungen bis zum 17. Januar 2025 vollständig umsetzen.

Der DORA sieht einen umfangreichen Pflichtenkatalog vor. Neben ausführlichen Pflichten zur Vornahme eines IKT-Risikomanagementrahmens mitsamt Strategien, Verfahren, Protokollen und Tools zur Sicherung des Schutzes von IKT-Assets (Art. 5 ff. DORA) bestehen auch besondere Management-, Überwachungs-, Melde- und Protokollierungspflichten zur Behandlung von IKT-bezogenen Vorfällen (Art. 17 ff. DORA), Resilienztestpflichten (Art. 24 ff. DORA) und Pflichten zum Management des IKT-Drittparteienrisikos mitsamt Führung eines Informationsregisters (Art. 28 ff. DORA).

Der Stand der Technik wird als Rechtsbegriff nicht explizit in dem DORA genannt. Er findet jedoch Eingang durch unbestimmte Rechtsbegriffe: Beispielsweise durch die Erfordernisse eines "ordnungsgemäßen und angemessenen" Schutzes der IKT-Assets (Art. 6 Abs. 2 DORA).

1.1.2.3 KI-Verordnung

Mit der "Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz" (KI-Verordnung/KI-VO) vom 13. Juni 2024 regulierte die Europäische Union erstmals die Entwicklung, den Handel mit und den Einsatz von Künstlicher Intelligenz. Sie dient dem Schutz der Gesundheit, Sicherheit und Grundrechte vor schädlichen Auswirkungen von KI-Systemen und soll gleichzeitig die Innovation im Bereich KI durch einen harmonisierten europäischen Rechtsrahmen stärken. Auch die KI-Verordnung verfolgt einen risikobasierten Ansatz. Während KI-Systeme mit untragbarem Risiko grundsätzlich verboten sind (Art. 5 KI-VO), unterliegen Hochrisiko-KI-Systeme strengen Anforderungen (Art. 6 ff. KI-VO). KI-Systeme mit beschränktem Risiko unterliegen hingegen bloßen Transparenzpflichten (Art. 50 KI-VO). Weitgehend risikofreie KI-Systeme können bestimmte Anforderungen und Verhaltenskodizes freiwillig übernehmen (Art. 95 KI-VO). Adressiert werden durch die KI-VO eine Vielzahl unterschiedlicher Akteure, für die sich teilweise überschneidende und teilweise unterschiedliche Pflichten gelten (Anbieter, Betreiber, Einführer, Händler, Bevollmächtigter).

Neben KI-Systemen werden auch GPAI-Modelle durch die KI-VO reguliert, wobei GPAI-Modelle mit systemischem Risiko verschärfte Anforderungen zu erfüllen haben (Art. 51 ff. KI-VO).

Der Stand der Technik findet sich an mehreren Stellen der KI-VO: Beim Einhalten der Anforderungen an Hochrisiko-KI-Systeme muss dem *allgemein anerkannten* Stand der Technik in Bezug auf KI und KI-bezogene Technologien Rechnung getragen werden, Art. 8 Abs. 1 KI-VO. Vereinbarungen zwischen Anbietern von Hochrisiko-KI-Systemen und Dritten in der Wertschöpfungskette haben Unterstützungspflichten nach dem *allgemein anerkannten* Stand der Technik zu beinhalten. Auch bei den Transparenzpflichten nach Art. 50 KI-VO haben die Anbieter von KI-Systemen dafür zu sorgen, dass ihre technischen Lösungen wirksam, interoperabel, belastbar und zuverlässig sind und dabei auch den *allgemein anerkannten* Stand der Technik zu berücksichtigen, *wie er in den einschlägigen technischen Normen zum Ausdruck kommen kann.* Hier findet sich also ausnahmsweise eine geringfügige Konkretisierung des Begriffs. Schließlich findet sich der Stand der Technik bei den Pflichten der Anbieter von GPAI-Modellen mit systemischem Risiko wieder: Die Modellbewertung der Anbieter nach Art. 55 Abs. 1 lit. a KI-VO muss mit standardisierten Protokollen und Instrumenten durchgeführt werden, die dem Stand der Technik entsprechen. Auch in den Erwägungsgründen findet sich der Stand der Technik vielfach wieder.

Die KI-Verordnung zeigt damit eindrucksvoll, wie bedeutsam der Stand der Technik als Rechtsbegriff ist, um die dynamischen Entwicklungen neuer Technologien rechtswirksam einzufangen.

1.1.2.4 EUCS

Darüber hinaus arbeitet die Europäische Union (EU) mit dem EUCS (European Union Cybersecurity Certification Scheme for Cloud Services) an einem einheitlichen Zertifizierungsrahmen für Cloud-Dienste, basierend auf der Verordnung (EU) 2019/881 (Cybersecurity Act). Ziel ist es, durch eine europaweit harmonisierte Sicherheitszertifizierung die Verlässlichkeit und Transparenz von Cloud-Angeboten zu erhöhen - insbesondere im öffentlichen Sektor und in regulierten Märkten. Der EUCS sieht drei Sicherheitsniveaus vor ("basic", "substantial" und "high"), deren Anforderungen sich eng an den Stand der Technik anlehnen. Sobald der EUCS in Kraft tritt, wird er für Anbieter, die z. B. KRITIS, Behörden oder das Gesundheitswesen bedienen, ein maßgeblicher Compliance-Baustein sein - auch im Hinblick auf den Stand der Technik und Vertrauenswürdigkeit von Verarbeitungspfaden.

1.1.2.5 EHDS

Mit der Verordnung (EU) 2025/327 über den europäischen Gesundheitsdatenraum (European Health Data Space - EHDS) schafft die EU zudem einen regulatorischen Rahmen für die grenzüberschreitende Nutzung elektronischer Gesundheitsdaten. Der EHDS stellt hohe Anforderungen an technische Sicherheit, Interoperabilität und Zugriffskontrolle. Die Berücksichtigung des Standes der Technik ist bei der Gestaltung von Plattformen, Zugangsinfrastrukturen und Speicherlösungen implizit angelegt und wird voraussichtlich in Durchführungsakten konkretisiert. Für Anbieter und Betreiber im Gesundheits-IT-Umfeld ist der EHDS von strategischer Bedeutung - insbesondere im Zusammenspiel mit der DSGVO und sektoralen Sicherheitsgesetzen.

1.1.3 Sonstige nationale Rechtsquellen

- **EnWG:** § 11 EnWG sieht verschiedene IT-sicherheitsbezogene Pflichten für Betreiber von Energieanlagen und Energieversorgungsnetzen vor. Die Vorgaben gehen dabei dem allgemeineren § 8a BSIG vor, vgl. § 8d Abs. 2 Nr. 2 BSIG. Neben Registrierungs- und Meldepflichten sowie der Pflicht zur Umsetzung eines Sicherheitskatalogs umfasst der Pflichtenkatalog auch die Pflicht zum Einsetzen von risikoangemessenen Systemen zur Angriffserkennung, um fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie eingetretene Störungen zu beseitigen. Hierbei soll auch der Stand der Technik eingehalten werden. Der Einsatz von solchen Systemen muss zudem regelmäßig nachgewiesen werden.
- **AtomG:** Das AtomG enthält in § 44b AtomG eine spezielle Vorschrift mit Bezug zur IT-Sicherheit. Die Norm statuiert eine besondere Meldepflicht bei Beeinträchtigungen von IT-Systemen der Betreiber kerntechnischer Anlagen, wenn sie zu einer Gefährdung oder Störung der nuklearen Sicherheit führen können oder geführt haben.
- **SGB V:** Mit dem zum 01.07.2024 eingeführten § 393 SGB V wurden IT-Sicherheitsanforderungen für die Verarbeitung von Gesundheits- oder Sozialdaten in der Cloud eingeführt. Eine Voraussetzung auch hier ist, dass *nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sind*.
- **TKG:** § 165 TKG sieht u.a. eine Pflicht für Betreiber öffentlicher Kommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste vor, technische und organisatorische Vorkehrungen zu treffen, um die Telekommunikations- und Datenverarbeitungssysteme vor Störungen und Risiken zu schützen. Auch hierbei muss der Stand der Technik berücksichtigt werden, § 165 Abs. 2 S. 3 TKG.
- **TDDDG:** Nach § 19 IV TDDDG haben Anbieter von digitalen Diensten im Rahmen des technisch Möglichen und wirtschaftlich Zumutbaren durch technische und organisatorische Vorkehrungen sicherzustellen, dass die technischen Einrichtungen, die sie für das Angebot ihrer digitalen Dienste vor unerlaubten Zugriffen oder Störungen hinreichend geschützt sind. Dabei muss der Stand der Technik berücksichtigt werden.
- **GeschGehG:** Das Geschäftsgeheimnisschutz-Gesetz schützt Inhaber von Geschäftsgeheimnissen vor unbefugtem Erlangen, Nutzen oder Offenlegen dieser. Informationen sind jedoch nur dann als Geschäftsgeheimnis einzuordnen, wenn sie Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber ist. Welche Geheimhaltungsmaßnahmen angemessen sind, bestimmt sich nach den Umständen des Einzelfalls. Der Inhaber des Geheimnisses hat die Möglichkeit, organisatorische, technische und rechtliche Maßnahmen zum Schutz des Geheimnisses zu ergreifen. Im Rahmen der Angemessenheit als ausfüllungsbedürftiger Rechtsbegriff kann erneut der Stand der Technik berücksichtigt werden.

1.2 Branchenspezifische Sicherheitsstandards (B3S)

Gemäß § 8a Abs. 2 S. 1 BSIG können Betreiber Kritischer Infrastrukturen und ihre Branchenverbände dem BSI branchenspezifische Sicherheitsstandards (B3S) zur Gewährleistung der Anforderungen vorschlagen. Das BMI trifft sodann eine Eignungsfeststellung.[1]

Die B3S sollen den Unternehmen der jeweiligen Branche beim Nachweis der geeigneten Sicherheitsmaßnahmen helfen. Am Umfang und den sonstigen Maßgaben zur Auswahl und Unterhaltung on IT-Sicherheitsmaßnahmen ändert die Nutzung von B3S nichts.

Demgemäß sind in den branchenspezifischen Sicherheitsstandards auch konkrete Festlegungen zu treffen, wie der Stand der Technik dauerhaft in gesetzlicher Weise als Soll-Pflicht erfüllt wird. Das jedoch sehen die B3S üblicherweise gerade nicht vor.

Die meisten B3S stehen der breiten Öffentlichkeit nicht zur Verfügung.

1.3 Angemessenheit der Maßnahmen

Die Gesetzgebung fordert von ausgewählten Anwenderkreisen die Einhaltung oder Berücksichtigung des Stands der Technik der Informationssicherheit[2]. Hinsichtlich der Auswahl konkreter Sicherheitsmaßnahmen sowie Kriterien, nach welchen diese auszuwählen sind, bleibt die Gesetzgebung verständlicherweise jedoch unkonkret. Sie erlaubt jedoch bei der Auswahl der Sicherheitsmaßnahmen die Angemessenheit zu wahren. Das bedeutet konkret, dass die Anwenderunternehmen die Sicherheitsmaßnahmen unter Wirtschaftlichkeitsaspekten auswählen dürfen.

Die Sicherheitsmaßnahmen sollten unter einer Risikobetrachtung ausgesucht werden. Bewährte Grundlagen hierfür sind z.B. die Schutzbedarfsfeststellung gemäß BSI IT-Grundschutz oder die Schutzbedarfsanalyse nach ISO27001ff. Als Ideengeber für die Auswahl der Sicherheitsmaßnahmen kann diese Handreichung dienen.

Auch wenn es aus der rechtlichen Sicht zulässig ist, dass bei der Auswahl der umzusetzenden Sicherheitsmaßnahmen ihre wirtschaftliche Angemessenheit betrachtet wird, so sollten ebenfalls die Effizienz sowie Effektivität bereits vorhandener Sicherheitsmaßnahmen betrachtet werden. Unerlässlich ist daher die individuelle Betrachtung der eigenen Infrastruktur, Anwendungslandschaft, Geschäftsprozesse, Bedrohungslage und der bereits eingesetzten Sicherheitsmaßnahmen im Unternehmen.

Aufgrund dieser Komplexität wurde in dieser Handreichung auf die individuelle Prüfung der Angemessenheit der Sicherheitsmaßnahmen verzichtet.

[1] Übersicht der branchenspezifischer B3S bei BSI: www.bsi.bund.de

[2] In der Gesetzgebung wird oftmals nur schriftlich Bezug auf IT-Sicherheit genommen. Jedoch unter der Betrachtung inhaltlich vorgegebenen Schutzmaßnahmen, muss das Anwendungsgebiet breiter gefasst werden. Daher wird in dieser Handreichung die Informationssicherheit als übergreifendes Themengebiet betrachtet.

2 Bestimmung des Technologiestandes

2.1 Begriffsklärung

Der Technologiestand[3] "Stand der Technik" muss von ähnlich lautenden Begriffen wie den "allgemein anerkannten Regeln der Technik" (im Folgenden "aaRdT" genannt) und dem "Stand der Wissenschaft und Forschung" (im Folgenden "SdWF" genannt)[4] inhaltlich 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.[5]

Eingeführt wurden diese drei Begriffe mit der Kalkar-Entscheidung[6] 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:

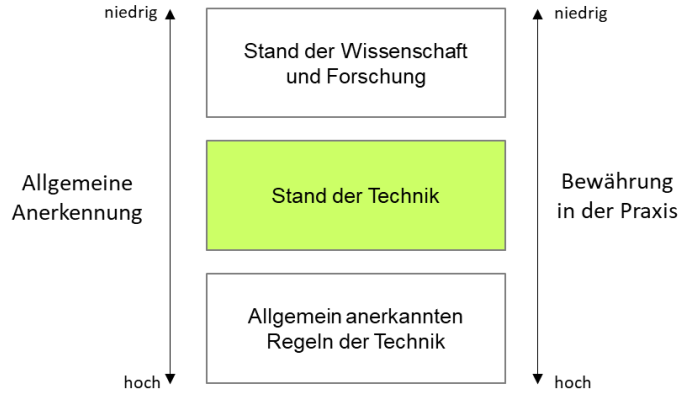


Abbildung 1: Drei-Stufen-Theorie nach Kalkar-Entscheidung

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 objektiv-technisch 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 bezeichnet werden, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele wirkungsvoll gewährleisten kann.[7]

Verkürzt heißt es: Der "Stand der Technik" bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme zur Erreichung des gesetzlichen IT-Sicherheitsziels. Dabei wird aus der technischen Sicht unter Bestleistung insbesondere die Effizienz und Effektivität der Sicherheitsmaßnahmen verstanden.

---

[3] Substitutiv für "Technologiestand" wird der Begriff "Technologieniveau" verwendet.
[4] 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.
[5] Dr. Mark Seibel, Richter am OLG, www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[6] BVerfGE, 49, 89 [135 f]
[7] 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.

Die Verwendung des Begriffes "Stand der Technik" in der Gesetzgebung stärkt die Annahme, dass eine sehr konkrete Maßnahme gemeint ist. In der Praxis gibt es jedoch nicht die eine Maßnahme, die dem "Stand der Technik" entspricht und andere nicht. Je nach Schutzbedarf und Bedrohung kann es viele Lösungsansätze oder Maßnahmenbündel geben, die zum Stand der Technik gezählt werden können.

Technische Maßnahmen im Stadium "Stand der Wissenschaft und Forschung" sind sehr dynamisch in ihrer Entwicklung und gehen mit der Erreichung ihrer Markteinführung in das Stadium "Stand der Technik" über. Gleichwohl können neue und innovative Produkte oft "Kinderkrankheiten" haben, die in eng getakteten Intervallen behoben werden müssen und sich auf die Effektivität der Maßnahme auswirken.

Mit zunehmender Standardisierung nimmt die Dynamik ab. Auch technische Maßnahmen im Stadium "allgemein anerkannte Regeln der Technik" sind am Markt verfügbar. Ihr Innovationsgrad nimmt ab, sie sind in der Praxis stark verbreitet und werden oftmals in den entsprechenden Standards beschrieben. Diese Maßnahmen sind nicht per se schlecht, nur weil sie sich lange am Markt bewährt haben. Sie können jedoch Schwächen aufweisen, weil die Angreifer einen Weg gefunden haben, ihre Schutzmechanismen zu umgehen. Manchmal genügen jedoch gezielte Anpassungen, um die gewünschte Schutzwirkung wiederherzustellen.

Während der Übergang von "Stand der Wissenschaft und Forschung" zu "Stand der Technik" relativ einfach über den Markteintritt identifizierbar ist, gestaltet sich die Abgrenzung zwischen dem "Stand der Technik" und "allgemein anerkannten Regeln der Technik" eher schwierig. Bei technischen Maßnahmen sind es oftmals neue Versionen einer Sicherheitslösung oder einer Software im Rahmen eines Produkt-Lebens-Zyklus, die eindeutig verortet werden. Bei den organisatorischen Maßnahmen sind es jedoch oftmals verschriftlichte Standards, die anderswo unter dem Begriff "*best practice"* geführt werden. Sie haben sich in der Praxis bewährt und unterliegen kaum einer methodischen Modernisierung.

Es gibt darüber hinaus Maßnahmen, die am Markt verfügbar sind, auch wenn ihre Anerkennung durch die Fachleute bezüglich ihrer Wirksamkeit gesunken ist. Das ist beispielsweise der Fall bei Maßnahmen, die kompromittiert wurden. Ebenfalls Maßnahmen, die sich am Ende ihres Produktlebenszyklus (eol im PLC) befinden und vom Hersteller nicht mehr supportet werden gehören in diese Kategorie. Solche Maßnahmen dürfen nicht mehr eingesetzt werden, da ihre Schwachstellen vom Angreifer leicht ausgenutzt werden können.

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 in den "Stand der Technik" über;
3. und mit zunehmender Verbreitung und Anerkennung am Markt wird sie irgendwann den "allgemein anerkannten Regeln der Technik" zugeordnet.
4. Bei Verlust der Anerkennung ist diese Maßnahme nicht mehr einsetzbar.

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 Einordnung des Technologiestandes

Die in dieser Handreichung beschriebenen Maßnahmen wurden anhand einer praktikablen Methode bewertet, die auf einem einfachen Prinzip der Beantwortung von Leitfragen zu den Dimensionen "Anerkennung durch Fachexperten" und "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 eines 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 Tabelle zeigt die durch den Arbeitskreis "Stand der Technik" verwendeten Kriterien und ihre Interpretation für die Bewertung des Technologiestandes der Maßnahmen:

- **Grad der technologischen Anerkennung**

Bewertungskriterium	Konkretisierung des Bewertungskriteriums
Welche **Dokumentation** über die Maßnahme steht öffentlich zur Verfügung?	Ausschließlich wissenschaftliche Publikationen zeugen von einem niedrigen Reifegrad und hohem Innovationsgrad. Hingegen starke Präsenz in den Massenmedien deutet auf allgemeine Regeln der Technik hin. Unter Fachmedien werden aktuelle unabhängige Medien verstanden, deren Inhalte sich an Sicherheitsexperten richten.
Nimmt die Maßnahme Bezug auf internationale oder nationale **Normen**?	Es geht es um den Grad der Standardisierung. Wenn eine Maßnahme bereits in nationalen und internationalen Normen (ISO/IEC 27001ff, NIST, ENISA) und Maßnahmenkatalogen (BSI TR, BSI IT-GS) abgebildet ist, wird sie zu allgemein anerkannten Regeln der Technik zugeordnet. Im Sinne dieses Dokuments wird das Wort "Regelwerk" dem Wort "Norm" gleichgestellt.
Wurde die Maßnahme von nationalen und internationalen Gremien / Verbänden **empfohlen**?	Nationale Gremien sind Fachverbände (TeleTrusT, Bitkom, VDE etc.) aber auch Regulierer (BSI, BNetzA etc.). Internationale Gremien sind beispielsweise ENISA, NIST etc. Wenn eine Maßnahme noch nicht von Gremien empfohlen wurde, geht man davon aus, dass sie noch unbekannt ist. Handelt es sich hingegen um eine Maßnahme, die von vielen Gremien empfohlen wurde, genießt sie eine hohe Anerkennung in den Fachkreisen.
Wird die konzeptionelle Eignung der Maßnahme unabhängig **überprüft**?	Wenn die Eignung der Maßnahme von einer unabhängigen Instanz regelmäßig überwacht wird (z.B. TÜV, DEKRA, BSI, Sachverständige), muss diese einen hohen Reifegrad erreicht haben und wird daher zu allgemein anerkannten Regeln zugeordnet. Wenn die Eignung einer Maßnahme noch nicht unabhängig überprüft wurde, liegt keine ausreichende Standardisierung vor und sie wird tendenziell eher zum Stand der Wissenschaft und Forschung gezählt.

- **Grad der Bewährung in der Praxis**

Bewertungskriterium	Konkretisierung des Bewertungskriteriums
Wie ist der **Innovationsgrad** der Maßnahme einzustufen?	Eine Maßnahme, die die Effizienz bei der Erkennung oder Behandlung von Bedrohungen erhöht oder neue Ansätze (innovativ) bei der Erkennung und Behandlung von Bedrohungen bringt, ist dem Stand der Wissenschaft und Forschung einzuordnen.
Wo wurde die aktuelle Version der Maßnahme **erprobt**?	Üblicherweise sind die von uns betrachteten Maßnahmen für den professionellen Einsatz vorgesehen. Hier geht es darum, zu unterscheiden, ob es sich um eine Maßnahme handelt, die noch entwickelt wird oder diese schon auf dem Markt zu erwerben ist.
Existieren **vergleichbare** Maßnahmen am Markt, die das geforderte Ziel effektiver oder effizienter erreichen lassen?	Wenn es keine vergleichbaren Maßnahmen gibt, die effizienter oder effektiver sind, wird die Maßnahme eher Stand der Wissenschaft und Forschung zugeordnet. Hingegen, wenn es viele Alternativen gibt (Maßnahmen oder Maßnahmenbündeln), um das gleiche Ziel zu erreichen, spricht das eher für die allgemein anerkannten Regeln der Technik.
Wie oft wird die Maßnahme **konzeptionell aktualisiert**?	Maßnahmen, die einen hohen Reifegrad haben, werden eher seltener konzeptionell aktualisiert. Andere hingegen müssen öfter an die Gegebenheiten angepasst werden.

Anhand eines Punktesystems (1-5) wird ausgehend von den gemachten Antworten jeweils ein Mittelwert gebildet. Die ermittelten Werte ermöglichen die Einordnung der Maßnahme in der folgenden Grafik:

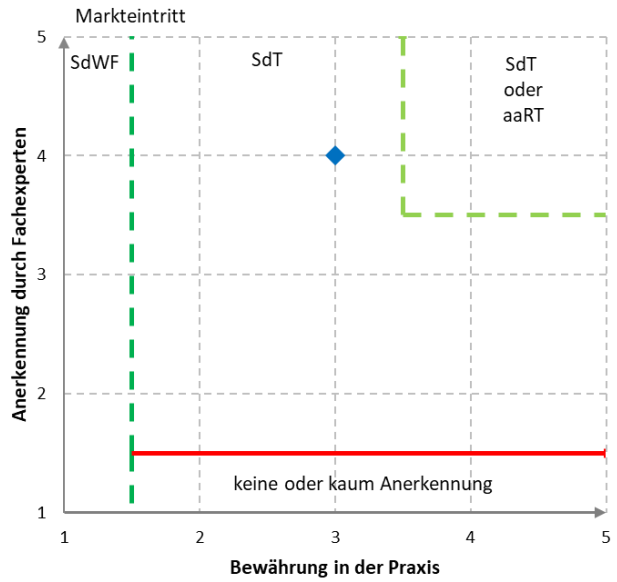


Abbildung 2: Beispiel der Einordnung des Technologiestandes

In der Grafik lassen sich die oben beschriebenen Technologiestände "Stand der Wissenschaft und Forschung", "Stand der Technik" und "allgemein anerkannten Regeln der Technik" einordnen.

Der "Stand der Wissenschaft und Forschung" ist links vom Markteintritt zu positionieren, kann sich jedoch über die gesamte Y-Achse aufgrund der möglichen Anerkennung durch Fachexperten erstrecken.

Wird die oben beschriebene Definition vom "Stand der Technik" zugrunde gelegt, versteht man unter "Stand der Wissenschaft und Forschung" Verfahren, Einrichtungen oder Betriebsweisen, deren

Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele tendenziell gewährleisten können, jedoch ihre Wirkung noch nicht praktisch erprobt wurde.

Mit dem Markteintritt gehen solche Maßnahmen in den Technologiestand "Stand der Technik" über. Sie sind fortschrittlich und können die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten.

Mit zunehmender Standardisierung erfährt die Einordnung der Maßnahme eine Verschiebung nach oben rechts. Dort befinden sich alt-bewährte, standardisierte Maßnahmen, die ausreichend sind, um die gesetzlichen Ziele zu erfüllen. Sie sind oftmals das Grundgerüst der IT-Sicherheit, jedoch unterliegen der Gefahr durch fortschrittlichere, effizientere und effektivere Maßnahmen ersetzt zu werden. Ihre Anerkennung kann schnell umschlagen, so dass sie sich im unteren Bereich der Grafik ("keine oder kaum Anerkennung") wieder finden.

In dieser Handreichung werden Technologien und Maßnahmen beschreiben und gemäß der oben beschriebenen Methode eingeordnet. Es werden keine Sicherheitsprodukte im engeren Sinne beschrieben. Daher wird beispielsweise die Eignung der hier beschriebenen Maßnahmen für den jeweiligen Zweck als erfüllt angenommen und nicht auf den Einzelfall weiter validiert.

In der unternehmerischen Praxis kann 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.

2.3 Prozess zur Qualitätssicherung der Handreichung

Der Arbeitskreis "Stand der Technik" ist bemüht, eine hohe Qualität der Inhalte der Handreichung sicherzustellen. Damit das gelingt, wurde im AK SdT ein Prozess etabliert, in dem die Beiträge mehrere Stufen erfolgreich bestehen müssen:

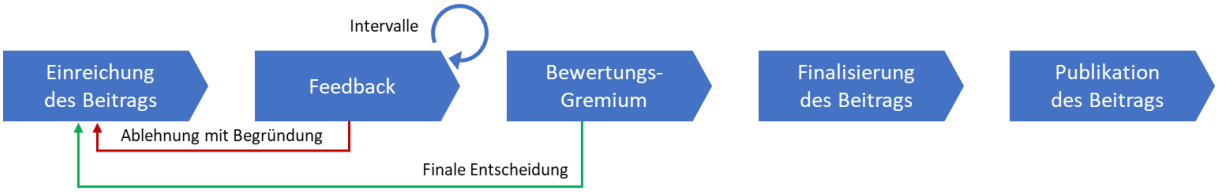


Abbildung 3: Prozessskizze für die Bewertung der Maßnahmen im Arbeitskreis

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[8] 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.

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

2.4 Geforderte Schutzziele

Die IT-Sicherheit verfolgt mehrere Schutzziele, um Informationen und Systeme vor Bedrohungen zu schützen. Die drei grundlegenden Schutzziele[9], die auch gesetzlich gefordert werden, sind:

- **Vertraulichkeit**
  Die Vertraulichkeit ist gegeben, wenn die schützenswerten Daten nur in der zulässigen Art und Weise ausschließlich an die Befugten verfügbar gemacht werden.

- **Integrität**
  Die Integrität der Verarbeitung ist gegeben, wenn keine Veränderung der Daten ungewollt und unbemerkt erfolgt. Für die Sicherstellung der Integrität müssen ebenfalls die Kategorien Übereinstimmung, Genauigkeit, Korrektheit und Vollständigkeit betrachtet werden.

- **Verfügbarkeit**
  Die Verfügbarkeit von informationstechnischen Systemen und Komponenten ist vorhanden, wenn diese stets gemäß ihrem Zweck und Funktionsumfang genutzt werden können. Für die Sicherstellung der Verfügbarkeit müssen die Kategorien Fehlertoleranz, Zuverlässigkeit, Robustheit und Wiederherstellbarkeit betrachtet werden.

Neben diesen durch das IT-SiG fokussierten Schutzzielen der IT-Sicherheit, bestehen weitere Gewährleistungsziele aus Sicht des Datenschutzes, die insbesondere aufgrund hier der behandelten Datenschutzgrundverordnung erwähnt werden. Das sind z.B. Nichtverkettbarkeit (Zweckbindung), Transparenz der Verarbeitung oder Intervenierbarkeit.[10]

Diese zusätzlichen Ziele stehen teilweise in Konkurrenz zu den zuvor erwähnten Schutzzielen der IT-Sicherheit. Da die gesetzlichen Vorgaben 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 personenbezogener Daten. Das Verständnis über diese unterschiedlichen Sichten ist wichtig, um Schutzmaßnahmen festzulegen und entsprechend zu implementieren.

[9] Neben diesen drei Schutzzielen wird oftmals noch die Authentizität gefordert. Die Authentizität ist die Eigenschaft der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Information. Durch die Authentifikation des Datenursprungs kann nachgewiesen werden, dass die Information einem angegebenen Sender zugeordnet werden kann. Durch digitale Signaturen wird es ermöglicht die Authentizität einer Nachricht sicherzustellen.
[10] In Anlehnung an das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), www.datenschutzzentrum.de/

3 Technische und organisatorische Maßnahmen (TOM)

Zahlreiche gesetzliche und normative Vorgaben 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 häufig nicht. Daher müssen für die 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 Publikation eine vollumfassende Auflistung der Anwendungen zu erstellen und diese Anwendung auch zu beschreiben. IT-Sicherheit kann auf verschiedene Arten umgesetzt werden. Es gibt nicht nur eine einzige Möglichkeit, eine sichere Architektur zu schaffen. 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 Umsetzung sollte die fortschrittlichen Verfahren berücksichtigen, wobei der Einsatz der konkreten Sicherheitsmaßnahme oder des Maßnahmenbündels einer gesonderten Schutzbedarfsanalyse zugrunde gelegt werden sollte. Beispiele der Sicherheitsmaßnahmen sind:

- Multi-Faktor-Authentifizierung
- Gegenseitige Authentisierung
- Verschlüsselung der Kommunikation während des Transports
- Verschlüsselung der Daten (z.B. bei der Speicherung)
- Sicherung des privaten Schlüssels und der Software-Zertifikaten 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,
- Vertraulichen Datenverarbeitung,
- Umsetzung des Zero Trust Prinzips 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 Bausteine 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 sollen internationale Standards berücksichtigen und interoperabel mit Standard-Protokollen sein, soweit diese verwendet werden.

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

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

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

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

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

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

- Finanzieller Background des Herstellers garantiert weitere Lebenszyklen des Produktes.

- Es existiert ein etabliertes Produktmanagement für das jeweilige Produkt und 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 proaktiv auf bekannt gewordene Schwachstellen, die sein Produkt betreffen und schließt diese kurzfristig und stellt umgehend 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 Authentisierung

Ein Anwender darf nur auf Ressourcen im IT-System zugreifen, wenn dessen Identität bestätigt und die Rechte überprüft wurden. Dazu meldet er sich mit seiner Nutzerkennung beim System an, das dessen Identität anhand von Faktoren verifiziert. Als Grundlage der Authentisierung werden drei Kategorien unterschieden:

- Wissen (z.B. Passwort)
- Besitz (z.B. Token)
- Biometrie (z.B. Fingerabdruck)

Unter die wissensbasierten Faktoren fallen z.B. Passwort, PIN und Passphrase. Ein Passwort besteht im Idealfall aus einer zufälligen Ziffern-, Buchstaben- und Sonderzeichenfolge. Hingegen besteht die persönliche Identifikationsnummer (PIN) meist aus einer 4- oder 6-stelligen Ziffernfolge, mit welcher sich der User an einem Gerät identifizieren kann. Beide Methoden werden üblicherweise in Verbindung mit einem Benutzernamen angewandt. Eine Passphrase besteht im Vergleich zu einem Passwort aus mehreren Worten oder einer längeren, sinnvollen Zeichenkette, die sich der Nutzer leichter einprägen kann, die aber wegen der größeren Länge resistenter gegen Angriffe ist.

Besitzbasierte Faktoren stellen u.a. FIDO- und OTP-Sicherheitstoken sowie Smartphones und klassische Smartcards dar. Sicherheitstoken dienen meist der zusätzlichen Absicherung von Benutzerkonten als zweiter Faktor, oftmals in Form eines USB-Sticks. Sie können einem Benutzer eindeutig zugeordnet und somit personalisiert werden. Sicherheitstoken generieren ein One Time Password (OTP) und reagieren auf Berührung bzw. verwenden zusätzlich ein biometrisches Merkmal. Das Smartphone dient als vielfältiges Authentifizierungsmedium. So kann ein OTP per Authenticator-Anwendung auf dem Gerät erzeugt werden.

Die dritte Kategorie der Authentisierungsmethoden bilden die biometrischen Faktoren. Darunter fallen z.B. Fingerabdruck- und Iris-Scanner sowie Venen- oder Gesichtserkennung, Tippverhalten und Spracherkennung. Davon durchgesetzt haben sich Fingerabdruck- und Gesichtserkennung.

Ein weiteres Verfahren ist die sog. "Conditional" / "Adaptive"-Authentisierung. Bei dieser Methode wird zunächst ein Authentisierungsfaktor mit einer Verhaltensmuster- oder Kontextanalyse kombiniert. Erst wenn dabei Anomalien erkannt werden, wird ein weiterer Faktor zur Verifizierung benötigt.

3.2.2 Bewertung und Durchsetzung starker Passwörter

Die Maßnahme unternimmt eine umfassende Inventur und Bewertung aller, auch unbekannter, Passwörter. Dazu werden auch Angriffe auf sicher gespeicherte Hashwerte von Anmeldedaten / Passwörter simuliert und deren objektive Widerstandsfähigkeit auf Grundlage mathematischer Methoden, persönlicher Verhaltensweisen etc. gemessen. Dabei ermittelt die Maßnahme den Erfüllungsgrad der Compliance zu unternehmensinternen Richtlinien und ermöglicht die Durchführung sicherheitsrelevanter Maßnahmen, wie zum Beispiel die Benachrichtigung von Mitarbeitern bei Verwendung unsicherer Passwörter. Dies gilt auch für die Überprüfung neu gesetzter Passwörter.

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

Unberechtigter Zugriff auf Nutzerkonten durch:

- Erraten von schwachen Passwörtern durch Dritte
- Verwendung kompromittierter Passwörter durch Dritte

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

Unternehmensnetzwerke verwenden in der Regel einen zentralen Speicher für Benutzer-Anmeldedaten, die eingesetzt werden, um Benutzer zu authentifizieren (z.B. Microsoft Active Directory).

Soweit Passwörter zur Authentisierung verwendet werden, speichert man diese nicht im Klartext, sondern als Hashwert des Passworts. Das soll verhindern, dass ein Angreifer durch unberechtigten Zugriff auf Passwortdaten in den Besitz fremder Passwörter gelangt und sich dadurch Zugriff auf weitere Systeme oder Benutzerkonten verschafft. Während diese Hashing-Funktionalität einen entscheidenden Schutz der Passwörter gegen unbefugten Zugriff darstellt, verhindert sie gleichzeitig die Bewertung der Passwörter hinsichtlich ihrer Stärke. Dies ist aber notwendig, um geeignete Maßnahmen gegen mögliche Angriffe umzusetzen, wie z.B. den Vergleich von neu gesetzten Passwörtern mit Wörtern aus einem Wörterbuch den Vergleich mit bekannten kompromittierten Passwörtern oder das Erraten der Passwörter aufgrund persönlicher Informationen über den anvisierten Benutzer.

Der erste Teil der Maßnahme, die Bewertung der Passwort-Sicherheit, identifiziert die Widerstandsfähigkeit von Passwörtern, indem in regelmäßigen Intervallen ein realer Angriff durch Einsatz einschlägiger Tools simuliert wird. Dadurch können mögliche Schwachstellen wie z.B. vorhersehbare, schwache und fehlerhafte kryptographische Implementierungen erkannt werden. Die Kennzahlen ermöglichen geeignete Awareness- und Trainingsmaßnahmen und deren Überprüfung und Optimierung auf Effektivität.

Der zweite Teil der Maßnahme ist die Durchsetzung starker Passwörter. Sie erzwingt die Verwendung von starken und sicheren Passwörtern. Die erforderliche Stärke jedes neuen Passwortes wird durch ein Regelwerk an das Sicherheitslevel des jeweiligen Benutzerkontos angepasst. Das definierte Sicherheitslevel basiert auf den möglichen Auswirkungen einer Sicherheitskompromittierung dieses Kontos. Neu gesetzte Passwörter werden gegen ein zum Sicherheitslevel passendes Set von Regeln geprüft, die jedem Account zugeordnet sind. Diese Regeln enthalten 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 historischen Wiederverwendung von Passwörtern.

Die Regeln sind nicht auf klassisches "Blacklisting" beschränkt, sondern können individuell parametrisiert werden.

Klartext-Daten werden zu keiner Zeit gespeichert oder angezeigt. Sollte beim erforderlichen Passwortwechsel das Passwort abgelehnt worden sein, wird der Anwender durch eine individuelle Nachricht mit Begründung informiert.

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

Die beschriebene Maßnahme führt zur zentralen Durchsetzung der jeweilig angemessenen Passwortstärke und gibt der Organisation vollständige Kontrolle, Steuerung und Dokumentation über die Stärke der verwendeten Passwörter im Unternehmen. Bei regelmäßiger Anwendung der Maßnahmen kann messbar gemacht werden, ob die Regeln wie erwartet greifen oder sie ggf. korrigiert werden müssen, um geeignete Passwortstärke unternehmensweit zu erzielen.

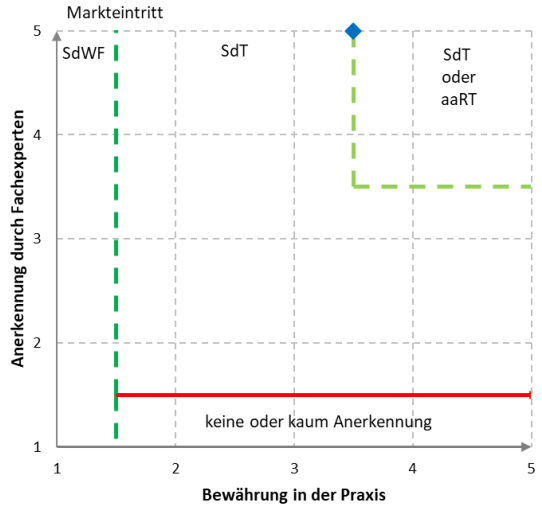
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.3 Multifaktor-Authentifizierung

Als Multi-Faktor-Authentifizierung (MFA) bezeichnet man den Nachweis und Prüfung der Identität eines Nutzers Der Nutzer präsentiert im Anmeldeprozess eine Kombination aus mehreren Authentisierungsmethoden (z.B. Passwort + Sicherheitstoken, Passwort + OTP oder Passwort + Fingerabdruck) zum Nachweis seiner Identität (Authentisierung, siehe Abschnitt 3.2.1), die wiederum durch ein Computersystem geprüft wird (Authentifizierung).

Die Multi-Faktor-Authentifizierung gilt heute als etablierter Standard und sollte daher, wo immer möglich, zur Absicherung der Identität in Anmeldeprozessen verwendet werden.

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

Wenn ein System lediglich mit einem Faktor (Ein-Faktor-Authentifizierung) gesichert ist, unterliegt die Nutzeridentität einem erhöhten Risiko des

- Identitätsdiebstahls,
- Identitätsmissbrauchs und
- Identitätsbetrugs.

Zur Absicherung von schutzwürdigen Benutzeranmeldungen an Computersystemen / Applikationen / Webanwendungen ist ein Faktor allein nicht ausreichend - die Methoden der digitalen Angreifer werden immer versierter und die möglichen Schäden aufgrund der fortschreitenden Vernetzung und Digitalisierung immer drastischer. "Phishing", die unberechtigte Aneignung von Zugangsdaten (min. Benutzername und Passwort), wird auf eine dramatische Art durch Kriminelle professionalisiert. Speziell mit dem Einsatz künstlicher Intelligenz sind entsprechende Vorgehensmodelle (Mails, gefälscht Webseiten usw.) in den letzten Jahren stark professionalisiert worden.

- Menschliche Risiken im Umgang mit Passwörtern:
    - unzureichende Qualität der Passwörter,
    - Wiederverwendung gleicher Passwörter in verschiedenen Anwendungen,
    - bewusste Passwortweitergabe (z.B. Teilen mit anderen Personen) oder
    - unbewusste Passwortweitergabe (z.B. Aufschreiben).

- Technische Risiken im Umgang mit Zugangsdaten:
    - "Man in the middle"-Attacken,
    - Phishing-Attacken, heute stark KI basiert und hoch professionell
    - Keylogger-basierte Attacken,
    - Brute-Force-Attacken etc.
    - Sicherheitsmängel in Anwendungen

Der Einsatz von MFA-Lösungen reduziert diese Risiken erheblich.

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

MFA-Systeme kombinieren in der Regel jeweils zwei Methoden aus unterschiedlichen Kategorien zu einer Authentisierungskette, wobei einige MFA-Systeme auch die Verkettung von beliebig vielen Methoden zulassen. Die Kombination von Methoden aus nur einer Kategorie ist nicht ratsam. Es ist zu beachten, dass nicht zwangsläufig alle Methoden aus den drei Kategorien, auch in ihrer Kombination gleichwertig sind.

Als derzeitig sicherste Methoden gelten Phishing resistente Verfahren wie Passkeys, die auf dem FIDO2 / WebAuthn-Standard basieren. Passkeys ersetzen das klassische Passwort vollständig durch ein kryptografisches Schlüsselpaar, hierbei wird zwischen gerätegebunden Passkeys (Schlüsselmaterial im sicheren Element des Endgerätes "TPM" gespeichert) und synchronisierten Passkeys (Schlüsselmaterial wird in einem zentralen System z.B.: Cloud gespeichert). Die Anmeldung erfolgt durch einen Besitznachweis (z.B. über ein Smartphone oder Computer) kombiniert mit Biometrie (z.B. Fingerabdruck oder Gesichtserkennung) oder einem PIN.

Jedoch stellt jegliche Kombination, auch ohne Einsatz Phishing resistenter Verfahren eine Verbesserung gegenüber dem alleinigen Einsatz von Passwörtern dar. Die Kombination von

Authentifizierungsmethoden kann oder sollte abhängig des Schutzbedarf der Anwendung bzw. Nutzeridentität sowie den technischen Voraussetzungen gewählt werden.

Die flexible Kombination verschiedener Authentisierungsmethoden ermöglicht dem Nutzer eine benutzerfreundliche "passwortlose Authentifizierung". Die "passwortlose Authentifizierung" kann in zwei Formen unterschieden werden:

- Systemseitig (technisch) passwortbasiert, aus Benutzersicht passwortlos
  Ein System erfordert im Hintergrund weiterhin ein Passwort zur Authentifizierung, jedoch wird dies nicht aktiv vom Nutzer in seinem Anmeldeprozess abgefragt/benötigt

- Vollständig passwortlos
  Weder aus technischer noch aus der Sicht des Nutzers wird ein Passwort benötigt. Die Anmeldung erfolgt ohne ein Passwort. In der Regel wird aus technischer Sicht ein asymmetrischen Schlüsselverfahren systemseitig verwendet. Die Nutzung der vollständigen passwortlosen Authentifizierung ist empfohlen, kann aus heutiger Sicht nicht in jeglichen gewachsenen Infrastrukturen aufgrund veralteter Software umgesetzt werden.

Darüber hinaus bieten moderne MFA-Systeme einen dynamisierten Ansatz zur Benutzerauthentifizierung (Adaptive Authentisierung). Hierbei wird die zum Identitätsnachweis notwendige Authentisierungsmethode oder deren Kombination, nicht mehr statisch, sondern situationsabhängig und flexibel festgelegt. Beispielsweise können folgende Eigenschaften einzeln oder in Ihrer Kombination (als Risikobewertung) einbezogen werden: Gruppen- / Rollenzugehörigkeit, geografischer Standort des Anwenders, Bewegungsgeschwindigkeit, eindeutige Geräte-ID / Geräte-IP, typische Arbeitszeit des Benutzers etc.

MFA kann heute in vielen Applikationen aktiviert werden bzw. ist Teil der Produktoptionen. Ist dies bei schutzwürdigen Anwendungen nicht der Fall oder werden in einem Unternehmen mehrere schutzbedürftige Applikationen betrieben, wird der Einsatz einer zentralen Authentifizierungslösung über alle Anwendungen und Nutzer hinweg empfohlen. Ein Parallelbetrieb verschiedener Lösungen sollte aus Rücksicht zunehmender Komplexität, höhere Kosten und erhöhten Administrationsaufwand, sinkende Benutzerakzeptanz und erhöhten Administrationsaufwand vermieden werden, daher sind moderne MFA-Lösungen mit einem zentralistischen Ansatz empfohlen da diese eine hohe Flexibilität gegenüber den unterschiedlichsten Authentisierungsmethoden, Applikationen, Benutzer und Systeme zu bieten und offene technische Standards, wie z.B. Oauth2, OIDC, WS-Fed, SAML oder REST-API integrieren.

Aufgrund der vorgenannten menschlichen und technischen Risiken der Ein-Faktor-Authentifizierung fordern diverse nationale und internationale Regelwerke wie DORA, NIS2, PSD2, KRITIS, DSGVO oder die BAFIN den Einsatz von MFA zur Absicherung des Benutzerzugangs zu einem schutzbedürftigen Computersystem.

Bei der Auswahl eines Multi-Faktor-Authentifizierungssystems folgendes zu beachten:

- Vielfalt der Methoden:
  Unterstützung verschiedener Methoden wie Passkeys, Einmalpasswörtern, biometrische Daten und viele weitere um den unterschiedlichen Anforderungen der Anwendungsfälle, Benutzergruppen und Rollen und gerecht zu werden
- Integration und Kompatibilität:
  Das MFA-System muss sich nahtlos in die bestehende IT-Infrastruktur integrieren um Anmeldungen jeglicher Art (Betriebssystem, Web-basiert, VPN) durch offene technische Standards wie Oauth2 / OIDC, SAML, WS-Fed, RADIUS oder Web-API.
- Benutzerfreundlichkeit und Verwaltung:
  Ein zentralisiertes System zur Verwaltung der Authentifizierungsmethoden, das sowohl für Administratoren als auch für Endbenutzer einfach zu bedienen ist 1. Funktionen wie Self-Service-Optionen für Benutzer und detaillierte Berichte für Administratoren können die Effizienz und Zufriedenheit erhöhen.
- Effiziente Rollout-Prozesse:
  Vereinfachen der Rollout-Prozesse durch eine zentrale MFA-Lösung mit einem Workflow gesteuerten Registrierungsportal, welches an das Unternehmenslayout angepasst ist, um eine schnelle und unkomplizierte Registrierung der Methoden eines Benutzers ermöglichen.
- Skalierbarkeit und Zukunftssicherheit:
  Ein MFA-System muss skalierbar sein, um den zukünftigen Anforderungen und technologische Entwicklungen zu entsprechen für einen langfristig effektiven und effizienten Betrieb.

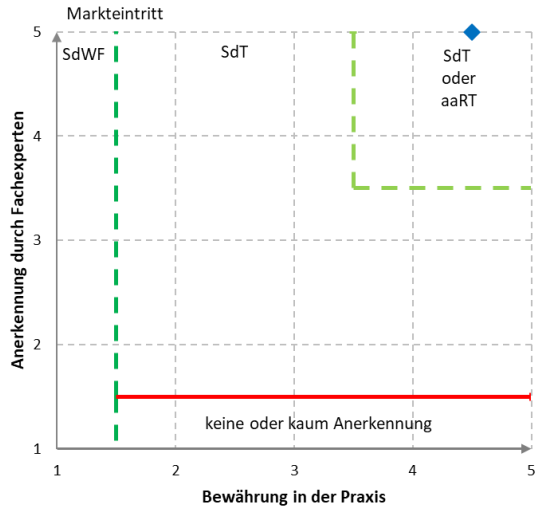
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.4 Kryptographische Verfahren

Kryptographie im Sinne der Informationssicherheit beschäftigt sich mit der Konzeption, Definition und Aufbau von Informationssystemen, die gegen Manipulation und unbefugtes Lesen möglichst widerstandsfähig sind.

Kryptografische Verfahren sind anwendbare Methoden, um sensible Inhalte zu schützen. Die Güte der kryptografischen Verfahren hängt insbesondere vom verwendeten Verschlüsselungsverfahren (z.B. AES, ECIES), der gewählten Schlüssellänge (z.B. 512 Bit), der Sicherheit des Schlüssels und der umgesetzten Sicherheitskonfiguration eingesetzter Produkte ab. Mit zunehmender Schlüssellänge wächst die Anzahl der Möglichkeiten, um eine verschlüsselte Nachricht zu entschlüsseln und erhöht somit die Sicherheit.

In der modernen Kryptographie sollen die eingesetzten Verfahren das sogenannte Kerckhoffs'sche Prinzip erfüllen. Das besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht. Daher kann das verwendete Verfahren offengelegt werden.

Es wird zwischen den symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden:

Symmetrische Verfahren	**Asymmetrische Verfahren**
▪ Komplizierte Schlüsselverteilung (wenn kein sicherer Kommunikationskanal vorhanden ist). ▪ Alle Teilnehmer, die an der gleichen Kommunikation beteiligt sind, verwenden nur einen, den gleichen Schlüssel. Es wird also der gleiche Schlüssel für die Ver- und Entschlüsselung verwendet. Für jede neue Kommunikationsinstanz muss ein neuer Schlüssel erzeugt werden: N Instanzen benötigen $\frac{(n\cdot(n-1))}{2}$ Schlüssel, was einem quadratischen Wachstum entspricht.	▪ Für unabhängig verschlüsselte Kommunikationskanäle wächst die benötigte Anzahl der Schlüssel nur linear mit der Anzahl der Teilnehmer (vgl. symmetrische Verschlüsselung mit quadratischem Wachstum). ▪ Alle bekannten Verfahren sind im Vergleich zu symmetrischen Verschlüsselungsverfahren mit vergleichbarer Schlüssellänge sehr langsam. ▪ Die benötigte Schlüssellänge ist in der Regel größer als bei symmetrischer Kryptographie, um die gleiche Sicherheit zu bieten.

▪ Schnelle Verschlüsselung von Massendaten. ▪ Einzige nachweislich sichere Verschlüsselungsmethode ist Vernam-Cipher / one-time-pad. Diese Methode findet in der Praxis jedoch kaum Anwendung. ▪ Spontane verschlüsselte Kommunikation ohne vorheriges Vertrauensverhältnis (zumindest zum Austausch des Schlüssels) ist unmöglich, es sei denn, es wird Quantenkryptographie verwendet.	▪ Digitale Signaturen sind möglich. ▪ Einfacher Schlüsselaustausch. Es existieren jeweils zwei Schlüssel (öffentlicher und privater). Der öffentliche Schlüssel wird für die Verschlüsselung, der private nur für die Entschlüsselung verwendet. Private Schlüssel werden nicht ausgetauscht. ▪ Nicht geeignet für größere Datenmengen.

Im hybriden Verfahren, was in der Praxis meist angewandt wird, werden die symmetrische und asymmetrische Verschlüsselung kombiniert, um die Vorteile der jeweiligen Technik zu nutzen. In der Praxis wird die auszutauschende Nachricht symmetrisch mit einem Sitzungsschlüssel verschlüsselt. Dieser muss ausreichend groß sein, um ein Brute-Forcing des gesamten Schlüsselraums zu verhindern. Anschließend wird dieser Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und an die verschlüsselte Nachricht angehängt.

Mit zunehmender technischer Entwicklung und der damit gestiegenen Rechenleistung besteht die Gefahr, dass die geheimen Schlüsselinformationen ermittelt und somit die bisher eingesetzten Verfahren gebrochen werden. Genau das wird im Zusammenhang mit Quantencomputern erwartet.

Um dieser Entwicklung auf der Verschlüsselungsseite entgegenzuwirken, hat das US-amerikanische National Institute of Standards and Technology (NIST) drei Standards für Verfahren zur quantenresistenten Kryptografie verabschiedet (FIPS-203[11], FIPS-204[12], FIPS-205[13]).

Unabhängig davon wird empfohlen die verwendeten Verschlüsselungsverfahren regelmäßig (z.B. jährlich) auf Ihre Wirksamkeit und Aktualität zu überprüfen und bei Bedarf gemäß gängigen Empfehlungen anzupassen. Das kann beispielsweise durch Änderung der Schlüssellänge (z.B. von 256 Bit auf 512 Bit) erfolgen.

Vor dem Hintergrund der zuvor skizzierten Entwicklung muss jetzt schon darauf geachtet werden, dass für den Schutz langfristig wichtiger Informationen zukünftig die kryptografischen Verfahren ausgetauscht werden können. Diese Krypto-Agilität ist zwingend erforderlich, um auch noch in der Zukunft das erforderliche Sicherheitsniveau sicherzustellen.

In der BSI Technischen Richtlinie (BSI TR-02102-1) werden die Verschlüsselungsverfahren dediziert vorgestellt und ihre Einsatzdauer in Abhängigkeit von der verwendeten Schlüssellänge empfohlen.[14] Weitere Empfehlungen zu Tools und Verfahren existieren ebenfalls seitens ENISA[15].

[11] csrc.nist.gov/pubs/fips/203/final
[12] csrc.nist.gov/pubs/fips/204/final
[13] csrc.nist.gov/pubs/fips/205/final
[14] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html
[15] www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

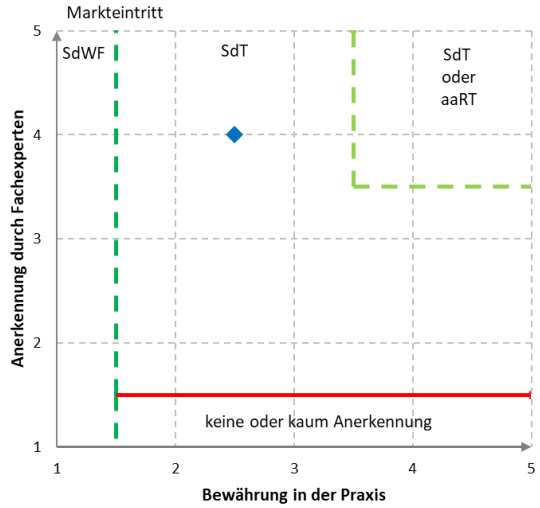
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.5 Verschlüsselung von Datenträgern

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

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 (sog. "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 Daten, da diese verschlüsselt vorliegen.

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 als auch für eine ausgebaute Festplatte.

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 Backup-Zwecken, in die Cloud gesichert wer weise ich auf ein Bekannte Schachstelle hin, die mit PBA den.

Bei der Festplatten-Vollverschlüsselung sollte großer Wert auf eine Pre-Boot-Authentifizierung, komplexe Passwörter sowie 2-Faktor-Authentisierung gelegt werden, idealerweise mittels "Wissen und Besitz", etwa mit zusätzlichem Token (s. Maßnahme 0 MFA). Dies ermöglicht zusätzlich den Einsatz von Hardware-gestützten Verzögerungsmechanismen bei mehrfacher Passwort-Falscheingabe.

Soweit vom Gerät ermöglicht, etwa bei Windows 10 (und höher) Systemen, sollte auch der sogenannte "Secure Boot" unterstützt werden. Damit wird beim Boot-Prozess gewährleistet, dass nur Boot Loader mit einer gültigen Signatur geladen und ausgeführt werden und dadurch die darauf folgende Entschlüsselung der Betriebssystempartition nicht unterwandert werden kann.

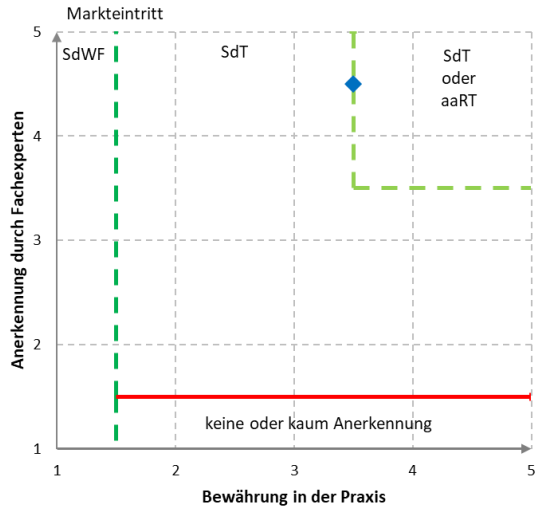
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

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. Objektverschlüsselung bietet die Möglichkeit Dateien und Ordner sicher von einem Ort zu einem anderen zu transportieren und eine Einsichtnahme durch Unbefugte zu verhindern. Die hierfür verfügbaren Programme entschlüsseln die Daten entweder automatisch nach Anmeldung an das Betriebssystem oder nach expliziter Anwenderaktion. Danach stehen die Daten transparent zur Verfügung, d.h. der Nutzer kann mit den Objekten arbeiten, als wären sie unverschlüsselt.

Es wird sichergestellt, dass niemand außer den autorisierten Personen Zugriff auf die geschützten Informationen erhält. Dies könnte persönliche Daten einzelner oder im schlimmsten Fall die Existenzgrundlage eines Unternehmens gefährden.

Des Weiteren bietet sich die Objektverschlüsselung bei der Verwendung von externen Cloud-Diensten an. Sofern der Cloud-Betreiber keinen Zugriff auf verwendete Verschlüsselungsschlüssel erhält, lässt sich damit die Einsichtnahme der Daten durch den Betreiber wirkungsvoll verhindern. Mit der Verschlüsselung von Daten in der Cloud gibt es allerdings i.d.R. Einschränkungen bezüglich Indexierung von Daten, Volltextsuche, Antivirusschutz oder Data Leakage Protection. Diese können zum Teil durch zusätzliche, aufwändige Techniken wie z.B. den Einsatz von Verschlüsselungsgateways gemindert werden.

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?

Die Datei- und Ordner-Verschlüsselung umfasst die Verschlüsselung einzelner Objekte, wie z.B. Container, Ordner oder einzelner Dateien. Damit können Dateien und Ordner sicher von einem Ort zum anderen transportiert, an jedem Ort sicher gespeichert und dabei eine Einsichtnahme durch Unbefugte verhindert werden.

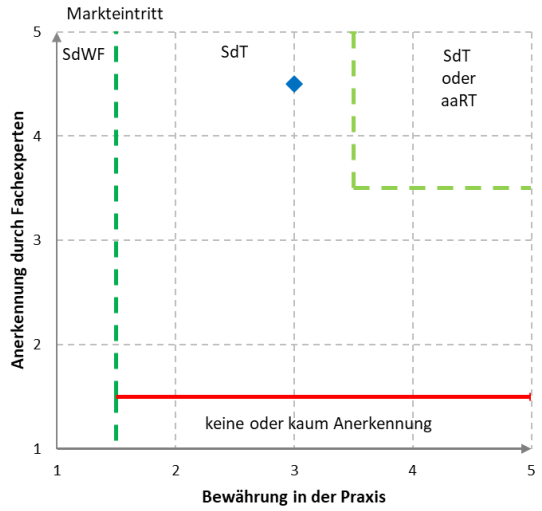
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☐ Integrität

☒ Vertraulichkeit

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 übermittelt werden, die besonderen Schutzbedarf haben, so z.B. Gesundheitsdaten, Daten von Mandanten z.B. von Rechtsanwälten oder besonders wertvolle Firmengeheimnisse, wie z.B. Konstruktionsdaten.

Daraus ergeben sich folgende Sicherheitsanforderungen an E-Mail:

- Schutz vor unbefugter Einsichtnahme oder Veränderung im Transport und bei gespeicherten E-Mails (Schutzziel: Vertraulichkeit),

- Schutz vor nachträglicher Veränderung von E-Mails bei langfristig archivierten E-Mails (Schutzziel: Integrität).

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

Im E-Mail-Verkehr sollte zur Transportverschlüsselung TLS (Transport Layer Security) in der aktuell gültigen Version, wie in RFC 5246 definiert, 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 Inhaltsverschlüsselung nur zwischen Organisationen sinnvoll sein; d.h. E-Mails werden im Übergang vom öffentlichen Internet zum privaten Netz der Organisation (Gateway) verschlüsselt bzw. entschlüsselt (Organisations-Ende-zu-Ende-Verschlüsselung), ggf. kombiniert mit einer unternehmensinternen Inhaltsverschlüsselung.

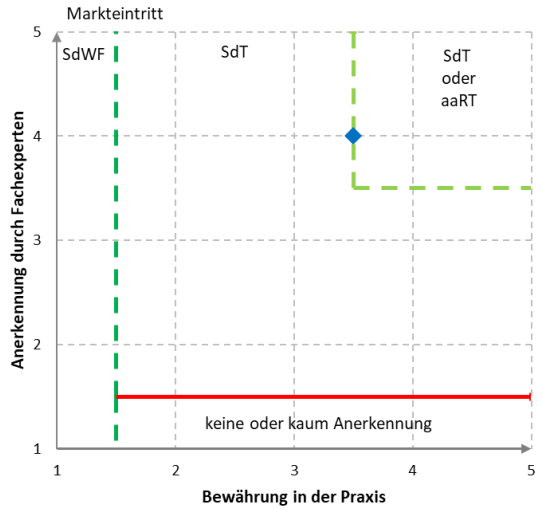
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.8 Schutz 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, Rückruf, Management und Prüfung elektronischer Zertifikate voraus, welche den Nachweis von elektronischen Identitäten vertrauenswürdig sicherstellen: eine Public-Key-Infrastructure (PKI).

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 elektronischer 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 Verschlüsselung in verkabeltes oder drahtloses Netzwerk (IEEE 802.1X)
- Authentisierung und Integritätssicherung bei ausführbarem 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 Cross-Zertifizierung mit anderen PKI ist realisierbar.

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

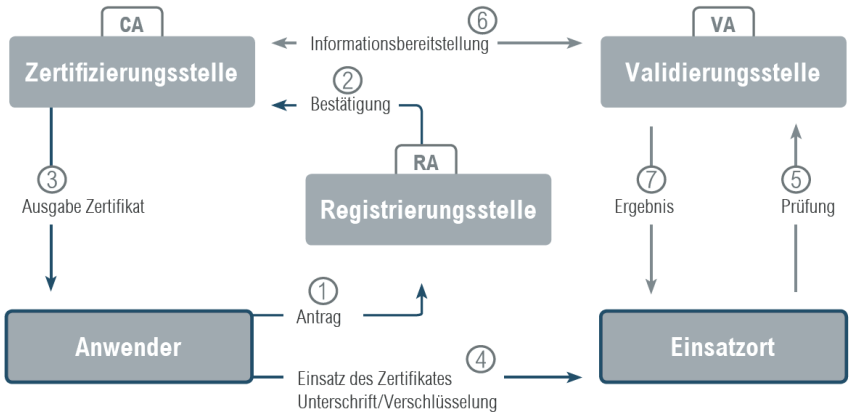


Abbildung 4: Aufbau und das Zusammenwirken von PKI-Komponenten

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).[16]

[16] Weitere Hinweise sind zu finden unter www.ebca.de

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

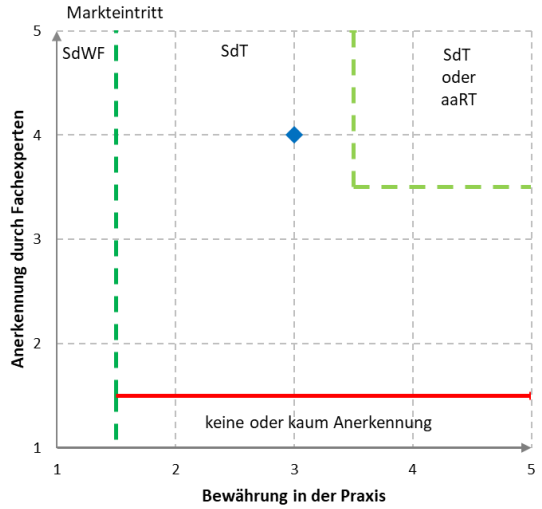
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.9 Einsatz von verschlüsselten VPN-Lösungen (Layer 3)

Ein Layer 3 VPN bezeichnet die Verbindung von Netzen auf Layer 3 des OSI-Modells, d.h. insbesondere den Transport von IP-Datenverkehr innerhalb eines Tunnels über nicht vertrauenswürdige Netze. Auch wenn ein unverschlüsselter Transport möglich wäre, schließt das heute übliche Verständnis von VPN eine Verschlüsselung ein. Die etablierten VPN-Verfahren basieren i.A. auf offenen Standards oder Spezifikationen wie bei IPSec bzw. Open Source Implementationen wie OpenVPN oder Wireguard. Der Tunnel für den Datentransport wird dabei typischerweise auf Layer 3 (IP) und 4 (TCP, UDP, ESP) etabliert.

Die klassischen Anwendungen von Layer 3 VPN im Enterprise-Umfeld sind die Vernetzung von Standorten und die Anbindung mobiler Arbeiter. Neuere Anwendungen sind Netzwerk-Overlays z.B. im Kontext von Multi-Cloud-Szenarien oder die Anbindung an Cloud-basierte Zero-Trust Infrastrukturen. VPN-Services werden ebenfalls an Privatkunden vermarktet, z.B. für die sichere Nutzung von offenen WLAN-Hotspots oder die Umgehung GeoIP-basierter Restriktionen. Diese Consumer-VPN werden im Weiteren nicht betrachtet.

Gegen welche Bedrohungen der IT-Sicherheit wird die Maßnahme eingesetzt?

Durch eine Authentisierung der Gegenstellen und die Verschlüsselung der Daten schützen VPN gegen:

- Verlust von Vertraulichkeit oder Integrität bei unverschlüsselten bzw. schwach verschlüsselten Verbindungen, ggf. auch als zusätzliche Verschlüsselungsschicht in einer Defense-in-Depth Architektur.
- Externe Angreifer, die lesenden Zugriff auf die transportierten Daten haben.
- Externe Angreifer, die die transportierten Daten manipulieren können.

Die eingesetzten VPNs unterliegen selbst auch weiteren Bedrohungen:

- Abfluss des Schlüsselmaterials
- Schwache Kryptographie
- Schwache bzw. fehlerhafte Authentisierung der Gegenstellen
- 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 von Netzen 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 in bestimmten (seltenen) Einsatzszenarien nicht 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 Remote Access Layer 3 VPN benötigt, im Gegensatz zu Site-to-Site VPN Layer 3 VPN, 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. Alternativen sind Mesh-Architekturen, bei denen die verschiedenen Teilnehmer direkt miteinander kommunizieren. Als zentraler Bestandteil einer IT-Infrastruktur muss der Konfiguration und dem Betrieb eines Layer 3 VPN besondere Aufmerksamkeit zugutekommen.

Ein VPN muss die Vertraulichkeit und Integrität der durchgeleiteten Daten sicherstellen. Dazu muss das Gerät eine Verschlüsselung und Authentisierung mit als sicher geltenden Algorithmen und Parametern durchführen. Ob diese kritischen Parameter ausreichend sicher konfiguriert sind, ist für einen Nutzer nicht offensichtlich, da das VPN oft selbst bei Schwächen in der Konfiguration Verbindungen herstellen kann.

Für VPN existieren solide Open-Source-Implementierungen und auch Hersteller setzen in ihren Produkten oft auf diese auf. Neben der Verfügbarkeit von Support und aktivem Patchmanagement bieten kommerzielle Lösungen hier i.Allg. eine geringere Komplexität bei der Konfiguration insb. für große und komplexe Einsatzumgebungen, ein besserer Schutz vor unsicherer Fehlkonfiguration, eine bessere Unterstützung von Hochverfügbarkeitsanforderungen sowie die Integration mit Enterprise-spezifischer Authentisierung. Zusätzlich bieten einige Hersteller Zulassungen bzw. Zertifizierungen, welche aus regulatorischen Gründen in bestimmten Einsatzumgebungen gefordert sind.

VPN stehen an einer kritischen Position im Netzwerk. Fehler in der Implementation durch den Hersteller können einem Angreifer nicht nur Zugang zu der Kommunikation geben, sondern auch Zugriff auf das interne Netzwerk. Entsprechende Schwachstellen oder gar explizite Backdoors sind in der Vergangenheit leider keine Einzelfälle gewesen und betrafen auch renommierte Hersteller. 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.

Bei den Schutzzielen Vertraulichkeit, Integrität und Authentizität der durchgeleiteten Daten ist ebenfalls die Integrität der Plattform entscheidend. VPN-Geräte sollten auf einer besonders gehärteten Plattform aufgebaut sind, einen ausgezeichneten Selbstschutz haben und frei von Backdoors sein. Die

Sicherheitsprotokolle, die ein Layer 3 VPN nutzt, garantieren bei der korrekten Konfiguration 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 Lösungen zu bevorzugen, die nachweislich eine sichere Zufallszahlengenerierung, eine sichere Schlüsselhaltung der privaten Authentisierungsschlüssel (z.B. auf Chipkarten) ermöglichen und das Alter von verwendeten Verschlüsselungsschlüssel mitverfolgen. Eine besondere Herausforderung sowohl für sicheren Zufall als auch für den Schutz von Schlüsselmaterial stellt dabei der Aufbau von VPN-Endpunkten in Cloud-Umgebungen dar.

Um die Verfügbarkeit des Layer 3 VPNs sicherzustellen, sind entsprechende Maßnahmen bei der Hardware und der Software der VPN-Endpunkte (z.B. VPN-Konzentratoren) notwendig. Bei der Hardware sollten redundante Netzteile und Lüfter sowie ausreichender Rechenleistung gegeben sein. Da diese Maßnahmen allein 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 sollten die Produkte ein entsprechendes Monitoring z.B. mittels SNMP unterstützen. 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.

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.

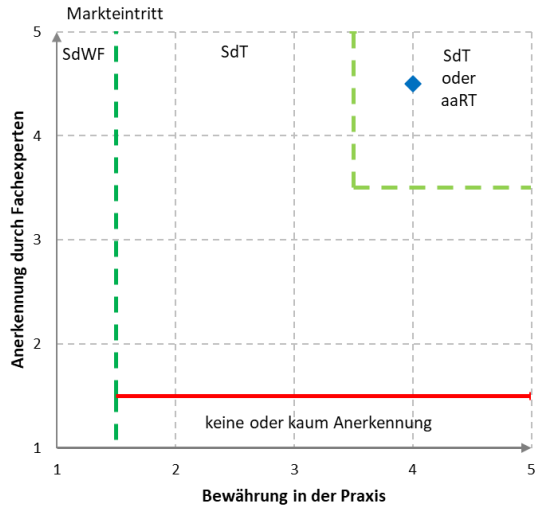
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.10 Verschlüsselung auf Layer 2

Layer 2-Verschlüsselung ist eine Sicherheitslösung als Alternative zu Layer 3-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 Layer 2-WAN Backbones und direkte Links (z.B. dark fiber, Satcom).

Layer 2-Verschlüsselung ist eine Sicherheitslösung, die in bestimmten Anwendungsszenarien eine zweckmäßige Alternative zu Layer 3-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), die spezielle Ethertypes unterstützen.

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 echtzeitrelevanten 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.

MACsec ist ein weit verbreitetes Protokoll für die Layer-2-Verschlüsselung. Es ist im Standard IEEE-802.1AE spezifiziert und wurde entwickelt, um Ethernet-Verkehr gegen Manipulation und Abhören zu schützen. Die Daten werden auf den Verbindungen zwischen benachbarten Netzwerkkonten verschlüsselt übertragen (Hop-by-Hop-Verschlüsselung). Viele in der Praxis eingesetzte Layer-2-Verschlüsselungslösungen basieren auf dem MACsec-Protokoll, ermöglichen aber eine Ende-zu-Ende-Verschlüsselung.

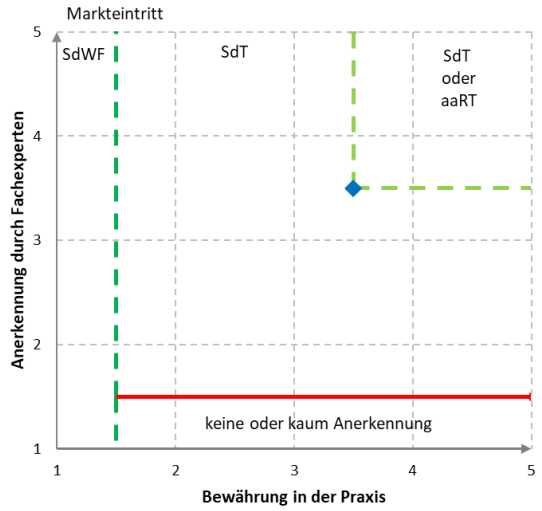
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.11 Schutz in der Cloud gespeicherter Dateien

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 gespeicherten Daten unterliegen den folgenden Bedrohungen:

- Unbefugter Zugriff und Einsicht durch den Betreiber des Dienstes
- Unbefugter Zugriff und Einsicht durch Dritte während der Verarbeitung oder Speicherung
- Unbefugter Zugriff und Einsicht 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. Verschlüsselung der Daten unabhängig vom Dateiaustauschdienst durch
   a. clientseitige (Ende-zu-Ende-)Verschlüsselung der Daten vor der Übertragung in den Cloud-Speicher (z.B. durch in den Datenaustauschdienst integrierte Verschlüsselung in zum Cloud-Speicher gehörender Client-Software oder durch separate Ende-zu-Ende-Verschlüsselungssoftware auf dem Client)
   b. Gateway Verschlüsselung
   (siehe Kapitel "Datenablage in der Cloud")

Dabei sind insbesondere die folgenden Fragen zu beachten:

1. Wer betreibt den Dienst und hat der Betreiber Zugriff auf die Daten?
2. Welche gesetzlichen Offenlegungs- / Auskunftspflichten hat der Betreiber gegenüber staatlichen Stellen (bspw. U.S. Cloud Act)?
3. Wie sind die Daten bei der Verarbeitung / Dateiablage geschützt?
4. 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 selbst unter Umständen verzichtet werden, sie ist aber grundsätzlich auch bei vertrauenswürdigen Betreibern sinnvoll.

Es sind Dateiaustauschdienste verfügbar, bei denen Daten vor dem Upload transparent, durch eine vom Betreiber des Dienstes bereitgestellte Client-Software ohne besondere Aktion des Benutzers verschlüsselt und nach dem Download wieder entschlüsselt werden. Der Cloud-Betreiber sieht dann nur verschlüsselte Daten. In diesem Fall muss jedoch dem Betreiber des Filesharing-Dienstes als Lieferant der Software vertraut werden bzw. sichergestellt werden, dass der Betreiber keinen Zugriff auf die genutzten Schlüssel hat. 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 in der aktuellen Version).

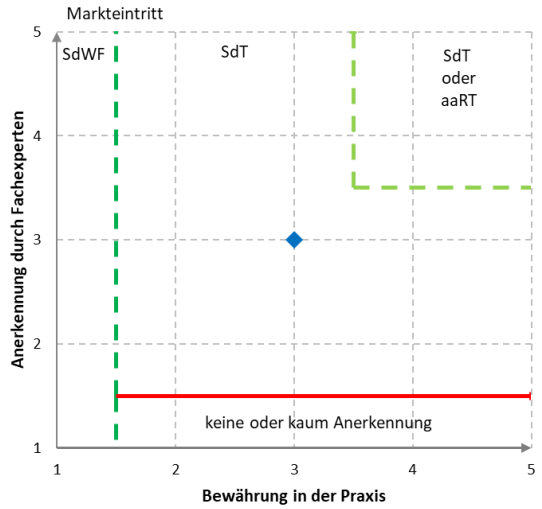
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.12 Datenverarbeitung in der Cloud

Sobald (hoch-)sensible Daten eine sichere, interne Umgebung verlassen, um in der Cloud gespeichert zu werden, sollten diese vor der Übermittlung verschlüsselt werden und zwar zusätzlich zur Transportverschlüsselung: Dabei sollte die Verschlüsselung ausschließlich in der Kontrolle der

Anwenderorganisation bleiben, um unberechtigte Datenzugriffe auch durch externe Administratoren auszuschließen. Denn wer die Daten verschlüsselt (z.B. im Falle von BYOK-Angeboten), hat automatisch Zugriff auf die unverschlüsselten Daten. Und das sollte nur die Anwenderorganisation sein. Eine Lösung nach Stand der Technik muss deshalb eine entsprechende, vollständig intern kontrollierte Datenverschlüsselung oder -Tokenisierung erlauben. 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 weiterhin ermöglichen.

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

Sobald sensible Daten an SaaS-Anwendungen übermittelt und dort verarbeitet werden, unterliegen sie spezifischen Bedrohungen, darunter insbesondere:

- Unbefugter Zugriff auf gespeicherte oder verarbeitete Daten durch externe oder interne Akteure, z. B. Cloud-Administratoren.
- Abfangen der Daten während der Übertragung zwischen Organisation und Cloud (MitM-Angriffe).
- Verfälschung oder Löschen der Daten bei der Übertragung in die Cloud.
- Datenexfiltration im Fall erfolgreicher Angriffe auf den Cloud-Anbieter oder über privilegierte Zugänge.
- Diebstahl oder unberechtigte Nutzung der Identität, die gegenüber dem Cloud-Dienst vereinbart wurde.

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

Um sensible Daten in der Cloud effektiv zu schützen, wird empfohlen, sie verschlüsselt an die Cloud-Anwendung zu übergeben und sie dort ausschließlich in verschlüsselter Form zu verarbeiten. Dabei darf die Verschlüsselung die Funktionalität der Anwendung - etwa Suchen, Filtern oder Auswertungen - nicht einschränken.

Neben Client-seitiger Verschlüsselung (siehe vorhergehendes Kapitel dieser Handreichung) ist hierfür eine bewährte technische Lösung der Einsatz von Verschlüsselungsgateways:

Ein Verschlüsselungsgateway agiert als Proxy zwischen interner Umgebung und Cloud-Anwendung. Es übernimmt die Verschlüsselung und Pseudonymisierung sensibler Daten vor dem Versand an die Cloud und entschlüsselt Rückgaben nur für autorisierte Nutzer. Die kryptografischen Schlüssel verbleiben hierbei vollständig in der Kontrolle der Anwenderorganisation. Weder Cloud-Anbieter noch deren Administratoren erhalten somit Zugriff auf Klartextdaten. Durch selektive Verschlüsselung oder Re-Implementierung der Funktionalität auf Seite des Verschlüsselungsgateways können relevante Funktionen der Cloud-Anwendung weiterhin genutzt werden - z. B. Suchen, Sortieren oder automatisierte Verarbeitung.

Die eingesetzte Lösung sollte hierbei die folgenden Kriterien erfüllen, um zukunftssicher aufgestellt zu sein:

- Die Schlüsselverwaltung sollte intern auf mehrere Verantwortliche verteilt werden können, um Missbrauch und Fehler zu vermeiden.
- Um ein gleichbleibend hohes Sicherheitsniveau bei allen Cloud-Anwendungen zu erlauben, sollte die Lösung zudem Multi-Cloud fähig sein, d.h. mehrere Cloud-Anbieter unterstützen und, je nach Bedarf, selbst geschriebene Anwendungen in der Cloud.
- Zusätzlich sollte die Lösung Tokenisierung unterstützen, um formaterhaltende Ersatzwerte zu generieren (siehe entspr. Kapitel dieser Handreichung), sowie Voraussetzungen für Crypto Agility (siehe entspr. Handreichung von TeleTrusT) erfüllen, um Algorithmen bei Bedarf auszutauschen.
- Außerdem sollte sie mittels Confidential Computing gehostet werden können. Dabei werden sensible Daten in einer abgesicherten, hardwarebasierten Ausführungsumgebung (Trusted Execution Environment, TEE) verarbeitet. Die Daten liegen dabei nur innerhalb dieser Umgebung im Klartext vor, sodass selbst System-Administratoren keinen Zugriff auf sie erhalten (siehe hierzu auch die Handreichung "Cloud Security" von TeleTrusT).

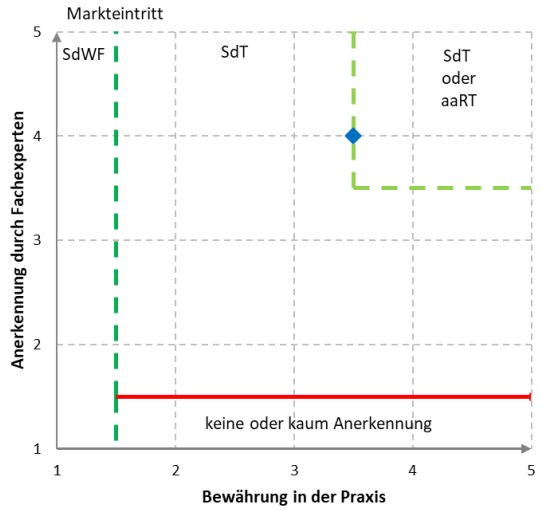
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.13 Schutz mobiler Sprach- und Datendienste

Mobilfunk-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 Web-Konferenz-Anwendungen, eines der direktesten und persönlichsten Kommunikationswerkzeuge. Sie birgt jedoch einige Gefahren und bietet potenzielle Angriffsvektoren. Die überwiegende Zahl auch der von Festnetzendgeräten ausgehenden Telefonate findet unter Beteiligung eines Mobiltelefons statt.

- Ausspähen von Mobilfunkgesprächen und Datenverkehr im Netzwerk der Mobilfunk- und Telefonie-Netzbetreiber, das die Basisstationen untereinander und die Festnetzanschlüsse verbindet und das u.a. auf IP-Technologie basiert
- Ausspähen von Mobilfunkgesprächen und Datenverkehr sowie deren Übertragung an Command & Control Server der Angreifer durch im Mobiltelefon 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 Mobilfunk-Gespräche und Datenverkehre können mit kostengünstiger Hardware auf der Luftschnittstelle abgehört werden. Dazu müssen Angreifer weder das Mobiltelefon infizieren noch ins Kommunikationsnetz einbrechen. Sie müssen sich allerdings im Empfangsbereich des betreffenden Mobiltelefons befinden. Angreifer täuschen beispielsweise vor, Teil des Mobilfunknetzes zu sein, um ein Einbuchen des Mobiltelefons in ihre Abhöreinrichtung zu erreichen und dann Gespräche und Datenverkehre 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 Schutzmaßnahmen werden empfohlen:

- Verschlüsselung der Sprach- und Datenkommunikation durch geeignete und vertrauenswürdige Apps oder Hardware auf Applikationsebene, die nach den aktuellen Verschlüsselungsstandards 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 Mobiltelefon-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.

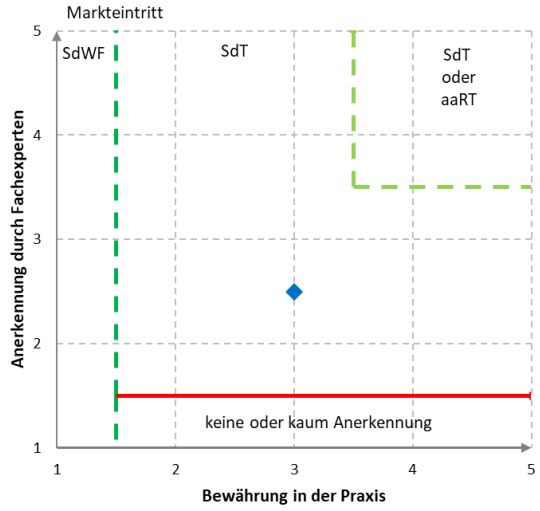
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.14 Schutz der 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 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:

- Mitschneiden, Auswerten und Verändern der Inhalte durch eine unbefugte dritte Partei (Man-in-the-Middle-Angriff)
- Identitätsdiebstahl innerhalb eines Kommunikationssystems
- Diebstahl eines Geräts, um Instant Messaging Daten nachträglich unbefugt auswerten zu können
- Unbekannte / Unberechtigte Teilnehmer in einem Gruppen-Chat

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 4096 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.

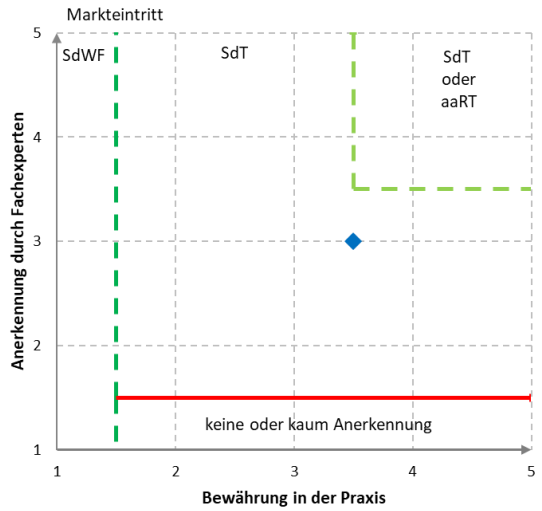
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.15 Schutz 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 sensible 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. Datendiebstahl: Wenn ein mobiles Endgerät gestohlen wird oder Daten über unsichere Kommunikationswege oder Applikationen abfließen, ist die Vertraulichkeit der Unternehmensdaten nicht mehr gewährleistet.
3. Schadsoftware: Durch die Verwendung öffentlicher WLAN-Netze, unterlassene Installation von Updates und die unkontrollierte Installation von Anwendungen aus zweifelhaften Quellen können mobile Geräte mit Schadsoftware infiziert werden.

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

Mobile Device Management (MDM)-Lösungen ermöglichen Unternehmen und Organisationen u.a. die Durchsetzung von Richtlinien zur Verbesserung der Sicherheit von Geräten und Unternehmensdaten. MDM-Lösungen verhindern unsichere Kommunikation durch den Einsatz von VPNs, die sichere Nutzung von WLANs und die Nutzung freigegebener Anwendungen aus bekannten Quellen. Die Gerätesicherheit wird durch erzwungene starke Authentifizierung, Konformitätsprüfungen (z.B. Prüfung von Systemeinstellungen oder erlaubter Applikationen) und Aktualität des Betriebssystems und installierter Anwendungen gewährleistet. Im Falle eines Geräteverlustes können Geräte gesperrt und Daten per Fernzugriff gelöscht werden. Der Schutz und die Verfügbarkeit der Daten auf den Geräten wird durch die zentrale Konfiguration der Verschlüsselung und regelmäßige Datensicherung erreicht.

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

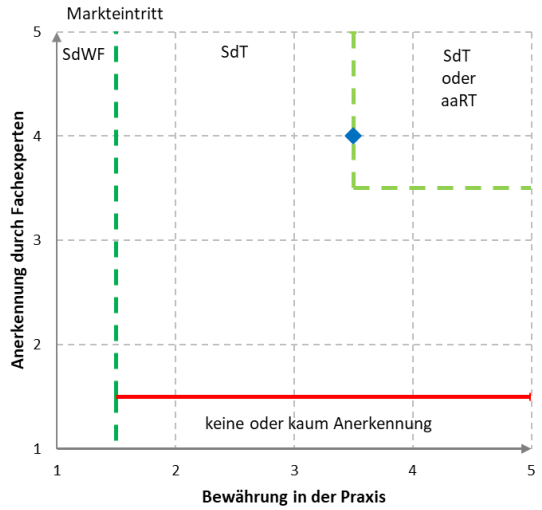
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.16 Routersicherheit

Router sind zentrale Infrastrukturkomponenten, die den Austausch von Netzwerkpaketen zwischen mehreren Netzwerken 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. Die genannten 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 abgewehrt 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 (sog. Hintertüren / Backdoors)
8. Ausführen von Fremdcode und Integration in Botnetze
9. Manipulation von Routing-Informationen

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 in einem solchen Fall 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. VPN-Router: Aufbau von VPN-Verbindungen nach Möglichkeit nicht über Pre-Shared Keys, sondern zertifikatbasiert
11. Router als VoIP-Gateway: Einsatz von Geräten mit integriertem Session Border Controller. Firewalls sind nicht in der Lage, die SIP-Signalisierung und die RTP-Pakete mit der beinhalteten Sprachinformation auf Applikationsebene zur prüfen. Somit entsteht hierdurch die Gefahr eines Angriffs über Voice-over-IP-Verbindungen. Der Routerbetrieb sollte zentral überwacht werden.
12. Die eingesetzten Routing-Protokolle sollten kryptografische Verfahren zur Prüfung von erhaltenen dynamischen Routinginformationen einsetzen und ausgehende Routing-Informationen auch entsprechend mit authentisierenden Informationen versehen.

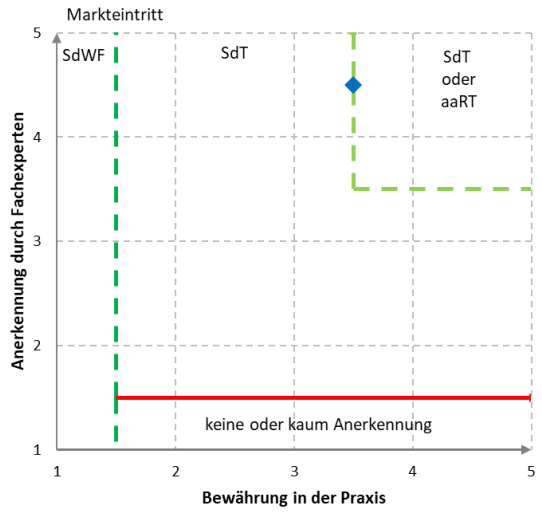
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.17 Netzwerküberwachung mit IDS

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) ist ein IT-System zur Erkennung und Protokollierung von potenziellen Bedrohungen im IT- / OT-Netz, wobei das IPS zusätzlich selbsttätig Abwehrmaßnahmen einleitet.

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

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

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

Ein IDS oder IPS erkennt und protokolliert Angriffsaktivitäten und Anomalien in IT- und OT-Netzen. Das Ziel beider Systeme ist es, unberechtigte Zugriffe und angriffstypische Aktionen (Reconnaissance, Lateral Movement, Persistence) sowie die Einbringung von Schadsoftware möglichst bereits vor Schadenseintritt zu erkennen. Im Gegensatz zum IDS, welches ausschließlich Informationen von verdächtigen oder schädlichen Aktivitäten anzeigt und Alarme generiert, kann ein IPS auch selbsttätig eingreifen, um Angriffe zu mitigieren. Dadurch kann z.B. die Ausnutzung konkreter Angriffsvektoren (wie manipulierte Abfragen, welche eine bestimmte Software-Verwundbarkeit ausnutzen), behandelt werden, z.B. durch das Verwerfen der Pakete auf der Netzwerk-Ebene. 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 und zu Falsch-positiv-Erkennungen und unerwünschten Störungen führen kann.

Netzwerk-basierte IDS/IPS-Systeme werden als eigenständige Lösungen, aber auch als Funktion von sogenannte UTM und Next Generation Firewalls angeboten. Bei den Client- / Serverseitigen IDS und IPS-Lösungen in der Büro-IT werden die Funktionen heute auch über moderne EDR-Lösungen (siehe auch 3.2.22 Endpoint Detection & Response) abgedeckt, welche die Anomalieerkennung, Verhalten von Prozessen, Cyber Threat Intelligence und Exploit-Schutz kombinieren.

Zunächst müssen IDS/IPS-Systeme einen Einblick in den Datenverkehr erhalten. Hierzu empfiehlt sich bei hardwarebasierten Systemen die Ausleitung der produktiven Daten mittels Test Access Point (TAP), um entsprechende Überbuchungen und Interpretationen zu vermeiden, wie es bei SPAN-Ports auf Switches geschehen kann. Zur Filterung auf die relevanten Daten können zudem Network Packet Broker (NPB) zum Einsatz kommen, um die Last der IDS/IPS zu verringern. Sie ermöglichen beispielsweise eine Eingrenzung auf Header- / Metadaten oder bestimmte Paketlängen. Ob Header- / Metadaten ausreichend sind, sowie die Positionierung des IDS/IPS im Netzwerk orientiert sich am Einsatzweck.

Das Erkennen von Anomalien basiert auf zwei unterschiedlichen Verfahren. Beim sogenannten "Pattern Matching" wird bereits bekannte Schadsoftware auf Basis von Mustern (Signaturen) oder die Ausnutzung einer Schwachstelle durch die Analyse der Netzwerkpakete 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. Hier unterstützt die Anwendung von Machine-Learning-gestützten Verfahren insbesondere dabei, den Aufwand zur Erstellung und Pflege manueller Regelwerke zu reduzieren oder zu vermeiden, sofern die Güte und Menge der Trainingsdaten ausreichend ist.

Ein IDS muss im Falle der Erkennung einer Schadsoftware oder eines Angriffes bzw. bei Abweichungen des validen Sollzustandes der Kommunikation entsprechende Ereignismeldungen automatisiert erzeugen. Alle Ereignismeldungen sollen zu Analysezwecken in einem ausreichend langen Zeitraum im

System vorgehalten werden und bei Bedarf in einem offenen bzw. standardisierten Format exportierbar sein. Die Ereignismeldungen müssen alle relevanten Informationen zur Ereignisanalyse und Initiierung von Gegenmaßnahmen wie z.B. erkannte Signatur bzw. auffällige Kommunikationsverbindung enthalten. Zusätzlich sollten auch detaillierte Netzwerkpaket-Analysen für weitere Auswertungen möglich sein. Die Alarmmeldungen sollen auf der Managementkonsole vordergründig erkennbar sein. Darüber hinaus sollen Alarme automatisch an definierte Empfänger gesendet sowie ggf. die Detaildaten zu einem mutmaßlichen Angriff über eine Export-Schnittstelle (Syslog, API, Webhook etc.) einem übergreifenden Security Information und Event-Management-System (siehe Kapitel "Angriffserkennung und Auswertung (SIEM)") zur Korrelation und weiteren kontextuellen Anreicherung (z.B. mit Daten aus EDR-Systemen) zur Verfügung gestellt werden.

Ein IPS sollte 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 innerhalb von internen IT-Netzwerken zu analysieren. Bei einem temporären Ausfall von IDS/IPS-Komponenten müssen die Daten temporär zwischengespeichert werden und nach Betriebsfähigkeit wieder zusammengeführt und ausgewertet werden können. Es darf keine unerwünschte Kommunikation der IDS/IPS-Komponenten zu Dritten zugelassen werden. Außerdem sollten alle IDS/IPS-Komponenten im Netzwerk nicht erkennbar sein, den Datenverkehr nicht beeinflussen, keine Dienste (außerhalb des Management Netzes) anbieten sowie selbst vor Kompromittierung geschützt sein. Die Kommunikation zwischen den einzelnen Komponenten muss vertraulich und integer erfolgen.

Neben der reinen Implementierung eines IDS/IPS ist auch ein ganzheitliches Konzept für die Überwachung des Netzwerks wichtig. Network-Security-Monitoring (NSM) ist eine Erweiterung von IDS/IPS für eine umfangreichere Übersicht aller Aktivitäten mit zugehörigen Kontextdaten im gesamten Netzwerk. Dabei liegt der Fokus auf der Bereitstellung und Aufbereitung der Transaktions-, Session- und Inhaltsdaten, die für Analyse des jeweiligen Events verwendet werden können.

Die mittels IDS/IPS gesammelten Daten sind so zu speichern, dass sie bei weiteren Analysen (z.B. Forensik) verwendet werden können. Die Speicherfristen der Daten sind von den individuellen Vorgaben des jeweiligen Unternehmens abhängig.

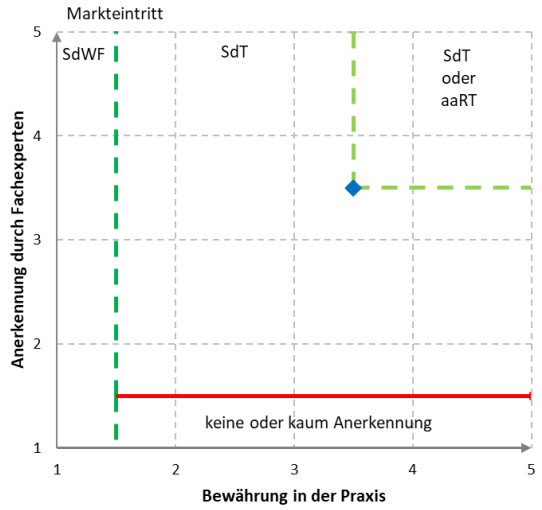
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

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 als Teil eines Proxy-Servers oder einer Firewall 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 Premises, oder als lokal auf dem System des Endnutzers betriebene Software.

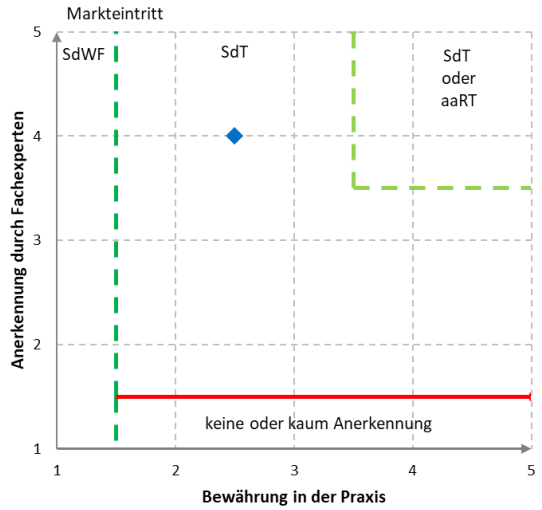
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.19 Schutz von Web-Anwendungen

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, wie SQL Injection 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) 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.

Hinweis: In einem technischen Kontext (Softwareentwicklung) kann SQL in einem Chat eine normaler Anwendungsfall sein und sollte dann bei der Konfiguration der WAF, risikobasiert, angepasst 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
- Schutz von Websocket-Verbindungen

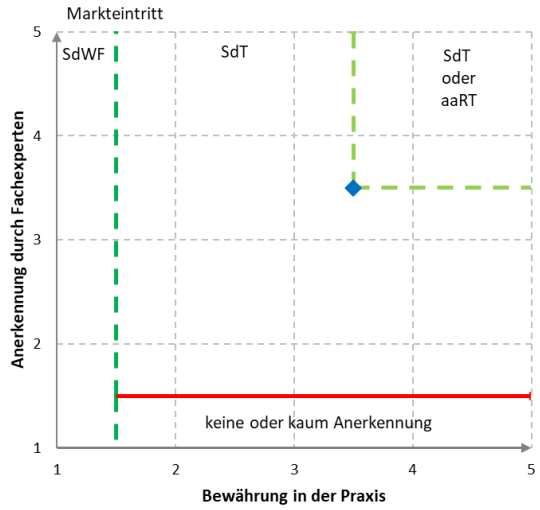
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.20 Schutz des Fernzugriffs auf Netzwerke

Entfernte Netzwerke müssen zwecks Service- 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.

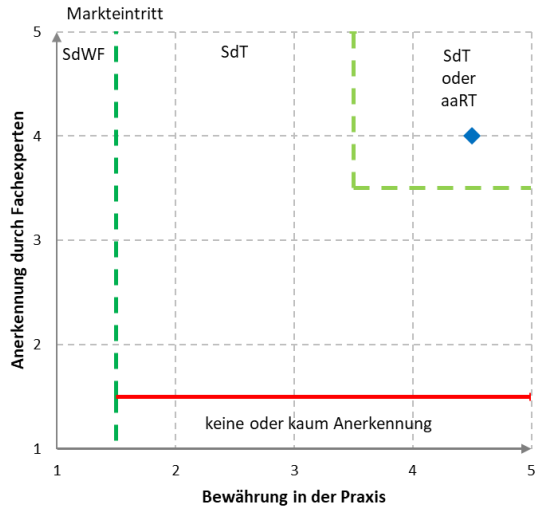
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.21 Systemhärtung

Eine wirkungsvolle Maßnahme zur Reduzierung der Angriffsfläche von IT-Systemen stellt die Systemhärtung dar. Die Systemhärtung führt eine möglichst sichere Konfiguration des Betriebssystems und den Anwendungen des IT-Systems durch, unabhängig davon, ob es sich um ein physikalisches, virtuelles oder Cloud-basiertes System handelt. Ein ganzheitlicher Härtungsansatz für die gesamte Infrastruktur (On-Premise und Cloud) wird empfohlen. IT-Systeme jeglicher Art können gehärtet werden. Darunter fallen insbesondere Client- und Serversysteme, aber auch Hardware Appliances (z.B. Firewalls). Eine besondere Rolle spielt außerdem die sogenannte PAW (Privileged Access Workstation), die als besonders stark gehärteter Client zur hochprivilegierten Administration eingesetzt wird.

Gängige Betriebssysteme (z.B. Microsoft Windows oder Linux) besitzen standardmäßig keine sehr restriktive Sicherheitskonfiguration und sind potenziell mit ungenutzten Komponenten ausgestattet. Gerade diese ungenutzten und nicht konfigurierten Funktionalitäten werden häufig als Einfallstor von Angreifern missbraucht. Bei der Systemhärtung werden diese Funktionalitäten sowie deren Schnittstellen abgeschaltet bzw. eingeschränkt und eine starke Sicherheitskonfiguration eingerichtet. Das erhöht die Sicherheit der Systeme maßgeblich. Daher sollte die Systemhärtung 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 Systemen sind:

- Datenmanipulation von personenbezogenen Daten und sensiblen Unternehmensdaten
- Datenabfluss (z.B. Abzüge gesamter Datenbanken von Datenbanksystemen)
- Manipulation oder Sabotage von Betriebs- und Produktionsabläufen sowie Störung der Betriebsfunktionen (z.B. DDoS)
- Diebstahl von Identitäten (z.B. Übernahme von hochprivilegierten Konten bzw. Dienstkonten)
- Einbringung von Malware jeglicher Art und Verteilung der Malware zu anderen Systemen (inkl. Ransomware)
- Missbrauch der Systemkapazität für Prozesse des Angreifers (z.B. Crypto-Mining, Spamversand)
- Ausnutzung als Sprungsystem für Angreifer, um dann weitere Systeme anzugreifen (z.B. Lateral movement, supply chain attack)

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

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

1. Deaktivierung von Komponenten

    - Regelmäßige Überprüfung, ob aktivierte Dienste für den Betrieb noch notwendig sind
    - Deaktivierung oder Deinstallation von nicht notwendigen Betriebssystemkomponenten / Diensten inklusive Hintergrunddiensten
    - Deinstallation nicht benötigter Software
    - Deaktivierung von nicht notwendigen Autostart- oder zeitgesteuerten Prozessen
    - Deaktivierung von nicht benötigten, technisch veralteten oder als unsicher geltenden Schnittstellen oder Protokollen
    - Deaktivierung von Übertragungen (z.B. von Telemetriedaten), soweit sie nicht für ein zentrales Monitoring mit abgestimmter Richtlinie benötigt werden
    - Deaktivierung von ungenutzten Dateifreigaben
    - Deaktivierung bzw. Limitierung der Zugriffe auf administrative Webseiten
    - Ggf. Deaktivierung von nicht benötigten Ports oder anderen physischen Anschlüssen
    - Ggf. Deaktivierung bzw. Limitierung von nicht benötigten Accounts
    - Besondere Überwachung für Dual-Use Tools auf verdeckte Aktivitäten ("LOL-bins") - auch in der Cloud.

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", Control Flow Guard "CFG")
    - Aktivierung des BIOS-Zugriffspassworts, Limitierung der Bootreihenfolge auf die notwendigen Devices
    - Ggf. Aktivierung von Schutzverfahren gegen Seitenkanalangriffe
    - Ggf. 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 (z.B. Windows User Account Control)
    - Aktivierung des Malware-Schutzes auf dem System bereits beim Bootvorgang (Secure Boot)
    - 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
    - Absichern von Zugangspunkten für den Fernzugriff und Remote-Benutzern
    - Ggf. automatisiertes Einspielen von Patches und Updates
    - Sichere Konfiguration von Software (z.B. Deaktivierung von Makros bzw. JavaScript in Office-Anwendungen) und Browser
    - Spezielle Absicherung des Active Directory

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 / -zugänge

- Einschränkung des Zugriffs auf die Konfigurationsdateien des Betriebssystems
- Zugangsberechtigung zum physikalischen Server einschränken (insbesondere zur Vermeidung von Anschluss von unberechtigten externen Datenträgerlaufwerken)

5. Konten und Kennwörter

- Einsatz starker einheitlicher Kennwortrichtlinien für Benutzerpasswörter (z.B. Kennwortlänge, unterschiedliche Passwörter für alle Accounts, Komplexität, Sperrzähler, Änderungszyklus etc.) und Verwendung von 2-Faktor-Authentifizierung (siehe Kap. 3.2.1 - 3.2.3)
- 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
- Deaktivierung oder Umbenennung von Standard-Benutzerkonten
- Deaktivierung von lokalen Gast-Konten
- Sperre der Anmeldung von lokalen Benutzerkonten über das Netzwerk
- Deaktivieren von Standard-, Test- und anonymen Konten für alle installierten Services / Softwarekomponenten

6. Netzwerkkomponenten

- Einschränkungen bei den Netzwerkeinstellungen (z.B. TCP/IP-Konfiguration), Abschaltung von ungenutzten und unsicheren Netzwerkprotokollen (z.B. Telnet, FTP, HTTP, SSL)
- Deaktivierung von ungenutzten Netzwerk-Ports
- Unterbinden eines Versions-Downgrades beim Verbindungsaufbau ("handshake") (z.B. Downgrade von TLS 1.3 auf TLS 1.0)
- Beschränkung der über einen Dienst laufenden Verbindungen auf das erforderliche Minimum
- Ggf. Aktivierung von Paketfiltern / Firewall und deren Öffnung der minimal benötigten Zugänge

Für gängige Betriebssysteme sind detaillierte Härtungsrichtlinien im Internet öffentlich abrufbar:

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

Eine Großzahl der aufgeführten Härtungsmaßnahmen ist durch technische Einstellungen realisierbar. Dazu können beispielsweise Skripte verwendet werden, die die Härtung automatisiert auf den Systemen durchführen. Um eine automatische Verteilung der Härtungseinstellungen in Windows-basierten Infrastrukturen zu ermöglichen, können auch Gruppenrichtlinien zum Einsatz kommen. Bei der Härtung von bestehenden Systemen kann die Härtung zum Ausfall von Funktionalitäten führen, daher muss eine Datensicherung erstellt und die Härtung ausgiebig getestet werden.

Eine einmalige Systemhärtung ohne fortlaufende Erhaltung des Sicherheitsniveaus ist wirkungslos. Das kann insbesondere durch folgende Maßnahmen erreicht werden:

- BOM/DSL
- Changemanagement
- Problem- / Patchmanagement
- Releasemanagement

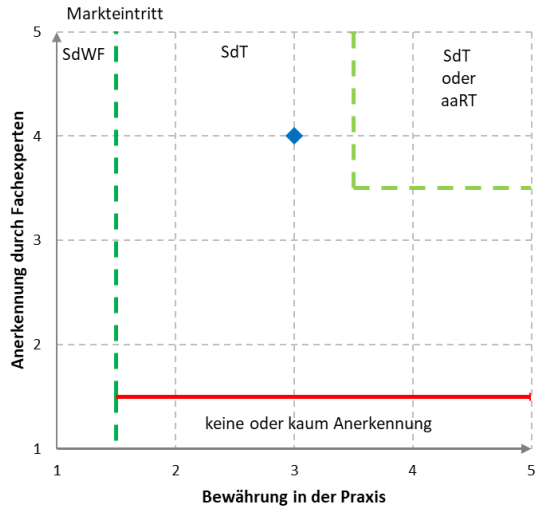
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.22 Endpoint Detection & Response Platform

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 Skripte
- 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 Betriebssystemgrenzen 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.

Mittels moderner Sensor-Architektur wird die signaturbasierte Gefahrenerkennung durch einen Detektionsansatz zur Anomalie-Erkennung ergänzt. Das bedeutet:

- Erkennung bekannter Malware über signaturbasierte Schutzkomponenten (sicherer, spart Rechenzeit),
- Signaturlose Erkennung und aktive Blockierung von Schadcode idealerweise durch supervised 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 Daten aus verschiedenen Quellen normalisiert und 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, Backdoor-Einrichtung, laterale Bewegung innerhalb der Organisation, Rechte-Eskalation etc.)
- Optional kann Threat Intelligence aufzeigen, wer der mutmaßliche Akteur/Gegner ist (Cybercrime oder nationalstaatlich motivierter Angriff) und welche Ziele und Branchen die Angreifer verfolgen.

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.

Neben der Erkennung von sicherheitsrelevanten Ereignissen stellen EDR-Lösungen Möglichkeiten für die manuelle und automatische Reaktion (Response) auf diese Gefahren, wie z.B. automatische Isolation des Geräts oder Deaktivierung von Benutzerkonten, bereit. Darüber hinaus gibt es Funktionen zur Unterstützung von Incident Response-Untersuchungen, wie z.B. Fernzugriffsmöglichkeiten oder die Bereitstellung zusätzlicher Daten mit der Bereitstellung von Triage-Paketen.

Darüber hinaus muss ergänzt werden, dass zu einer ganzheitlichen Absicherung von Endgeräten insbesondere die folgenden Punkte berücksichtigt werden sollten:

- Berechtigungen / Rollen (Stichwort: administrative Berechtigungen)
- Update-Mechanismen (Betriebssystem und Software)
- Einschränkungen / Kontrolle der installierten Software (Application Control)
- Verschlüsselung der Endgeräte
- 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 (Device Control)
- Einsatz von Authentisierungsverfahren (Username / Passwort, PIN, Biometrie, usw.)

Im Markt ist eine Weiterentwicklung zu Extended Detection and Response (XDR) Lösungen zu beobachten. Die Kombinationen reichen von Patch Management, Device Management, Backup-Tools, Verschlüsselung bis hin zu netzwerkbasierter Erkennung.

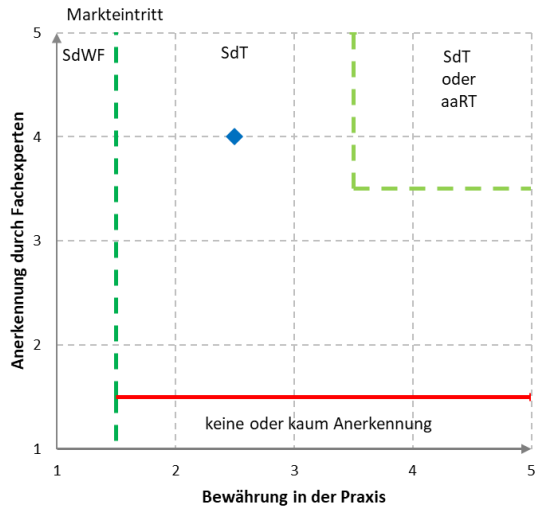
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.23 Web-Isolation der Internetnutzung

Web-Isolation separiert den Arbeitsplatz des Anwenders von den Browser-Sitzungen 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 beispielsweise 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.

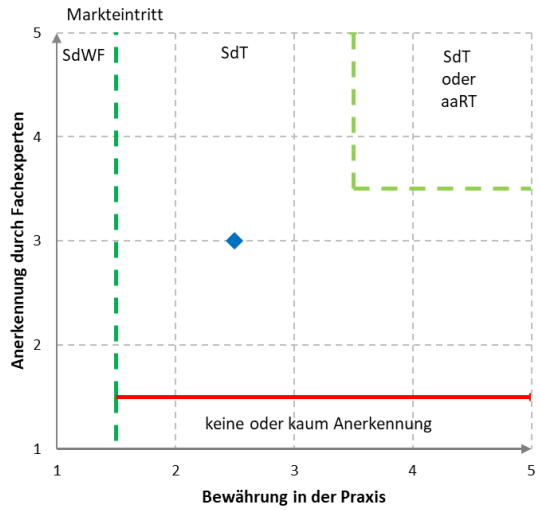
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

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.

Cloud-basierte 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 (EDR/XDR) mit seinen Schnittstellen zu Security Orchestration, Automation and Response (SOAR), User and Entity Behavior Analytics (UEBA), Netzwerk-Security Produkten wie Next-Generation Firewalls sowie integrierter Threat Intelligence eine sinnvolle Alternative darstellen.

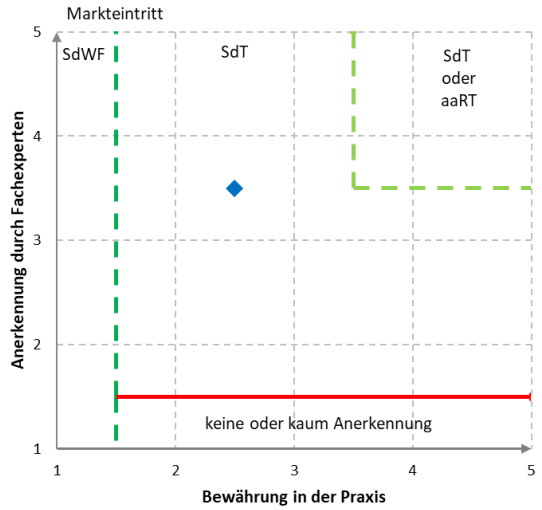
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.2.25 Vertrauliche Datenverarbeitung in der Cloud

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 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 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 (virtuelle Maschine, Applikation, oder Funktion), in dem die komplette Datenverarbeitung im unverschlüsselten Zustand stattfindet. Diese Abschirmung kann entweder direkt auf dem Prozessorchip der Server (hardware-basierte vertrauenswürdige Ausführungsumgebung) 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.

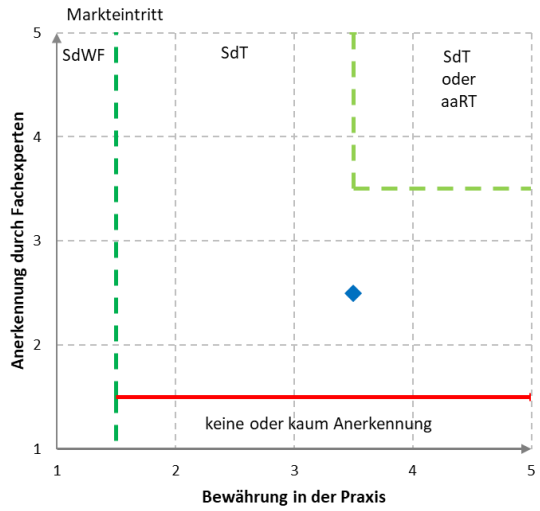
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

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, dann 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 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 Open Source 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.

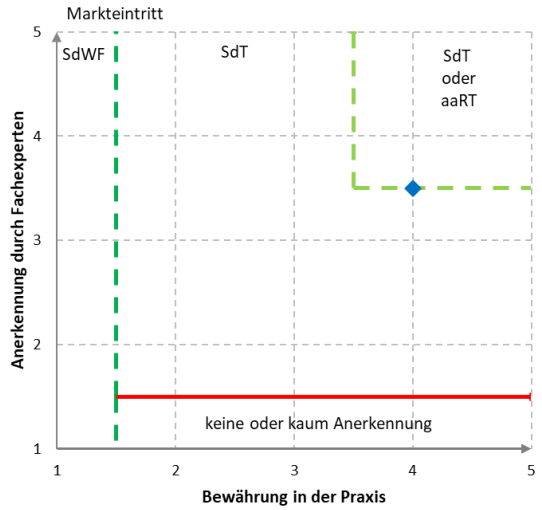
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

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, Cyber-Angriffe 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 Cyber-Sicherheitsmaßnahmen wie Vorfalls-Analysen, Incident Response und proaktives Threat Hunting umsetzen. Die Leistungsfähigkeit von Cyber-Sicherheitsmitarbeitern (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 Cyber-Sicherheit.

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

Cyber Threat Intelligence informiert über alle Arten von aktuellen und potenziellen Cyber-Bedrohungen 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 Cyber-Angriffen 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.

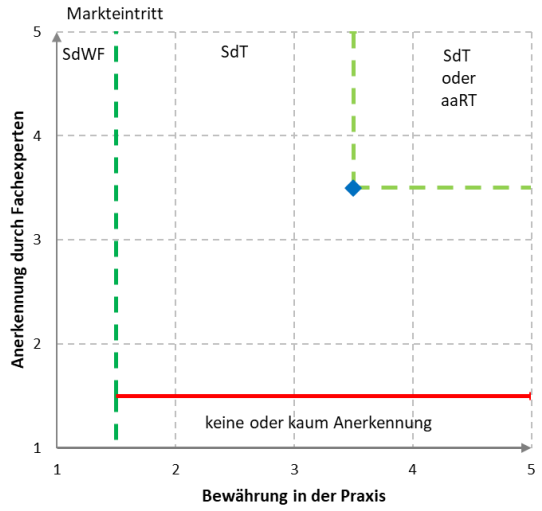
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.28 Absicherung administrativer IT-Systeme

Unter administrativen IT-Systemen werden Clients und Server verstanden, welche unter Nutzung von Management-Anwendungen weitere IT-Systeme verwalten und überwachen. Administrative IT-Systeme befinden sich - im Vergleich zu Standard-Arbeitsplätzen - zumeist in dedizierten Netzwerksegmenten, in denen zusätzliche Netzwerkprotokolle verwendet werden und von welchen die administrativen Schnittstellen von Systemen erreichbar sind. Auf Grund dieser speziellen Verwendung von administrativen IT-Systemen geht von diesen Systemen ein Risiko mit großem Schadenspotenzial aus (z.B. beim Zugriff durch Unbefugte). Daher müssen dem Risiko angemessene Regelungen und Maßnahmen zum Schutz vor unbefugten Zugriffen sowie zur Wahrung einer sicheren IT-System-Administration - insbesondere in Bezug auf den Schutz der auf den Systemen verwendeten privilegierten Accounts sowie den erforderlichen Verbindungen - getroffen werden.

Anforderungen an administrative IT-Systeme

Administrative IT-Systeme sind gemäß der Maßnahme Systemhärtung (siehe Kapitel 3.2.21) abzusichern.

Für die Verwendung und den Umgang mit administrativen IT-Systemen sowie für deren Schutz müssen Regelungen und Maßnahmen festgelegt werden. Vor einer Gewährung eines Zugriffs für einen Benutzer muss dieser zuerst diese Regelungen akzeptieren und sich verpflichten, diese einzuhalten. Ein Verstoß gegen die definierten Regelungen muss aufgeklärt werden und Konsequenzen nach sich ziehen. Ein Zugriff auf administrative IT-Systeme darf nur von qualifizierten Mitarbeitern erfolgen bzw. für diese freigegeben werden. Administrative IT-Systeme sind dediziert nur für die Administration von Systemen zu verwenden und sind entsprechend ihres Schutzbedarfs mit Härtungsmaßnahmen und starken Authentifizierungsmethoden abzusichern. Ihre Schutzanforderungen müssen ermittelt und durch geeignete Maßnahmen geschützt werden.

Der Zugang zu administrativen IT-Systemen darf nur für berechtigte Administratoren nach einer erfolgreichen Authentifizierung über ein sicheres Anmeldeverfahren möglich sein. Hierzu ist ein geeignetes Authentifizierungsverfahren zur Identifikation des Benutzers erforderlich, welches dem Schutzbedarf des zu administrierenden Systems entspricht (z.B. Multi-Faktor-Authentifizierung, vgl. Kap. 3.2.3). Bei der Eingabe von Zugangsdaten wie beispielsweise Passwörtern oder PINs dürfen diese Daten vom System nicht angezeigt werden. Bei Anmeldungen auf administrativen IT-Systemen über das Netzwerk müssen die Daten zur Authentifizierung des Benutzers unter der Verwendung von sicheren Protokollen verschlüsselt übertragen werden. Inaktive Remote-Sitzungen müssen nach einer definierten Zeitdauer automatisch abgemeldet / beendet werden.

Ist für die Administration eine Verbindung in ein Netzwerksegment mit Systemen mit einem hohen oder sehr hohen Schutzbedarf erforderlich (z.B. in ein Netzwerksegment mit SCADA / ICS-Systemen), muss die Administration bzw. die Netzwerkverbindung über einen Sprungserver / Proxyserver in einer DMZ zwischen diesen Netzwerksegmenten erfolgen.

Für administrative IT-Systeme muss es Mindeststandards für Passwörter geben. Diese Systeme sind zudem in Autorisierungssysteme nach Stand der Technik einzubinden, wobei die Anbindung und das Autorisierungssystem selbst besonders zu sichern / härten sind. Des Weiteren sind personalisierte Accounts zu verwenden, welche einer Person eindeutig zugeordnet werden können. Standardbenutzer und -Kennwörter dürfen nicht verwendet werden.

Es muss sichergestellt sein, dass nur zulässige Softwarekomponenten, Programme und Skripte auf administrativen IT-Systemen ausgeführt werden. Ist eine Ergänzung von Softwarekomponenten, Programmen oder Skripten erforderlich, muss vor dessen Verwendung eine Freigabe im Rahmen eines entsprechenden Prozesses erfolgen und der Einsatz ist zu dokumentieren und zu überwachen.

Auf administrative IT-Systemen sind die Anmeldevorgänge und Tätigkeiten der Administratoren zu protokollieren, damit nachvollzogen werden kann, welche Tätigkeiten durch welche Personen (Accounts) durchgeführt wurden. Um die Nachweisbarkeit der durchgeführten Tätigkeiten sicherzustellen, dürfen Administratoren die Log- und Auditprotokolle über ihre eigenen Tätigkeiten nicht mit deren Accounts ändern oder löschen. Für kritische Administrationstätigkeiten sollte das Mehraugenprinzip zur Anwendung kommen.

Für die Etablierung werden exemplarisch folgende Maßnahmen für einen angemessenen Schutz empfohlen:

- ISO/IEC 27002
  Der Standard enthält Empfehlungen zur Umsetzung der in ISO/IEC 27001 Anhang A geforderten Maßnahmen für die Zugriffskontrolle sowie für die Betriebssicherheit von Systemen, die auch für administrative IT-Systeme gelten. Wird eine Zertifizierung gemäß ISO/IEC 27001 angestrebt, sind diese Maßnahmen im Geltungsbereich des ISMS umzusetzen. Umsetzungshinweise für diese Maßnahme finden sich vor allem in den Abschnitten 9 "Zugriffskontrolle" und 12 "Betriebssicherheit".
- BSI IT-Grundschutz-Kompendium
  Das BSI IT-Grundschutz-Kompendium beschreibt in seinen Bausteinen SYS.1, SYS.2 und IND.1 zahlreiche Maßnahmen zum Schutz von Systemen. Diese Bausteine sind auch für administrative IT-Systeme relevant und anzuwenden. Die Umsetzung der für einen hohen oder sehr hohen Schutzbedarf aufgeführten Anforderungen in den Bausteinen wird empfohlen.
- BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
  Im BDEW Whitepaper finden sich unterstützende Hinweise für die Absicherung von administrativen IT-Systemen, wie z.B. die Verwendung sicherer Protokolle und Sprungserver für den (Fern-)Zugriff sowie die Platzierung der Systeme in dedizierten Netzwerkzonen.

Die Vorgaben zur Betriebssicherheit und zum Zugriffsschutz administrativer IT-Systeme sind periodisch (mindestens jährlich) auf Vollständigkeit und Angemessenheit zu prüfen und in Abhängigkeit mit einer Zugriffs- bzw. Zugangskontrollrichtlinie zu aktualisieren.

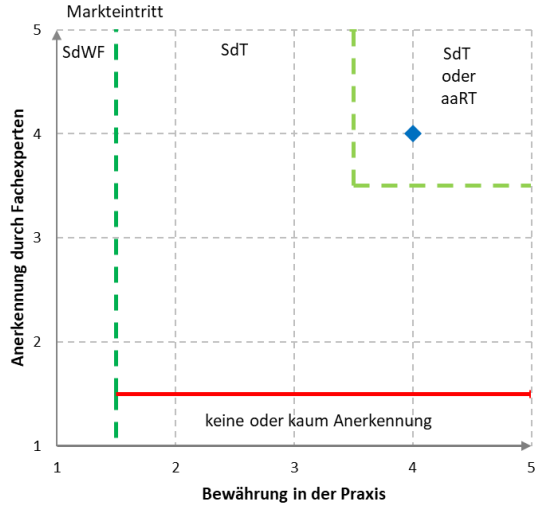
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.29 Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung

Ein großer Anteil schwerwiegender Cyber-Angriffe durch staatlich motivierte Akteure und Cyber-Kriminelle involviert Verzeichnisdienste und Benutzerkonten. Dazu zählen komplexe Angriffe über die Lieferkette und in deren Folge Spionage und Sabotage. Für Unternehmen und Organisationen ist es daher unerlässlich, ihre Angriffsfläche zu reduzieren, unnötige Risiken frühzeitig zu erkennen und zu vermeiden. Angriffsversuche und ungewöhnliche Zugriffe sollen bereits in der Entstehung erkannt und in Echtzeit eingedämmt werden - selbst dann, wenn der Angreifer erbeutete, valide Zugangsdaten verwendet und Endpoint Protection und IPS-Systeme versagen.

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

- Angriffe, die erbeutete / 'geleakte' Benutzernamen und Passwörter ausnutzen (z.B. aus einem Breach im Darkweb gehandelte Zugangsdaten) und keine Malware-Komponente involvieren
- Ausnutzung von Schwachstellen in Verzeichnisdiensten (unzureichend geschützte Service Accounts)
- Ausbreitung und Bewegung eines Angreifers in der Organisation (Lateral Movement)
- Kompromittierung und Missbrauch von privilegierten Konten und Rechteerweiterung

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

Assessment / Audit von Verzeichnisdiensten: Moderne Schutzlösungen kombinieren den Hygiene-Status von Verzeichnisdiensten wie Microsoft Active Directory, Microsoft Entra ID und anderen "Identity as a Service"-Lösungen, um Schwachstellen prophylaktisch zu behandeln und Risikoprofile zu erstellen. Dazu zählen:

- Erkennung schlecht geschützter Service Accounts
- Identifizierung von versteckten Privilegien die über eine Gruppenmitgliedschaft hinaus gehen, wie Delegation oder Missbrauch privilegierter SIDs,
- Erkennung von Angriffspfaden zu privilegierten Konten die typischerweise nur im Rahmen aufwändiger Audits (z.B. über Tools wie SharpHound / Bloodhound) aufgedeckt werden
- Bedrohungsmonitoring mit Darknet-Überwachung

Echtzeitüberwachung und Analyse aller relevanten Authentifizierungsverkehre, sowohl Lokal, wie Kerberos, NTLM, LDAP, RDP, RPC etc., sowie aus Cloud-basierten IDaaS und Federation Services um bereits Angriffsversuche oder die Verwendung von sogenannten Reconnaissance Tools zu erkennen und dem Security Operation Center umfassend und angereichert dazustellen. Durch die Integration mit Cloud-basierten Diensten lassen sich auch Geo-Lokationsbedingte Anomalien erfassen und Abweichungen der normalen Nutzung erkennen.

Aus dem individuellen Schutzbedarf der jeweiligen Organisation kann dann unter Berücksichtigung der Risikoprofile ein identitätsbezogenes Regelwerk umgesetzt werden, welches z.B. verhindert, dass Nutzerkonten mit einem schlechten Risiko-Scoring auf kritische Anwendungen oder auch lokale kritische Ressourcen zugreifen können. Ebenso sollte es möglich sein, auf ungewöhnliches Benutzerverhalten automatisch zu reagieren und Maßnahmen wie z.B. die Abfrage eines weiteren Authentifizierungsfaktors (MFA) zu fordern. Somit wird ein Schutz ermöglicht, der den Focus von spezialisierten klassischen Lösungen wie Privileged Access Management (PAM) mit dem von User & Entity Behaviour Analytics vereint und gleichzeitig einfach in der Praxis anzuwenden ist, z.B. durch das Ausbringen einer Sensor-Applikation in die Verzeichnisserver, sowie der API-basierten Integration in Fedaration-Services und Cloud-Verzeichnisdienste. Die Anwendung von Machine-Learning-Modellen reduziert den Aufwand hier deutlich.[17]

Die konsequente Segmentierung von Identitäten innerhalb von Identitätsprovidern - etwa im weit verbreiteten Verzeichnisdienst Microsoft Active Directory - stellt eine wirksame Maßnahme zur Verhinderung von Lateral Movement über Bereichsgrenzen hinweg dar. Hierbei werden sämtliche Identitäten sowie deren zugehörige Ressourcen (z.B. Benutzergruppen oder Computerkonten) in logisch voneinander getrennte Schichten innerhalb des Identitätsproviders organisiert und strikt voneinander abgegrenzt. Im Falle einer Kompromittierung ist der Zugriff eines Angreifers auf die Identitäten innerhalb einer einzelnen Schicht zwar nicht auszuschließen, ein Übergreifen auf andere Schichten wird jedoch durch die Segmentierung unterbunden. Dadurch bleiben nicht betroffene Bereiche geschützt und das Risiko einer vollständigen Kompromittierung des Identitätssystems wird signifikant reduziert. Dieser Ansatz orientiert sich konzeptionell an der Netzwerksegmentierung - jedoch erfolgt die Abgrenzung nicht physisch, sondern logisch innerhalb des Identitätsspeichers. Ergänzend sind entsprechende Richtlinien zu definieren und durchzusetzen, die einen Übergang zwischen den Schichten verhindern. Die Umsetzung dieses Prinzips ist in der Praxis häufig unter den Begriffen "Tier-Model" oder in erweiterter Form als "Plane-Model" bekannt und Microsoft bezeichnet es auch als "Enterprise access model" (EAM).

Anmerkung: Alle o.g. Teilbereiche stellen wichtige Bausteine dar und tragen aktiv zur Umsetzung eines Zero Trust Framework bei. Es lassen sich wirksam Zugriffsrechte umsetzen, auch ohne, oder in

[17] Siehe auch Kapitel 3.2.1 Authentisierung, 3.2.3 Multifaktor-Authentifizierung und 3.2.24 Angriffserkennung und Auswertung (SIEM)

Ergänzung netzwerkseitiger Beschränkungen (Firewalls). Zu beachten ist hier auch der Datenschutzaspekt, insbesondere wenn es um die Analyse von Benutzeraktivitäten geht.

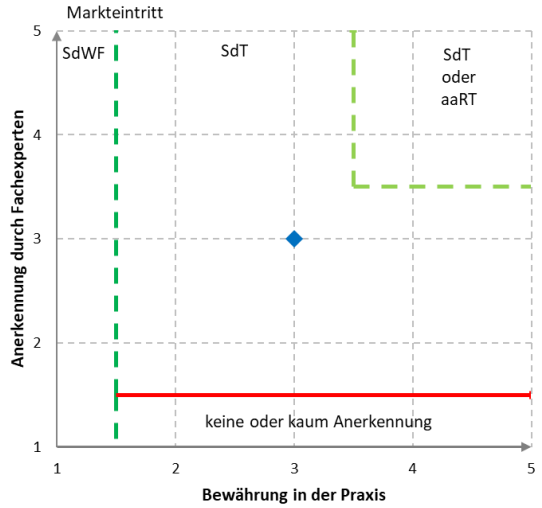
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.30 Netzwerksegmentierung und Separierung

Die Aufteilung von Netzwerken durch Netzwerksegmentierung und -separierung ist eine effektive Maßnahme zur Reduktion von Bedrohungen gegen die Verfügbarkeit, Vertraulichkeit und Integrität von Netzwerken sowie darin enthaltener Systeme. Die Segmentierung und Separierung unterstützen auch die Absicherung im Rahmen des Defense-in-Depth-Ansatzes.

Bei der Netzwerksegmentierung wird ein Netzwerk in mehrere Segmente unterteilt, von denen jedes als eigenes Teilnetzwerk fungiert. Die Kommunikation zwischen diesen Segmenten erfolgt eingeschränkt über definierte Zonengrenzen (Boundary Protections) mit einer Prüfung / Überwachung der Netzwerkverbindungen. Durch Zonengrenzen zwischen Netzwerken wie beispielsweise zwischen der Informationstechnologie (IT) und der Operational Technologie (OT) werden viele mit dem IT-Netzwerk verbundene Risiken, wie z.B. Bedrohungen durch Schadsoftware, verringert. Die Zonentrennung bzw. Segmentierung schränkt den Zugriff auf Systeme, Daten und Anwendungen ein und begrenzt die Kommunikation zwischen den Netzwerken. Durch diesen Ansatz werden Segmente im Netzwerk vor Angriffen aus anderen, bereits betroffenen Segmenten geschützt.

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

- Laterale Bewegung von Angreifern im Netzwerk (Network Lateral Movement)
- Ungehinderte Verbreitung von Schadsoftware in Netzwerken
- Bedrohungen durch Insider (z.B. der unberechtigte Zugriff auf Systeme aus anderen Abteilungen oder Standorten).
- Unzulässiger oder böswilliger Datenverkehr ist auf Grund von Netzwerkgrößen und Datenmengen u.U. schwieriger zu identifizieren
- Ausnutzung von Zugangsmöglichkeiten zu vernetzten IT-Systemen
- Verlust der Verfügbarkeit, Integrität und Vertraulichkeit von einer großen Anzahl von Systemen, wenn diese in einem flachen Netzwerk betrieben werden und kompromittiert sind

- Verlust der Verfügbarkeit kritischer Systeme im Netzwerk durch Angriffe auf unkritische Systeme, welche weniger Sicherheitsmaßnahmen aufweisen

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

Für eine Netzwerksegmentierung ist ein Netzwerk in mehrere so genannte Netzwerkzonen (oder auch Teilnetzwerke) zu unterteilen, wobei eine Netzwerkzone eine logische Gruppe von Geräten, Anwendungen und Systemen mit gemeinsamen Sicherheitsanforderungen (gleichem Schutzbedarf) bildet. Die Verwendung von kritischen und unkritischen Systemen in einer Netzwerkzone, auch wenn diese thematisch in einer Gruppe zusammengefasst werden können oder eine hohe Kommunikation miteinander aufweisen, ist unzulässig.

Die Trennung der Netzwerkzonen kann logisch (z.B. durch VLANs) und/oder physisch (z.B. durch eine dedizierte Switch-Infrastruktur für die Zone) erfolgen. Die Entscheidung, ob eine physische Trennung erforderlich ist, muss entweder aufgrund regulatorischer Vorgaben oder mit einem risikobasierten Ansatz erfolgen.

Jeglicher Datenverkehr zwischen verschiedenen Netzwerkzone hat über definierte und angemessene Zonenübergänge zu erfolgen und ist vorab freizugeben. Bei Zonenübergängen ist eine Einschränkung, Kontrolle und Überwachung des Netzwerkverkehrs mit z.B. Firewalls / IPS / ACL zu implementieren. Mechanismen zur Erkennung von sicherheitsrelevanten Ereignissen im Netzwerkverkehr (z.B. Firewall / IPS, Logging auf Netzwerkgeräten und Sensoren / IDS) sind risikobasiert zu implementieren und können beispielsweise durch ein SIEM analysiert und bewertet werden.

Bei Zonenübergängen ist ein Whitelisting-Ansatz anzuwenden. Jeglicher Datenverkehr wird standardmäßig blockiert und nur definierter Datenverkehr wird erlaubt (deny by default, allow by exception). Netzwerkverbindungen zwischen Systemen in verschiedenen Netzwerkzonen (insbesondere mit unterschiedlichem Schutzbedarf) sind auf das notwendige Minimum zu beschränken und es sind bei Erfordernis eigene Übergabeschnittstellen in separaten Zonen (z.B. DMZ) zu implementieren.

Für eine Netzwerksegmentierung ist eine Architektur nach dem Defense-in-Depth Prinzip zu planen und umzusetzen. Hierfür sind Zonen für externe oder nicht vertrauenswürdige Netze (z.B. Internet oder Besucher-WLANs), Zonen für DMZ-Systeme (z.B. Proxy-Systeme oder Sprungserver für externe Zugriffe) und Zonen für interne Systeme (z.B. Server, Clients, Drucker etc.) vorzusehen. Für zu isolierende Systeme (z.B. Systeme ohne Sicherheitsupdates / Wartung) sind eigene Zonen vorzusehen. Industrielle Netzwerke, iSCSI / Storage-Netzwerke und IT-Netzwerke sind grundsätzlich physisch voneinander zu separieren.

Jeglicher Netzwerkwerkverkehr mit Drittnetzen (z.B. Internet für den Download von Updates, Fernzugriff von externen Dienstleistern) ist durch Proxys, Sprungserver, VDI-Umgebungen usw. in einer DMZ-Zone zu terminieren und der Netzwerkverkehr zu prüfen. Eine direkte Kommunikation von Drittnetzen zu internen Netzwerkzonen ist nicht zulässig.

Für die einzelnen Zonen sind je nach Schutzbedarf und Kritikalität erforderliche Schutz- / Härtungsmaßnahmen zu definieren und umzusetzen.

Abgesehen von aktiven Netzwerkgeräten sollte sich jedes System logisch nur in einer Zone befinden. Ein Routing von Netzwerkverkehr auf Hosts / VMs zwischen Netzwerkadaptern oder die Platzierung von Systemen in mehreren Netzwerken (Multihoming) muss grundsätzlich vermieden werden und darf nur in freigegebenen und dokumentieren Situationen nach einer zuvor durchgeführten Risikoanalyse und mit erforderlichen Schutzmaßnahmen und Zonenübergängen erfolgen, um keine unkontrollierten Übergänge zwischen Zonen zu schaffen. Des Weiteren sollte Split-Tunneling für entfernte Geräte, die eine Verbindung zu Unternehmenssystemen herstellen, verhindert werden. Durch Split-Tunneling kann eine entfernte Person oder ein Gerät eine Verbindung zu einem sicheren Netzwerk herstellen und gleichzeitig über eine andere Verbindung mit einer Ressource in einem externen / unsicheren Netzwerk kommunizieren. Ausnahmen, in denen ein Split-Tunneling beabsichtigt ist wie beispielsweise für Videokonferenzlösungen, die ohne Tunnel auf zentrale Cloud-Systeme zugreifen dürfen, müssen definiert werden.

Für administrative Systeme sind dedizierte Netzwerke vorzusehen, welche nur für die Administration verwendet werden dürfen. Ein administrativer Zugriff auf Out-Of-Band-Netzwerke auf Management-Interfaces von Servern, Netzwerkgeräten oder KVM-Systemen darf nur von Netzwerken für administrative Systeme möglich sein.

In Verbindung mit dem Zero-Trust-Prinzip wird zunehmend die sogenannte Mikro-Segmentierung eingesetzt. Hier wird die Angriffsfläche reduziert, indem das Netzwerk in Segmente aufgeteilt wird, die zur Ausführung einer Anwendung benötigt werden (z.B. virtuelle Maschinen, Container, Dienste).

Für die Umsetzung der Maßnahme werden nachfolgende Standards empfohlen:

- **BSI IT-Grundschutz-Kompendium**
  Das BSI IT-Grundschutz-Kompendium beschreibt im Baustein NET.1.1 "Netzarchitektur und -design" Anforderungen für die Spezifikation, Planung, Umsetzung und Prüfung von Netzwerksegmentierungen sowie zur Absicherung der über die Zonen stattfindenden Netzwerkkommunikationsverbindungen.
- **ISO/IEC 27002:2022**
  Der Standard ISO/IEC 27002 enthält Empfehlungen zur Umsetzung von Maßnahmen im Bereich Netzwerksicherheit (Control 8.20), Sicherheit von Netzwerk-Services (Control 8.21) sowie zur Trennung von Netzwerken (Control 8.22).
- **IEC 62443-3-3**
  Der Standard IEC 62443-3-3 enthält Vorgaben zur Netzwerksegmentierung sowie zur Kontrolle von Netzwerkzonenübergängen in industriellen Kommunikationsnetzwerken im FR 5 "Restricted Data Flow".

Periodisch und anlassbezogen sind Audits durchzuführen, um zu prüfen, ob die bestehenden Netzwerke und Netzwerksegmente den definierten Vorgaben und Regelungen sowie der aktuellen Dokumentation entsprechen.

Die dokumentierten und für den Betrieb wesentlichen Richtlinien, Verfahren und Kontrollmaßnahmen zur Netzwerktrennung sind periodisch auf Vollständigkeit, Wirksamkeit, Angemessenheit und auch auf geänderte Rahmenbedingungen zu prüfen und gegebenenfalls zu aktualisieren.

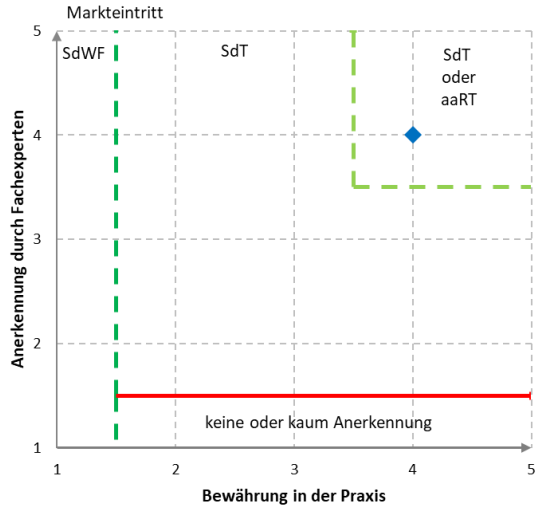
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.31 Cloud-Sicherheitsplattform

Eine Cloud-Sicherheitsplattform ist eine technische Maßnahme, welche die Risiken und Bedrohungen in der Erstellung und dem Betrieb von Infrastruktur und Applikationen bei Cloud Service Providern abdeckt. Sie wird häufig auch als CNAPP (Cloud Native Application Protection Platform) bezeichnet und fasst Einzelbereiche wie Container-Scanning, Cloud Workload Protection (CWP / CWPP), Cloud Security Posture & Compliance sowie die Sicherheit von aktiven Workloads zusammen, die damit eine holistische Sicht auf die Cloud-Sicherheit ermöglichen. Cloud-Sicherheitsplattformen können die Betriebsaufwände senken und ermöglichen durch die automatische Verknüpfung sonst isolierter Sicherheitsinformationen eine schnellere und akkurate Erkennung und Behandlung von Sicherheitsvorfällen und deren Behebung.

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

- Fehlkonfigurationen in Cloud-Infrastrukturkomponenten und deren Konfiguration werden fortlaufend überwacht. Einstellungen und Eigenschaften, welche nicht den Empfehlungen anerkannter Security "best practices", wie CIS-Benchmark, oder auch Compliance Frameworks wie ISO27001, SOC2 etc. sowie eigenen definierten Anforderungen entsprechen, werden ausgewertet und die Verantwortlichen entsprechend alarmiert. Hierzu zählt auch die Analyse von Infrastructure as Code (IaC). Infrastructure as Code können z.B. Terraform HCL, Cloud Formation, CDK, Docker Files, Kubernetes Manifests sein
- Schwachstellen (Vulnerability Management): Verwundbarkeiten in Applikationen in allen Phasen des Development Lifecycle von der Entwicklung, in Testing / Staging bis hin zur Produktion mit Priorisierung durch Erkennung aktiver Pakete und Images durch Laufzeitüberwachung
- Schädliche Eingriffe in Cloud Provider Accounts durch unberechtigte Dritte und Angriffe, Erkennung durch UEBA - User & Entity Behavior Analytics. Dies geschieht durch fortlaufende Analyse von Cloud Audit Logs, Kubernetes Activity Logs auf bekannte und bislang unbekannte Angriffsaktivitäten - ohne konkretes Vorwissen zum Angriffsvektor (Verwundbarkeit, Pattern, IoC)
- Fehlkonfiguration und Überwachung der Sicherheitseigenschaften von Serverless Functions, Containern, Container Orchestration und Virtuelle Maschinen behandelt - vor und während der Ausführung (CWPP)
- Unnötig hohe Berechtigungen (CIEM) durch Darstellung und Auflösung von komplexen Berechtigungsketten von Konten und Ressourcen.

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

Eine Cloud-Sicherheitsplattform deckt den gesamten Lebenszyklus von Cloud-Anwendungen von der Entwicklung der Applikationen, über die Provisionierung bis hin zur Laufzeit in der Produktion ab. Somit ist es möglich, Schwachstellen und Fehlkonfigurationen bereits vor der Inbetriebnahme zu entdecken und Entwicklern, sowie DevOps-Teams Hilfestellung zu bieten und dadurch unnötige und inakzeptable Risiken zu vermeiden. Gleichzeitig wird die Übereinstimmung mit den für den Anwender relevanten Compliance Frameworks geprüft. Die Prüfung kann durch die Integration von Scannern innerhalb der Software Pipelines erfolgen und es werden auch entsprechende Policy-Enforcements auf der Ausführungsebene (z.B. Kubernetes Admission Controller) umgesetzt.

In der Produktion wird durch Sensoren auf den Compute-Instanzen und Kubernetes Worker-Nodes die kontinuierliche Überwachung der sicherheitsrelevanten Workload und Netzwerkverbindungen sichergestellt, um Angriffsversuche oder schädliche Aktivitäten frühzeitig zu erkennen. Machine-Learning-basierte Verfahren können die Sicherheitsteams entlasten, da die Erstellung und fortlaufende Anpassung von Regelwerken weitgehend entfällt und Angriffe auch ohne konkretes Vorwissen (Verhalten / Datei-Hashes / IP-Adressen etc.) erkannt werden. Diese Vorfälle werden kontextuell angereichert. Dies ermöglicht eine bessere Klassifizierung, Bewertung oder Priorisierung. Sensoren, in Form von Agenten auf den jeweiligen Hostsystemen im eigenen Rechenzentrum unterstützen hybride Architekturen und Cloud-Migrationsprojekte. Agentenlose Maßnahmen komplettieren den Schutz in Umgebungen, in denen ein Agent nicht eingesetzt werden kann. Anforderungen wie Host Intrusion Detection, File Integrity Monitoring, Malware Scanning und die Erkennung von Secrets (wie SSH Keys) oder der Erkennung möglicher Angriffspfade gehören zu wichtigen Grundfunktionen und stellen selbst wichtige Maßnahmen zur Erfüllung von Compliance-Anforderungen dar.

Eine vom Cloud-Infrastrukturbetreiber unabhängige Cloud-Sicherheitsplattform ermöglicht die Absicherung von Multi-Cloud-Architekturen. Gleichzeitig verhindert die Unabhängigkeit von Cloud-providerspezifischen Werkzeugen einen sogenannten "Vendor-Lock In", also die technologische Abhängigkeit von

einem bestimmten Cloud Service Provider. Die nahtlose Integration in vorhandene Arbeitsabläufe und Werkzeuge (z.B. Ticketing, Alerting etc.) ermöglicht eine interdisziplinäre und sowohl team- als auch projektübergreifende Kooperation.

Zusammenfassend sind die empfohlenen Maßnahmen einer Cloud-Sicherheitsplattform mindestens:

- Prüfung von Infrastructure-as-Code vor der Bereitstellung von Ressourcen (Compliance, Fehlkonfigurationen (IaC / Code Security)
- Compliance-Prüfung und Erkennung von Fehlkonfigurationen in Cloud (CSPM) und Kubernetes (KSPM) Ressourcen gegen relevante Compliance und Recommended Best Practices Frameworks
- Priorisierte Schwachstellenanalyse von der Entwicklung bis zur Laufzeit (Vulnerability Management)
- Darstellung von möglichen Angriffspfaden, Verkettung von Schwachstellen, Berechtigungsschlüssel und Fehlkonfigurationen (CASM)
- Inventarisierung von Cloud-Infrastrukturkomponenten
- Prüfung von Berechtigungen (CIEM)
- Verhaltensanalyse und frühzeitige Erkennung schädlicher Aktivitäten innerhalb von Cloud Accounts (UEBA)
- Unmittelbare Erkennung von schädlichen Aktivitäten durch Sensorik innerhalb aktiver Workloads, inkl. Malwareerkennung und File Integrity Monitoring (CWPP)

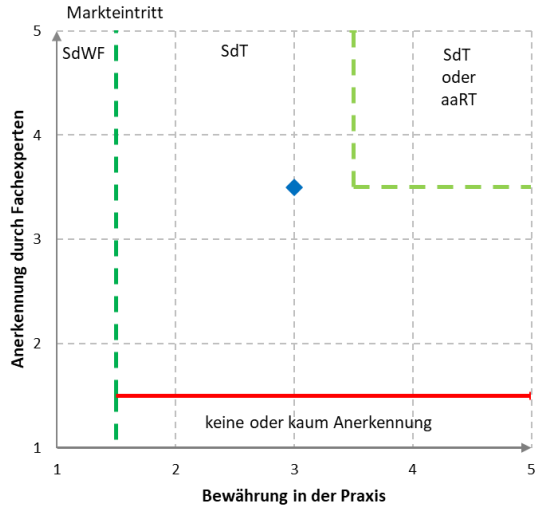
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.32 Tokenisierung

Bei Tokenisierung handelt es sich um eine Methode der Datenpseudonymisierung, welche alternativ zur Verschlüsselung eingesetzt werden kann. Hierbei wird einem Originalwert ein zufällig generierter Ersatzwert zugewiesen und beide Werte werden (verschlüsselt) als Verknüpfung in einer Mapping-Table abgelegt, um bei Bedarf den Originalwert wiederherzustellen.

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

- Bruch der Vertraulichkeit von (hoch-)sensiblen Daten, wie z.B. Kundendaten, Mitarbeiterdaten, oder Daten aus Produktion oder Entwicklung (z.B. ggü. Administratoren und Softwareentwicklern, die keinen Zugriff auf Produktivdaten haben dürfen)
- Laut der EU-Datenschutz-Grundverordnung (DSGVO) minimiert Pseudonymisierung das Risiko, dass personenbezogene Daten in die falschen Hände geraten. Dies gilt insbesondere bei unbefugtem Zugriff oder Nutzung. Tokenisierung als spezifisches Pseudonymisierungsverfahren schützt hochsensible Daten in Cloud-basierten Umgebungen und während der Übermittlung.

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

Tokenisierung beschreibt ein Verfahren zur Datenpseudonymisierung, welches sich durch die Fähigkeit auszeichnet, das Format der Zielwerte zu erhalten. Deshalb bietet es sich insbesondere zur Generierung von Testdaten oder zum Schutz von Daten in Cloud-basierten Applikationen (s. auch Kap. 3.2.11, Cloud-basierter Datenaustausch) an.

Meistens erfolgt Tokenisierung komplementär zur Verschlüsselung, da sie dieser nicht per se überlegen ist, aber dennoch einige Vorteile bietet:

1. Formaterhaltung: Der generierte Ersatzwert muss einem vorab definierten Format entsprechen, sodass Feldvalidierungen weiterhin erfolgreich sind, z.B. für E-Mail-Adressen oder Bankverbindungen.
2. Statistische Verteilung: Die statistische Verteilung der generierten Ersatzwerte entspricht im Standard der der Originalwerte, was z.B. bei statistischen Erhebungen von Vorteil sein kann (man denke an Postleitzahlen, Blutwerte etc.). Ein Tool zur Tokenisierung sollte jedoch für maximale Flexibilität die Möglichkeit zur Konfiguration dieses Verhaltens bieten.
3. Mathematische Unabhängigkeit: Da, anders als bei Algorithmus-basierter Verschlüsselung, keine mathematische Berechnung Originalwert und Ersatzwert verbindet, sondern nur die Mapping-Table Kenntnis dieser Beziehung hat, kann Tokenisierung erschwert überwunden werden, solange die Token-Datenbank vertraulich bleibt. Gemäß der Empfehlung des Europäischen Datenschutzausschusses müssen technische und organisatorische Maßnahmen implementiert werden, um sicherzustellen, dass die Zuordnung von Token zu Originaldaten nur durch autorisierte Parteien möglich ist. Zusätzlich wird daher empfohlen, ein HSM zu verwenden, um die Originalwerte in der Mapping-Tabelle zu verschlüsseln.

Jedoch bietet Tokenisierung auch Nachteile gegenüber der Datenverschlüsselung:

1. Um die Performance während der Verarbeitung zu erhalten, wird eine entsprechende Rechenleistung benötigt. Für große Datenmengen ist daher eine Algorithmus-basierte Verschlüsselung oft die bessere Wahl.
2. Es muss ein sog. Token Vault angelegt werden, in dem die Originalwerte neben den Ersatzwerten sicher und verschlüsselt abgelegt werden. Hierbei können größere Datenmengen anfallen, welche entsprechende Speicherkapazitäten erfordern.
3. Der Token-Raum ist endlich: Je strikter die Anforderungen an das Format der Ersatzwerte, desto kleiner die mögliche Menge an zu generierenden Ersatzwerten.
4. Ein weiterer Aspekt ist, dass pseudonymisierte Daten weiterhin als personenbezogen gelten, wenn zusätzliche Informationen für eine Rückführung verfügbar sind. Daher müssen diese Informationen besonders geschützt und getrennt aufbewahrt werden.

Tokenisierung ist bei allen Vorteilen kein Selbstzweck: Im Vordergrund steht der Schutz der Daten, weshalb Software-Lösungen zur Tokenisierung folgende Convenience-Features mitbringen sollten:

1. Unabhängige Lösung: es sind keine Änderungen an den Zielanwendungen erforderlich, in denen die tokenisierten Daten liegen.
2. Möglichkeit zur Tokenisierung von Einzelwerten in Dateien, Datenbanken, sowie in Webanwendungen, zusätzlich zur Basisfunktionalität, welche Tokens mittels moderner Schnittstellen zur Verfügung stellt.

3. Verfügbarkeit von komplexen Token-Profilen wie z.B. dem Luhn-Algorithmus zur korrekten Erzeugung von Kreditkartennummern, oder der Möglichkeit, aussprechbare Zeichenketten als Ersatzwert zu generieren.

Möglichkeit zur selektiven Tokenisierung, sodass Felder wahlweise geschützt oder im Klartext beibehalten werden, je nach Sensibilität der Daten und dem jeweils benötigten Schutzniveau.

Tokenisierung erfüllt die Anforderungen des Datenschutzes durch Technikgestaltung gemäß Art. 25 DSGVO, wenn sie mit geeigneten technischen Maßnahmen kombiniert wird, z.B. durch den Einsatz von kryptografischen Methoden oder die Implementierung eines Hardware-Sicherheitsmoduls (HSM). Die Wirksamkeit hängt von der Trennung der Pseudonymisierungskomponente von der Datenverarbeitung ab.

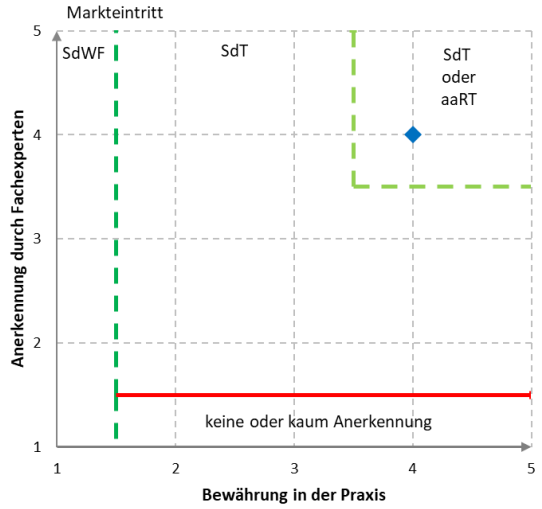
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☐ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.2.33 VOIP-Verschlüsselung mit SIPS/SRTP

Die heutige Telekommunikation baut auf IP-basierenden Netzen auf. Zur Steuerung der Verbindungen (z.B. Anrufauf- und -abbau, Umleitungen sowie Veränderungen der Verbindungsparameter), der Signalisierung, wird das Session Initiation Protocol (SIP) verwendet. Für die Übertragung der digitalisierten Sprache dient das Real-time Transport Protocol (RTP). Beide arbeiten im Normalfall unverschlüsselt. Sie sind somit zunächst für die Bedrohungen der Einsichtnahme, des Mithörens und der Manipulation und Störung der Verfügbarkeit durch unbefugte Dritte anfällig. Zudem ließen sich auch Kommunikationsmuster ableiten.

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

- Abhören und Mitschneiden von Telefongesprächen (schon wenige Sprachdaten können mit KI zum Klonen von Stimmen verwendet werden)
- Vortäuschen falscher Identitäten oder unberechtigte Umleitung von Gesprächen durch Manipulation (Caller ID Spoofing)
- Injektion unberechtigter Sprachdaten oder Stille
- Mit Rauschen überlagerte Sprachdaten können sprachgesteuerte Geräte kontrollieren

- Aufbau unberechtigter Verbindungen
- Denial-of-Service-Attacken

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

Zur Verschlüsselung der Signalisierung kann eine Transportverschlüsselung auf Basis von SIP über TCP und TLS in Kombination mit dem SIPS URI-Schema zur Anwendung kommen. Für die verschlüsselte Sprachübertragung dient das Secure Real-time Transport Protocol (SRTP).

Das SRTP ermöglicht die verschlüsselte Übertragung der Sprachdaten mit den evtl. enthaltenen sensitiven und personenbezogenen Inhalten. Das Protokoll bietet Vertraulichkeit, Integrität und Schutz vor Replay-Attacken. Es nutzt dazu eine symmetrische Verschlüsselung auf Basis des Advanced Encryption Standard im Counter Mode (AES-CM). Je nach Schlüsselaustauschverfahren können Schlüssellängen mit bis zu 256 Bit zur Anwendung kommen. Dabei ist jedoch zu beachten, dass lediglich die Nutzdaten verschlüsselt sind. Der Header ist lediglich authentifiziert. Als Hashing-Verfahren dient HMAC-SHA1 mit 80 Bit zur Sicherstellung der Integrität.

Der Einsatz von Security Descriptions for Media Streams (SDES) zum Schlüsselaustausch hat nur in Kombination mit einer TLS-verschlüsselten SIP-Signalisierung Sinn, da in diesem Fall der Schlüsselaustausch für SRTP innerhalb der Signalisierung im Klartext stattfindet und ansonsten eine nachträgliche Entschlüsselung möglich wäre.

Die Datagram Transport Layer Security (DTLS) stellt das UDP-basierende Pendant zu TLS dar. Es handelt sich dabei also um eine Transportverschlüsselung, die auf X.509-Zertifikaten aufbaut, um die Schlüssel und Algorithmen für SRTP auszutauschen. Die Übertragung der Nutzdaten findet jedoch nicht über DTLS statt, sondern über SRTP. Die symmetrischen SRTP-Schlüssel werden dabei direkt über den Medienpfad ausgetauscht und nicht innerhalb der Signalisierung. Die Endpunkte übertragen einen Fingerprint der Zertifikate in der SIP-Signalisierung als Authentifizierung. Lediglich die Medienendpunkte haben Zugriff auf die Schlüssel.

Die Verschlüsselung der Signalisierung über SIP-TLS arbeitet grundsätzlich "hop by hop". Dies bedeutet, dass die Verschlüsselung zunächst nur bis zum nächsten SIP-Proxy sichergestellt ist. Dieser nächste SIP-Proxy kann die Daten entschlüsseln und eine Weiterleitungsentscheidung auf Basis der Signalisierung im Klartext treffen. Etwas weiter bringt es SIP-TLS auf Basis des sogenannten SIPS-URI-Schemas. Dabei kommt eine Verschlüsselung bis zur Zieldomäne zum Einsatz und sollte somit bevorzugt eingesetzt werden.

Die Authentifizierung kann grundsätzlich entweder rein serverbasiert (über SIP-Proxy bzw. SBC) oder gegenseitig zwischen Client und Server (sog. Mutual TLS) erfolgen. Dabei sollte die gegenseitige Authentifizierung präferiert werden.

Für SIP-TLS sollte nur die Version TLS 1.3 zum Einsatz kommen. Die entsprechenden Algorithmen und Hashing Verfahren sollten gemäß der BSI-Empfehlung TR-02102[18] ausgewählt werden. Auch bei DTLS im Zusammenhang mit SRTP sollte nur noch DTLS 1.3 zum Einsatz kommen. Aufgrund der Tatsache, dass personenbezogene Daten übertragen werden, soll Forward Secrecy zur Anwendung kommen, um eine nachträgliche Entschlüsselung zu vermeiden.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

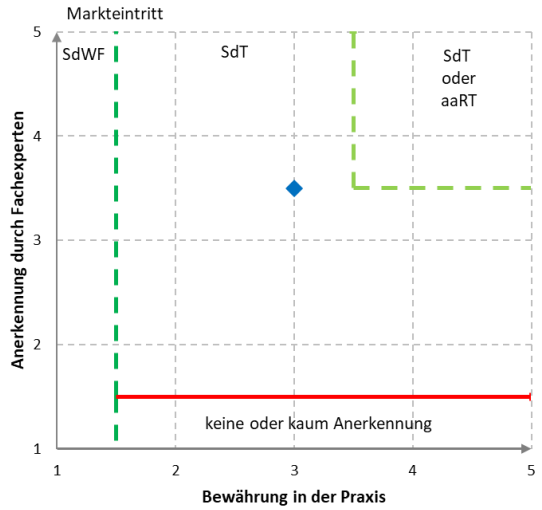
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

[18] Technische Richtlinie TR-02102-2: Verwendung von Transport Layer Security (TLS)

Einordnung der Maßnahme



3.2.34 Verschlüsselung (Layer 1)

Die unterste Netzschicht des OSI-Modells dient der physikalischen Übertragung von Nachrichten über ein Medium zwischen zwei Punkten. Eine Verschlüsselung soll sicherstellen, dass die übertragenen Informationen nicht von Unbefugten abgehört werden können. Alle Verbindungen und Protokolle der darüber liegenden Netzschichten werden durch eine gemeinsame Verschlüsselung auf Layer 1 gesichert. Der Schutz auf Layer 1 ist insbesondere bei Übertragungsmedien mit einfachen Zugriffsmöglichkeiten oder großen transportierten Datenmengen sinnvoll. Im "VS-Produktkatalog des BSI" wird für Produkte mit Verschlüsselung auf dem Layer 1 eine eigene Produktklasse ausgewiesen.[19]

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

Der physische Zugang zu einem Übertragungsmedium ermöglicht einem Angreifer das Mithören der übermittelten Informationen. Ein hohes Risiko besteht insbesondere bei Medien, auf die einfach zugegriffen werden kann, wie beispielsweise bei Kupferkabeln, Stromleitungen mit Powerline oder Funk. Auch Glasfasern, die für den Transport großer Datenmengen über große Entfernungen eingesetzt werden, sind ein attraktives Ziel für Lauschangriffe. Glasfaserkabel sind in Trassen verlegt, die teilweise einen sehr einfachen Zugang ermöglichen.

Die Verschlüsselung der Nutzdaten auf der untersten Netzschicht gewährleistet die Vertraulichkeit der gesendeten Informationen. In Verbindung mit Hash-Funktionen oder digitalen Signaturen kann zudem die Integrität der Daten sichergestellt werden.

Bei der Verschlüsselung auf Layer 1 werden alle Daten der höheren Netzschichten inklusive Metadaten wie beispielsweise IP- und MAC-Adressen geschützt. Dadurch ist es einem Angreifer nicht möglich, Informationen zu Kommunikationsbeziehungen oder Verhaltensmustern der Nutzer des Netzes zu erlangen. Im Hochsicherheitsbereich wird Layer-1-Verschlüsselung zur Verschleierung der Verkehrsbeziehungen eingesetzt.

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

Die Verschlüsselung auf der Netzschicht 1 gewährleistet den Schutz aller Informationen, die zwischen den Endpunkten der physischen Verbindung übertragen werden. Die beiden Endpunkte müssen sich zuverlässig authentifizieren und auf einen gemeinsamen, geheimen Schlüssel einigen bzw. einen Schlüssel geschützt zwischen den Endstellen austauschen. Der genannte Schlüssel wird anschließend zur Ver- bzw. Entschlüsselung der Nutzdaten verwendet, wobei hier ein symmetrischer Algorithmus zum Einsatz kommt. Es wird empfohlen, den geheimen Schlüssel in regelmäßigen Abständen zu erneuern, um die Möglichkeit der Entschlüsselung von in der Vergangenheit und Zukunft übertragenen Daten zu verhindern.

[19] VS-Produktkatalog des BSI, Version 1.8 vom 18.04.2024; Bundesamt für Sicherheit in der Informationstechnik

Eine Verbindung auf dem untersten Layer des Schichtenmodells kann den aggregierten Verkehr von vielen Verbindungen auf höheren Layern transportieren. Die höhere Bitrate des aggregierten Verkehrs ermöglicht eine schnellere Taktung der Verschlüsselung, was zu geringen Verzögerungen bei der Verschlüsselung auf Layer 1 im Vergleich zur Verschlüsselung individueller Verbindungen auf höheren Netzschichten führt. Die geringe Latenz der Layer-1-Verschlüsselung ist insbesondere für zeitkritische Anwendungen von großer Bedeutung, beispielsweise für Anwendungen im Finanzbereich oder für die Übertragung von hochgenauen Zeitinformationen.

Layer-1-Übertragungssysteme werden in der Praxis häufig über längere Zeiträume genutzt als IT-Anwendungen der höheren Netzschichten, die deutlich kürzeren Innovationszyklen unterworfen sind. Sie müssen auf eine lange Nutzungsdauer ausgelegt werden und daher auch auf die potenzielle Bedrohung durch zukünftige Quantencomputer vorbereitet sein. Es wird empfohlen, bereits heute auf quantensichere Methoden des Schlüsselaustauschs zu setzen. Hierfür stehen verschiedene Möglichkeiten zur Verfügung, darunter Postquanten-Kryptografie, QKD-Technik oder hybride Verfahren, die etablierte Methoden und quantensichere Methoden kombinieren. Bei Verwendung des AES-Algorithmus mit einer Schlüssellänge von mindestens 256 Bit ist die Verschlüsselung der Nutzdaten quantensicher.[20]

Ein wesentlicher Einsatzbereich der Layer-1-Verschlüsselung sind Glasfasernetze, die große Datenmengen über lange Strecken übertragen. Aufgrund der weiträumigen Infrastruktur kann ein Zugang zum Übertragungsmedium nicht zuverlässig verhindert werden. Der Zugriff auf die optischen Signale in der Glasfaser wird durch Koppelelemente ermöglicht, die bei der Installation oder während des Betriebs als Faser- oder Biegekoppler eingebracht werden. Dadurch können die übertragenen Informationen mitgelesen und störende oder gefälschte optische Signale eingekoppelt werden.

Bei praktischen Lösungen für die Layer-1-Verschlüsselung von optischen Verbindungen bilden die OTN-Spezifikationen die Grundlage. Dadurch lassen sich standardisierte Schnittstellenmodule einsetzen. Die Verwendung von optischen Verstärkern ermöglicht Reichweiten von über 1.000 km. Der Schlüsselaustausch erfolgt über einen Hilfskanal, wodurch eine Reduzierung des Durchsatzes im Nutzkanal vermieden wird. Eine Verschlüsselung von aggregiertem Verkehr auf Layer 1 erfolgt ohne jeglichen Overhead, wodurch ein 100-prozentiger Durchsatz gewährleistet wird.

Die hohe Bandbreite von OTN-Signalen ermöglicht eine schnelle Taktung des Verschlüsselers, wodurch sich sehr geringe Latenzzeiten ergeben.

Die Verschlüsselung auf der Netzschicht 1 erlaubt die sichere Übertragung eines breiten Spektrums an Protokollen und Schnittstellen in der Payload. Die OTN-Technologie bietet die Möglichkeit, eine Vielzahl von Protokollen und Schnittstellen sicher in der Nutzlast zu übertragen, darunter OTN, SDH, IP / Ethernet. Auch der Transport von speziellen Protokollen zwischen Rechenzentren oder Videostudios ist damit möglich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Übertragungssysteme mit Layer-1-Verschlüsselung für den Transport von Verschlusssachen zugelassen.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

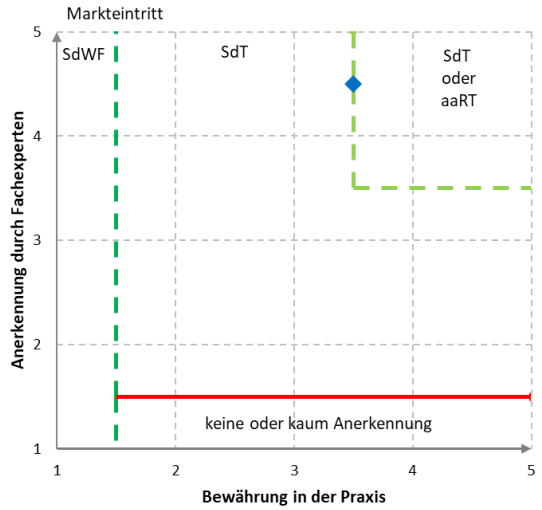
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

[20] Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen; Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Bro21/01

Einordnung der Maßnahme



3.3 Organisatorische Maßnahmen

Da Informations- und Kommunikationseinrichtungen nicht immer grundsätzlich auf Sicherheit 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 Informationssicherheitsmanagementsystem (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 generellen unternehmensinternen Sicherheitsmanagements 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 wird 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 mit Bezug zur Informationssicherheit. Sie können als Grundlage für die Ausrichtung der Sicherheitsstrategie des Unternehmens dienen und bei der Einführung eines ISMS unterstützen. Wie auch bei den technischen Maßnahmen, ist der kontinuierliche Wandel der organisatorischen Maßnahmen eine langfristige Aufgabe, 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. Teilweise kommt es zu Überschneidungen, die aber in der Regel als Synergien genutzt werden können, so dass sich ein positiver Einfluss im Sinne der Informationssicherheit ergibt.

Die ISO/IEC 27000er-Normenwelt

Bei der ISO/IEC 27000-Reihe (manchmal auch nur kurz ISO27k genannt) handelt es sich um eine Reihe von Standards der Informationssicherheit. 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 Normenreihe zusammengefasst sind.

ISO/IEC Norm	Inhalt
ISO/IEC 27000	Überblicksdokument und Terminologie zur Normenreihe ISO/IEC 27000
ISO/IEC 27001	Anforderungen an ein ISMS
ISO/IEC 27002	Leitfaden zur Bestimmung und Umsetzung der Anforderungen der ISO/IEC 27001
ISO/IEC 27003	Leitfaden zu den allgemeinen Anforderungen eines ISMS nach ISO/IEC 27001
ISO/IEC 27004	Leitfaden zur Überwachung und Messung der Wirksamkeit des ISMS
ISO/IEC 27005	Leitfaden zum Risikomanagement
ISO/IEC TR 27019	Sektorspezifischer Leitfaden als Erweiterung der Maßnahmen eines ISMS für Prozessleitsysteme in der Energieversorgungsindustrie
ISO/IEC 27031	Leitfaden für die Bereitschaft von Informations- und Kommunikationstechnologien für Business Continuity
ISO/IEC 27034	Leitfaden für die Sicherheit von Anwendungen
ISO/IEC 27035	Leitfaden für das Management von Informationssicherheitsvorfällen

Tabelle 1: Übersicht der ISO/IEC 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:

	technisch	weniger technisch	nicht technisch
Unternehmens-standard		BSI-Standard 200/ BSI IT-Grundschutz	ISO/IEC 9000 ISO/IEC 20000 ISO/IEC 27000 ISO/IEC 22301 COBIT ISF SOGP
Systemstandard		ULD Datenschutz-Gütesiegel, Euro-PriSe-Privacy Seal, TÜViT Trusted Process / Site / Product	
Produktstandard	ITSEC ISO/IEC 15408		

	(CC) ISO/IEC 19790 (FIPS 140) BSI C5		

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/IEC 27001 von ISO/IEC 9001, ISO/IEC 20000-1, ISO/IEC 22301, CoBIT und ISF SOGP.

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

ISO/IEC 27001 auf der Basis von IT-Grundschutz

Hierbei handelt es sich um die Umsetzung der ISO/IEC 27001 mit Hilfe der IT-Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik (dokumentiert in BSI-Standard 200-2) und des IT-Grundschutz-Kompendium.

Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein ISMS. Er ist grundsätzlich kompatibel zum ISO/IEC-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der anderen ISO/IEC-Standards der ISO/IEC 27000 Normenreihe wie beispielsweise ISO/IEC 27002. Er bietet Interessierten eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

BSI-Standard 200-2 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/IEC 27001-Umsetzung vom Grundschutz-Ansatz des BSI ist der u.a. Tabelle zu entnehmen:

Kategorie	ISO27001	BSI IT-Grundschutz
Regulatorischer Umfang	Relevante Normen < 100 Seiten	Grundschutz-Kompendium > 4.000 Seiten
Anforderungen	Abstrakte und generische Rahmenbedingungen	Konkrete Vorgaben praktischer Maßnahmen
Risikoanalyse	Vollständige Analyse jedes Zielobjektes	Vereinfachte Analyse bei erhöhtem Schutzbedarf
Maßnahmen	ca. 100 konzeptionelle Anforderungen	> 1.100 konkrete Maßnahmen
Zertifizierung	Zertifizierung	Auditor-Testate + Zertifizierung
Gültigkeit	3 Jahre, jährliche Überwachungsaudits	3 Jahre, jährliche Überwachungsaudits

Tabelle 2: Abgrenzung ISO/IEC 27001 vs. BSI-Grundschutz

ISO/IEC 20000-1

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

angewandt, während der Geltungsbereich der ISO/IEC 27001 alle Arten von Organisationen umfassen kann.

ISO/IEC 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/IEC 22301 haben auch (aber nicht nur) einen IT-Bezug. Mit dem Thema BCM beschäftigt sich auch ein Themenbereich der ISO/IEC 27001, allerdings nur aus der Perspektive der Informationssicherheit (d.h. inwiefern die Geschäftskontinuität durch Informationssicherheitsvorfälle gefährdet werden kann).

BSI 200-4

Der BSI-Standard 200-4 bietet eine Methodik für die Einführung eines Systems für ein BCM, dass mit einem Reifegradmodel die schrittweise Einführung eines BC-Managementsystems mit dem Aufbau einer Organisationsstruktur beschreibt. Dabei werden die Stufen: Reaktiv-BCMS, Aufbau-BCMS und Standard-BCMS definiert und ein schrittweises Vorgehen empfohlen.

ISO/IEC 9001

Diese Norm spezifiziert Anforderungen an Qualitätsmanagementsysteme, enthält aber auch 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/IEC 27001 auf die Steuerung des Informationssicherheitsprozesses fokussiert.

Standard of Good Practice (SOGP)

Der Standard des Information Security Forum (ISF) of Good Practice for Information ist ein "good practice" Ansatz für die betriebliche Informationssicherheit, der auch "Security Benchmarking" erlaubt. Der SOGP 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/IEC 27001.

3.3.2 Sicherheitsorganisation

Die Sicherheitsorganisation konzentriert sich darauf, Personen, Informationen und Vermögensgegenstände vor potenziellen Bedrohungen zu schützen. Eine gut strukturierte und funktionierende Sicherheitsorganisation ist entscheidend, um ein einheitliches Sicherheitsniveau zu erreichen und Sicherheit im Unternehmen als integralen Bestandteil zu verankern.

Die Aufgaben der Sicherheitsorganisation umfassen insbesondere:

- Identifikation und Bewertung von Sicherheitsrisiken (Risikoanalyse)
- Entwicklung und Implementierung von Maßnahmen zur Risikomitigation (Strategie)

- Kontinuierliche Überprüfung und Anpassung von Sicherheitsmaßnahmen (Monitoring)

Die wesentlichen Rollen und Zuständigkeiten innerhalb einer Sicherheitsorganisation sind:

Rolle im Unternehmen[21]	Zuständigkeiten
Geschäftsführung (GF), Vorstand (CxO)	• Strategische Verantwortung (dediziert), jedoch in letzter Instanz auch die Gesamtverantwortung für die Informationssicherheit • Verantwortung für alle Risikoentscheidungen
Chief Information Security Officer (CISO), IT-Sicherheitsbeauftragter (ISB/ITSB)	• 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, 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 (DSB), Data Protection Officer (DPO)	• Nicht zwingend als Teil des IS-Managements anzusehen, aber als wichtiger Stakeholder 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.

Tabelle 3: Rollen und Zuständigkeiten innerhalb einer Sicherheitsorganisation

Unabhängig der in der Tabelle aufgeführten Zuständigkeiten, bleibt die Gesamtverantwortung bei der Leitungsebene (Geschäftsführung, Vorstand). Das wird in der aktuellen Gesetzgebung mit Fokus auf die Informationssicherheit und Datenschutz zusätzlich zu den bereits geltenden Vorgaben (z.B. AktienG) bekräftigt.

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.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

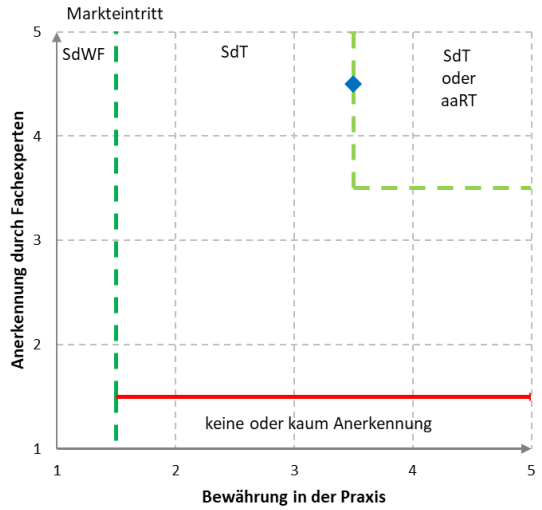
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

[21] Die Rollenbezeichnungen können in einzelnen Unternehmen variieren

Einordnung der Maßnahme



3.3.3 Informationssicherheitsmanagementsystem (ISMS)

Ein Informationssicherheitsmanagementsystem (ISMS) soll durch die Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens sowie die damit verbundene Umsetzung von Sicherheitsmaßnahmen die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen in seinem Geltungsbereich sicherstellen. Dadurch wird die Informationssicherheit dauerhaft geplant, gelenkt und kontrolliert, um das erforderliche Sicherheitsniveau zu erreichen, aufrechtzuerhalten und kontinuierlich zu verbessern.

Anforderungen

Die Basis für das ISMS bildet die Festlegung des Geltungsbereichs (Scope) sowie in welchem Kontext des Unternehmens das ISMS etabliert und betrieben werden soll. Für die Scope-Definition sind u.a. interne und externe Anforderungen, Erwartungen hinsichtlich der ISMS Zielsetzung, beteiligte Parteien sowie gesetzliche und regulatorische Anforderungen zu berücksichtigen.

Ein ISMS benötigt einen kontinuierlichen Verbesserungsprozess (KVP), welcher in Form des PDCA-Zyklus (Plan, Do, Check, Act) umgesetzt wird, um die Aufrechterhaltung der Informationssicherheit im Unternehmen zu gewährleisten. Für die Realisierung eines wirkungsvollen und effektiven ISMS sind nachfolgende Anforderungen umzusetzen.

Es ist die Unterstützung der höchsten Managementebene (Geschäftsleitung, Vorstand usw.) für die Etablierung und Weiterentwicklung eines ISMS sicherzustellen, da von der höchsten Managementebene Entscheidungen zur Zielsetzung, zum Geltungsbereich und zur Umsetzung des ISMS getroffen und Ressourcen freigegeben werden müssen. Die Unterstützung der höchsten Managementebene für das ISMS erfolgt durch die Verabschiedung (Unterschrift) der Informationssicherheitsleitlinie. In dieser Leitlinie werden die mit den Geschäftszielen und -strategien abgestimmten Informationssicherheitsziele des Unternehmens im Geltungsbereich des ISMS definiert und es wird die Verpflichtung der höchsten Managementebene zur laufenden Verbesserung des ISMS festgelegt. Dies ist essenziell, da die Gesamtverantwortung für die Informationssicherheit immer bei der höchsten Managementebene verbleibt. Die Leitlinie ist allen Mitarbeitern im Geltungsbereich bekanntzugeben.

Zur Etablierung eines ISMS sowie zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen muss eine geeignete, übergreifende Organisationsstruktur für Informationssicherheit im Geltungsbereich vorhanden sein. Die Rollen und Verantwortlichkeiten aller involvierten Personen und Parteien sind klar zu definieren. Alle Personen im Geltungsbereich müssen angemessen, entsprechend ihrer Aufgaben, Rollen und Verantwortlichkeiten in einem Schulungs- und Sensibilisierungs-Programm berücksichtigt werden.

Für den erfolgreichen Betrieb des ISMS sowie zur Unterstützung des Informationssicherheitsprozesses, sind des Weiteren interne/externe Kommunikationsanforderungen sowie ein Prozess zur Dokumentation des ISMS (dokumentierte Informationen und Aufzeichnungen) festzulegen.

Ein Schwerpunkt im Rahmen des ISMS ist das Risikomanagement, um (IT)-Risiken für die Organisation zu identifizieren, zu analysieren und durch entsprechende Maßnahmen möglichst beherrschbar zu machen oder auf ein vertretbares Maß zu reduzieren. Das Risikomanagement muss dafür an das Unternehmen angepasst und in den Informationssicherheitsprozess integriert werden.

Empfehlungen/Umsetzung

Für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) werden nachfolgende Standards empfohlen:

- ISO/IEC 27001:2022
  Der Standard stellt Anforderungen an ein zertifizierbares ISMS dar und beschreibt erforderliche Prozesse zur Implementierung, Steuerung, Kontrolle und fortlaufenden Verbesserung. Wird eine Zertifizierung des ISMS angestrebt, sind zusätzliche Vorgaben aus den in Anhang A angeführten Kontrollen umzusetzen.

- BSI-Standard 200-1
  Der BSI-Standard 200-1 beschreibt die allgemeinen Anforderungen an ein ISMS und verbindet dabei die IT-Grundschutz-Methodik mit den Anforderungen aus der ISO/IEC 27001, um mit dieser kompatibel zu sein, wodurch eine ISO/IEC 27001 Zertifizierung auf der Basis von IT-Grundschutz möglich ist.

- VdS-Richtlinien 10000 (VdS 10000)
  Die VdS Schadenverhütung GmbH als Tochterunternehmen des Gesamtverbands der Deutschen Versicherungswirtschaft stellt einen praxisnahen kompakten Maßnahmenkatalog zum Aufbau eines ISMS speziell für kleine und mittlere Unternehmen zur Verfügung. Eine Zertifizierung durch die VdS ist ebenfalls möglich. Die Richtlinien orientieren sich an den Standards ISO/IEC 27001 und dem BSI-Grundschutz.

- Informationssicherheitsmanagementsystem in 12 Schritten (CISIS12)
  Das "Netz für Informationssicherheit im Mittelstand" - mit Mitgliedern wie dem bayerischen IT-Sicherheitscluster e.V. und der Universität Regensburg - bietet auf Grundlage der Standards ISO/IEC 27001 und dem BSI-Grundschutz ein wissenschaftlich gestütztes Modell zur praxisnahen Einführung eines ISMS in 12 Schritten für kleine und mittlere Institutionen an. Eine Zertifizierung ist möglich.

- Österreichisches Informationssicherheitshandbuch
  Das österreichische Informationssicherheitshandbuch beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden ISMS und bietet auf Grund der gewählten Struktur eine Implementierungshilfe für die Umsetzung gemäß ISO/IEC 27001. Das Handbuch hat in wesentlichen Teilen Überlappungen mit dem BSI IT-Grundschutz.

Qualitätssicherung

Für die Umsetzung des PDCA-Zyklus im Rahmen des ISMS müssen periodisch Audits (mindestens jährlich) durchgeführt werden, um zu überprüfen, ob technische und organisatorische Maßnahmen wirksam sind und entsprechend der Informationssicherheitsleitlinie implementiert und angewandt werden. Zu diesem Zweck muss eine Regelung zur Überprüfung und Verbesserung des Informationssicherheitsprozesses sowie ein regelmäßiger, zumindest dreijähriger Auditplan zur Durchführung von internen und externen Audits festgelegt werden. Audits sind periodisch gemäß Auditplan sowie anlassbezogen von fachlich qualifizierten Personen durchzuführen. Anlässe für Audits sind beispielsweise Prozessänderungen, Änderungen des Geltungsbereichs, Infrastrukturänderungen oder die Identifikation neuer, kritischer Risiken.

Die höchste Managementebene muss periodisch regelmäßig über den Stand der Informationssicherheit, der z.B. aus internen/externen Audits abgeleitet wird, informiert werden und muss das ISMS in Form von Management Reviews bewerten, damit die Eignung, Angemessenheit, Wirksamkeit und die laufende Verbesserung des ISMS sichergestellt wird.

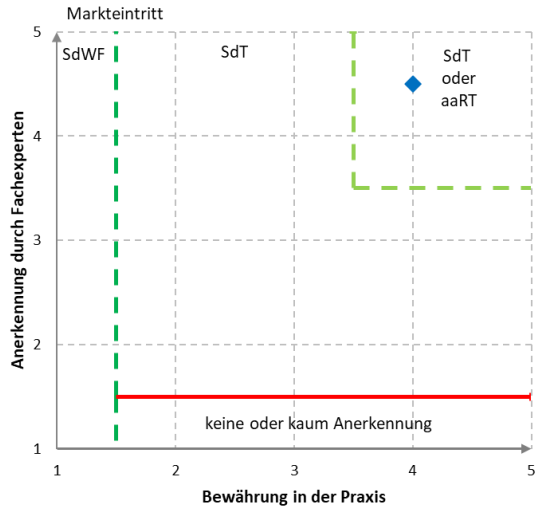
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.3.4 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.

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[22] definiert bereits eine Reihe von Security-Anforderungen, die berücksichtigt werden sollten:

- 15a. Access Requirements
- 15b. Integrity Requirements

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

- 15c. Privacy Requirements
- 15d. Audit Requirements
- 15e. Immunity Requirements

Softwaredesign

Ein sicheres Design muss alle Sicherheitsanforderungen berücksichtigen, um so den identifizierten Bedrohungen entgegenwirken zu können. Ergebnis des Designprozesses ist u.a. die Sicherheitsarchitektur inklusive 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 großem 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 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.

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 den Ergebnissen 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.

Software-Sicherheitstests

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 mit spezialisierten Tools 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 dynamischer Analyse des Systems gut erkannt werden. Im Gegensatz zu manuellen Sicherheitstests 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. Daher sind Penetrationstests aus der Angreifersicht und Breach and Attack Simulations (BAS) durch entsprechendes geschultes Personal oder mit entsprechend spezialisierten Anwendungen zu empfehlen.

Schutz von Quellcode und Ressourcen

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.

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 sein, 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 bekanntwerdende 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.

Auslieferung der Software

Eine Schwachstelle bei der Auslieferung und Einrichtung der Software kann das Ergebnis aller vorherigen Sicherheitsmaßnahmen im Softwareentwicklungsprozess zunichtemachen. 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 Produktivumgebung gewährleistet sein und dabei nicht-autorisierte Änderungen der Konfiguration verhindert werden. Als Sicherheitsmaßnahme bieten sich hier geeignete Standardeinstellungen (Secure by Default), das Vier-Augen-Prinzip und Schulung für Administratoren an. Um den möglichen Schaden eines Angriffs gering zu halten, muss die Anwendung so wenig Berechtigungen wie möglich haben (Least Privilege). Vor allem in Containerumgebungen werden Anwendungen häufig unnötigerweise als root Benutzer ausgeführt, was unbedingt vermieden werden sollte. Essenziell für die Sicherheit der Anwendung ist zudem, dass diese hinsichtlich Sicherheits-Updates stets aktuell gehalten werden muss.

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 zurückfließen, dass diese behoben werden.

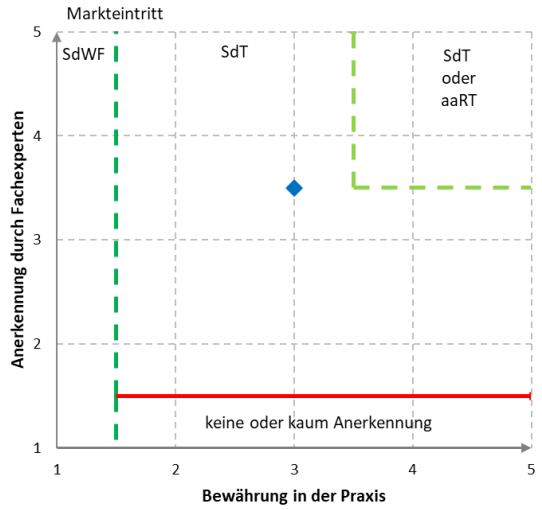
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.3.5 Prozesszertifizierung

Um die Informationssicherheit und den Datenschutz in einem Unternehmen erfolgreich umzusetzen, müssen relevante 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 Außenwirkung, 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/IEC 27001 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 Normenkonformität des ISMS 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 Beteiligten 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/IEC 27001 oder ISO/IEC 27001 auf der Basis von BSI IT-Grundschutz) nachweisen.

Soll ein ISMS zertifiziert werden, muss das Auditverfahren von einer akkreditierten Zertifizierungsstelle durchgeführt werden. Zertifizierungsstellen für ISO/IEC 27001 besitzen eine Akkreditierung nach ISO/IEC 17021 und ISO/IEC 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/IEC 27001 bzw. des BSI IT-Grundschutzes. Die Audits müssen die Standards ISO/IEC 27002 und ISO/IEC 27005 berücksichtigen (und ggf. weiterer branchenspezifischer Ergänzungen der 27000-er Normenreihe). Auditoren von Zertifizierungsstellen für ISO/IEC 27001 sind angehalten, im Rahmen des Auditverfahrens die Standards ISO/IEC 19011 und ISO/IEC 27007 zu berücksichtigen. Bei Audits gemäß BSI IT-Grundschutz muss das jeweils gültige Zertifizierungsschema des BSI beachtet werden.

Zertifizierungen nach ISO/IEC 27001 bzw. ISO/IEC 27001 auf der Basis von BSI IT-Grundschutz haben eine Gültigkeitsdauer von 3 Jahren und werden mindestens jährlich im Rahmen sogenannter Überwachungsaudits geprüft. Soll 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 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. VdS 10000, CISIS12, IDW EPS 980 nF, HIPAA, EuroCloud StarAudit, CSA CCM, ITIL, SOC, PCI DSS, Fedramp).

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[23] 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/IEC 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/IEC 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" 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);

[23] 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*".

- 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.

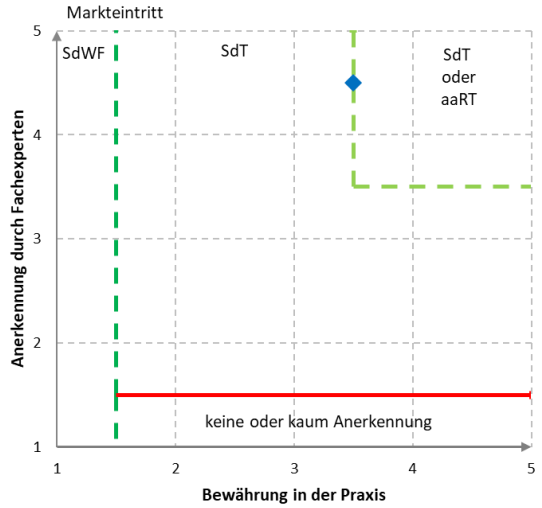
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.3.6 Schwachstellen- und Patchmanagement

Das Schwachstellen- und Patchmanagement haben den Zweck Sicherheits- und Funktionalitätsschwächen in Software und Firmware zu identifizieren und auszubessern. Patches[24] sollen identifizierte Schwachstellen beheben, um ihre Ausnutzung zu verhindern. Der Prozess zum Schwachstellen- und Patchmanagement umfasst die Beurteilung, Identifikation, Evaluierung von Schwachstellen 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.

- 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 oder der Cloud-Umgebung der Organisation 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.

- 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 Schwachstellen- und 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 Schwachstellen und 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. Patches 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.

- Bereitstellung

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.

[24] Die drei wichtigsten Bereiche sind:
- Bugfix: Unter Bugfix ist die Behebung 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

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. Dennoch kann es vorkommen, 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.

- Behandlung von Ausnahmen

Für Systeme oder Anwendungen, für die

- keine Updates seitens des Herstellers mehr verfügbar (sog. Legacy-Systeme) sind,
- noch keine Betriebssystemupdates 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 anderweitige technische Maßnahmen identifiziert und umgesetzt werden. Da in der Regel eine Abschaltung oder einfache Neukonfiguration nicht mit den betrieblichen Erfordernissen vereinbar ist, sollten

- netzwerkseitige Maßnahmen, wie 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.

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.

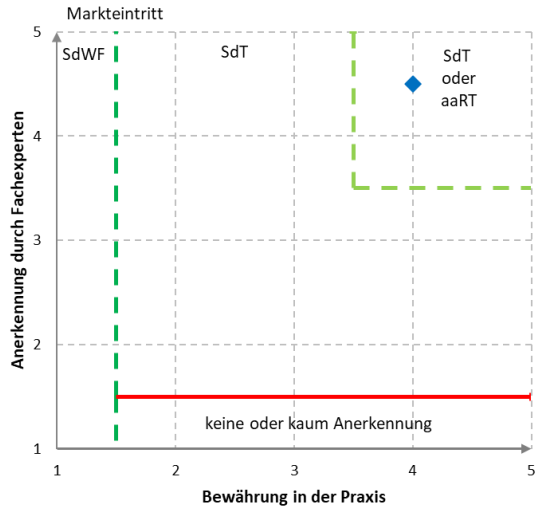
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung des Technologiestandes



3.3.7 Risikomanagement

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[25] 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/IEC 31000. Der speziell auf Informationssicherheitsrisiken anwendbare Standard ist ISO/IEC 27005[26]. Letzterer orientiert sich vom Prozess her sehr eng an ISO/IEC 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 Netzwerk- und Informationssicherheitsrichtinie 2 (NIS-2) mit dem deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, die Datenschutz-Grundverordnung (kurz: DSGVO) oder den IT-Sicherheitskatalog der Bundesnetzagentur (kurz: IT-SiKat), die alle ergänzenden Vorgaben zum Risikomanagement enthalten. Auch branchenspezifische Sicherheitsstandards, die sogenannten B3S, 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/IEC 31000.

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

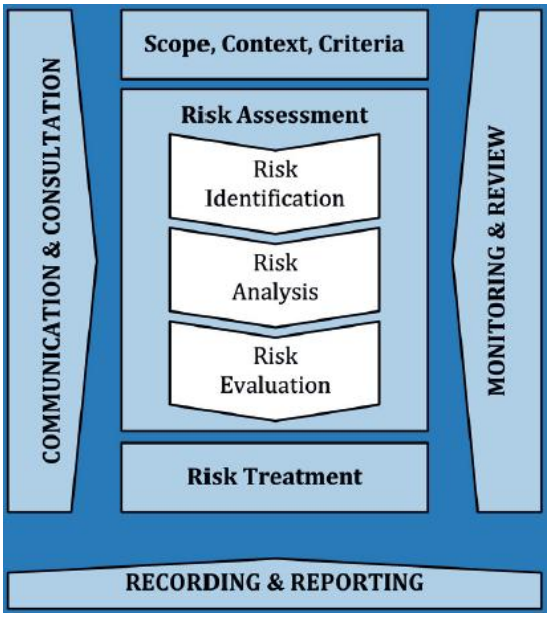


Abbildung 6: Risikoprozess nach ISO/IEC 31000

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 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/IEC 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"[27] 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 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[28]-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.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

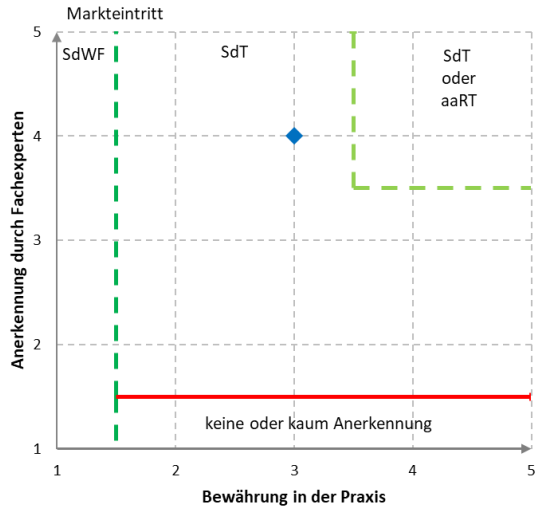
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

[27] Der Begriff "risk owner" aus der ISO 27001 wird je nach den Verantwortlichkeiten der betreffenden Person auch mit "Risikoverantwortlicher" oder "Risikoträger" übersetzt.
[28] Bei den Common Vulnerabilities and Exposures (CVE) handelt es sich um eine standardisierte Liste über Schwachstellen und Sicherheitsrisiken von Computersystemen.

Einordnung des Technologiestandes



3.3.8 Personenzertifizierung

Zu den organisatorischen Maßnahmen gehört u.a. der Einsatz qualifizierten Fachpersonals. Das gilt insbesondere in den unternehmenskritischen Bereichen und bei kritischen Infrastrukturen (KRITIS). Nur so kann es gelingen, die unternehmerischen Vermögenswerte (Assets) zu schützen und die vielfach gesetzlich verankerten Vorgaben hinsichtlich des Qualitätsnachweises des eingesetzten Personals zu erfüllen.

Gerade durch die zunehmende Vielfalt der technischen Lösungen ist es zwingend notwendig, alle im IT-Bereich tätigen Mitarbeitenden über die Grundlagen und Neuerungen fortlaufend zu schulen. Die Mitarbeitenden sollten entsprechend der jeweiligen Tätigkeit und des daraus abzuleitenden Bedarfs sowohl in Bezug auf die zu erfüllende Rolle (z.B. Administrator, Entwickler, IT-Architekt, Auditor, Information Security Officer, Datenschutzbeauftragter) als auch in Bezug auf die branchenspezifischen (z.B. Telekommunikation, Verkehrswesen) und lösungsspezifischen (z.B. On premises, Cloud) Besonderheiten geschult und zertifiziert sein.

Mit der Personenzertifizierung wird die fachliche Qualifizierung nachgewiesen. Denn ein Personenzertifikat wird in der Regel erst nach einer erfolgten Fachschulung und darauf basierten erfolgreich bestandenen Prüfung ausgestellt.

Je nach Zweck und Einsatzbereich existieren am Markt unterschiedliche Zertifizierungsprogramme. Nachfolgend werden wenige Beispiele aufgeführt:

- **Administratoren**
  - Es existieren diverse herstellerabhängige Zertifizierungsprogramme, die auf den Einsatz und die Konfiguration, sowie die Administration des jeweiligen Produktes ausgerichtet sind. Dazu gehören insbesondere Zertifikate von Microsoft, Oracle, Cisco, IBM aber auch Zertifizierungsprogramme der Cloud-Diensteanbieter wie Microsoft, AWS und Google.

  - ITIL-Practioner und Manager sind herstellerunabhängig und an den Wertschöpfungsprozessen der informationstechnischen Industrie ausgelegt.

- **Softwareentwickler**
  - TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) von TeleTrusT Schwerpunkt der T.P.S.S.E.-Zertifizierung ist die Expertise, wie und wo Sicherheitsaspekte in die Softwareentwicklung integriert werden. (www.teletrust.de/tpsse/)

- Certified Secure Software Lifecycle Professional (CSSLP) von ISC²
  Es ist eine herstellerneutrale Zertifizierung, die die Fachkenntnisse einer Person nachweist, Sicherheit innerhalb eines Softwareentwicklungs-Lebenszyklus zu implementieren. (www.isc2.org/Certifications/CSSLP)

- **Softwaretester**
  - Certified Tester verschiedener Stufen in verschiedenen Testbereichen des International Software Testing Qualifications Board (ISTQB) (www.istqb.org/certifications/certification-list/)

- **IT-Architekten**
  - Certified Professional for Software Architecture (CPSA) von iSAQB
    Das International Software Architecture Qualification Board (iSAQB) ist ein Zusammenschluss von Fachexperten zu Softwarearchitektur aus Industrie, Beratungs- und Trainingsunternehmen, Wissenschaft und anderen Organisationen. (www.isaqb.org/certifications/)

  - TOGAF, das The Open Group Architecture Framework (TOGAF) bietet einen Ansatz für Entwurf, Planung, Implementierung und Wartung von Unternehmensarchitekturen. Als operationelles Framework der Gruppe Government and Agency Frameworks bietet das TOGAF mit der Architecture Development Method (ADM) ein Vorgehensmodell zur Entwicklung von technischen Architekturen.

- **IT-Security-Auditoren**
  - Certified Information Systems Auditor (CISA) von ISACA
    CISA ist eine weltweit anerkannte Zertifizierung im Bereich Revision, Kontrolle und Sicherheit von Informationssystemen. (www.isaca.de/de/zert-start/international/cisa)

  - ISO/IEC 27001 Lead Auditor
    Der Fokus liegt auf der Vorbereitung und Durchführung eines Audits des Information Security Management Systems (ISMS). Die Zertifizierung wird von diversen Trägern angeboten.

  - IT-Grundschutz-Auditor
    Zertifizierung zur Durchführung von Audits gemäß den BSI-Standards und dem IT-Grundschutz-Kompendium.

- **IT-Security-Experten**
  - TeleTrusT Information Security Professional (T.I.S.P.) von TeleTrusT
    Die Inhalte, die für das T.I.S.P.-Zertifikat vermittelt werden, umfassen die wichtigsten Aspekte der Informationssicherheit, technische und organisatorische Maßnahmen sowie die deutsche und europäische Gesetzgebung. (www.teletrust.de/tisp/)

  - Certified Information Systems Security Professional (CISSP) von ISC²
    Zur Erlangung des Zertifikats ist Fachwissen zu sicherheitsrelevanten Aspekten aus verschiedenen Bereichen des sogenannten Common Body of Knowledge (CBK) nachzuweisen. (www.isc2.org/Certifications/CISSP)

  - Comptia Security+ von Computing Technology Industry Association (COMPTIA)
    Das Zertifikat fokussiert Basiswissen zu Sicherheitskonzepten und technischen sowie organisatorischen Maßnahmen. (www.comptia.org/de/zertifizierungen/security)

  - Certified Information Security Manager (CISM) von ISACA
    Der Fokus liegt auf der Planung, Umsetzung sowie Steuerung und Überwachung von IT-Sicherheitskonzepten für Fach- und Führungskräfte. (www.isaca.de/de/zert-start/international/cism1)

Gerade für den deutschen Markt hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusätzlich eine Schulungsreihe[29] für IT-Sicherheitsexperten mit Fokus auf das BSI IT-Grundschutzkompendium etabliert. Das sind insbesondere:

- BSI IT-Grundschutz-Praktiker
- BSI IT-Grundschutz-Berater
- BSI IS-Penetrationstester

- **Datenschutzbeauftragter / Datenschutzkoordinator / Datenschutzberater**
  - Bis dato existiert für keinen der beratenden, gestaltenden und kontrollierenden Berufe im Bereich des Datenschutzes eine Zertifizierung nach einem anerkannten unabhängigem Zertifizierungsverfahren von einem unabhängigen Zertifizierer gemäß ISO/IEC 17024. Ein angemessenes Datenschutzfachwissen ist von einer Vielzahl von Faktoren abhängig und kann nicht durch einen singulären Lehrgang vermittelt werden. [30] Hierfür werden umfassendere Schulungen im Bereich Datenschutz empfohlen. Beispielsweise:
    - Certified Information Privacy Professional (CIPP)
      Diese IAPP-Schulung konzentriert sich auf Datenschutzgesetze, -richtlinien und -standards in den wichtigsten internationalen Rechtsordnungen, auf die für das Management von Datenschutzvorgängen erforderlichen Fähigkeiten und auf die Vorbereitung auf die Zertifizierungsprüfung. (iapp.org/train/)

- **Branchenspezifische Zertifikate**
  - Telekommunikation
    - Zero-Outage
      Die Inhalte der Zero-Outage-Zertifizierungen umfassen Best Practices und Standards für die Bereitstellung sicherer, zuverlässiger und hochverfügbarer End-To-End IT-Services und Lösungen im Bereich Telekommunikation. (zero-outage.com/)
  - Verkehrswesen
    - Zertifikate für betriebsnahe ITK im Eisenbahnbetrieb
      Die Inhalte der Zertifizierungen für betriebsnahe ITK im Eisenbahnbetrieb umfassen die Best Practices, Standards und Normen, die bei IT-Projekten und IT-Anwendungen im Eisenbahnbetrieb zu berücksichtigen sind. (www.hmocs.de/)
    - RCS Academy (SBB)
      Die Inhalte der RCS Academy Zertifizierungen umfassen die Best Practices, Standards und Normen, die bei IT-Projekten und IT-Anwendungen im Bereich Disposition des Eisenbahnbetriebs speziell in der Schweiz zu berücksichtigen sind.
  - Automobilbranche
    - TISAX-Auditor
      Trusted Information Security Assessment Exchange (TISAX) hat als Ziel den Schutz von Informationssicherheit in der automobilen Lieferkette. Es orientiert sich stark an ISO/IEC 27001, ist aber speziell auf die Anforderungen der Automobilindustrie zugeschnitten.

Teilweise existieren in anderen europäischen Ländern eigene, individuelle Zertifizierungsprogramme, die noch nicht einer einheitlichen Regelung unterliegen. Eine Übersicht der Zertifizierungsprogramme der europäischen Länder wurde von European Cyber Security Organisation (ECSO) zusammengestellt.[31]

[29] www.bsi.bund.de/
[30] BvD, Berufliches Leitbild der Datenschutzbeauftragten, www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf
[31] www.ecs-org.eu/documents/publications/5fad54a94cfac.pdf

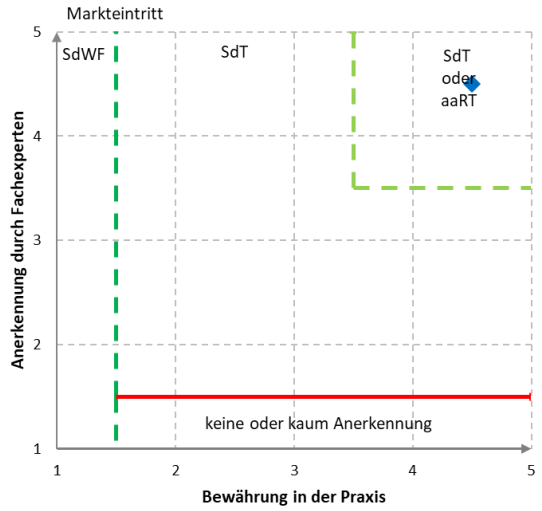
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.3.9 Absicherung privilegierter Benutzerkonten

Für die Administration von Systemen sind privilegierte Benutzerkonten mit weitreichenden Berechtigungen erforderlich. Aufgrund einer möglichen unbefugten oder missbräuchlichen Verwendung bringen diese Konten und damit verbundene Rechte ein Risiko mit großem Schadenspotenzial mit sich. Daher müssen angemessene Regelungen zur Wahrung einer ordnungsgemäßen IT-System-Administration - insbesondere in Bezug auf die Vergabe, den Gebrauch und Entzug von administrativen Zugriffsrechten - getroffen werden.

Neben interaktiven Benutzerkonten mit administrativen Zugriffsrechten werden zumeist auch Servicekonten für Applikationen bzw. Applikationsdienste eingesetzt, die keine unmittelbare Interaktion seitens des administrativen Benutzers erfordern. Darunter fallen ebenfalls die sogenannten Service- Accounts (z.B. für Cron-jobs). Die falsche (meist zu großzügige) Rechtevergabe von Servicekonten stellt in den meisten Firmen eine große Schwachstelle dar, die auch von Angreifern besonders stark in den Fokus genommen wird.

Anforderungen an administrative Benutzerkonten und Zugriffsrechte

Es müssen Richtlinien und Regelungen für die Nutzung und den Umgang mit administrativen Berechtigungen und Accounts festgelegt werden. Vor einer Gewährung eines administrativen Accounts für einen Benutzer sollte dieser zuerst diese Richtlinien und Regelungen akzeptieren und sich dazu verpflichten, diese einzuhalten. Ein Verstoß gegen die definierten Richtlinien und Regelungen muss aufgeklärt werden und Konsequenzen nach sich ziehen.

Es muss eine restriktive Berechtigungsstrategie verfolgt werden, nach welcher ein Zugriff auf Ressourcen grundsätzlich untersagt ist, wenn dieser nicht explizit erlaubt bzw. freigegeben wurde. Hierzu sollte ein definiertes Modell bzw. eine festgelegte Vorgehensweise für die Berechtigungsvergabe angewandt werden. Eine Möglichkeit ist beispielsweise das Role Based Access Control (RBAC) Modell. Bei RBAC handelt es sich um eine funktionsbasierte Zugangssteuerung, wobei die Berechtigungsvergabe anhand von definierten Rollen vorgenommen wird. Benutzer werden dabei einer oder mehreren Rollen zugeordnet und erhalten dadurch die Zugriffsberechtigungen dieser Rollen. Die jeweiligen Rollen werden bei RBAC anhand von Tätigkeitsprofilen definiert.

Für die Vergabe von administrativen Berechtigungen müssen das Need-to-know- und das Least- Privilege-Prinzip beachtet werden. Beim Need-to-know-Prinzip erhält jede Person nur jenes Wissen, jene Berechtigung und/oder jenen Besitz von vertraulichen Informationen, welche zur Erfüllung der eigenen Aufgaben benötigt wird. Beim Least-Privilege-Prinzip erhält jeder Benutzer genau jene Rechte, welche für die Erfüllung seiner Aufgaben unbedingt benötigt werden.

Die Vergabe von administrativen Berechtigungen ist in einem definierten und kontrollierten Prozess durchzuführen, bei welchem eine Anforderung genehmigt und dokumentiert wird. Eine Vergabe von administrativen Rechten darf erst erfolgen, wenn dieser Prozess durchlaufen wurde.

Für administrative Zugriffsrechte müssen dedizierte administrative Accounts erstellt und verwendet werden, die sich von den Benutzeraccounts für die normale, nicht administrative Arbeit unterscheiden. Tätigkeiten, die auch ohne administrative Rechte durchgeführt werden können, dürfen nicht von privilegierten Accounts durchgeführt werden.

"Super-Administratoren" mit Berechtigungen für sämtliche Systeme sind zu vermeiden. Bei vorhandenen Standard-Accounts zur Administration müssen diese je nach Möglichkeit deaktiviert, umbenannt und nicht bzw. eingeschränkt verwendet werden.

Jedes administrative Benutzerkonto muss eindeutig einer Person zuordenbar sein. Sollte dies aufgrund der Systemeigenschaften nicht möglich sein, ist die Verwendung eines anonymen administrativen Benutzerkontos durch begleitende organisatorische und/oder technische Maßnahmen abzusichern und der Umgang damit zu protokollieren. Erforderliche Gruppen-Accounts für administrative Tätigkeiten müssen genau spezifiziert (insb. der erlaubte Personenkreis) und der Umgang damit ebenso dokumentiert werden und sind nur in Ausnahmefällen zulässig. Die Verwendung von Gruppen-Accounts ist durchgängig zu protokollieren.

Für alle administrativen Aufgaben sind Vertretungsregeln zu definieren. Es müssen zudem Notfallaccounts mit administrativen Berechtigungen erstellt werden, deren Zugangsdaten sicher zu verwahren sind. Ein Einsatz dieser Accounts darf nur eingeschränkt und kontrolliert möglich sein (z.B. Vier-Augen-Prinzip) und ist zu dokumentieren. Bei Notfallaccounts mit Multi-Faktor-Authentifizierung (MFA) ist zu beachten, dass alle Faktoren für die Authentifizierung auch in Notfällen vorhanden und betriebsbereit bzw. zugreifbar sein müssen.

Bei einer Vergabe von temporären administrativen Berechtigungen müssen diese eine zeitliche /logische Beschränkung haben und müssen bei Wegfall der Notwendigkeit wieder entzogen werden.

Administrative Accounts mit privilegierten Berechtigungen sind mit einem starken Authentisierungsverfahren (Kopplung mehrerer Authentisierungsmerkmale, Challenge-Response- oder zertifikatsbasierte Verfahren) zu schützen, in welchem die Identität des Benutzers eindeutig feststellbar ist. Benutzerkonten mit weitreichenden Berechtigungen müssen mit Authentisierungsmerkmalen unterschiedlicher Art (z.B. Wissen und Besitz) geschützt werden. Sollte ein dem Risiko angemessenes Authentisierungsverfahren nicht möglich sein, muss geprüft werden, ob aufgrund des Risikos zusätzliche technische oder organisatorische Maßnahmen zur Absicherung erforderlich sind. Eine Verwendung gleicher Passwörter für mehrere administrative Accounts ist nicht zulässig.

Es ist eine aktuelle und vollständige Dokumentation aller administrativen Accounts mit ihren jeweiligen Berechtigungen zu verwalten. Dies gilt sowohl für eingesetzte Systeme wie z.B. Betriebssysteme oder Geräte-Firmware als auch für Fachanwendungen wie z.B. für zentrale Applikationen.

Für sicherheitskritische Tätigkeiten ist gemäß dem Prinzip der Aufgabentrennung eine Aufteilung der Tätigkeit oder eine Trennung von Aufgaben zu implementieren. Diese Aufteilung oder Trennung ist so auszugestalten, dass eine Durchführung von sicherheitskritischen Tätigkeiten an die Anwesenheit mehrerer Benutzer (z.B. durch das Vier-Augen-Prinzip) gebunden oder eine Tätigkeit auf mehrere Personen aufgeteilt wird, die sich nicht gegenseitig vertreten dürfen. Administrative Rollen sind jedenfalls von kontrollierenden Rollen wie z.B. der internen Revision zu trennen.

Alle von administrativen Accounts durchgeführten Anmeldungen und Tätigkeiten sind zu protokollieren, damit nachvollzogen werden kann, welche Tätigkeiten durch welche Accounts durchgeführt wurden. Um die Nachweisbarkeit der von administrativen Accounts durchgeführten Tätigkeiten sicherzustellen, dürfen Administratoren Log- und Auditprotokolle über ihre eigenen Tätigkeiten nicht selbst ändern oder löschen können. Eine Überprüfung dieser Log- und Auditprotokolle muss regelmäßig stattfinden, um die Aktivitäten der Administrationen auf ihre Konformität zu prüfen.

Service Accounts im Machine-2-Machine (M2M)-Bereich

Accounts von Administratoren sind oft gut abgesichert, wohingegen die Absicherung von Service-Accounts oft vernachlässigt wird. Mit der Ausnutzung dieses Umstandes gelingt den Angreifern sehr häufig das sogenannte "Lateral Movement", also die Fortbewegung von einem kompromittierten System zu den nächsten (oft kritischeren) Systemen.

Service-Accounts sind häufig besonders gefährdet, da:

- Diese Accounts keine Multi-Faktor-Authentifizierung (MFA) nutzen
- Gespeicherte Kennwörter dieser Accounts sehr einfach ausgelesen werden können (administrative Rechte vorausgesetzt)
- Die Kennwörter dieser Accounts oft nicht geändert werden und auch nicht neuen Kennwortrichtlinien unterliegen, sind sie daher aufgrund ihres Alters oft noch sehr einfach zu kompromittieren
- Die Kennwörter dieser Accounts oft vielen Personen bekannt sind und nicht dokumentiert ist, welcher Personenkreis darauf Zugriff hat
- Diese Accounts oft zu weitreichende Berechtigungen besitzen und daher das das Least-Privilege-Prinzip nicht befolgen
- Diese Accounts oft für zu viele Zwecke eingesetzt werden und dadurch unnötig viele Berechtigungen aufsummieren

Alle Service-Accounts sind nach einem definierten Verfahren anzulegen und zu dokumentieren. Für diese Accounts sind starke, zufällig generierte Passwörter zu verwenden und diese sind nur einem kleinen, definierten Personenbereich zugänglich zu machen. Verlassen Personen mit Kenntnis der Zugangsdaten dieser Accounts das Unternehmen oder Wechseln die Funktion, sind die Passwörter nach einer entsprechenden Risikobeurteilung zu ändern.

Für die Absicherung von Service-Accounts sollten bei diesen Accounts der interaktive Zugriff nicht erlaubt sein und jeder Versuch sich mit einem solchen Account interaktiv anzumelden, ist zeitnah zu untersuchen. Für jede Aufgabe und jeden Service sollten eigene, dedizierte Accounts erstellt werden (und nicht z.B. nur ein Account je System) und das Least-Privilege-Prinzip muss strikt eingehalten werden. Um nicht aus Versehen zusätzliche Rechte aus anderen Accounts zu übernehmen, sollten Service-Accounts nicht von anderen Accounts kopiert werden.

Empfehlungen / Umsetzungen

Für das Management von administrativen Accounts und deren Zugriffsrechte sowie für die Umsetzung von Regelungen wird der Einsatz einer Privileged Access Management (PAM) Lösung empfohlen. Relevante Standards sind:

- ISO/IEC 27002:2022
  Der Standard enthält Empfehlungen zur Umsetzung der in ISO/IEC 27001 Anhang A geforderten Maßnahmen für die Zuteilung, Verwaltung und Prüfung/Kontrolle administrativer Accounts. Wird eine Zertifizierung gemäß ISO/IEC 27001 angestrebt, sind diese Maßnahmen im Geltungsbereich des ISMS umzusetzen. Umsetzungshinweise für diese Maßnahmen finden sich vor allem in den Abschnitten 8.2 "Privilegierte Zugriffsrechte", "8.15 Protokollierung" und "8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten".
- BSI IT-Grundschutz-Kompendium (Februar 2022)
  Das BSI IT-Grundschutz-Kompendium beschreibt im Baustein OPS.1.1.2 Gefährdungen im Zusammenhang mit administrativen Accounts und daraus abgeleitet Anforderungen für den Umgang mit diesen.
- Österreichisches Informationssicherheitshandbuch
  Das Österreichische Informationssicherheitshandbuch gibt Empfehlungen zum Management von Benutzern, zu welchen auch administrative Accounts zählen. Empfehlungen finden sich zur Vergabe, Verwaltung und Dokumentation von Zugriffsrechten sowie zur Regelung von Zugriffsmöglichkeiten in Vertretungs- und Notfällen.
- BDEW-Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme 2.0
  Im BDEW-Whitepaper finden sich neben der Anforderung zur Einhaltung des Need-to-know-Principles in den allgemeinen Anforderungen auch die Empfehlung, dass auch Anwendungen und Fachapplikationen Benutzerkonzepte umsetzen müssen, in dem Administrator-Rollen mit einer granularen Zugriffskontrolle abgebildet und werden können.

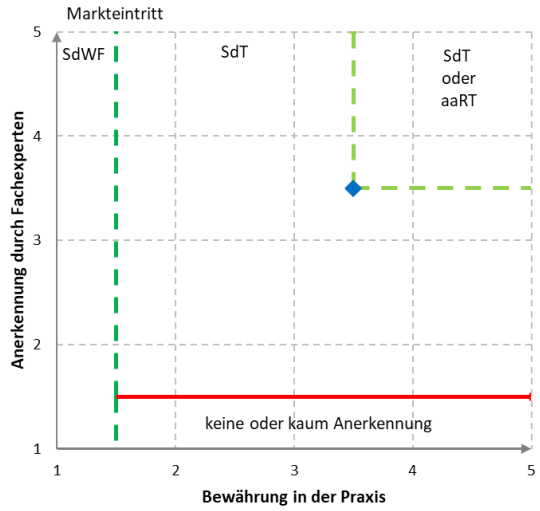
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.3.10 Dark Web Monitoring

Abhanden gekommene geschäftskritische Informationen können schwerwiegende Folgen haben. Wer über den Verlust informiert ist, kann reagieren. Wie in der realen Welt, wo Diebesgut auf dem Schwarzmarkt gehandelt wird, werden im Internet entwendete Unternehmensinformationen (z.B. Informationen über Schwachstellen, Erkenntnisse aus verwendeten Cookies, gestohlene Anmeldeinformationen, Zahlungsverkehrsinformationen) im sog. Dark Web[32] gehandelt. Darunter versteht man eine Vielzahl separater Netzwerke (Darknets) innerhalb des Internets.

Das Dark Web wird von Angreifern genutzt, um sich untereinander auszutauschen und entwendete Unternehmensinformationen zur Schau zu stellen und/oder zu verkaufen. Das erfolgt in der Regel unmittelbar nach dem Angriff. Technische Kompromittierungen von Unternehmen, Systemen und Netzwerken finden häufig unbemerkt statt. Sie führen zu einem Datenabfluss oder können der Vorbereitung einer gezielten Attacke dienen. Die Beobachtung des Dark Web kann daher dazu beitragen, Belege für einen erfolgten oder kurz bevorstehenden Angriff auf ein Unternehmen zu identifizieren, zu dokumentieren und ausgehend von den vorliegenden Informationen entsprechende Korrekturmaßnahmen zu initialisieren.

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

Ein regelmäßiges, gezieltes Monitoring des Dark Web[33] durch beauftragte spezialisierte Dienstleister oder Anwendungen kann dazu beitragen, dass geplante oder zukünftig zu erwartende Angriffe auf ein Unternehmen (z.B. durch eine Ransomware-Attacke, illegale Daten-Hehlerei oder Folgeangriffe durch weitere Angreifer) verhindert werden können. Die Maßnahme trägt somit zu einer Risikominimierung bei. Auch können dadurch sog. Supply-Chain-Attacken (auch als Angriff auf die Lieferkette, Drittanbieter-Angriff, Angriff auf die Wertschöpfungskette bekannt) aufgedeckt werden, um zu verhindern, dass ein Angriff auf das eigene Umfeld indirekt über Drittanbieter oder Lieferanten oder über die Lieferkette ausgeübt werden kann.

[32] Auch Darknet oder Deep Web genannt
[33] Als besondere Form der Cyber Threat Intelligence (siehe Kap. 3.2.27)

Das Dark Web Monitoring schützt nicht gegen die Bedrohung einer Kompromittierung (Eindringen von Tätern) selbst. Die aus dem Dark Web Monitoring folgenden Erkenntnisse können aber Risiken der betroffenen Organisation minimieren, indem geeignete Reaktionsmaßnahmen eingeleitet werden, um weiteren Schaden zu verhindern oder zumindest zu beschränken.

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

Manuelle Analysen der öffentlich verfügbaren Informationen über ein Unternehmen und der aktuellen Bedrohungslage für die jeweilige Industrie werden durchgeführt um nachfolgend automatisierte, für das jeweilige Unternehmen individuell angepasste, Regelwerke aufzusetzen.

Diese gewährleisten die regelmäßige (mind. tagesaktuelle) Überwachung beispielsweise von:

- Markplätzen und -foren im Dark Web (u.a. über spezielle Anbieter möglich)
- veröffentlichten Daten-Leaks (z.B. Identity Leak Checker des Hasso-Plattner-Instituts[34])
- öffentlicher und nicht-öffentlicher Kommunikation im World Wide Web und auf Social Media Plattformen inkl. einschlägiger geschlossener Benutzergruppen
- Behördenwarnungen relevanter Stellen (z.B. BSI oder US-Cert)
- Berichterstattungen in den Medien

Die manuellen Analysen der Informations- und Bedrohungslage werden je nach Bedarf iteriert, um eine kontinuierliche Optimierung der Regelwerke zu gewährleisten.

Ein hoher Automatisierungs- und Professionalisierungsgrad ist aufgrund der zu erwarteten großen Datenmenge in der Regel nur durch ein Managed Service zu erreichen. Darüber hinaus sollten spezialisierte Datenanalysten mit ermittlungstaktischem Hintergrund mit den Aufgaben involviert werden.

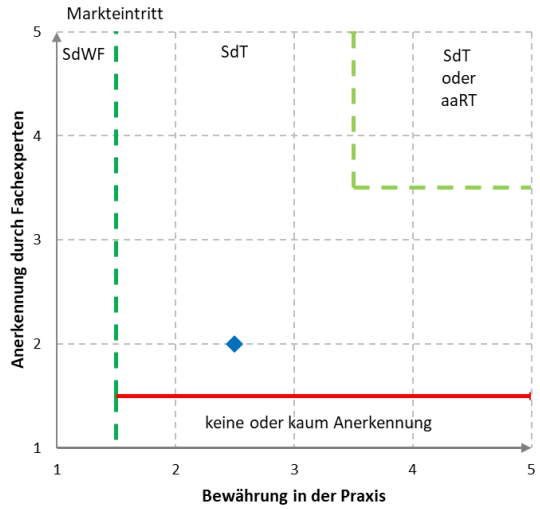
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



[34] sec.hpi.de/ilc/search

3.3.11 Umgang mit Dienstleistern

Die Auslagerung von Dienstleistungen (Outsourcing) kann vorteilhaft sein, wenn Dienstleister fokussierter, innovativer und in der Sache besser oder günstiger als der Auftraggeber den beauftragten Dienst erbringen können bzw. eine besondere Technologie im Einsatz haben.

Allerdings gehen mit der Beauftragung von Dienstleistern zum Teil nicht unerhebliche Risiken einher (z.B. Abhängigkeit, Verlust von Kontroll- und Steuerungsmöglichkeiten, Risiken für die Informationssicherheit). Diese Risiken können im schlechtesten Fall die Existenz des Auftraggebers gefährden. Umso vertraulicher, schutzbedürftiger oder mit Restriktionen (z.B. Geheimhaltung, Datenschutz) belegt Daten sind, desto größer ist das Risiko. Vor diesem Hintergrund kommen der Auswahl, Steuerung, Überwachung und Überprüfung von Dienstleistern als organisatorische Maßnahme eine zentrale Bedeutung zu.

Mit der Auslagerung von Dienstleistungen (z.B. Netzwerkadministration) gehen diverse Bedrohungen der IT-Sicherheit (auch Informationssicherheit) einher, z.B.:

- Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung oder unbefugten Zugang zu Daten führt
- Vertragswidriger oder unangemessener Umgang durch Dritte mit den zum Zweck der Vertragserfüllung überlassenen Daten
- Missbrauch erhaltener Zugriffsrechte durch den Dienstleiter und der daraus resultierende Diebstahl, Verlust oder die unautorisierte Weitergabe der überlassenen Daten
- Menschliches und organisatorisches Versagen oder Fehlverhalten durch die Nichteinhaltung von vereinbarten technischen und organisatorischen Maßnahmen
- Rechtliche Risiken (z.B. Schadenersatz wegen Handlungen oder Unterlassungen von Dienstleistern, Geld- oder Freiheitsstrafen, behördliche Anordnungen)
- Finanzielle Risiken (z.B. Ausfall des Dienstleisters durch Insolvenz)

Um diesen Bedrohungen entgegenzuwirken, werden die nachfolgenden Maßnahmen empfohlen:

1. **Maßnahmen zur Auswahl von Dienstleistern:**
    - Gestaltung bzw. Anpassung des Einkaufsprozesses mit dem Ziel, Datenschutz und Informationssicherheit in den Fokus zu nehmen - z.B. durch die frühzeitige Einbindung entsprechender Stellen in den Auswahlprozess und die Festsetzung von Mindeststandards (Baseline Standards) anhand von individuellen oder allgemein anerkannten Standards (z.B. Trusted Computer System Evaluation Criteria (TCSEC))
    - Durchführung von Leistungsanfragen (Request for Information - RFI) in strukturierter Form mit Fragen zur Informationssicherheit und zum Datenschutz mit der Aufforderung zur verbindlichen Stellungnahme durch den Dienstleister
    - Aufforderung von verschiedenen Dienstleistern zur Angebotsabgabe (Request for Proposal - RFP) basierend auf einer detaillierten Leistungsbeschreibung bzw. einem Pflichtenheft sowie den individuellen Anforderungen an Datenschutz und Informationssicherheit
    - Due Diligence, also sorgfältige Prüfung mit Bewertung sämtlicher mit einem Rechtsgeschäft einhergehenden relevanten rechtlichen Risiken

2. **Maßnahmen zur Steuerung und Überprüfung von Dienstleistern:**
    - Es empfiehlt sich in jedem Fall eine interne Festlegung und Delegation von Verantwortlichkeiten hinsichtlich der Überwachung von Dienstleistern
    - Art und Umfang der Maßnahmen sind abhängig von verschiedenen Faktoren, wie z.B. der Unternehmensgröße, Komplexität der Service-Level-Agreement (SLA) und der Organisationsstruktur sowie bereits bestehender Prozesse im Unternehmen
    - Festlegung und Anwendung von Kriterien zur kontinuierlichen Kontrolle der Fähigkeit von Dienstleistern in Übereinstimmung mit den festgelegten und vertraglich vereinbarten Anforderungen (entsprechend Unterabschnitt 8.4 der ISO/IEC 9001)
    - Idealerweise sind die Maßnahmen in ein IT-Risikomanagement integriert, das in die bestehenden Unternehmensprozesse (z.B. IT-Sicherheitsmanagement, Compliance-Management, Datenschutzmanagement) eingebettet ist.

3. **Maßnahmen zur Überwachung von Dienstleistern:**
    - Priorisierung von Aufgaben und Festlegung von Prüfintervallen
    - Bestimmung von Art und Umfang von Prüfmaßnahmen (z.B. Vor-Ort-Audit-Maßnahmen, Einsatz von Fragebögen oder kommerzieller Datenbanken zum Dienstleister-Risikomanagement) etc. durch Bewertung des individuellen, mit der Beauftragung des jeweiligen Dienstleisters einhergehenden Risikos anhand der Höhe der Eintrittswahrscheinlichkeit bestimmter Risiken, des Grads der Beeinflussbarkeit des Risikos und des dazu notwendigen Aufwands
    - Dienstleister- / Lieferantenaudits (IT-Sicherheitsaudits, Datenschutzaudits, Physical Security Audits) während der Vertragsdurchführung
    - Management von Verträgen, Zertifikaten und sonstigen Dokumentationen

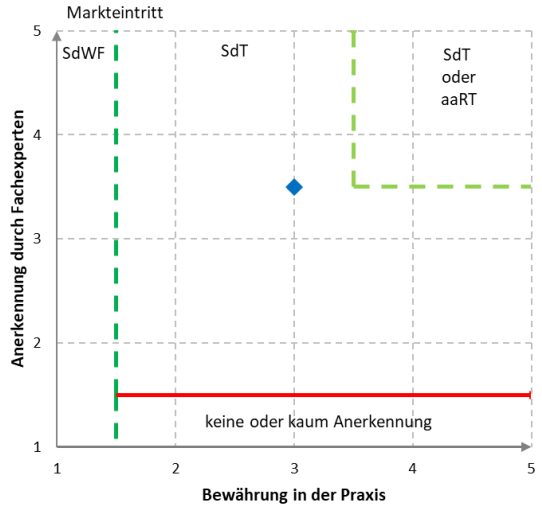
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.3.12 Software Bill of Materials (SBOM)

Eine Software Bill of Materials (SBOM) oder Software-Stückliste ist eine Liste von Komponenten und deren Abhängigkeiten, die eine IT-Anwendung oder ein IT-Service benötigt bzw. hat. Diese Liste ist maschinenlesbar und sorgt für Transparenz über die eingesetzten Komponenten Dritter. Damit lassen sich Schwachstellen bestimmen, die durch zugrunde liegende Komponenten verursacht werden.

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

Die Maßnahme soll die Identifikation der potenziellen Angriffsfläche bei sog. "Supply-Chain-Angriffen" ermöglichen, die unter Ausnutzung von Sicherheitslücken in genutzten Komponenten (z.B. Software-Bibliotheken) ausgeführt werden. Ohne SBOM fehlen Informationen darüber, welche Komponenten in einer genutzten IT-Anwendung oder einem IT-Service eingesetzt werden. Eine Erkennung potenzieller Schwachstellen ist dadurch erheblich erschwert, wenn nicht unmöglich.

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

SBOM liefert eine vollständige Stückliste aller in einer IT-Anwendung oder einem IT-Service genutzten Komponenten. Diese Information ermöglicht den Abgleich mit einer Liste von Schwachstellen, die in einer bestimmten Komponente ggf. vorhanden sind und dadurch Information darüber, ob die genutzte IT-Anwendung oder der genutzte IT-Service möglicherweise ebenfalls von dieser Schwachstelle betroffen ist.

Für SBOM wurden verschiedene Datenformate entwickelt. ISO-Standards gibt es für die Formate SPDX[1] und SWID[2], von OWASP wurde der Standard CycloneDX[3] verabschiedet. SWID und SPDX dienen primär der eindeutigen Identifikation von Software zu verschiedenen Zwecken (nicht nur der Sicherheit). CycloneDX dagegen fokussiert auf die Sicherheit von Anwendungen und die Analyse der Komponenten der Supply-Chain, auch über Software hinaus, unter Einbeziehung z.B. von Hardware-Komponenten und Cloud Services. Die Formate sind zueinander nicht kompatibel.

SBOM ist eine zentrale Maßnahme zur Abwehr von Supply-Chain-Angriffen. Die U.S.-Administration hat durch eine Executive Order im Mai 2021[4], konkretisiert durch das U.S. Department of Commerce (Juli 2021)[5] und NIST (Februar 2022)[6] die Bereitstellung und Verwendung von SBOM durch Lieferanten der U.S.-Administration vorgeschrieben.

Die EU-Kommission im Rahmen des Cyber Resilience Acts die Bereitstellung einer SBOM als eine der zentralen Sicherheitsanforderungen formuliert.[35] Darüber hinaus hat BSI mit der TR03183 die fachlichen Vorgaben an einer Software-Stückliste (SBOM) festgelegt.[36].

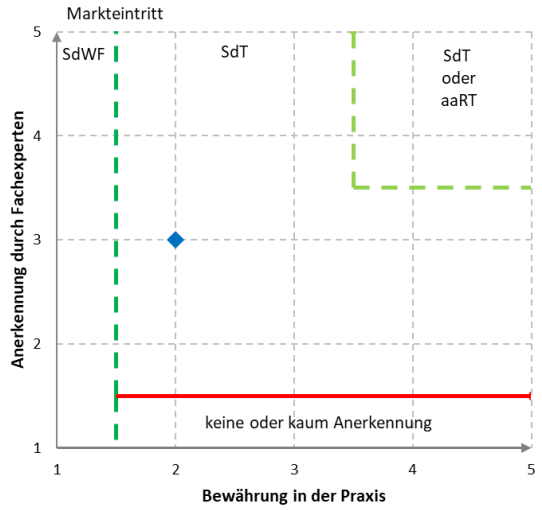
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



[35] EU CRA, digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[36] BSI, SBOM-Anforderungen: TR-03183-2, www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html

3.3.13 Geo-Redundanzen

Die effiziente Nutzung der eingesetzten Systeme und Anwendungen ist u.a. von ihrer ständigen Verfügbarkeit abhängig. Ein Ausfall der IT-Infrastruktur (z.B. Netzwerke, Anwendungen, Speicher, Datenbanken, Rechenkapazitäten) hat direkte negative Auswirkung auf den Geschäftsbetrieb. Wenn eine hohe Verfügbarkeit erforderlich ist, muss die IT-Infrastruktur redundant aufgesetzt sein und im Notfall kurzfristig verfügbar gemacht werden. Die Redundanz muss dabei so ausgestaltet sein, dass ein Ausfall einer einzelnen Komponente nicht zum Ausfall der gesamten IT-Infrastruktur führt. In Abhängigkeit einer Risikoanalyse kann die Georedundanz eine besondere Rolle spielen.

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

Die Liste der elementaren Gefährdungen [37]des Bundesamts für Sicherheit in der Informationstechnik (BSI), auch bekannt als G0-Katalog, hat sich als Standard etabliert und bietet eine strukturierte Übersicht über 47 potenzielle Bedrohungen und Schwachstellen in Informationssystemen. Durch die Vereinheitlichung der Anwendung dieses Katalogs bei der Schutzbedarfsfeststellung und Risikoanalyse können Organisationen ein einheitliches Verständnis von Risiken entwickeln und inklusive deren Bewertung und Priorisierung effizienter arbeiten. Zudem fördert die Standardisierung die Vergleichbarkeit von Sicherheitsmaßnahmen und verbessert die Kommunikation zwischen verschiedenen Akteuren im Bereich der Informationssicherheit.

Auszug elementarer Gefährdungen mit Schwerpunkt Bedrohung der Verfügbarkeit:

- Feuer (G.01), Wasser (G.03), Naturkatastrophen (G.05)
- Ausfall der Stromversorgung (G.08)
- System-, Netzwerk- (G.09) und Dienste-Ausfall (G.011)
- Physische Beschädigungen, Einbruch (G.044), Vandalismus (G.044), Diebstahl (G.044) etc.

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

Zur Sicherstellung einer hohen Verfügbarkeit sollte die eingesetzte IT-Infrastruktur redundant aufgestellt sein. Dabei bedeutet "Redundanz", dass eine Komponente mehrfach (mindestens zweimal) in der gleichen Konstellation und Konfiguration verfügbar ist. Welche Komponente der IT-Infrastruktur redundant, oder gar georedundant, aufgesetzt werden soll, wird durch die Risikoanalyse bestimmt.

Eine IT-Infrastruktur ist redundant, wenn es von seinem technischen Zwilling

- gleichwertige Ressourcen vorhält,
- baulich getrennt ist,
- vollständig unabhängig in Bezug auf die Stromversorgung, Klimatisierung und Netzanbindung
- und rückwirkungsfrei voneinander aufgesetzt ist.

Bei einem Ausfall, z.B. aufgrund von Unwettern, Erdbeben, Sabotage, Stromausfällen oder Komponentenfehlern, übernimmt die redundant aufgesetzte IT-Infrastruktur in Teilen oder ganz die Verarbeitung, um den Betrieb des gesamten Systems aufrechtzuerhalten.

Die Konfiguration der Redundanz ist abhängig von der Risikobewertung und der möglichen potenziellen Schadenshöhe. Je kürzer die aus betrieblicher Sicht tolerierbaren Ausfallzeiten, desto mehr redundante Komponenten der IT-Infrastruktur müssen bereitgestellt werden. Das wiederum führt zu höheren Kosten für ihre Vorbereitung und fortlaufend aktualisierte Vorhaltung.

Bei der Geo-Redundanz wird zusätzlich der Standort als geografisches Kriterium berücksichtigt. Die Standortwahl ist individuell zu betrachten, da sie auf der individuellen Risikoanalyse des Unternehmens basiert. Empfehlungen zu relevanten Kriterien können beispielsweise beim BSI nachgelesen werden.[38]

[37] BSI - Elementare Gefährdungen Stand 07.12.2020, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html

[38] BSI - Standort-Kriterien für Rechenzentren (bund.de), www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/Standort-Kriterien_HV-RZ/Standort-Kriterien_HV-RZ_node.html

Dort sind insbesondere die räumlichen Abstände von redundanten Rechenzentren ersichtlich, die als grobe Richtlinie verwendet werden könnten.

Im Kontext der zunehmenden Nutzung der Cloud-Dienste, sollten im Rahmen einer durchzuführenden Risikobetrachtung validiert werden, ob Redundanzen der verwendeten Betriebskomponenten aufgebaut werden sollen. Üblicherweise werden diese nicht automatisch durch den Cloud Service Provider (CSP) angelegt, sondern müssen individuell konfiguriert werden. Auch hier ist es sinnvoll, vorweg ein Redundanz-Konzept zu erstellen, das zur Risikobewertung und -bereitschaft des Unternehmens passt.

Cloud-Angebote weisen vielfach sehr frei wählbare Möglichkeiten zur Georedundanz auf, die mit entsprechenden Kosten gebucht werden können. Eine Abwägung zwischen Anforderungen und Kosten ist erforderlich, hierzu sollten die vorab bestimmten als relevant erachteten Risikofaktoren berücksichtigt werden.

Auch rechtliche Aspekte müssen bei der Konzeption und der Umsetzung der Georedundanz berücksichtigt werden. Relevant ist das insbesondere bei der Nutzung von außereuropäischen Dienstleistern und Rechenzentren, da diese möglicherweise einer anderen Rechtsprechung unterliegen und somit Potential für unterschiedliche Auslegung bergen (z.B. Vergleich vom CLOUD Act vs. DSGVO).

In der höchsten Sicherheitsstufe sollte auch eine unabhängige Weiterentwicklung der Cloud-Service betrachtet werden. Dazu sind u.a. Escrow-Verfahren, Betrieb unabhängig vom Hersteller und ein Aufbau technischer Expertise notwendig.

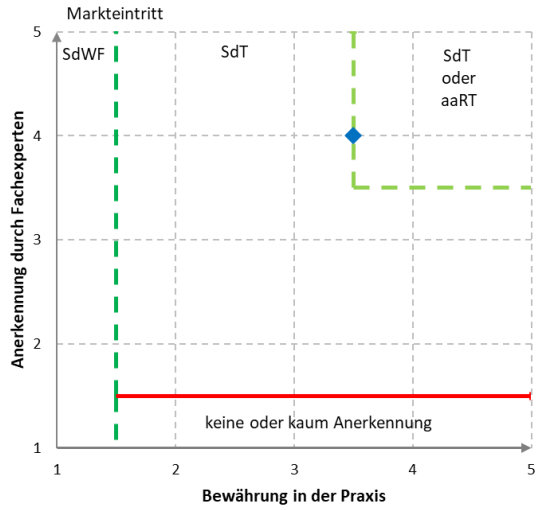
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



3.3.14 Sensibilisierung der Anwender

Von Mitarbeitenden wird erwartet, dass sie bei ihrer täglichen Arbeit alle informationssicherheitsrelevanten Regeln und Vorschriften einhalten. Wenn Arbeitsabläufe (z.B. Öffnen eines E-Mail-Anhangs) zur Gewohnheit geworden sind, lassen sie sich schwer wieder ändern. Daher bedarf es neuer "sicherer" Routinen. Diese können nicht allein angeordnet, sondern müssen eingeübt werden. Überdies muss ein Grundverständnis und Motivation bei den Mitarbeitern erzeugt werden, damit sie die Maßnahmen langfristig und nachhaltig umsetzen.

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

- Begünstigung von Angriffen (z.B. "Social engineering", Ransomware) durch unzureichendes Bewusstsein für Informationssicherheit und potenziell schädliches Handeln
- Kompromittierung von Accounts für Angriffe oder Ausnutzung durch Betrüger
- Verlust oder Offenlegung von vertraulichen Daten durch unachtsames Handeln
- Nichterkennen von Sicherheitsvorfällen und unzureichendes Handeln nach einem Sicherheitsvorfall

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

Organisationen müssen dafür sorgen, dass Mitarbeitende[39] ihre Tätigkeiten unter Beachtung der Informationssicherheitsregeln ausführen. Bewusstsein und Wissen allein reichen hierfür nicht aus. Benötigt werden neue *sichere* Verhaltensweisen. Diese müssen eingeübt und als neue Routine im täglichen Arbeiten verankert werden. Überdies sollte die Leitung als gutes Vorbild vorangehen und diese Routinen vorleben.

Die Herangehensweise der Organisation an das Thema Awareness muss strukturiert erfolgen. Die folgenden Schritte sind dabei zu durchlaufen:

1. Auswahl der Themen bzw. Themenbereich
2. Festlegen der Ziele der Awareness-Kampagne(n)
3. Umsetzung und Überprüfung der Wirksamkeit

Bei der **Auswahl der Themen bzw. Themenbereich** sollen zuvorderst die Ergebnisse des eigenen Risikomanagements und die eigenen Informationssicherheitsziele berücksichtigt werden. Auch weitere Aspekte wie Informationssicherheitsvorfälle in der eigenen oder bei vergleichbaren Organisationen, eine Betrachtung der eigenen Informationswerte ("Kronjuwelen"), die eigene Unternehmenskultur, Anforderungen wichtiger Stakeholder, die Analyse und Bewertung der eigenen Informationssicherheitskennzahlen sowie die Ergebnisse von Audits sollen in die Auswahl einfließen.

Die **Ziele der Awareness-Kampagne(n)** sollen als konkrete, operative Ziele formuliert sein. Messbarkeit erfordert Kriterien, anhand derer bestimmt werden kann, zu welchem Grad das Ziel erreicht wurde (Zielerreichungskriterien). Die Ziele sind vor dem Start festzulegen und zu dokumentieren. Zudem sollte über eine Bekanntmachung gegenüber der Mitarbeitenden erwogen werden, wenn es die Zielerreichung verbessert.

Die **Umsetzung** erfolgt in neun größtenteils aufeinander aufbauenden Schritten[40]:

1. **Sicherheits-Hygiene:** Zunächst sind die eigenen Regelungen auf tatsächliche und praktische Umsetzbarkeit zu prüfen. Niemandem darf zugemutet werden, Regeln zu befolgen, die im Kontext der eigenen Tätigkeit nicht oder nur unter erheblichen Erschwernissen umzusetzen sind. Ist das der Fall, sollte geprüft werden, ob die Regeln dahingehend veränderbar sind, so dass sie das gewünschte Ziel begünstigen und umsetzbar sind. Sicherheit lässt sich am effektivsten verbessern, wenn sie einfach umsetzbar ist und sich nahtlos in die bestehenden Prozesse integrieren lässt.
2. **Information:** Mitarbeitende brauchen Informationen über die bestehenden Regelungen, d.h. sie müssen bekannt gemacht werden und verfügbar sein.
3. **Sensibilisierung:** Mitarbeitende müssen sensibilisiert werden. Dabei sollten keine Bedrohungsmodelle genutzt und keine Angst erzeugt, sondern motiviert werden. Das kann erreicht werden, indem der berufliche und persönliche Mehrwert aufgezeigt wird.
4. **Wissen und Verstehen:** Mitarbeitende müssen wissen und grundlegend verstehen, wie ihr "unsicheres" Verhalten durch die Bedrohungen ausgenutzt werden kann.
5. **Zustimmung:** Mitarbeitende sollen aktiv und möglichst freiwillig zustimmen, ihren Teil zu leisten, d.h. ihr eigenes Verhalten zu ändern.
6. **Selbstwirksamkeitserwartung:** Mitarbeitende müssen davon überzeugt sein, dass man das gewünschte Verhalten tatsächlich leisten kann und hierdurch einen wichtigen Beitrag leistet.

[39] Alle Personen, die unter der Aufsicht der Organisation Tätigkeiten ausüben. Wenn in diesem Kapitel von Mitarbeitern gesprochen wird, ist dies stets in diesem weiteren Sinne gemeint.
[40] Human-Centred Security am Horst-Görtz-Institut für IT-Sicherheit, Ruhr Universität Bochum (hgi.rub.de/)

7. **Fähigkeiten implementieren:** Daraufhin werden die neuen Fähigkeiten implementiert. Das erwünschte neue Verhalten wird eingeübt. Dabei werden Mitarbeitende daran erinnert, dass sie den neuen Verhaltensweisen zugestimmt haben, wie das alte Verhalten aussah und warum es nicht mehr ausgeübt wird.
8. **Verankerung:** Das neue Verhalten muss verankert und ein Rückfall in alte Gewohnheiten unterbunden werden. Die Verankerung kann durch Wiederholungen, Methoden des willentlichen Vergessens oder Nudging[41] umgesetzt und unterstützt werden.
9. **Sicheres Verhalten:** Im letzten Schritt ist das neue sichere Verhalten zur Routine geworden. Um dieses neue Verhalten zu stützen, kann ein Belohnungssystem eingeführt werden.

Zu jedem Schritt sind geeignete Werkzeuge und Methoden zur Unterstützung zu wählen. Bei der Auswahl von externen Dienstleistern und Services muss darauf geachtet werden, dass die Teilschritte des dargestellten Umsetzungsprozesses abgedeckt sind. Ggf. müssen diese durch weitere Maßnahmen ergänzt werden.

Alle Maßnahmen sollten entsprechend der Bedürfnisse der verschiedenen Adressaten (SW-Entwickler, IT, Personalabteilung, Marketing, Vertrieb etc.) zielgruppengerecht ausgewählt und umgesetzt werden.

Um sicher zu gehen, dass die Voraussetzungen für die Durchführung des jeweils nächsten Prozessschrittes gegeben sind und das Erreichen der definierten Ziele insgesamt zu gewährleisten, sollte nach jedem Prozessschritt eine Wirksamkeitsprüfung durchgeführt werden. Ggf. ist der Schritt zu wiederholen bzw. zu vertiefen.

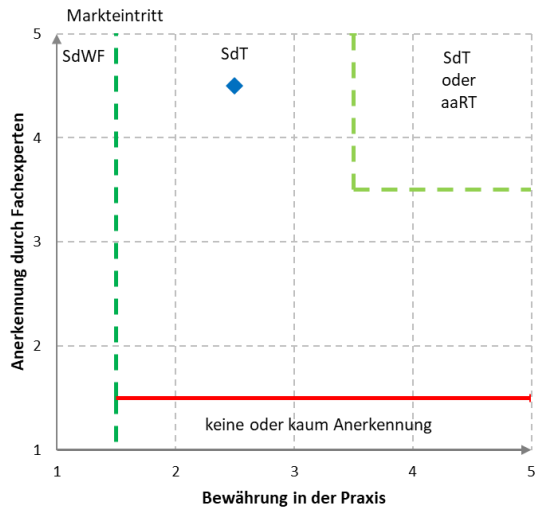
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



[41] Stups oder Schubs, im Sinne von Denkanstoß. Schaffung von Rahmenbedingungen, die Menschen dazu anregt, ein (auch von ihnen selbst) gewünschtes Verhalten zu zeigen, z.B. die Positionierung von gesunden Speisen in Blick und Griffhöhe in einer Kantine.

3.3.15 Asset Management

Als "Asset" wird jede Art von (Vermögens-Informations-)Wert einer Organisation bezeichnet. Beim "Asset Management" geht es um die Richtlinien und Prozesse, die dabei helfen, über die einzelnen Assets während ihres jeweiligen Lebenszyklus Rechenschaft abzulegen. Aus Sicht der IT (IT Asset Management) geht es um das Management von IT-Ressourcen - Hardware, Software aber auch Daten und von der Organisation genutzte Cloud Services.

Aus Sicht der Informationssicherheit liefert die Auflistung der Werte und Eigentümer die Grundlage für eine Schutzbedarfsanalyse und hilft bei der Priorisierung von Risikobehandlung und Wahl der Schutzmaßnahmen. Wesentlich ist, dass das Assetverzeichnis nicht eine abschließende Liste ist, sondern analog der CMDB bei ITIL zu verstehen ist und grob in immaterielle (intangible) und materielle (tangible) Assets aufgeteilt werden kann.

Aus Sicht der IT-Sicherheit liefert IT-Asset Management die Grundlage für eine umfassende Sicht auf die IT-Landschaft der Organisation und damit für alle Maßnahmen der IT-Sicherheit betreffend IT-Assets; u.a. Risikoeinschätzung, Patchmanagement, Security Monitoring und Zero Trust.

Ohne ein strukturiertes Asset Management können Unternehmen anfällig für unbefugten Zugriff, Verlust oder Zerstörung kritischer Informationen sein. Denn wenn die Unternehmenswerte unbekannt sind, kann man ihren Schutzbedarf nicht feststellen und auch keine passenden Schutzmaßnahmen initiieren.

Das Asset Management ermöglicht die Einhaltung gesetzlicher und regulatorischer Anforderungen und fördert die betriebliche Effizienz durch eine klare Zuordnung von Verantwortlichkeiten und Ressourcen. Außerdem verhindert ein vollständiges Asset-Management das Auftreten von sogenannter "Schatten-IT", die den Angreifern aussichtsreiche Angriffsvektoren bieten können, die vom Unternehmen nicht kontrolliert werden. Daher sollte das Asset Management in die wesentlichen Beschaffungsprozesse eingebunden werden.

Zu den wesentlichen Aufgaben im Asset Management gehören:

- **Erfassung und Inventarisierung**: Alle Unternehmenswerte sollten systematisch erfasst, klassifiziert und inventarisiert werden.
- **Verantwortlichkeiten zuweisen**: Für jedes Asset sollte eine klare Verantwortlichkeit definiert werden, einschließlich der Schutzverantwortung.
- **Klassifizierung**: Unternehmenswerte sollten nach ihrer Bedeutung klassifiziert werden, um sicherzustellen, dass sie entsprechend geschützt werden.
- **Richtlinien und Verfahren**: Implementierung klarer Richtlinien und Verfahren für die Handhabung und den Schutz von Medien, um die unberechtigte Weitergabe, Veränderung oder Zerstörung zu vermeiden.
- **Regelmäßige Überprüfung**: Regelmäßige Überprüfung und Aktualisierung des Asset-Management-Plans, um sicherzustellen, dass er aktuelle Bedrohungen und Geschäftszielen entspricht.

Die erprobten Praktiken und Empfehlungen sind zahlreichen Normen und Regelwerken beschrieben, darunter:

- BSI-Standard 200-2: Definiert einen strukturierten Ansatz zur Ermittlung der Assets und der Einordnung des Schutzbedarfs von normal bis sehr hoch
- ISO/IEC 27001: Diese internationale Norm für Informationssicherheitsmanagementsysteme (ISMS) betont die Bedeutung des Asset-Managements.
- NIST SP 800-53: Das Rahmenwerk des National Institute of Standards and Technology (NIST) enthält Richtlinien zur Verwaltung von Informationssystemressourcen.
- ISO/IEC 19770-1: Spezifiziert die Anforderungen an ein IT Asset Management System im Kontext der Organisation
- COBIT: Das Control Objectives for Information and Related Technologies (COBIT) Framework der ISACA umfasst Prinzipien und Praktiken für das IT-Management, einschließlich des Asset-Managements.

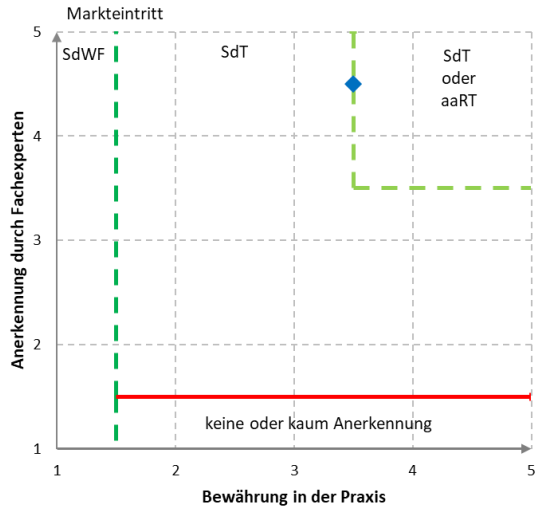
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

Einordnung der Maßnahme



3.3.16 Incident Management

Im Rahmen des Sicherheits-Incident-Managements werden technische und organisatorische Maßnahmen als Reaktion auf erkannte oder potenzielle 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 juristische Fragestellungen einschließt.

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

Die wesentlichen Aktivitäten des Incident Managements sind:

- Erfassung: Identifikation und Meldung des Vorfalls
- Klassifizierung: Bewertung und Einordnung als Sicherheitsvorfall
- Analyse: Untersuchung des Vorfalls und Bestimmung des Ausmaßes
- Reaktion: Umsetzung von Maßnahmen zur Eindämmung und Behebung
- Wiederherstellung: Rückkehr zum Normalbetrieb und Sicherstellung der Integrität
- Nachbereitung: Dokumentation und Analyse zur Vermeidung zukünftiger Vorfälle
-

Da Incidents oftmals mit der Verletzung des Sicherheitsschutzziels "Verfügbarkeit" einhergehen, muss initial eine qualifizierte Erstanalyse und Klassifizierung eines Incidents erfolgen. Ausgehend davon wird die Bearbeitung dann je nach Ergebnis vom jeweiligen Fachteam übernommen. Da ist es sinnvoll, zwischen funktionalen und Sicherheits-Incidents zu unterscheiden (oder diese zumindest gesondert zu kennzeichnen), da beide unterschiedliche Herangehensweisen, Skills und Maßnahmen erfordern. Funktionale Incidents betreffen die allgemeinen Betriebsabläufe und IT-Dienste, während Sicherheits-Incidents spezifisch auf die Bedrohung und Verletzung der Informationssicherheit abzielen. Letztere benötigen oft dringlichere und spezialisierte Maßnahmen, um den Schaden zu minimieren und die Integrität der Systeme zu gewährleisten.

Von den Bearbeitern von Sicherheits-Incidents werden z.B. Kenntnisse der IT-Sicherheit und der Netzwerkarchitektur des jeweiligen Unternehmens sowie operative Erfahrung in der Forensik von Sicherheitsvorfällen gefordert.

Um diese Anforderungen fortlaufend sicherzustellen, ist der Einsatz von sogenannten SOC- und CSIRT-Teams sinnvoll. Das Security Operations Center (SOC) ermöglicht die kontinuierliche Überwachung der IT-Infrastruktur, schnelle Identifikation von Bedrohungen und koordinierte Reaktionsmaßnahmen. Ein Computer Security Incident Response Team (CSIRT) konzentriert sich auf einzelne, schwerwiegende und komplexe Vorfälle. Dadurch wird die Effizienz und Effektivität des Incident Managements erheblich gesteigert.

Die Zusammenführung von Datenquellen in SIEM (Security Information and Event Management)-Systemen oder anderen Plattformen zur Identifizierung und Bewertung von Sicherheitsvorfällen ist eine wichtige Voraussetzung für die frühzeitige Erkennung und Analyse von Bedrohungen. (Teil-)automatisierte Abläufe, gegebenenfalls unter Verwendung von Security Orchestration, Automation and Response (SOAR)-Lösungen, sind für schnelle Reaktionszeiten empfehlenswert.

Neben der Definition und Dokumentation eines standardisierten Verfahrens des Sicherheits-Incidents Managements muss auch die Schulung der Mitarbeitenden sichergestellt werden, um das Sicherheitsbewusstsein des Personals zu stärken und den Umgang mit Sicherheitsvorfällen zu üben.

Der Aufbau eines Security Incident Teams kann anhand der Rahmenwerke ISO/IEC 27035, NIST SP 800-61 oder CIS Controls erfolgen.

Der Übergang von einer schwerwiegenden Serviceunterbrechung kann von Incident zu Major Incident und weiter zur Einberufung des Notfallstabs führen.

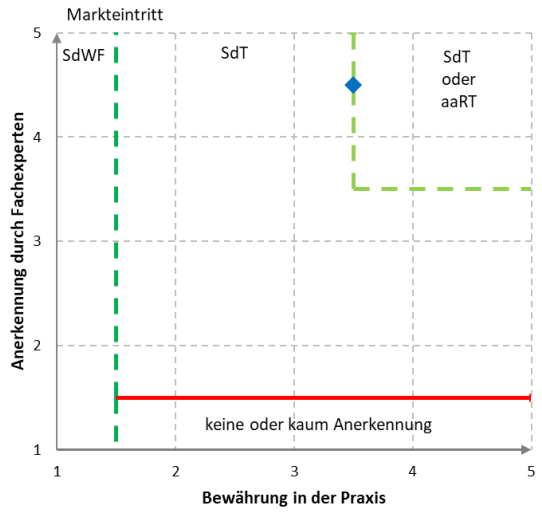
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



3.3.17 Geschäftskontinuitäts-Management (BCM)

Business Continuity Management (BCM) ist ein systematischer Ansatz, der sicherstellt, dass Unternehmen auch in Krisensituationen handlungsfähig bleiben. Es umfasst Strategien und Maßnahmen zur Sicherung zeitkritischer Geschäftsprozesse und zur Minimierung von Ausfallzeiten.

Die Einführung eines BCM erfordert die Unterstützung, Ausrichtung und Bereitstellung von Ressourcen durch die oberste Leitung, dies wird durch die BCM-Leitlinie dokumentiert und damit das BCM in Kraft gesetzt.

BCM ist unerlässlich, um die Resilienz eines Unternehmens gegenüber verschiedenen Bedrohungen zu gewährleisten. Ohne ein robustes BCM-System können Unternehmen im Falle von Störungen oder Krisen erhebliche finanzielle Verluste, Reputationsschäden und operative Ausfälle erleiden. Die Notwendigkeit von BCM ergibt sich aus der Vielzahl potenzieller Bedrohungen, denen Unternehmen ausgesetzt sind:

- **Naturkatastrophen**: Ereignisse wie Erdbeben, Überschwemmungen oder Stürme können die physische Infrastruktur eines Unternehmens schwer beschädigen und den Geschäftsbetrieb unterbrechen.
- **Cyber-Angriffe**: Angriffe auf die IT-Infrastruktur (z.B. Malware, DDoS, Ransomware) können zu erheblichen Datenverlusten und Betriebsunterbrechungen führen.
- **Technische Ausfälle**: Stromausfälle, Hardware-Defekte oder Software-Fehler können den Betrieb kritischer Systeme beeinträchtigen.
- **Pandemien und Epidemien**: Gesundheitskrisen (z.B. COVID-19-Pandemie) können die Verfügbarkeit von Personal und Ressourcen stark einschränken.
- **Lieferketten Ausfälle**: Die zunehmende Abhängigkeit von Informationstechnologie (IT), funktionierenden Lieferketten und externen Dienstleistern (z.B. Dienstleistungs-, Zulieferungs- und Versorgungsunternehmen) macht Institutionen anfällig für Störungen. Diese Störungen beeinträchtigen die Verfügbarkeit der Geschäftsprozesse und stellen somit ein erhebliches Risiko für das Business Continuity Management System (BCMS) dar. Ein robustes BCMS muss daher explizit Maßnahmen zur Identifizierung, Bewertung und Bewältigung solcher Lieferkettenstörungen beinhalten.

Mit BCM wird die allgemeine Situation und Resilienz des Unternehmens betrachtet. Sie betrifft überwiegend die Aufrechterhaltung zeitkritischer Geschäftsprozesse und der dafür notwendigen technischen und organisatorischen Komponenten und Maßnahmen.

Ein effektives BCMS besteht aus mehreren Kernkomponenten:

1. **Risikobewertung und Bedrohungsanalyse**: Identifikation und Bewertung potenzieller Risiken und Bedrohungen für das Unternehmen. Sie bilden die Grundlage für alle weiteren BCM-Aktivitäten.
2. **Business Impact Analysis (BIA)**: Dabei werden die kritischen Geschäftsprozesse identifiziert, Auswirkungen von Störungen auf den Geschäftsbetrieb betrachtet und die Prioritäten für die Wiederherstellung festgelegt.
3. **Strategieentwicklung**: Sie ermöglich die Entwicklung von Strategien und Maßnahmen zur Aufrechterhaltung oder schnellen Wiederherstellung der Geschäftsprozesse. Neben den Maßnahmen ist es wesentlich, dass die Rollen und Verantwortlichkeiten innerhalb des Unternehmens verbindlich festgelegt sind. Es muss sichergestellt werden, dass alle Beteiligten ihre Aufgaben kennen und im Krisenfall effektiv handeln können.
4. **Implementierung und Testen**: Schließlich werden die entwickelten Strategien und Notfallpläne umgesetzt. Ihre Wirksamkeit muss regelmäßig getestet und bei Bedarf angepasst werden. Die regelmäßige Überprüfung und Aktualisierung der BCM-Pläne basierend auf den Ergebnissen von Tests und realen Vorfällen.

Die Implementierung eines BCM-Systems kann im Wesentlichen entlang dieser Rahmenwerke erfolgen:

- **ISO 22301**: Diese internationale Norm stellt den anerkannten Standard für die Einrichtung und den Betrieb eines Business Continuity Management Systems (BCMS) dar. Sie strukturiert die Anforderungen für die Planung, Implementierung und Überwachung eines BCMS nach den

ISO-Anforderungen für Managementsystemnormen und bildet die Grundlage für die Möglichkeit der Zertifizierung eines BCM-Systems.

- **BSI-Standard 200-4**: Der BSI-Standard 200-4 bietet eine umfassende praxisnahe Anleitung zum Aufbau einer BCM-Organisation und Implementierung eines BCMS insbesondere in Verbindung mit dem IT-Grundschutz auf Basis ISO 27001. Der Standard 200-4 wird mit umfangreichen Hilfsmitteln durch das Bundesamt für Sicherheit in der Informationstechnik kostenfrei bereitgestellt.

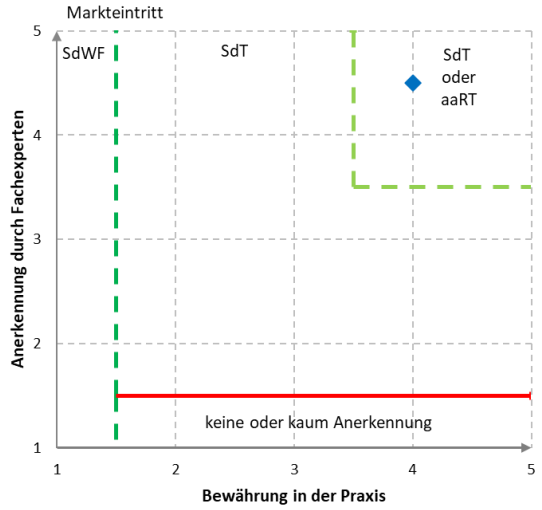
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



3.3.18 Notfall- und Krisenmanagement

Notfallmanagement bezieht sich auf die Planung und Durchführung von Maßnahmen, um auf IT-Notfälle, wie Systemausfälle oder Cyber-Angriffe, schnell und effektiv zu reagieren. Ziel ist es, die Auswirkungen solcher Vorfälle zu minimieren und den Geschäftsbetrieb so schnell wie möglich wiederherzustellen.

Krisenmanagement hingegen umfasst die Reaktion auf schwerwiegendere und oft unvorhersehbare Ereignisse, die eine flexible und umfassende Handlungsweise erfordern. Es geht darum, strategische Entscheidungen zu treffen, um die langfristige Stabilität und Sicherheit der Organisation zu gewährleisten.

Aus einem Notfall kann eine Krise entstehen oder als solche deklariert werden. Hierfür bedarf es einer standardisierten Vorgehensweise und abgestimmter Kriterien, nach welchen die entsprechende Kritikalitätsstufe und hierfür vorgesehenes Ablaufprotokoll aktiviert wird.

Ein (zyklischer) Krisenmanagementprozess besteht aus:

1. Lagefeststellung / Kontrolle
2. Lagebewertung
3. Maßnahmenplanung und -Auswahl
4. Delegation und Implementierung von Maßnahmen

Obwohl sich Business Continuity Management (BCM) sowie Notfall- und Krisenmanagement sehr ähneln, unterscheiden sie sich in ihrer Betrachtungsweise:

	BCM	Notfall- Krisenmanagement
Fokus	Langfristige Sicherstellung der Geschäftskontinuität	Kurzfristige Reaktion und Bewältigung von akuten Bedrohungen
Ziel	Erfüllung der Verfügbarkeitsanforderungen kritischer Geschäftsprozesse	Schutz von Menschen und Vermögenswerten, Minimierung von Schäden
Aktivitäten	Vorbereitung und Erprobung von Geschäftsfortführungsplänen (GFP) für kritische Geschäftsprozesse und Services	Sofortige Reaktionsmaßnahmen, operative und strategische Entscheidungen während einer Krise
Szenarien	Notfallpläne liegen für Ausfallszenarien vor und Abläufe sind bekannt.	Unbekannte bzw. besonders schwerwiegende Szenarien für die keine Notfallpläne vorliegen.

Tabelle 4: Abgrenzung BCM vs. Notfall- und Krisenmanagement

Eine Struktur für die ersten Stunden und Tage einer Krise sollte abgestimmt und dokumentiert sein. Insbesondere die Alarmierung und Eskalation, die Zusammensetzung und Arbeitsfähigkeit des Krisenstabes sowie Maßnahmen für eine schnelle Wiederherstellung der Geschäftsprozesse sollten festgehalten werden.

Mit Hilfe, der in einer BIA erhobenen Parameter kann, das Schadenspotential eines Ausfalls bewertet werden. Vereinheitliche Bewertungen zusammen mit der Betrachtung der Zeithorizonte helfen das sog. Untragbarkeitsniveau zu definieren und daraus entsprechende Maßnahmen abzuleiten.

Hinweis: Wichtige Parameter und Begriffe des BCM und Notfallmanagement sind im Glossar des BSI-Standard 200-4 definiert: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=3

Krisendefinition und Aktivierung Krisenorganisation
Es muss eindeutig geregelt sein, wer unter Berücksichtigung aller zu dem Zeitpunkt vorliegenden Informationen, die aktuelle Lage zu einer Krise erklären darf und damit die definierten Prozesse und Ressourcen aktiviert. Diese Entscheidung kann entlang zuvor definierter Kriterien hinsichtlich Auswirkung und Umfang des Vorfalls erfolgen. Im Wesentlichen immer dann, wenn die Behandlung des Vorfalls die Möglichkeiten der etablierten Strukturen übersteigt und die Auswirkungen weder zeitlich noch in den Auswirkungen abzusehen ist. Mit dem Ausrufen der Krise übernimmt dann der Krisenstab, geleitet vom Krisenmanager, die Verantwortung für die Bewältigung der Situation.

Krisenstab und Verantwortlichkeiten
Die Zusammensetzung des Krisenstabs kann je nach Art der Krise variieren. Neben dem Krisenmanager ist es empfehlenswert, mindestens ein Mitglied der Geschäftsleitung vorzusehen, um den Krisenstab weitgehend entscheidungsfähig zu machen, ohne das weitere Gremien hinzugezogen werden müssen. Es ist sinnvoll, einen Kernkrisenstab mit den in jeder Krise notwendigen Rollen zu bilden. Dieses Kernteam wird situativ durch weitere Rollen ergänzt. Je nach Bedarf kommen in Frage:

Kernteam	Situative Ergänzung
• Geschäftsleitung, • Kommunikation, • Recht, • Protokoll (Lagebild)	• Vertreter kritischer Fachabteilungen • IT • Kommunikation • Personal • Finanzen • Recht • Datenschutz • externe Krisenberater • Betriebsrat • Protokollführer

Tabelle 5: Zusammensetzung des Krisenstabs

Für jede Position im Krisenstab muss eine klare Stellvertreterregelung und Erreichbarkeit definiert sein, um die Handlungsfähigkeit auch bei Abwesenheit einzelner Mitglieder sicherzustellen.

Situative Erweiterungen sind jederzeit mit dem Ziel möglich, alle notwendigen Kompetenzen zu beteiligen, die für eine schnelle Entscheidung der weiteren Vorgehensweise notwendig sind.

Kommunikation und Informationsweitergabe
Im Krisenfall müssen alle über den Krisenstab hinaus relevanten internen und externen Stakeholder über zuvor definierte Kommunikationswege informiert und in die Arbeit der Krisenorganisation eingebunden und die aktuelle Lage informiert werden. Ein Krisenkommunikationsplan sollte folgende Aspekte umfassen:

- Interne Kommunikation: regelmäßige Updates an Mitarbeiter
- Externe Kommunikation: Medienmanagement, Kundeninformation, Behördenkommunikation
- Vorgefertigte Kommunikationsvorlagen für verschiedene Krisenszenarien
- Festlegung von Sprecherrollen und Kommunikationskanälen

Meldepflichten und rechtliche Anforderungen
Es sind verschiedene Meldepflichten zu beachten, die einzuhalten sind:

- Betreiber Kritischer Infrastrukturen (KRITIS, NIS2) müssen Vorfälle, gemäß der Vorgaben und Meldewege, an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.
- Abhängig von der Branche können weiter Meldepflichten relevant sein. Beispielsweise für Telekommunikationsunternehmen (Bundesnetzagentur) oder Finanzinstitute (BaFin).
- Sofern der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ist gemäß DSGVO innerhalb von 72 Stunden eine Meldung an die zuständige Datenschutzbehörde zu erstatten.

Neben diesen gesetzlichen oder regulatorischen Meldepflichten sollten auch interne Meldepflichten entsprechend vorbereitet und berücksichtigt werden (Cyber-Versicherung, Anzeige bei der Polizei, …). Es ist wichtig, diese Meldepflichten regelmäßig, mindestens jährlich, auf Aktualität zu überprüfen und gegebenenfalls anzupassen. Für jede Meldepflicht sollten konkrete Ansprechpartner oder Stellen benannt und deren Kontaktdaten stets aktuell gehalten werden.

Regelmäßige Überprüfung und Anpassung
Die Krisenmanagementpläne sollten verfügbar sein, regelmäßig überprüft und aktualisiert werden, um auf neue Herausforderungen oder Veränderungen in der Unternehmensstruktur oder im rechtlichen Umfeld zu reagieren.

Diese Überprüfung kann in regelmäßigen (mindestens jährlichen) Übungen erfolgen (bspw. Schreibtischübungen, Planbesprechungen, Stabsübungen,…), um so die Effektivität der Krisenprozesse sicherzustellen. Ebenso sollte nach Beendigung einer Krise eine Nachbereitung erfolgen, um die vorhandenen Pläne auf Basis der gewonnenen Erkenntnisse zur Effektivität und Verbesserungspotentialen zu aktualisieren.

Als sehr hilfreich haben sich die BSI-Notfallkarte[42] und das Notfallhandbuch[43] erwiesen. Sie bieten operative Vorlagen mit den wichtigsten Daten auf einen Blick, um für den Fall der Fälle gerüstet zu sein.

[42] BSI Notfallkarte: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html
[43] BSI Notfallhandbuch: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html

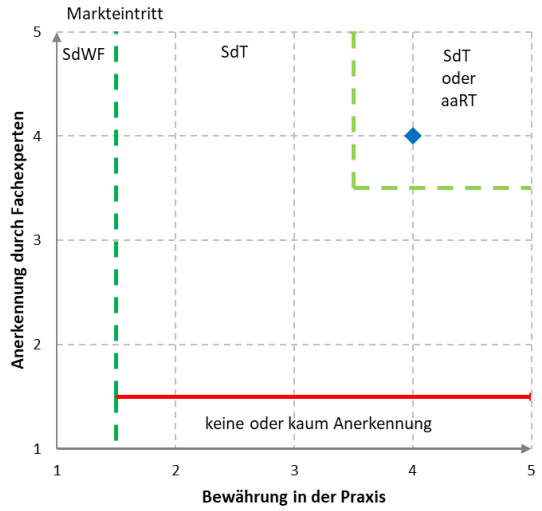
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



3.3.19 Notfallübungen

Weltweit nimmt die Anzahl der Cybersecurity-Angriffe und der Bedrohungen weiter zu. Demnach ist die Frage "ob ein Unternehmen angegriffen wird" obsolet. Vielmehr müssen sich die Unternehmen auf einen Angriff und den hieraus resultierenden organisatorischen Maßnahmen vorbereiten und diese regelmäßig testen und üben.

Im Rahmen einer Notfallübung können potenzielle Auswirkungen eines erfolgreichen Cybersecurity-Angriffs simuliert werden. Es sind verschiedene Formen von Notfallübungen, wie z.B. Planübungen (Tabletop exercises), Krisenstabsübungen und Vollübungen möglich. Notfallübungen können isoliert, z.B. abteilungsintern, oder integriert (Notfallverbundübung) geplant werden. Die Übung als Planspiel ermöglicht die Erprobung des Umgangs mit einem fiktiven Angriff sowie das Testen der eigenen Reaktionsfähigkeit. Das Ziel der Übung ist es, mögliche organisatorische Schwachstellen zu identifizieren, um diese im Ernstfall zu vermeiden.

Mit der Notfallübung wird der Umgang mit den zuvor festgelegten Sicherheitsbedrohungen und insbesondere die Wirksamkeit bestehender organisatorischer Maßnahmen erprobt und Schwachpunkte identifiziert. Die Teilnehmer werden mit einer unbekannten Situation konfrontiert, mit denen sie sich diskursiv auseinandersetzen müssen (z.B. durch Fragen oder Aufgaben und Handlungen). Eine solche Notfallübung ermöglicht insbesondere:

- sich mit konkreten Bedrohungsszenarien in einer gezielten Übung vor dem Ernstfall zu befassen
- Diskussionen über bestehende Richtlinien, Notfallpläne und Verfahren zu führen und diese zu testen
- organisatorische Maßnahmen zu entwickeln und zu testen, inwiefern diese Maßnahmen gegen bestimmte Bedrohungen wirken
- Erprobung bestehender organisatorischer Maßnahmen
- Bewusstsein über Rollen, Kompetenzen und Zuständigkeiten zu schaffen
- Verantwortlichkeiten und Kommunikationslinien zu prüfen und einer Belastungsprobe zu unterziehen
- Bereitschaft zu fördern und Vertrautheit mit Verfahrensweisen einzustudieren.

Die Durchführung von Sicherheitsübungen erfordert jeweils ein individuelles, für die jeweilige Organisation konzipiertes und auf deren Besonderheiten abzielendes Vorfallszenario. Je nach Bedarf lassen sich die individuellen Umstände der durchzuführenden Vorfälle während der Übung in ihrer Komplexität und Ausmaß steigern.

Vorweg zur Sicherheitsübung sollten Ziele festgelegt werden, um die Wirksamkeit der Übung zu validieren. Beispielsweise können die folgenden Ziele definiert werden:

- Prozesse des Informationsaustauschs zwischen Stakeholdern sollen geübt werden
- Die Wirksamkeit des Notfallplans soll getestet werden
- Maßnahmen gegen eine bestimmte Bedrohung sollen entwickelt werden
- Krisenkommunikation, intern und/oder extern, soll erprobt werden.

Um die relevanteste Bedrohung für das Szenario zu identifizieren, können Risikoanalyse und Threat Modeling genutzt werden. Sofern umsetzbar und sinnvoll können auch technische Tools eingesetzt werden, die das zu erprobendes Szenario messen und die Wirksamkeit bewerten.

Die Notfallübung sollte in einem vertrauten, informellen und fehlertoleranten Rahmen stattfinden, mit hinreichender Prozessorientierung. Da sich die Notfallübung auf die Prüfung von organisatorischen Maßnahmen im Rahmen eines erfolgreichen Angriffs fokussiert, ist kein virtuelles oder gesichertes digitales Netzwerk mit realen Werkzeugen und Techniken notwendig.

Benötigt wird allerdings organisatorisches Wissen, Expertise im Bereich Informationssicherheit, Kommunikationsfähigkeit und eine objektive Bewertungsfähigkeit als auch nötige Kreativität, um Szenarien zu entwickeln, die gleichzeitig realistisch sind und zum Ziel der Übung passen.

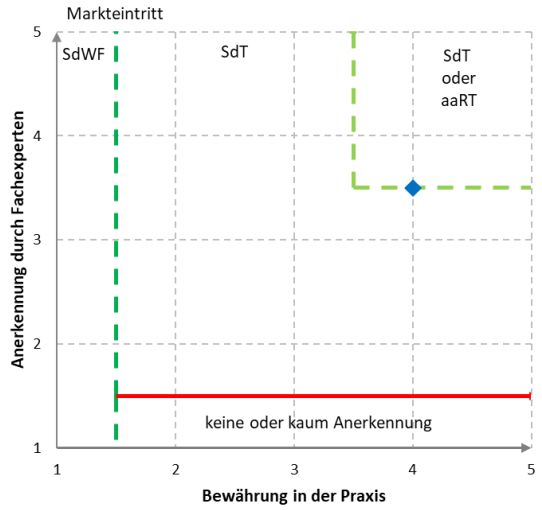
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



3.3.20 Technische Sicherheitsüberprüfung

In der Handreichung ist an verschiedenen Stellen die Rede von Audits, z.B. bei der Prüfung von Informationssicherheitsmanagementsystemen wie ISO 27001 oder BSI-Grundschutz. Die allermeisten Auditformen sind Prozessaudits und werden auf Basis von Nachweisen in Form von Dokumentation

erbracht. Es bietet sich jedoch an, Audits um technische Sicherheitsüberprüfungen zu ergänzen. Während Audits korrekte und sinnvolle Prozesse nachweisen, liefern daraus abgeleitete technische Sicherheitsüberprüfungen Nachweise über deren tatsächliche Wirksamkeit. Denn, selbst wenn bei einer perfekt dokumentierten Firewall und einem etablierten Change-Prozess können sich gravierende Sicherheitslücken verbergen.

Bei den hier vorgestellten Technischen Sicherheitsüberprüfungen handelt es sich um einmalige, im Kontext von Audits durchgeführte Prüfungen. Laufende technische Maßnahmen, die als kontinuierlicher Prozess im Unternehmen etabliert werden können - wie etwa permanente Schwachstellenscans - sind kein Gegenstand dieses Beitrags.

Je nach Umgebung gibt es eine Vielzahl möglicher Prüfmethoden. Die folgenden Optionen sind daher nicht abschließend und sollten situationsgerecht von Auditoren mit entsprechendem technischen Domänenwissen ausgewählt werden. Die Durchführung sollte stets durch erfahrene Fachexperten erfolgen, deren tägliche Arbeit technische Sicherheitsüberprüfungen umfasst.

Konfigurationsanalysen

Bei Konfigurationsanalysen wird idealerweise ein Abgleich aus vorliegenden Sicherheitskonzepten und etablierter Konfiguration und Change-Management vorgenommen. In der Regel handelt es hierbei um Stichprobenprüfungen. Im Ergebnis sollen dabei Unterschiede zwischen Vorgaben und der technischen Umsetzung aufgedeckt werden. Die folgenden beispielhaften Fragestellungen können als Orientierungshilfe dienen:

Bereich	Fragestellung
Active Directory	Sind die Passwortrichtlinien korrekt konfiguriert?
Backup-Konfiguration	Sind Backup-Jobs entsprechend der Dokumentation eingerichtet und werden sie gemäß Change-Management angepasst?
Client-Management	Sind alle Clients im Patch-Management verwaltet und aktuell?
Cloud-Konfigurationen	Sind IAM-Rollen und Berechtigungen in Cloud-Diensten (z.B. AWS IAM oder Microsoft Azure RBAC) entsprechend den Sicherheitskonzepten umgesetzt?
Datenbank-Management	Sind Benutzerkonten in produktiven Datenbanken korrekt dokumentiert und rollenbasiert mit minimal notwendigen Rechten ausgestattet?
Drucker und Multifunktionsgeräte	Sind Zugriffsbeschränkungen aktiviert und wird der Netzwerkzugriff auf das Notwendigste beschränkt?
E-Mail-Gateways	Sind Filter- und Schutzmechanismen (z.B. SPF, DKIM, DMARC) aktiv und korrekt konfiguriert?
Firewall-Nutzer	Sind alle Nutzer dokumentiert? Die Prüfung der individuellen Nutzerkonten und der sicheren Vorhaltung des "Admin"-Passworts erfolgt separat in der Prozessprüfung.
Firewall-Regeln	Sind diese eindeutig der Dokumentation und den Change-Requests zuordenbar?
Mobile-Device-Management	Sind mobile Endgeräte (z.B. Smartphones und Tablets) registriert, gemanaged und verschlüsselt?
Monitoring-Systeme	Sind Backup-Jobs entsprechend der Dokumentation eingerichtet und werden sie gemäß Change-Management angepasst?
Monitoring-Systeme	Sind alle kritischen Systeme im Monitoring korrekt eingebunden und werden Alarme gemäß definierter Schwellenwerte ausgelöst?
Serverkonfiguration	Entsprechen Dienste, Protokolle und Ports den freigegebenen und dokumentierten Vorgaben?
VPN-Zugänge	Ist der zweite Authentifizierungs-Faktor überall wo möglich aktiviert?
Webserver	Entsprechen SSL/TLS-Konfigurationen den dokumentierten Mindestanforderungen. Sie veralteten Protokolle deaktiviert (z.B. keine veralteten Protokolle wie TLS 1.0)?
WLAN-Konfiguration	Werden Unternehmens-WLANs durch WPA2-Enterprise oder höher geschützt? Sind Gastnetzwerke ausreichend segmentiert?

Tabelle 6: Beispielhafte Fragestellungen bei Konfigurationsanalysen

Härtungsüberprüfungen[44]

Im Rahmen von Härtungsüberprüfungen wird die Umsetzung technischer Mindeststandards auf Systemen und Anwendungen bewertet. Ziel ist es zu überprüfen, ob etablierte Härtungsvorgaben (z.B. CIS-Benchmarks oder eigene interne Standards) konsequent umgesetzt wurden. Dabei werden Unterschiede zwischen den Vorgaben für die Konfiguration und Common Practices identifiziert. Beispielhafte Fragestellungen sind:

Bereich	Fragestellung
Applikations-Härtung	Wurden Standardkennwörter entfernt und sichere Konfigurationsoptionen gewählt?
Backup-Systeme	Werden Backup-Server und -Speicher speziell gehärtet, z.B. durch restriktive Netzwerkzugriffe und separate Authentifizierung?
Client-Härtung	Ist der Zugriff auf administrative Funktionen für Benutzer eingeschränkt? Sind die zulässigen Applikationen (white listing) vorhanden und korrekt konfiguriert?
Container-Härtung	Werden Container-Images aus vertrauenswürdigen Quellen bezogen und regelmäßig aktualisiert? Sind unnötige Dienste innerhalb der Container deaktiviert?
Mobile Geräte	Ist eine Verschlüsselung des lokalen Speichers aktiv? Sind Gerätemanagementrichtlinien (z.B. Remote-Löschung) eingerichtet?
Systemhärtung	Sind unnötige, da nicht verwendete, Dienste deaktiviert und sichere Konfigurationen eingestellt?
Virtualisierungs-plattformen	Ist der Zugriff auf Hypervisor-Managementsysteme (z.B. vCenter) geschützt und auf autorisierte Personen beschränkt?

Tabelle 7: Beispielhafte Fragestellungen bei Härtungsüberprüfungen

Automatisierte Schwachstellenscans

Automatisierte Schwachstellenscans erfassen systematisch bekannte Schwachstellen in der technischen Infrastruktur. Sie sollten gezielt eingesetzt werden, um einen Überblick über den aktuellen Schwachstellenstatus zu erhalten. Beispiele:

- **Backup-Infrastrukturen:** Prüfen auf verwundbare oder veraltete Backup-Software und auf Fehlkonfigurationen, die einen unautorisierten Zugriff ermöglichen könnten.
- **Cloud-Infrastrukturen:** Scannen nach falsch konfigurierten Speicherbereichen (z.B. offene S3-Buckets), veralteten Images oder unsicheren Zugriffskontrollen.
- **Container-Umgebungen:** Erkennen von Schwachstellen in Container-Images oder veralteten Basis-Images, die aus bekannten Sicherheitslücken resultieren können.
- **E-Mail-Systeme:** Überprüfung auf fehlende Absicherungen wie fehlendes SPF, DKIM oder DMARC sowie bekannte Schwachstellen in verwendeten Mail-Servern.
- **Netzwerkgeräte**: Auffinden veralteter Firmware-Versionen oder unsicherer Standardkonfigurationen.
- **Server und Clients**: Erkennen von fehlenden Patches, unsicheren Konfigurationen oder bekannten Exploits.

Automatisierte Schwachstellenscans sind für Standardkomponenten gut geeignet. Allerdings können sie bei (Web-Anwendungen) nur sehr bedingt Schwachstellen erkennen, da diese oftmals individuell entwickelt wurden (Individualsoftware).

Penetrationstests

"Den einen" Penetrationstest per se gibt es nicht, da mittels Penetrationstests ein realer Angreifer simuliert werden soll. Die Penetrationstests sind daher individuelle Prüfungen, die insbesondere bei Prüfungen unternehmenskritischer (Web-)Anwendungen sinnvoll sind.

Penetrationstest zeigen auf, wie es um die Widerstandsfähigkeit der Systeme und Anwendungen gegenüber gezielten Angriffen bestellt ist. Vertiefende Informationen zu den Penetrationstest werden in

[44] Siehe auch Kapitel "Systemhärtung"

der Handreichung "Penetrationstests" von TeleTrusT beschrieben. Ihre Veröffentlichung ist 2025 geplant.

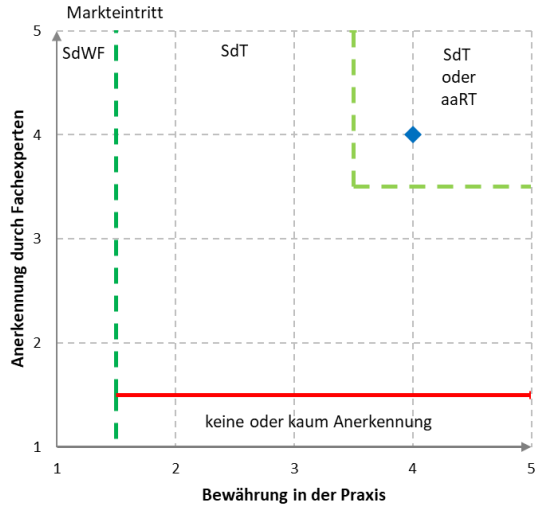
Welche Schutzziele werden durch die Maßnahme abgedeckt?

☒ Verfügbarkeit

☐ Integrität

☐ Vertraulichkeit

Einordnung der Maßnahme



4 Exkurse

Während sich die zuvor beschriebenen Maßnahmen auf die regulatorischen Vorgaben im Zusammenhang mit der Informationssicherheit fokussieren, so bleiben dennoch meist nur graue Theorie, Denn sie sind bewusst von der unternehmerischen Praxis getrennt, um die Technologie zu erklären und diese gemäß der initial erklärten Bewertungskriterien dem Technologieniveau einzuordnen.

Mit diesem Abschnitt soll der Zusammenhang zwischen den zuvor beschriebenen Sicherheitsmaßnahmen und der sich am Markt verändernden Sicherheitslage geschaffen werden. Auf diese Weise soll der Praxisbezug herausgearbeitet und die Anwendbarkeit der Maßnahmen dem Leser nähergebracht werden,

4.1 Maßnahmen gegen Ransomware-Angriffe

Ransomware beschreibt eine Angriffsart, die den Zugriff auf persönliche und Unternehmensdaten blockiert (in der Regel durch Verschlüsselung) und zur Freigabe dieser Daten ein Lösegeld (engl. "ransom") verlangt. In den meisten Fällen ist eine Rekonstruktion der originalen Daten ohne die Zahlung des Lösegelds nicht möglich. Oftmals ist ein Ransomware-Angriff mit der Drohung verbunden, sensible oder geheime Daten des Angriffsopfers zu veröffentlichen, um die Lösegeldforderung zu untermauern. Andere weitläufige Begriffe für Ransomware sind unter anderem "*Erpressungs-/Kryptotrojaner*" oder "*Erpressungssoftware*".

Die Bedrohung durch Ransomware ist in den letzten Jahren kontinuierlich gestiegen und gehört mit zu den größten Bedrohungen, denen sowohl Privatpersonen als auch Unternehmen ausgesetzt sind.

In der Öffentlichkeit wird oftmals von einer Ransomware-Attacke gesprochen. Allerdings ist das Vorgehen eines solchen Angriffs vielschichtiger und beginnt bereits viel früher als es auf den ersten Blick zu erkennen ist. Jeder Ransomware-Angriff differiert in einzelnen Schritten, jedoch ist die allgemeine Vorgehensweise vergleichbar.

Um der Komplexität eines Ransomware-Angriffs zu begegnen, ist der Einsatz nur einer Maßnahme (z.B. Antiviren-Software oder Proxy-Filter) unzureichend. Es müssen mehrere Maßnahmen gleichzeitig umgesetzt und somit mehrere Verteidigungslinien aufgebaut werden. Beispiele solcher Aktivitäten sind Erkennung kompromittierter Accounts und schwacher Passwörter, Einsatz von MFA, Systeme zur Angriffserkennung etc.

In der folgenden Grafik zeigen wir beispielhaft die einzelnen Schritte und die entsprechenden Schutzmaßnahmen auf, die in der Abhängigkeit des jeweiligen Schrittes eingesetzt werden sollten:

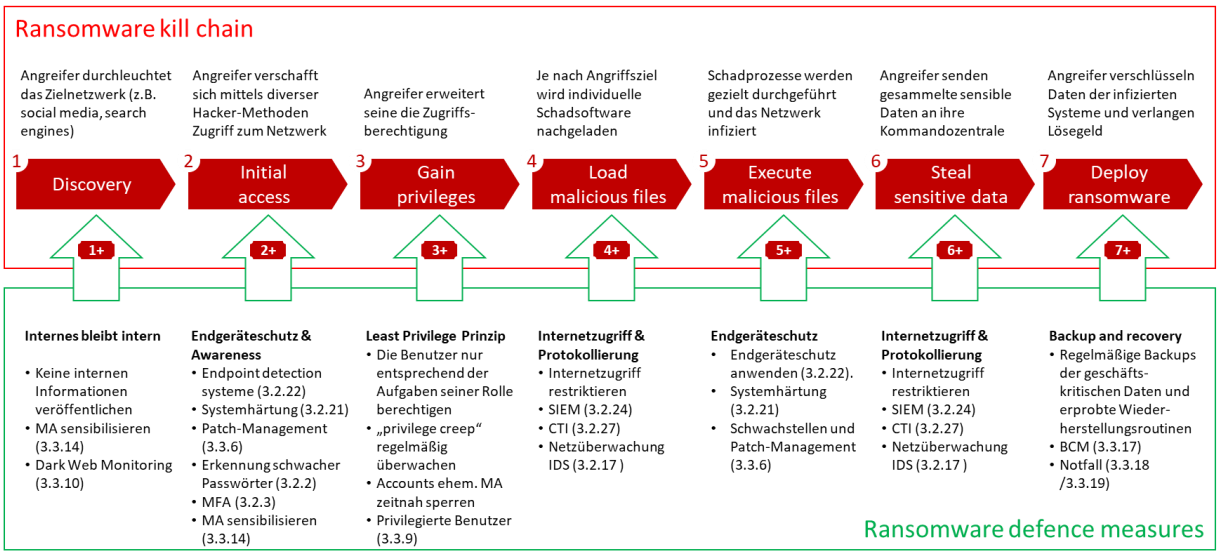


Abbildung 7: Ransomware-kill-chain und Schutzmaßnahmen (Beispiel)

Die möglichen Schritte und Schutzmaßnahmen werden in der nachfolgenden Tabelle kurz erläutert:

Ransomware-kill-chain (example)	Ransomware-Sicherheitsmaßnahmen
1) **Discovery** Angreifer sammeln möglichst viele Informationen über das Unternehmen, das angegriffen werden, beispielsweise in öffentlichen Suchmaschinen (Shodan, Censys) oder sozialen Netzwerken.	1+) **Internes bleibt intern** Keine Informationen veröffentlichen, die nur für den internen Zweck vorgesehen sind (Netzwerkpläne, IP-Adressen, Organigramme, Kontaktdaten etc.). Als möglicher Ansatz kann eine Klassifizierung der Dokumente und Daten (öffentlich, intern, geheim) vorgenommen werden. Auch die Mitarbeiter sollten darauf geschult werden (3.3.14 HR SdT). Überwachung des Dark Webs (3.3.10 HR SdT) kann unterstützen, die aktuellen Angriffsvektoren zu verstehen.
2) **Initial access** Angreifer verschafft sich mittels diverser Hacker-Methoden Zugriff zum Netzwerk. Eine erste Infektion erfolgt, häufig durch Phishing-Mails oder durch schädliche Webseiten. An dieser Stelle wird noch nicht der eigentliche Schadcode geladen.	2+) **Endgeräteschutz & Awareness** Maßnahmen zum Endgeräteschutz umsetzen (3.2.22 HR SdT). Mitarbeiter durch regelmäßige Awareness-Schulungen sensibilisieren (3.3.14 HR SdT). Ausführung von Makros deaktivieren bzw. nur auf signierte Macros einschränken. Maßnahmen zur Erkennung kompromittierter Accounts und schwacher Passwörter einsetzen (3.2.2 HR SdT). Wenn möglich MFA einsetzen (3.2.3 HR SdT). Aber auch weitere Maßnahmen, wie Serverhärtung (3.2.21 HR SdT) sowie Schwachstellen und Patch-Management (3.3.6 HR SdT)
3) **Gain privileges** Angreifer erhöhen die Rechte, mit denen sie agieren, um weitreichender Aktionen und damit ein höheres Schadenspotenzial zu erreichen.	3+) **Least Privilege Prinzip** (PoLP) Sicherstellen, dass die Benutzer nur die Zugriffsrechte erhalten, die sie für die Ausführung ihrer Aufgaben erforderlich sind. Regelmäßig das Berechtigungsmodell auf "privilege creep" überprüfen. Maßnahmen am "user account cycle" ausrichten und Accounts ehemaliger Mitarbeiter kurzfristig sperren. Privilegierte Accounts durch MFA schützen (3.2.3 HR SdT / 3.3.9 HR SdT).
4) **Load malicious files** Der Dropper lädt nun den eigentlichen Schadcode ("Payload") nach. Dieser Payload ist oft individuell programmiert und wird nicht von Antivirus-Software erkannt.	4+) **Internetzugriff & Protokollierung** Internetzugriff auf freigegebene Seiten zulassen, andere sperren. Je nach Schutzbedarf kann Einsatz von ReCoBS (3.2.23HR SdT) sinnvoll sein. Für die Protokollierung und Überwachung können weitere technische Maßnahmen wie SIEM (3.2.24 HR SdT) oder CTI (3.2.27 HR SdT) sowie Netzwerküberwachung mittels IDS (3.2.17 HR SdT) unterstützen.
5) **Execute malicious files** Weiterer Schadcode wird nachgeladen, die Angreifer breiten sich im Netzwerk aus ("Lateral Movement")	5+) **Endgeräteschutz** Maßnahmen zum Endgeräteschutz anwenden (3.2.22 HR SdT). Weitere Maßnahmen, wie Systemhärtung (3.2.21 HR SdT) sowie Schwachstellen und Patch-Management (3.3.6 HR SdT) umsetzen.
6) **Steal sensitive data** Sensible Daten wie beispielsweise Zugangsdaten werden an die Kommandozentrale ("Command-and-Control" Server) der Angreifer gesendet.	6+) **Internetzugriff & Protokollierung** Internetzugriff auf freigegebene Seiten zulassen, andere sperren. Je nach Schutzbedarf kann Einsatz von ReCoBS (3.2.23 HR SdT) sinnvoll sein. Für die Protokollierung und Überwachung können weitere technische Maßnahmen wie SIEM (3.2.24 HR SdT) oder CTI (3.2.27 HR SdT) sowie Netzwerküberwachung mittels IDS (3.2.17 HR SdT) unterstützen.
7) **Deploy ransomware** Der eigentliche Schadcode, mit dem die Daten verschlüsselt werden, wird ausgeführt.	7+) **Backup and recovery** Bei einem erfolgreichen Angriff, müssen natürlich zunächst viele Maßnahmen getroffen werden, um den Infektionsvektor zu finden und schließen sowie die Schäden zu begrenzen. Für den späteren Neuaufsatz der Systeme und Wiederherstellung der Daten sind aktuelle, nicht infizierte, Backups erforderlich.

Ransomware-kill-chain (example)	Ransomware-Sicherheitsmaßnahmen
	Weitere ergänzende Maßnahmen resultieren aus dem BCM (3.3.17 HR SdT) sowie den Vorbereitungen auf einen Notfall (3.3.18 und 3.3.19 HR SdT)

Tabelle 8: Maßnahmen gegen Ransomware-Angriffe

4.2 Einordnung der Maßnahmen in ISO/IEC 27001:2022

Die Norm ISO/IEC 27001:2022 ist ein international anerkanntes Rahmenwerk für das Informationssicherheitsmanagement (ISMS). Sie unterstützt Organisationen aller Größen und Branchen dabei, ihre Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten und zu behandeln. Die Norm basiert auf einem risikobasierten Ansatz und umfasst sechs zentrale Funktionen:

1. Kontext der Organisation (Context oft he organization): Die Organisation muss interne und externe Einflussfaktoren identifizieren, die sich auf das ISMS auswirken. Dazu gehören gesetzliche Anforderungen, Geschäftsziele und Stakeholder-Erwartungen.
2. Führung (Leadership): Die oberste Leitung trägt die Verantwortung für die Informationssicherheit. Sie muss eine klare Sicherheitsstrategie definieren, Ressourcen bereitstellen und sicherstellen, dass Sicherheitsziele mit der Unternehmensstrategie übereinstimmen.
3. Planung (Planning): Organisationen müssen Sicherheitsrisiken bewerten und geeignete Maßnahmen zur Risikobehandlung definieren. Dazu gehört auch die Festlegung von Sicherheitszielen sowie deren kontinuierliche Überprüfung.
4. Unterstützung (Support): Die erforderlichen Ressourcen, Kompetenzen und Kommunikationsmaßnahmen müssen sichergestellt werden, um das ISMS effektiv zu betreiben und aufrechtzuerhalten.
5. Betrieb (Operation): Sicherheitsmaßnahmen müssen implementiert und verwaltet werden. Dazu gehört auch das Management von Vorfällen sowie die kontinuierliche Überwachung der Sicherheitslage.
6. Bewertung und Verbesserung (Performance evaluation & Improvement): Regelmäßige Überprüfungen durch interne Audits und Managementbewertungen sind erforderlich, um die Effektivität des ISMS zu gewährleisten und es kontinuierlich zu verbessern.

Neben diesen Kernaspekten betont ISO/IEC 27001:2022 die Bedeutung eines kontinuierlichen Verbesserungsprozesses. Dies stellt sicher, dass Organisationen auf sich verändernde Bedrohungen und geschäftliche Anforderungen reagieren können.

Ein wesentlicher Bestandteil von ISO/IEC 27001:2022 ist Anhang A, der eine strukturierte Liste von Sicherheitsmaßnahmen (Controls) enthält. Diese Maßnahmen sind eng mit der Norm ISO/IEC 27002:2022 verknüpft, welche detaillierte Informationen zur Umsetzung dieser Controls bietet. Die Controls sind in vier Hauptthemen gegliedert: Organisatorische, Personenbezogene, Physische und Technologische Maßnahmen. Sie decken zentrale Sicherheitsaspekte wie Zugriffskontrollen, Verschlüsselung, Incident Management und Lieferketten-Sicherheit ab. Unternehmen nutzen diesen Anhang als Referenz, um Sicherheitsmaßnahmen gezielt auszuwählen und an ihre spezifischen Risiken anzupassen.

Ein entscheidender Vorteil von ISO/IEC 27001:2022 ist die Möglichkeit einer Zertifizierung. Organisationen können ihr Informationssicherheitsmanagementsystem (ISMS) durch eine unabhängige Zertifizierungsstelle auditieren lassen, um die Einhaltung der Norm nachzuweisen. Die Zertifizierung dient als international anerkanntes Gütesiegel und signalisiert Kunden, Partnern und Aufsichtsbehörden, dass die Organisation systematische und wirksame Maßnahmen zum Schutz von Informationen implementiert hat. Dies kann nicht nur das Vertrauen in die IT-Sicherheit stärken, sondern auch Wettbewerbsvorteile schaffen, indem es Unternehmen hilft, regulatorische Anforderungen zu erfüllen und neue Geschäftsmöglichkeiten zu erschließen.

Kapitelname	Kapitel #	ISO/IEC 27001:2022 Zuordnung				
		Kapitel 4-10	A.5	A.6	A.7	A.8
Authentisierung	3.2.1		A.5.15 A.5.16 A.5.17 A.5.18			
Bewertung und Durchsetzung starker Passwörter	3.2.2		A.5.17			
Multifaktor-Authentifizierung	3.2.3		A.5.17			
Kryptographische Verfahren	3.2.4					A.8.24
Verschlüsselung von Festplatten	3.2.5					A.8.1 A.8.24
Verschlüsselung von Dateien und Ordnern	3.2.6					A.8.24
Verschlüsselung von E-Mails	3.2.7					A.8.24
Schutz des elektronischen Datenverkehrs mit PKI	3.2.8					A.8.24 A.8.27
Einsatz von verschlüsselten VPN-Lösungen (Layer 3)	3.2.9					A.8.21 A.8.24
Verschlüsselung (Layer 2)	3.2.10					A.8.21 A.8.24
Sicherung Cloud-basierter Datenaustauschdienste	3.2.11		A.5.23			
Datenablage in der Cloud	3.2.12		A.5.23			
Schutz mobiler Sprach- und Datendienste	3.2.13					A.8.21 A.8.24
Schutz der Kommunikation mittels Instant-Messenger	3.2.14					A.8.21 A.8.24
Schutz mobiler Geräte	3.2.15					A.8.1
Routersicherheit	3.2.16					A.8.8 A.8.9
Netzwerküberwachung mittels Intrusion Detection System	3.2.17					A.8.7 A.8.15
Schutz des Web-Datenverkehrs	3.2.18					A.8.21 A.8.23
Schutz von Webanwendungen	3.2.19					A.8.23
Schutz des Fernzugriffs auf Netzwerke	3.2.20			A.6.7		A.8.20 A.8.22
Systemhärtung	3.2.21					A.8.9
Endpoint Detection & Response Plattform	3.2.22		A.5.24 A.5.25 A.5.26			
Web-Isolation der Internetnutzung	3.2.23					A.8.22
Angriffserkennung und Auswertung (SIEM)	3.2.24		A.5.24 A.5.25 A.5.26			
Vertrauliche Datenverarbeitung	3.2.25		A.5.12 A.5.23			A.8.2 A.8.5
Sandboxing zur Schadcode-Analyse	3.2.26		A.5.28			
Cyber Threat Intelligence	3.2.27		A.5.7			
Absicherung administrativer IT-Systeme	3.2.28					A.8.2
Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung	3.2.29		A.5.18			A.8.15

Kapitelname	Kapitel #	ISO/IEC 27001:2022 Zuordnung				
Netzwerksegmentierung und Separierung	3.2.30					A.8.22
Cloud-Sicherheitsplattform	3.2.31		A.5.23			
Tokenisierung	3.2.32					A.8.11
VOIP-Verschlüsselung mit SIPS/SRTP	3.2.33					A.8.21 A.8.24
Verschlüsselung auf Layer 1	3.2.34					A.8.24
Standards und Normen	3.3.1					
Sicherheitsorganisation	3.3.2	5.3				
Informationssicherheitsmanagementsystem (ISMS)	3.3.3	4 - 10				
Sichere Softwareentwicklung	3.3.4					A.8.25 A.8.26 A.8.27 A.8.28 A.8.29 A.8.30 A.8.31
Prozesszertifizierung	3.3.5					
Schwachstellen- und Patchmanagement	3.3.6					A.8.8
Risikomanagement	3.3.7	6, 8				
Personenzertifizierung	3.3.8	7.2	A.6.3			
Absicherung privilegierter Benutzerkonten	3.3.9					A.8.2
Dark Web Monitoring	3.3.10		A.5.7			
Umgang mit Dienstleistern	3.3.11		A.5.19 A.5.20 A.5.21 A.5.22			
Software Bill of Materials (SBOM)	3.3.12		A.5.9 A.5.21			A.8.8
Geo-Redundanzen	3.3.13					A.8.14
Sensibilisierung der Anwender	3.3.14	7.3	A.6.3			
IT-Asset Management	3.3.15		A.5.9 A.5.10 A.5.12			
Incident Management	3.3.16		A.5.24 A.5.25 A.5.26			
Geschäftskontinuitäts-Management (BCM)	3.3.17		A.5.29 A.5.30			
Notfall- und Krisenmanagement	3.3.18		A.5.30			
Notfall-Übungen	3.3.19		A.5.29 A.5.30			
Technische Systemaudits	3.3.20					A.8.8

Tabelle 9: Einordnung der Maßnahmen in ISO/IEC 27001:2022

4.3 Einordnung der Maßnahmen in das NIST-Rahmenwerk

Das NIST Cybersecurity Framework wurde in den USA entwickelt, um Organisationen aller Branchen dabei zu unterstützen, ihre Informations- und Cyber-Sicherheitsrisiken zu managen. Es bietet einen flexiblen und wiederholbaren Ansatz, der auf bestehenden Standards und Richtlinien basiert und fünf grundlegende Funktionen umfasst:

1. Identifizieren (**Identify**): Verstehen und Festlegen des organisatorischen Kontexts, der Systeme, Vermögenswerte, Daten und Fähigkeiten, die geschützt werden müssen. Verwalten Sie Assets, die auf die geschäftliche Bedeutung abgestimmt sind.
2. Schützen (**Protect**): Etablierung der geeigneten Schutzmaßnahmen, um sicherzustellen, dass kritische Dienste auch im Falle eines Vorfalls aufrechterhalten werden.
3. Erkennen (**Detect**): Entwickeln und Implementieren der notwendigen Maßnahmen zur frühzeitigen Erkennung von Cybersecurity-Vorfällen
4. Reagieren (**Respond**): Festlegen von Aktionen und Plänen zur effektiven Reaktion auf erkannte Cybersecurity-Vorfälle.
5. Wiederherstellen (**Recover**): Planung für die Wiederherstellung nach einem Cybersecurity-Vorfall und Maßnahmen zur Wiederherstellung der normalen Geschäftstätigkeit.

Neben den fünf zuvor genannten Funktionen wird "Govern" als zusätzlicher Teil des NIST Cybersecurity Frameworks angesehen. Die Funktion "Govern" spielt eine zentrale Rolle im gesamten Cyber-Sicherheitsprozess und wird in verschiedenen Aspekten des Rahmenwerks reflektiert.

6. Govern (Steuern): Die Strategie, die Erwartungen und die Richtlinien des Unternehmens für das Cyber-Sicherheitsrisiko-Management werden festgelegt, kommuniziert und überwacht.

Viele Unternehmen nutzen das NIST Framework als Referenz, um die eigenen Sicherheitsmaßnahmen zu verifizieren und zu optimieren. Das Framework fördert auch die Kommunikation über Cyber-Sicherheitsrisiken zwischen internen und externen Stakeholdern durch die Verwendung einer gemeinsamen Sprache. Es ist darauf ausgerichtet, sowohl für Organisationen mit geringer Cyber-Sicherheitsreife als auch für solche mit fortgeschrittenen Programmen anwendbar zu sein.

Diese Handreichung übernimmt eine Vermittlerrolle, um den Anwendungsunternehmen die Sicherheitsmaßnahmen sowie ihre Charakteristika nachvollziehbar zu erklären. Hierfür ist es der Sache dienlich, die beschriebenen Maßnahmen in Bezug zu den gängigen Rahmenwerken herzustellen.

Kapitelname	**Kapitel #**	**NIST Zuordnung**					
		Govern	Identify	Protect	Detect	Respond	Recover
Technische Maßnahmen	3.2						
Authentifizierung	3.2.1		X	X			
Bewertung und Durchsetzung starker Passwörter	3.2.2	X		X			
Multifaktor-Authentifizierung	3.2.3			X			
Kryptographische Verfahren	3.2.4			X			
Verschlüsselung von Festplatten	3.2.5			X			
Verschlüsselung von Dateien und Ordnern	3.2.6			X			
Verschlüsselung von E-Mails	3.2.7			X			
Sicherung des elektronischen Datenverkehrs mit PKI	3.2.8			X			
Einsatz von verschlüsselten VPN-Lösungen (Layer 3)	3.2.9			X			
Verschlüsselung (Layer 2)	3.2.10			X			
Cloud-basierter Datenaustausch	3.2.11			X			
Datenablage in der Cloud	3.2.12			X			
Schutz mobiler Sprach- und Datendienste	3.2.13			X			
Schutz der Kommunikation mittels Instant-Messenger	3.2.14	X		X		X	
Schutz mobiler Geräte	3.2.15	X		X			
Routersicherheit	3.2.16			X			
Netzwerküberwachung mittels Intrusion Detection System	3.2.17				X		
Schutz des Web-Datenverkehrs	3.2.18			X			

Kapitelname	Kapitel #	NIST Zuordnung					
		Gov-ern	Iden-tify	Pro-tect	De-tect	Res-pond	Reco-ver
Schutz von Webanwendungen	3.2.19			X			
Schutz des Fernzugriffs auf Netzwerke	3.2.20			X			
Systemhärtung	3.2.21			X			
Endpoint Detection & Response Plattform	3.2.22				X	X	X
Web-Isolation der Internetnutzung	3.2.23			X			
Angriffserkennung und Auswertung (SIEM)	3.2.24				X	X	X
Vertrauliche Datenverarbeitung	3.2.25	X		X			
Sandboxing zur Schadcode-Analyse	3.2.26				X		
Cyber Threat Intelligence	3.2.27				X		
Absicherung administrativer IT-Systeme	3.2.28			X			
Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung	3.2.29		X		X		
Netzwerksegmentierung und Separierung	3.2.30			X			
Cloud-Sicherheitsplattform	3.2.31			X			
Tokenisierung	3.2.32			X			
VOIP-Verschlüsselung mit SIPS/SRTP	3.2.33			X			
Verschlüsselung (Layer 1)	3.2.34			X			
Organisatorische Maßnahmen	**3.3**						
Standards und Normen	3.3.1	X					
Sicherheitsorganisation	3.3.2	X					
Informationssicherheitsmanagementsys-tem (ISMS)	3.3.3			X			
Sichere Softwareentwicklung	3.3.4			X			
Prozesszertifizierung	3.3.5	X		X			
Schwachstellen- und Patchmanagement	3.3.6		X	X			
Risikomanagement	3.3.7	X		X			
Personenzertifizierung	3.3.8	X		X			
Absicherung privilegierter Benutzerkonten	3.3.9		X	X			
Dark Web Monitoring	3.3.10				X	X	
Umgang mit Dienstleistern	3.3.11	X			X		
Software Bill of Materials (SBOM)	3.3.12		X	X			
Geo-Redundanzen	3.3.13			X			
Sensibilisierung der Anwender	3.3.14	X					
IT Asset Management	3.3.15		X				
Incident Management	3.3.16				X	X	X
Geschäftskontinuitäts-Management (BCM)	3.3.17					X	X
Notfall- und Krisenmanagement	3.3.18				X	X	X
Notfallübungen	3.3.19				X	X	X
Technische Systemaudits	3.3.20	X	X	X			

Tabelle 10: Einordnung der Maßnahmen in das NIST-Rahmenwerk

4.4 Auswirkung von KI auf Informationssicherheit

Der Begriff Künstliche Intelligenz umfasst mehrere Bereiche. Von größerer Bedeutung im Kontext IT-Security sind Machine Learning (ML), Deep Learning (DL) und Generative KI (GenAI). Deep Learning ist eine Untermenge von Machine Learning (mit mehrschichtigen neuronalen Netzen), während Generative KI wiederum ein Spezialfall von Deep Learning ist.

Die Gemeinsamkeit der drei KI-Bereiche: Alle KI-Modelle können nach dem Trainingsprozess selbstständig Muster in großen Datenmengen erkennen. Während aber Machine-Learning- und Deep-Learning-Modelle diese Datenmengen eher klassifizieren und kategorisieren, erzeugen Generative-KI-Modelle neue Inhalte auf Basis der gefundenen Muster und statistischer Annahmen.

Die zunehmende Integration von Künstlicher Intelligenz (KI) in Unternehmensprozesse verändert die Landschaft der Informationssicherheit und bringt sowohl positive Möglichkeiten als auch erhebliche Sicherheitsrisiken mit sich. Auf der einen Seite kann KI Muster und Anomalien erkennen, die auf potenzielle Bedrohungen hinweisen. Auf der anderen Seite kann die selbige Technologie von Angreifern genutzt werden, um Informationen über potenzielle Opfer zu finden, personalisierte Angriffe durchzuführen oder Schadsoftware zu entwickeln. Auch Angriffe auf KI-Anwendungen selbst sind möglich, etwa um deren Verhalten aktiv zu beeinflussen.

KI zur Verbesserung der Informationssicherheit

Einer der Hauptvorteile von KI ist die Fähigkeit, in großen Datenmengen Anomalien und ungewöhnliche Aktivitäten zu identifizieren. Im Gegensatz zu traditionellen Sicherheitstechnologien, bei denen die Erkennung meist auf dem Abgleichen von Mustern und Signaturen aus bisherigen Angriffen basiert, ist KI damit in der Lage, bisher unbekannte Gefahren zu erkennen.

KI ermöglicht es auch, Daten aus vielen verschiedenen Datenquellen in angemessener Zeit zu verarbeiten und zueinander in Beziehung zu setzen (zu korrelieren). KI- und Big-Data-Algorithmen decken Zusammenhänge auf, welche für einen menschlichen Beobachter oft unbemerkt geblieben wären.

Ein weiterer Vorteil für Unternehmen ist die Effizienzsteigerung, die durch den Einsatz von KI in Sicherheitstechnologien erreicht werden kann. KI-Systeme schonen personelle Ressourcen, indem sie es Sicherheitsanalysten ermöglichen, sich auf relevante Aktivitäten zu konzentrieren, die als ungewöhnlich erkannt wurden. Zudem können potenzielle Bedrohungen meist schneller erkannt werden, was die Reaktionszeit auf Sicherheitsvorfälle erheblich verkürzen kann.

KI als Werkzeug für Angreifer

Auch Angreifergruppen machen sich die Fähigkeiten von KI zunutze und verwenden diese gezielt für ihre Zwecke. Dies reicht von Social-Engineering-Angriffen bis hin zur automatisierten Entwicklung von Schadsoftware. Eine große Stärke von KI liegt in der effizienten Verarbeitung und Analyse von öffentlich verfügbaren Informationen. Angreifer nutzen diese Funktionalität, um Daten über potenzielle Opfer zu sammeln und zu aggregieren. Die zusammengetragenen Informationen bilden in Folge die Grundlage für maßgeschneiderte Angriffe. So können beispielsweise personalisierte Phishing-Mails erstellt werden, die auf die jeweilige Zielgruppe zugeschnitten sind. Während herkömmliche Phishing-Nachrichten oft durch Rechtschreibfehler oder schlechte Übersetzung auffallen, sind KI-generierte Nachrichten oft kaum von legitimen unterscheidbar. Gleichzeitig kann das Verschicken von Phishing-Nachrichten in hohem Maße automatisiert werden, wodurch die Erfolgsquoten von Angreifern wesentlich erhöht werden können.

Zusätzlich kann KI die Einstiegshürde bei der Erstellung von Schadsoftware für Angreifer erheblich senken. Schadsoftware kann mit Hilfe von KI-Modellen generiert werden, die speziell für diese Zwecke trainiert wurden.

Auch KI-Systeme selbst können Ziel von Angriffen werden, sowohl im Zuge der Trainingsphase als auch im Betrieb. Bei der sog. Model Inversion versuchen Angreifer mit Hilfe der Ausgaben der KI auf die dahinterliegende Architektur zu schließen und weitere Informationen zu extrahieren. Auch der Diebstahl eines trainierten KI-Modells kann für ein Unternehmen weitreichende Folgen haben. Die OWASP Foundation führt eine Liste von KI-bezogenen Risiken inkl. Risikofaktoren und Gegenmaßnahmen.[45]

[45] owasp.org/www-project-machine-learning-security-top-10/

Schutzmaßnahmen gegen KI-bezogene Risiken

Nachdem KI in beinahe allen Unternehmen in unterschiedlicher Form Einzug findet, sind entsprechende Schutzmaßnahmen notwendig, um sich vor KI-bezogenen Risiken zu schützen. Aus der Sicherheitsperspektive wirken sich Machine und Deep Learning auf der einen und Generative KI auf der anderen Seite unterschiedlich aus. Während die ersten beiden ihre *Ausgaben* direkt aus maschinenlesbaren Datensätzen (*Eingaben*) ableiten, erzeugt generative KI Ausgaben häufig interaktiv als Reaktion auf menschliche Eingaben. Diese direkte Nutzerinteraktion gepaart mit einer hohen Marktdynamik und einigen KI-Besonderheiten eröffnen speziell im Bereich Generative KI neue Angriffsflächen. Im Machine- und Deep-Learning-Bereich liegen die Risiken hingegen eher im Bereich der KI-Modell-Sicherheit und dem Aufbau einer sicheren Entwicklungs- und Testumgebung.

Vor der Entwicklung und dem Einsatz von KI-Anwendungen sind geltende rechtliche Anforderungen zu identifizieren. Werden Produkte oder Dienstleistungen auf der Grundlage von KI angeboten, gilt der EU-AI Act, welcher Regularien für den Einsatz von KI enthält. Auch die Bestimmungen der DSGVO müssen eingehalten werden. Beim Einsatz von KI-Anwendungen ist beispielsweise zu prüfen, ob die eingegebenen Daten an den Hersteller der KI-Anwendung oder an andere Dritte übermittelt werden, um zu verhindern, dass personenbezogene oder sensible Daten unberechtigt weitergegeben werden.

Die weiter unten aufgeführte Tabelle listet derzeit bekannte Sicherheitsrisiken von KI-Modellen und geeignete Präventivmaßnahmen auf. Sicherheitsfokussierte Organisationen wie OWASP beobachten diesen Raum permanent. Nicht nur liefert OWASP jährliche Listen der zehn bekanntesten Angriffsmethoden[46] gegen Generative-KI-Modelle sowie Checklisten zur KI-Sicherheit[47]. Die Organisation nennt auch konkrete Maßnahmen[48], um einen sicheren und risikofreien Einsatz von KI in Unternehmen zu erreichen. Sie unterscheidet dabei zwischen:

- Generellen Sicherheitskontrollen
  - Integration von KI in unternehmenseigene Security-Programme
  - Maßnahmen zur Datenkontrolle und Datensicherheit
  - Maßnahmen zur Eindämmung von unerwünschtem Verhalten der KI

- Maßnahmen bei der Nutzung von KI
  - Allgemeine Nutzungsüberwachung
  - Maßnahmen gegen Evasion-Angriffe
  - Maßnahmen gegen Prompt Injection
  - Maßnahmen gegen den Verlust sensibler Trainingsdaten
  - Maßnahmen gegen KI-Modell-Diebstahl
  - Maßnahmen gegen Fehlverhalten von KI-Modellen

- Maßnahmen gegen Bedrohungen zur Entwicklungszeit
  - Allgemeine Absicherung von Entwicklungsumgebung und Lieferketten
  - Maßnahmen gegen Model Poisoning
  - Maßnahmen gegen Data Leaks

- Maßnahmen gegen Bedrohungen zur Modell-Laufzeit
  - Absicherung gegen klassische Sicherheitsrisiken
  - Maßnahmen gegen Modellmanipulationen zur Laufzeit
  - Maßnahmen gegen Modelldiebstahl zur Laufzeit
  - Sicherer Umgang mit unsicheren Modellausgaben
  - Maßnahmen gegen die Eingabe sensibler Daten

Nicht alle Bedrohungsszenarien sind KI-spezifisch. KI-Anwendungen sind oft auch klassische SaaS-Anwendungen und unterliegen den damit verbundenen Sicherheitsrisiken. Das Absichern der Entwicklungsumgebung, aber auch der Anwendungs-API, gilt zum Beispiel generell für alle Softwareprojekte. Die folgende Tabelle gibt einen Überblick über KI-Sicherheitsrisiken, Schutzmaßnahmen und Zuständigkeiten für Gegenmaßnahmen.

[46] genai.owasp.org/llm-top-10/
[47] genai.owasp.org/resource/llm-applications-cybersecurity-and-governance-checklist-english/
[48] owaspai.org/docs/ai_security_overview/

	Secure Software Development Lifecycle	Code Review	Überwachung adverser Eingaben	EDR/XDR	Audits der Modelle gegen adverse Eingaben und Trigger	Data Loss Prevention	Säuberung der Trainingsdaten	Security Audits	Nutzer-Training	Nutzer-Authentifizierung	Zugriffskontrolle	Audit-Logs	Verträge	Kein Internetzugriff für Modelle	Bias-Detektion-Software	Explainable AI Frameworks	Individuelles Prüfen von Fakten	Reinforcement Learning mit Menschen im Loop und Feintuning der Modelle	Gesetzliche Vorgaben
Model Poisoning - Angreifer verfälschen Daten im Training	A	A		A	B		A	A			A	A				A			
Angreifer stehlen oder replizieren das Model	A		N	B		B		B		B	B	B							
Angreifer stehlen oder replizieren vertrauliche Unternehmensdaten, die im Modell stecken	A	A	N	A	B	B	A	B		B	B	B							
Hersteller triggern Backdoors bei bestimmten Themen / über Abhängigkeiten		N		N				N				N		N					
Hersteller bauen bewusst Falschaussagen in Modelle ein		N			N				N	N		N			N	N	N		
Modell schickt Kundendaten an Hersteller		N				N		N	N	N	N	N	N	N		N			N
Copyright-Verletzungen							A		A				B			N		A	A
Anbieter-Kompromittierung durch Sicherheitslücken in der Anwendung	A	B		B		N		B			B	B	B	N					A
Offenlegung des System Prompts durch Prompt Injection			A		A	A		A		A	A	A	A	B					A
Kompromittierung durch Supply-Chain-Angriffe	B	B		B		N		B			B	B	B	N					B
KI-Hersteller oder KI-Anbieter sammeln legal oder illegal die Nutzereingaben						N			N	N	N		B	N					A
KI-Komponenten in lokaler Software sammeln Kundendaten		N		N		N		N			N	N	B	N					A

	Secure Software Development Lifecycle	Code Review	Überwachung adverser Eingaben	EDR/XDR	Audits der Modelle gegen adverse Eingaben und Trigger	Data Loss Prevention	Säuberung der Trainingsdaten	Security Audits	Nutzer-Training	Nutzer-Authentifizierung	Zugriffskontrolle	Audit-Logs	Verträge	Kein Internetzugriff für Modelle	Bias-Detektion-Software	Explainable AI Frameworks	Individuelles Prüfen von Fakten	Reinforcement Learning mit Menschen im Loop und Feintuning der Modelle	Gesetzliche Vorgaben
Anbieter manipulieren die Ausgaben des KI-Modells					N				N				B		N	N	N		B
Modelle halluzinieren und konfabulieren							A		N							N	N	A	
Modelle reproduzieren Vorurteile in ihren Antworten															B	B	N	A	A
Angriffe von Dritten über manipulierte Webseiten, E-Mails und Phishing			N	N		N		N	N		N	N		B		B			
Nutzer testen Prompt Injections			B		B				N	N	N	B	B					A	A
Phishing-Mails generieren			B						N	B		B	B					A	N
Abrufen illegaler oder schädigender Informationen			B		B					B		B	B		B	A	N	A	A
Betrug und Manipulation mit maschinell erzeugten Texten und Bildern			B						N	B		B	B					A	N
Unternehmen oder Dritte erhalten von KI-Nutzern indirekt Falschinformationen									N				N				N		
Rezeption von ungeprüftem KI-Content über soziale Medien, Forschungsliteratur usw.									N				N				N		
Veröffentlichungen mit impliziter und nicht-erwähnter KI-Unterstützung									N				N				N		N

Tabelle 11: Sicherheitsrisiken von KI-Modellen und Schutzmaßnahmen

Legende:

A = Gegenmaßnahmen auf Seiten von Entwicklern und/oder Anbietern des Modells
N = Gegenmaßnahmen auf Seiten der Nutzer des Modells
B = Gegenmaßnahmen auf beiden Seiten

Die EU-Agentur ENISA listet "Missbrauch von KI für Cyber-Angriffe" unter die Top-Cybersecurity-Bedrohungen bis 2030[49]. KI-Algorithmen sowie Tools, welche diese nutzen, entwickeln sich stetig weiter. Angreifer profitieren von dieser Entwicklung - Angriffe werden zunehmend komplexer und sind für Erkennungstools schwieriger zu erkennen. Unternehmen, Behörden und Organisationen stehen daher vor der Herausforderung, die Erkennung und Abwehr von Angriffen auch mit Hilfe von KI zu optimieren und immer effektiver zu gestalten. Die Einführung und Integration von KI muss sorgfältig und zügig geplant, kontinuierlich überwacht werden, regelmäßig aktualisiert und weiterentwickelt werden.

Darüber hinaus ist auch die Weiterbildung des Personals und die Schaffung von Bewusstsein hinsichtlich der durch KI entstehenden Bedrohungen wesentlich. Angesichts der zunehmenden Integration von KI in unterschiedlichste Unternehmensprozesse ist ein grundlegendes Verständnis dieser Technologie sowie entsprechende Regelungen und Sicherheitsmaßnahmen notwendig.

4.5 Absicherung der Lieferkette

Die Resilienz von Lieferketten wird zunehmend zur zentralen, branchenübergreifenden Anforderung für Unternehmen. Bedingt durch geopolitische Spannungen, Cyber-Bedrohungen und regulatorische Verschärfungen wächst der Druck, Abhängigkeiten nicht nur wirtschaftlich, sondern auch sicherheitsbezogen zu bewerten. Mit der neuen NIS-2-Richtlinie, der aktualisierten ISO/IEC 27001:2022 sowie dem deutschen Lieferkettensorgfaltspflichtengesetz (LkSG) treten konkrete Anforderungen in Kraft, die sowohl Organisationen als auch ihre Dienstleister und Zulieferer betreffen. Ergänzend dazu bietet die ISO 28000 einen spezialisierten Rahmen zur strukturierten Bewertung sicherheitsrelevanter Aspekte innerhalb der gesamten Lieferkette.

Ein zentrales Merkmal der NIS2[50] ist der erweiterte Fokus auf vorgelagerte Dienstleister und Lieferanten. Unternehmen werden verpflichtet darzulegen, wie sie Risiken aus ihrer Lieferkette identifizieren, bewerten und kontrollieren. Dazu gehört auch die Möglichkeit, Vorfälle zu melden, sowie das Recht, Sicherheitsmaßnahmen bei Dritten zu prüfen.

Zur Umsetzung bietet sich die ISO/IEC 27001[51] in ihrer überarbeiteten Fassung von 2022 an. Die Norm verlangt ein systematisches Informationssicherheitsmanagement, das nicht an der Unternehmensgrenze endet. Die dort neu aufgenommenen Maßnahmen A.5.22 und A.5.23 fordern konkret, dass die Sicherheit in der Lieferkette gesteuert wird und bei ICT-Dienstleistern klare Kontrollmechanismen etabliert werden.

Ein weiterer gesetzlicher Baustein ist das deutsche Lieferkettensorgfaltspflichtengesetz (LkSG), das seit 1. Januar 2023 für Unternehmen mit mehr als 1.000 Mitarbeitenden verbindlich ist. Es verpflichtet Unternehmen zur systematischen Risikoanalyse entlang ihrer globalen Lieferketten. Unternehmen sollen nicht nur ihre direkten Geschäftspartner bewerten, sondern auch Verantwortung für vorgelagerte Stufen der Lieferkette übernehmen. Neben menschlichen und umweltbezogenen Risiken gewinnen dabei zunehmend auch IT-Sicherheitsrisiken an Bedeutung. Ein erfolgreicher Cyber-Angriff auf einen kritischen Zulieferer kann nicht nur operative Schäden verursachen, sondern auch rechtliche Konsequenzen nach sich ziehen - etwa dann, wenn durch eine Unterbrechung der Lieferbeziehung gegen Sorgfaltspflichten verstoßen wird.

Die ISO 28000 ergänzt diesen Ansatz sinnvoll, da sie sich speziell auf Sicherheitsaspekte in logistischen Prozessen konzentriert. Anders als die ISO 27001, die primär die Informationssicherheit adressiert, umfasst die ISO 28000 auch physische Risiken, Sabotage, Produktmanipulation und sicherheitskritische Unterbrechungen in Transport und Lagerung. Der Standard eignet sich insbesondere für global aufgestellte Unternehmen oder für Organisationen mit erhöhtem Risiko in der physischen Lieferkette. Durch ihre strukturierte Herangehensweise lassen sich Prozesse identifizieren, bewerten und verbessern, um die gesamte Wertschöpfungskette sicherer zu gestalten. Aus Sicht der Praxis empfiehlt es sich, vorhandene (Informationssicherheits-) Managementsysteme zu nutzen und gezielt zu erweitern.

Die Integration der Anforderungen aus NIS2, ISO/IEC 27001, ISO 28000 und LkSG ist möglich - und auch sinnvoll.

[49] ec.europa.eu/newsroom/ECCC/items/766303/en
[50] Zum Zeitpunkt der Veröffentlichung dieser Handreichung war die NIS2 in Deutschland noch nicht umgesetzt.
[51] Die Automobilzulieferer müssen die Vorgaben nach dem TISAX-Standard umsetzen.

Entscheidende Erfolgsfaktoren sind die Einbindung von Lieferanten in bestehende Sicherheitsprozesse und eine transparente Kommunikation über Erwartungen und Maßnahmen. So lässt sich die Erfüllung der steigenden gesetzlichen Anforderungen als strategischer Vorteil nutzen.

Zunächst muss ein Überblick über die Lieferantenlandschaft erstellt werden. Daraus muss klar werden, welche Lieferanten wie mit dem eigenen Unternehmen verbunden sind. Dabei geht es nicht nur um Lieferanten von Software-Produkten, sondern alle Lieferanten des Unternehmens, sofern diese über direkte oder indirekte technische oder prozessuale Schnittstellen zum Unternehmen angebunden sind.

Dabei sollten bestehende Verträge überprüft, Verantwortlichkeiten neu definiert und Risikobewertungen regelmäßig angepasst werden. Bei strategisch kritischen Lieferanten ist es sinnvoll, regelmäßig Lieferantenaudits durchzuführen, in denen auch die Sicherheitsaspekte betrachtet werden.[52]

Die Risikoanalyse ermöglicht die Identifikation kritischer Prozesse, die Feststellung der Abhängigkeiten, die Bewertung der Risiken in Verbindung mit der jeweiligen Bedrohungslage und ist somit auch die Grundlage für die Identifikation geeigneter Sicherheitsmaßnahmen. Auf der technischen Seite werden unter anderem der Zugriff auf Unternehmenssysteme, der Umfang und die Sensibilität verarbeiteter Daten, die regionale Risikolage sowie die bisherige Incident-Historie bewertet.

Für die ermittelten Risiken müssen Sicherheitsanforderungen definiert werden. Diese haben einen doppelten Zweck: einerseits dienen sie einer strukturierten Identifikation von Sicherheitsmaßnahmen für das eigene Unternehmen, andererseits unterstützen sie den Dialog mit den Lieferanten und schaffen gemeinsames Verständnis über die erforderlichen Maßnahmen. Aufgrund der starken Verflechtung der Prozesse, muss die Sicherheit der Lieferkette übergreifend betrachtet werden.

Ein modernes Lieferkettenmanagement, das den Anforderungen aus NIS2, ISO 27001 und dem LkSG gerecht werden will, benötigt ein Zusammenspiel aus Governance, Prozessen und Technik. Insbesondere auf der operativen Ebene müssen definierte Anforderungen in konkrete Sicherheitsmaßnahmen überführt werden, um tatsächliche Wirksamkeit zu erzielen.

Auf technischer Ebene bedeutet das zum Beispiel: der Zugang externer Dienstleister erfolgt ausschließlich über gesicherte, segmentierte Verbindungen. Dazu gehören Jump Hosts mit Session Recording, temporäre Zugriffsfreigaben, mehrstufige Authentifizierungsverfahren und Logging aller Aktivitäten. Bei besonders sensiblen Anbindungen sollten zusätzlich SIEM-Systeme eingesetzt werden, um verdächtiges Verhalten in Echtzeit zu erkennen.

Um die Sicherheit der Lieferkette zu gewährleisten, sind verschiedene Maßnahmen erforderlich. Der initiale Schritt beginnt bereits bei der Beschaffung der IT-Sicherheitskomponenten. Unter dem Schlagwort "Secure-by-Demand" hat die US-amerikanische Cybersecurity & Infrastructure Security Agency (CISA) einen Leitfaden mit 12 Anforderungen an Hersteller aufgestellt, die bei der Beschaffung berücksichtigt werden sollen.[53] Dieser Leitfaden wurde in erster Linie für die Beschaffung sicherer OT aufgestellt, jedoch kann er ebenfalls in leicht abgewandelter Form für IT-Komponenten verwendet werden. CISA betont, dass die Gewichtung der einzelnen Empfehlungen an die individuellen Rahmenbedingungen angepasst werden sollten. Das betrifft insbesondere die eingesetzten Systeme oder verfügbares Budget.

Insbesondere bei Software-Lieferanten oder software-lastigen IT-Produkten ist es erforderlich, die Bereitstellung einer SBOM[54] durch den Lieferanten einzufordern und fortlaufend aktuell zu halten. Die SBOM soll ermöglichen, die kritischen Softwareinhalte im Bedarfsfall schnell identifizieren und mitigieren zu können.

Auch das Schwachstellenmanagement spielt eine Rolle. Externe Webdienste und Schnittstellen sollten durch automatisierte Scans regelmäßig auf Konfigurationsfehler, veraltete Systeme oder unsichere Zertifikate überprüft werden. Für marktführende Produkte und Dienste können diese Informationen eventuell zugekauft werden. Sie fließen direkt in die Risikobewertung ein.

Auf Datenebene ist die konsequente Anwendung des Prinzips der minimalen Rechtevergabe essenziell. Dienstleister erhalten nur Zugriff auf das, was sie zwingend benötigen. Darüber hinaus müssen alle

[52] Siehe auch Kapitel "Umgang mit Dienstleistern"
[53] www.cisa.gov/resources-tools/resources/secure-demand-guide
[54] Siehe Kapitel "Software Bill of Materials" (SBOM)

Datenflüsse verschlüsselt erfolgen, sowohl bei der Übertragung als auch in der Speicherung. Verträge sollten dies klar und technisch nachvollziehbar regeln.

Ergänzend zu den umgesetzten technischen Sicherheitsmaßnahmen muss stets die Kontinuität des Geschäftsbetriebs betrachtet werden. So müssen auch Notfall- und Wiederanlauf-Pläne[55] vorbereitet und getestet werden.

Auch organisatorisch braucht es robuste Strukturen: ein Lieferantenregister mit Sicherheitsprofilen, Auditzyklen mit risikobasierten Intervallen, abgestimmte Eskalationsverfahren im Vorfallmanagement, sowie Schulungen für alle internen Fachbereiche, die mit Drittparteien zusammenarbeiten. Informationssicherheit muss dabei in den Alltag der Einkaufs-, Rechts- und Projektabteilungen integriert sein, als selbstverständlicher Teil der unternehmerischen Sorgfalt.

Die Absicherung der Lieferkette ist kein isoliertes Projekt, sondern Bestandteil einer langfristigen Sicherheitsstrategie. Unternehmen, die frühzeitig mit der Umsetzung beginnen und ihre Abhängigkeiten strukturiert analysieren, schaffen nicht nur Rechtssicherheit, sondern auch operative Belastbarkeit und damit höhere Resilienz in einem zunehmend instabilen Umfeld. Dies dient den Interessen aller Stakeholder und erhöht langfristig den Unternehmenswert.

[55] Siehe Kapitel "Notfall- und Krisenmanagement"

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 Fachleute, 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 Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

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

TeleTrusT
Pioneers in IT security.

TeleTrusT
Pioneers in IT security.