CYBERSICHERHEIT

**G15004** d Ausgabe November 2024

**INFORMATION**

# Leitfaden

# zur Umsetzung des Minimalstandards für die Sicherheit der Informations- und Kommunikationstechnologie in der Gasversorgung (G1008)

## mit Fokus auf das Schutzniveau C

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Bundesamt für Energie BFE**

SVGW

gaz energie

# Impressum

**Datum** 20. November 2024

**Ort** Zürich

**Herausgeber**

Fachverband für Wasser, Gas und Wärme
SVGW
Grütlistrasse 44
8027 Zürich
Tel: +41 44 288 33 33
info@svgw.ch
www.svgw.ch

Verband der Schweizerischen Gasindustrie
VSG
Grütlistrasse 44
8027 Zürich
Tel: +41 44 288 31 31
vsg@gazenergie.ch
www.gazenergie.ch

**Projektleitung**

Daniela DECURTINS (VSG)
Stéphane HENRY (BFE)
Karsten REICHART (SVGW)

**Hauptautor/in**

Fabio BASTINE-NIEHÖRSTER (VSG)
Marc BONVIN (BFE)

**Co-Autor/in**

Roger BÄCHTIGER (ERI)
Sandra BREITSCHMID (GVM AG)
Dominik CAVEGN (EGO AG)
Daniela DECURTINS (VSG)
Stéphane HENRY (BFE)
Hans-Peter KÄSER (BACS)
Wolfgang KOROSEC (St.Galler Stadtwerke)
Marcel KÜHNI (Regionalwerke AG)
Christof NIEHÖRSTER (VSG)
Sven PINTON (EZL AG)
Andreas WOLF (EGO AG)
Karsten REICHART (SVGW)

# Vorwort

Die Sicherheit der Schweizer Gasversorgung hängt unter anderem davon ab, wie widerstandsfähig die Schweiz gegenüber Cyberangriffen ist. Die Bedrohungen, denen sich der Energiesektor gegenübersieht, haben in den letzten Jahren drastisch zugenommen. Um sich gegen diesen Trend bestmöglich zu rüsten, sieht Art. 39a der Rohrleitungssicherheitsverordnung (RLSV; SR 746.12) die Verpflichtung zu Cybersicherheitsmassnahmen vor. Diese sind im Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung (IKT-Minimalstandard G1008[1]) festgelegt, der sich auf das *NIST Cybersecurity Framework V1.1*[2] (NIST CSF V1.1) stützt und gleichzeitig Anforderungen[3] definiert, die für jedes Schutzniveau (A, B oder C) erreicht werden müssen.

Um die Umsetzung des IKT-Minimalstandards G1008 zu erleichtern, steht ein Selbsteinschätzungstool (*Self-Assessment Tool*) zur Verfügung[4]. Dazu hat die Branche diesen Leitfaden erarbeitet. Er hat zum Ziel, bestimmte Begriffe des IKT-Minimalstandards G1008 zu erläutern und eine kohärente Struktur für die Umsetzung der Cybersicherheit zu bieten. Das Dokument richtet sich in erster Linie an KMU im Gassektor, da er sich auf die 39 Massnahmen konzentriert, die für das Schutzniveau C verbindlich sind. Selbstverständlich können die Empfehlungen auch von anderen Unternehmen befolgt werden.

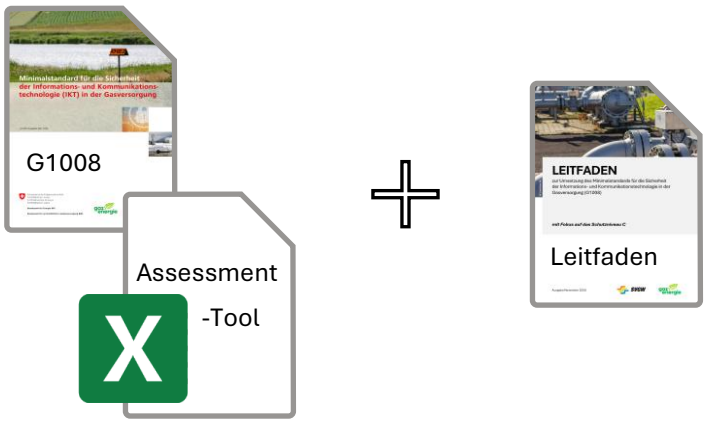



*Abbildung 1: Unterlagen zur Erhöhung der Cybersicherheit in der Gasversorgung*

Der Leitfaden besteht aus einem ersten Teil, der die grundlegenden Prinzipien und Begriffe der Cybersicherheit einführt. **Der zweite Teil des Dokuments ist den 39 Unterkategorien gewidmet, die für das Schutzniveau C ausgewählt wurden**. Für jede Unterkategorie wurden die Anforderungen präzisiert, die Erwartungen erläutert und eine Umsetzungshilfe formuliert.

[1] Der Standard kann unter https://www.svgw.ch/shopregelwerk/produkte/g1008-d-minimalstandard-fuer-die-sicherheit-der-informations-und-kommunikationstechnologie-ikt-in-der-gasversorgung/ heruntergeladen werden.
[2] Das *NIST Cybersecurity Framework 1.1* (CSF) kann unter https://www.nist.gov/cyberframework heruntergeladen werden.
[3] Die Anforderungen sind im Kapitel 5.2 des IKT-Minimalstandards G1008 zu finden.
[4] Das Selbsteinschätzungstool kann unter https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html heruntergeladen werden.

# Inhaltsverzeichnis

# Teil 1 – Einleitung

## Ausgangslage und Zielsetzung

IKT-Sicherheit bedingt ein risikobasiertes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich der jeweiligen Betreiber. Bereits durch die Umsetzung von empfohlenen Massnahmen, wie sie im IKT-Minimalstandard G1008 dargestellt werden, kann eine Vielzahl von IKT-Angriffen mit vertretbarem Aufwand abgewehrt werden. Der IKT-Minimalstandard G1008 hat zum Ziel, Unternehmen und Organisationen ein vielseitig einsetzbares Hilfsmittel zur Hand zu geben, mit dem diese individuell die Resilienz ihrer IKT-Infrastruktur verbessern können.

Die im IKT-Minimalstandard G1008 festgelegten Anforderungen werden durch Art. 39 Abs. 4 RLSV[5] für verbindlich erklärt. Gasunternehmen sind daher verpflichtet, die vorgesehenen Grundsätze der Cybersicherheit entsprechend ihrer Kategorie (A, B oder C) umzusetzen.

Dieser Leitfaden dient als Hilfe bei der Umsetzung der im IKT-Minimalstandard G1008 festgelegten Anforderungen. Es konzentriert sich auf die 39 Unterkategorien, die für das Schutzniveau C ausgewählt wurden. Die Empfehlungen der 39 Unterkategorien gelten selbstverständlich auch für die Schutzniveaus A und B.

Für jede der 39 Unterkategorien präzisiert der Leitfaden die Anforderungen. Es soll die Umsetzung der Massnahmen mit begrenzten Ressourcen erleichtern und den Unternehmen helfen, die Compliance-Ziele zu erreichen.

Obwohl dieser Leitfaden mit grösster Sorgfalt entwickelt wurde, garantiert es den Unternehmen keinen unfehlbaren Schutz vor Cyberangriffen und auch nicht die Einhaltung aller in Art. 39a RLSV festgelegten Anforderungen. Jedes Unternehmen bleibt für seine Cybersicherheit selbst verantwortlich. Auch wenn die im IKT-Minimalstandard G1008 vorgesehenen Massnahmen die Widerstandsfähigkeit erhöhen sollen, muss der Cybersicherheitsansatz jedes Unternehmens auf einem individuellen Risikomanagementprozess basieren. Je nach Zielsetzung können oder sollten daher zusätzlich zu den im IKT-Minimalstandard G1008 und in diesem Dokument aufgeführten Massnahmen weitere Massnahmen ergriffen werden.


*Abbildung 2: Übersicht der Cybersicherheitsmassnahmen*

Einige der 39 Massnahmen, die für das Schutzniveau C ausgewählt wurden, betreffen nur die organisatorische und managementbezogene Einrichtung der Cybersicherheit, jedoch noch nicht

[5] Geplantes Inkrafttreten am 01.07.2025.

die Durchsetzung durch technische Massnahmen. Die organisatorische Umsetzung eines Prozesses allein reicht natürlich nicht aus, um die Sicherheit des Unternehmens zu gewährleisten. Sie muss in jedem Fall von angemessenen technischen Massnahmen begleitet werden. Soweit möglich, werden in diesem Leitfaden Werkzeuge empfohlen, die die technische Umsetzung der Cybersicherheit ermöglichen bzw. erleichtern sollen.

Der IKT-Minimalstandard G1008 und dieser Leitfaden basieren auf dem NIST CSF V.1.1. Dieser Ansatz hat sich bei Unternehmen und innerhalb des Energiesektors bewährt. Es gibt jedoch noch weitere Möglichkeiten, um ein Programm zur Cybersicherheit zu implementieren und ähnliche Ergebnisse zu erzielen. Die Wahl der Methodik, um die festgelegten Anforderungen zu erreichen, steht jedem Unternehmen frei. Um die Implementierung zu erleichtern, können für jede Massnahme des IKT-Minimalstandards die Übereinstimmungen mit anderen anerkannten Standards (ISO, COBIT, NERC, BSI, ...) unter der Registerkarte „*Assessment*“ des Selbsteinschätzungstools eingesehen werden.[6]

[6] Das Selbsteinschätzungstool kann unter https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html heruntergeladen werden.

# Grundbegriffe

In diesem Kapitel werden grundlegende Begriffe und Prinzipien der Cybersicherheit definiert, auf die der IKT-Minimalstandard G1008 verweist, die aber nicht Teil der Anforderungen sind. Diese verschiedenen Konzepte ermöglichen ein besseres Verständnis der Cybersicherheit als Ganzes.

## Informationsschutz

Der Informationsschutz zielt auf den angemessenen Schutz von Informationen und der IKT-Infrastruktur in Bezug auf die festgelegten Schutzziele, wie **Vertraulichkeit, Integrität und Verfügbarkeit** ab. Ein unbefugter Zugriff auf Systeme oder die Manipulation von Informationen sollen verhindert und entstehende Risiken so weit als möglich gesenkt werden, um daraus resultierende wirtschaftliche Schäden zu verhindern.

Im Arbeitsalltag werden oft die Begriffe «Informationsschutz», «Datenschutz» und «IT-Sicherheit» verwechselt oder in einem falschen Kontext benützt.

Wie in der unterstehenden Grafik ersichtlich, sind der Datenschutz und die IT-Sicherheit Teil des Informationsschutzes welcher wiederum ein wichtiger Bestandteil des Unternehmensrisikomanagements und des *Business Continuity Management* (BCM) ist.

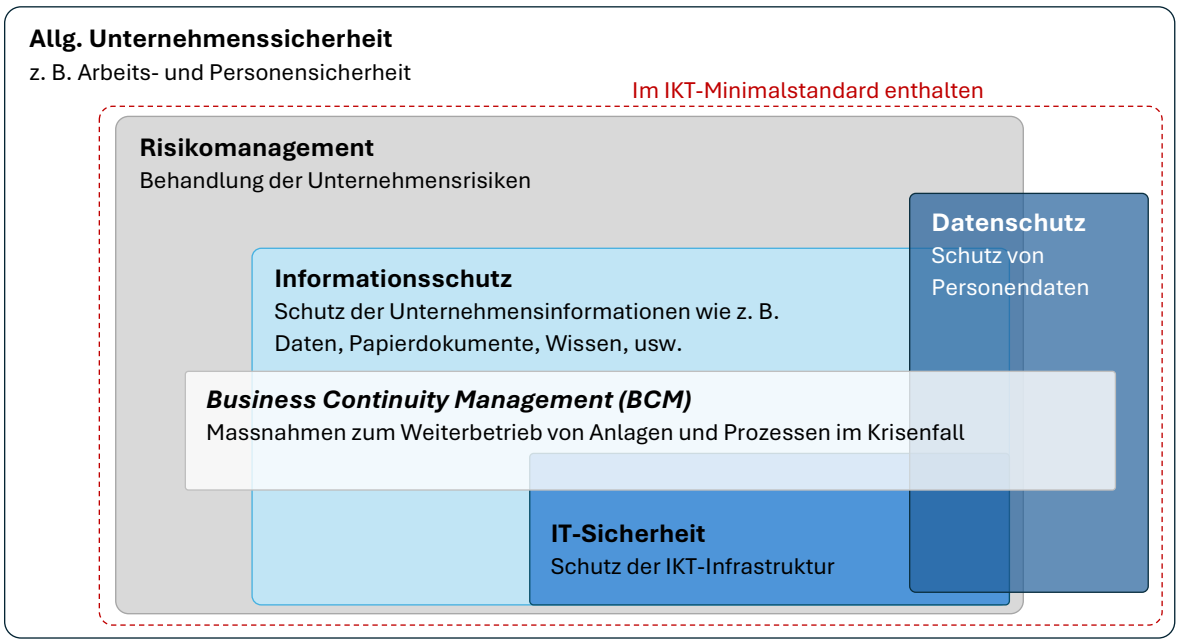



*Abbildung 3: Unternehmenssicherheit*

## Informationsschutzstrategie

Eine erfolgreiche Informationsschutzstrategie schützt die Mittel einer Organisation, die zur Ausführung der (kritischen) Geschäftsprozesse notwendig sind. Dabei gibt es keine allgemein gültige Definition von Anforderungen oder Lösungen.

Um die Sicherheitsrisiken im Bereich der kritischen Informations- und Kommunikationssysteme ganzheitlich identifizieren und behandeln zu können ist eine mehrschichtige Informationsschutzstrategie, welche dem «*Defense-in-Depth*»-Ansatz folgt, unerlässlich. Dieser basiert auf dem Prinzip, mehrere Sicherheitsschichten einzusetzen, um Angriffe abzuwehren und das Risiko eines vollständigen Systemdurchbruchs zu minimieren. Jede Ebene – von physischer Sicherheit über

Netzwerkschutz bis hin zu Zugriffskontrollen – dient als zusätzliche Barriere. Selbst wenn eine Schicht kompromittiert wird, bieten die anderen Ebenen weiterhin Schutz.

Diese Strategie sollte neben technischen Massnahmen auch die dazu benötigten Prozesse, die Ausbildung und Schulung der Mitarbeitenden sowie die benötigte *Security-Governance* umfassen. Letztere beschreibt die Verantwortung der Unternehmensführung, die IT-Organisation und die IT-Prozesse so zu gestalten, dass die gesetzten Ziele erreicht werden.

*Defense-in-Depth*-Strategien sind individuell und müssen sich an den Bedürfnissen, Möglichkeiten und Risiken der Organisation orientieren. Die risikobasierte Vorgehensweise berücksichtigt dabei neben den eigenen auch die Abhängigkeiten von externen Prozessen oder Ressourcen.

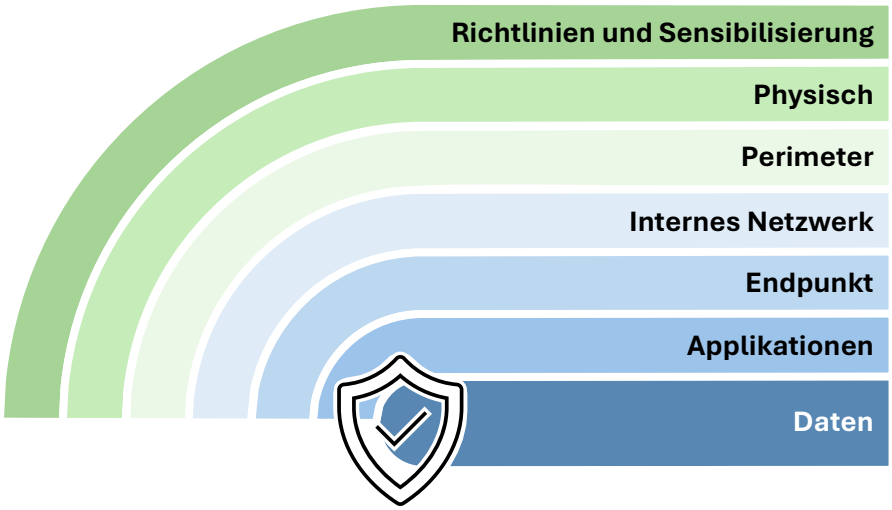



*Abbildung 4: Defense-in-Depth-Strategie*

Die ***Defense-in-Depth***-Strategie berücksichtigt, dass es keinen vollumfänglichen Schutz gegen jegliche Art von Cyber-Bedrohungen geben kann. Stattdessen ist man sich der eigenen Verwundbarkeit bewusst und entwickelt Strategien und Massnahmen, um die Gefährdung gegenüber Informationsschutz-Risiken zu identifizieren (IDENTIFIZIEREN), sich dagegen bestmöglich zu schützen (SCHÜTZEN), Verletzungen der Cybersicherheit zu detektieren (ERKENNEN), darauf zu reagieren (REAGIEREN) um schnellstmöglich wieder den Normalzustand zu erreichen (WIEDERHERSTELLEN).

## Datenschutz

Datenschutz beschreibt den Schutz von personenbezogenen Daten und besonders schützenswerten Personendaten sowie den Schutz des Rechts auf informationelle Selbstbestimmung. Er umfasst organisatorische sowie technischen Massnahmen gegen missbräuchliche Verarbeitung und Verwendung von personenbezogenen Daten.

Der Datenschutz in der Schweiz richtetet sich grundsätzlich nach dem Bundesgesetz über den Datenschutz (DSG; SR 235.1) sowie der Verordnung über den Datenschutz (DSV; SR 235.11). Sobald jedoch ebenfalls Daten von Bürgern (Kunden, Mitarbeiter) der Europäischen Union verarbeitet werden, kann es sein, dass die Vorgaben der Datenschutz-Grundverordnung der EU (Verordnung (EU) 2016/679 vom 27.04.2016, EU-DSGVO) auch in der Schweiz mitberücksichtigt werden müssen.

Die Bedeutung des Datenschutzes hat seit Beginn der Digitalisierung stetig zugenommen, da die Datenhaltung, Datenverarbeitung, Datenerfassung, Datenweitergabe und Datenanalyse immer umfangreicher und einfacher werden. Digitale Innovationen wie Internet, E-Mail, Mobiltelefonie,

Videoüberwachung sowie elektronische Zahlungsmethoden schaffen immer mehr und neue Möglichkeiten zur Erfassung von Personendaten.

Beim Speichern und Verarbeiten von personenbezogenen Daten gelten unter anderem die folgenden Grundsätze:

- Personendaten dürfen nur gesetzeskonform bearbeitet werden;
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

## IT-Sicherheit

Die IT-Sicherheit als Teilbereich des Informationsschutzes dient dem Schutz elektronisch gespeicherter Informationen (Daten), deren Verarbeitung sowie den Schutzzielen **Vertraulichkeit, Verfügbarkeit und Integrität**. Ebenfalls eingeschlossen ist das fehler- und unterbrechungsfreie Funktionieren und die Zuverlässigkeit der IKT-Systeme.

Hierbei müssen auch Systeme einbezogen werden, die häufig nicht unmittelbar als IKT-Systeme identifiziert werden, wie z. B. Telefonanlagen, Steuerungs- (ICS) oder IoT-Systeme. Beim Einsatz von *Cloud*-Systemen weitet sich das Handlungsfeld der klassischen IT-Sicherheit über den Unternehmensperimeter in den Cyberraum hinaus.

Die Begehrlichkeit, Betriebsdaten von Geräten und Systemen zu erheben und auszuwerten, hat bei den System-Lieferanten stark zugenommen. Einerseits, um ihre Produkte zu verbessern, anderseits, um deren Nutzung und Einsatz zu verfolgen. Die bewusste Herausgabe von solchen Informationen sollte im Vorfeld kritisch hinterfragt, eindeutig geklärt und vertraglich geregelt werden. Es sollte ebenfalls festgelegt werden, über welche sicheren Verbindungen und in welchen Intervallen (Realtime, täglich, wöchentlich etc.) die Informationen an die Lieferanten übermittelt werden.

# Teil 2 – Präzisierung der Anforderungen

In diesem Kapitel werden 39 der 108 Unterkategorien detaillierter beschrieben, damit die Umsetzung des IKT-Minimalstandards G1008 verständlicher ist. Diese 39 Massnahmen sind für das Schutzniveau C vorgeschrieben.

Aufgrund der Auswahl der für das Schutzniveau C relevantesten Massnahmen liegt der Schwerpunkt auf Schutzmassnahmen (SCHÜTZEN).

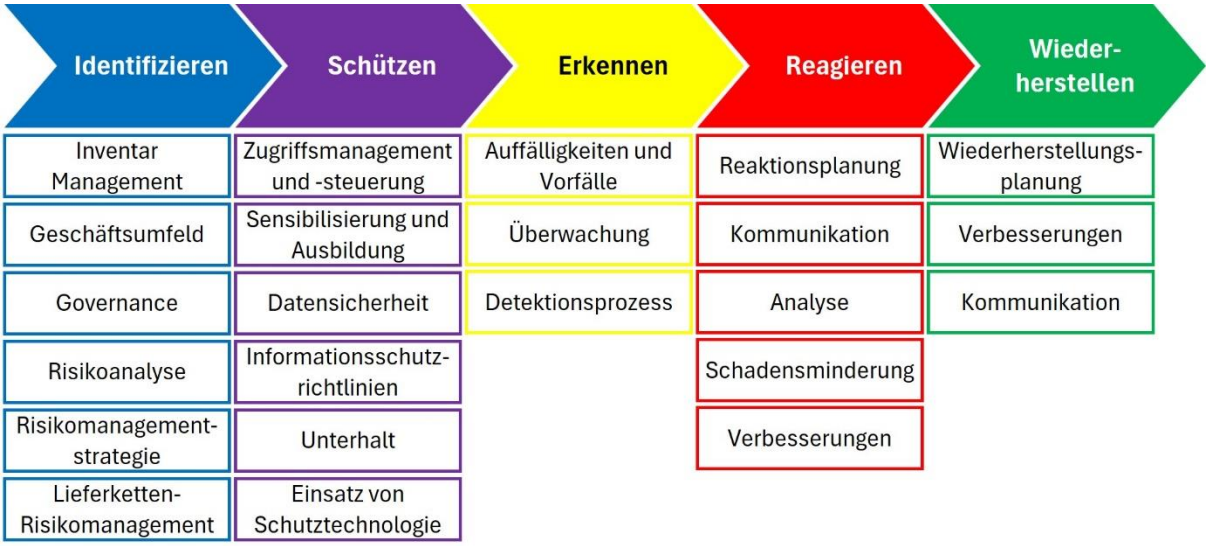



*Abbildung 5: Übersicht der Kategorien und Unterkategorien des NIST CSF V1.1*

Um das Verständnis der Erwartungen und die Umsetzung der Cybersicherheitsmassnahmen zu erleichtern, wurde nachfolgend für jede Unterkategorie folgende Struktur angewendet:

1. Worum geht es?
2. Was muss erfüllt werden?
3. Wie erfüllt man die Anforderungen?
4. Wann werden die Anforderungen erfüllt?
5. Wenn sinnvoll: "Was wird zur Umsetzung benötigt?"

Für jede Unterkategorie wird rechts unter «MS» die entsprechende Maturität für das Schutzniveau C angegeben. Weitere Informationen zu den Maturitätsstufen finden Sie im Kapitel 4.5 des IKT-Minimalstandard G1008.

| Unterkategorie | MS |
|---|---|
| Aufgabe | ... |

*Abbildung 6: Beispiel einer Unterkategorie mit Maturitätsstufe*

Die angegebene Maturität entspricht den gesetzlichen Mindestanforderungen. Um sich wirksam zu schützen, gehen die Empfehlungen in diesem Dokument manchmal über das hinaus, was für die Einhaltung der Compliance-Anforderungen erforderlich ist (insbesondere Zeitangaben). Jedes Unternehmen ist dafür verantwortlich, entsprechend seiner Situation zu entscheiden, wie regelmässig seine Cybersicherheitsmassnahmen überprüft, aktualisiert und verbessert werden sollen.

## Identifizieren (ID)

Die Kategorie „Identifizieren“ hilft bei der Entwicklung eines organisatorischen Verständnisses zum Management von Cybersicherheitsrisiken. Das Verständnis des geschäftlichen Kontexts, der Ressourcen, die kritische Funktionen unterstützen, sowie der damit verbundenen Cybersicherheitsrisiken ermöglicht es einer Organisation, ihre Bemühungen entsprechend ihrer Risikomanagementstrategie und den geschäftlichen Anforderungen zu fokussieren und zu priorisieren.[7]

### *Inventarmanagement (ID.AM)*

Die Informationen, Personen, Geräte, Systeme und Anlagen, einer Organisation sind in einer Art und Weise identifiziert, katalogisiert und bewertet, die ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse, sowie der Risikostrategie der Organisation entsprechen.

### *Governance (ID.GV)*

Die *Governance* bildet den Ordnungsrahmen für die Leitung und Überwachung der Cybersicherheit. Sie regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische und rechtliche Anforderungen aus dem Geschäftsumfeld sowie operationelle Anforderungen richtig verstanden werden und informiert das Management entsprechend.

### *Lieferketten-Risikomanagement (ID.SC)*

Legen Sie die Prioritäten, Einschränkungen und maximalen Risiken fest, die Ihre Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist. Verwenden Sie die Definition der Lieferantenrisiken als Grundlage zur Beurteilung operativer Risiken.

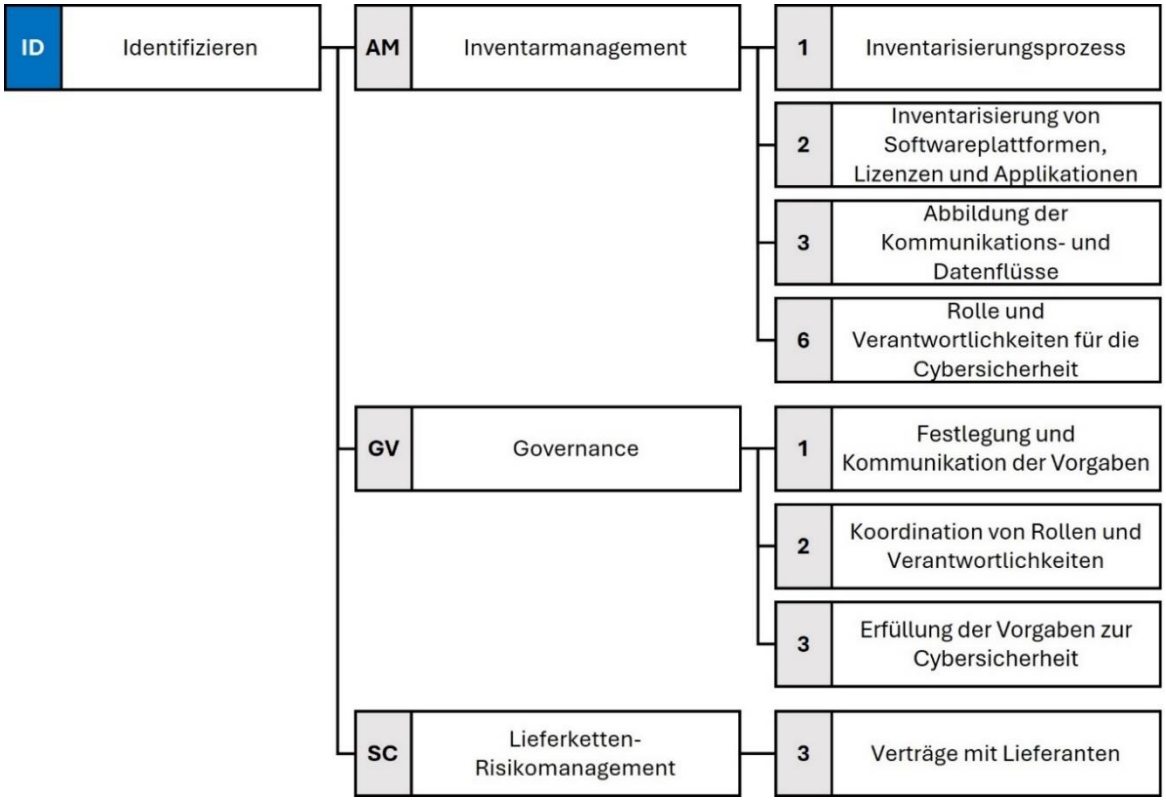



*Abbildung 7: Vorgeschriebene ID-Unterkategorien für Schutzniveau C*

[7] https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

## Inventarmanagement (ID.AM)

| ID.AM-1 Inventarisierungsprozess | MS |
|---|---|
| Erarbeiten Sie einen Inventarisierungsprozess, welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar all Ihrer IKT-Betriebsmittel (*Assets*) vorhanden ist. | 3 |

***Worum geht es?***

ID.AM-1 verlangt die Entwicklung eines Prozesses, der sicherstellt, dass jederzeit ein vollständiges und aktuelles Inventar aller IT- und OT-Betriebsmittel vorliegt. Ein solches Inventar ist entscheidend für effizientes Management und die Minimierung von Sicherheitsrisiken. Fehlende oder veraltete Inventare erhöhen das Risiko von Sicherheitslücken.

***Was muss erfüllt werden?***

Ein effektiver Inventarisierungsprozess erfordert:

- Vollständigkeit: Alle Betriebsmittel (zentral, lokal oder in der Cloud verwaltet) müssen erfasst sein.
- Aktualität: Das Inventar muss regelmässig bei Änderungen, wie Installationen und Systemaktualisierungen, aktualisiert werden.
- Eindeutigkeit: Jedes Betriebsmittel muss klar identifiziert sein, um Doppelungen zu vermeiden.
- Verantwortlichkeit: Klare Zuständigkeiten für Verwaltung und Pflege sind notwendig.

***Wie erfüllt man die Anforderungen?***

- Zentrales Inventar: Alle Betriebsmittel werden zentral erfasst mit Informationen wie Seriennummern und Systemdetails.
- Eindeutige Identifikation: Betriebsmittel werden mit individuellen Identifikatoren erfasst, Netzwerk-Scanner unterstützen die Erfassung.
- Automatisierte Aktualisierung: Prozesse zur automatischen oder regelmässigen manuellen Aktualisierung bei jeder Änderung sind erforderlich.
- Zuweisung von Verantwortlichkeiten: Zuständigkeiten für Pflege und Verwaltung müssen definiert und dokumentiert sein.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen gelten als erfüllt, wenn Folgendes implementiert ist:

- Ein vollständiges und aktuelles Inventar aller IKT-Betriebsmittel ist vorhanden.
- Alle Betriebsmittel sind eindeutig identifiziert und ohne Duplikate.
- Der Inventarisierungsprozess ist automatisiert oder wird in festgelegten Intervallen manuell überprüft.
- Verantwortlichkeiten sind klar zugewiesen und dokumentiert.

| ID.AM-2 Inventarisierung von Softwareplattformen, Lizenzen und Applikationen | MS |
|---|---|
| Inventarisieren Sie all ihre Softwareplattformen / -Lizenzen und Applikationen innerhalb ihrer Organisation. | 2 |

***Worum geht es?***

ID.AM-2 konzentriert sich auf die Inventarisierung aller Softwareplattformen, Lizenzen und Applikationen, die innerhalb der Organisation verwendet werden. Dies umfasst sowohl zentrale Softwarelösungen als auch lokal oder in der Cloud installierte Anwendungen. Ein vollständiges und aktuelles Software-Inventar ist entscheidend, um die Lizenz-Compliance sicherzustellen, Sicherheitslücken zu vermeiden und eine effiziente Verwaltung der Softwareumgebung zu ermöglichen.

***Was muss erfüllt werden?***

Ein effektiver Software-Inventarisierungsprozess erfordert:

- Vollständigkeit: Alle genutzten Softwareplattformen, Lizenzen und Applikationen müssen erfasst werden, einschliesslich der Informationen zu deren Versionen und Nutzung.
- Aktualität: Das Inventar muss regelmässig aktualisiert werden, insbesondere bei neuen Installationen oder Deinstallationen. Hierbei wird empfohlen mindestens eine jährliche Überprüfung durchzuführen.
- Lizenzkonformität: Die Lizenzen müssen regelmässig überprüft werden, um sicherzustellen, dass keine Über- oder Unterlizenzierung vorliegt.
- Verantwortlichkeit: Es müssen klare Zuständigkeiten für die Verwaltung und Pflege des Software-Inventars definiert werden, um die Lizenz-Compliance und den effektiven Einsatz der Applikationen sicherzustellen.

***Wie erfüllt man die Anforderungen?***

- Erstellung eines zentralen Software-Inventars: Erfassen Sie alle genutzten Softwareprodukte, Versionen, Lizenzen und Applikationen, einschliesslich der Lizenzverträge und der zugewiesenen Nutzer.
- Automatisierte oder manuelle Aktualisierung: Setzen Sie automatisierte Prozesse ein, um neue Software oder Aktualisierungen zu erfassen. Für manuell installierte Software sind regelmässige Überprüfungen erforderlich.
- Lizenzverwaltung: Regelmässige Überprüfung der Lizenzvereinbarungen, um sicherzustellen, dass die Organisation sowohl Compliance-Anforderungen erfüllt als auch kosteneffizient lizenziert ist.
- Verantwortlichkeiten festlegen: Verantwortlichkeiten für die Verwaltung von Software und Lizenzen müssen klar zugewiesen und dokumentiert sein.

***Wann werden die Anforderungen erfüllt?***

- Ein zentrales Inventar aller genutzten Softwareplattformen und Lizenzen ist vorhanden und aktuell.
- Lizenzen sind korrekt zugewiesen und es wird regelmässig überprüft, dass keine Verstösse gegen Lizenzvereinbarungen vorliegen.
- Verantwortlichkeiten für die Verwaltung und Pflege des Software-Inventars sind dokumentiert.

| ID.AM-3 Abbildung der Kommunikations- und Datenflüsse | MS |
|---|---|
| Organisatorische Kommunikation und Datenflüsse werden abgebildet | 2 |

***Worum geht es?***

ID.AM-3 betrifft die Steuerung und Überwachung der Informationsflüsse innerhalb einer Organisation und zwischen Systemen und Partnern. Ziel ist es, den gesamten Informationsfluss aufzulisten, um sicherzustellen, dass die richtigen Informationen von den autorisierten Systemen unter Einhaltung aller Sicherheits- und Datenschutzrichtlinien übertragen oder verarbeitet werden.

***Was muss erfüllt werden?***

Um die Anforderungen von ID.AM-3 zu erfüllen, müssen alle Informationsflüsse innerhalb der Organisation abgebildet und dokumentiert werden, indem die beteiligten Systeme, die Benutzer, die Arten der ausgetauschten Daten und die verwendeten Protokolle angegeben werden. Die Regeln und Mechanismen, die den Informationsfluss steuern, müssen klar beschrieben und korrekt umgesetzt werden.

***Wie erfüllt man die Anforderungen?***

- Richtlinien: Einführung von Richtlinien zur Steuerung der Informationsflüsse.
- Informationsflüsse: Identifizierung, Dokumentation und Visualisierung aller relevanten Datenströme zwischen Systemen und Nutzern, einschliesslich Protokollen und Sicherheitsmechanismen.
- Kommunikationskanäle: Kartierung aller internen und externen Kommunikationskanäle, inklusive Szenarien wie Fernwartung.
- Klassifizierung: Klassifizieren Sie die Informationen nach ihrer Sensibilität und stellen Sie sicher, dass Sie alle Vorschriften und Compliance-Anforderungen einhalten.
- Netzwerk-Architektur: Visualisierung des gesamten Netzwerks, inklusive physischer, WLAN- und virtueller Netzwerke, sowie der Verbindungen zwischen Geräten.
- Überwachung: Erkennen Sie unerlaubte Datenströme mithilfe von Tools zur Verwaltung von Sicherheitsereignissen (SIEM). Um die Informationen zu sichern, beachten Sie die Unterkategorie PR.DS-2.PR.DS-2 Datenübertragungssicherheit
- Regelmässige Aktualisierung: Anpassung der Dokumentation bei jeder Änderung in der Netzwerkarchitektur oder den Informationsflüssen.

***Wann werden die Anforderungen erfüllt?***

Alle Informationsflüsse kritischer Systeme werden abgebildet und enthalten folgende Informationen:

- Richtung der Flüsse
- Arten, Sensibilität und Speicherung der ausgetauschten Daten und Sensibilität
- Prozesse (Datenveränderungen)
- Externe Stellen (Quelle oder Ziel der Informationen)

Das Diagramm kann z. B. durch die verwendeten Protokolle und vorhandene Sicherheitsmechanismen ergänzt werden, sollte aber einfach zu verstehen bleiben.

| ID.AM-6 Rolle und Verantwortlichkeiten für die Cybersicherheit | MS |
|---|---|
| Cybersicherheitsrollen und -Verantwortlichkeiten für die gesamte Belegschaft und externe Stakeholder (z. B. Lieferanten, Kunden, Partner) sind festgelegt. | 3 |

***Worum geht es?***

ID.AM-6 legt klare Rollen und Verantwortlichkeiten für die Cybersicherheit fest, sowohl für Mitarbeiter als auch externe Partner, wie Lieferanten und Kunden. Ziel ist es, sicherzustellen, dass jeder weiss, wer für welche Sicherheitsaspekte verantwortlich ist.

***Was muss erfüllt werden?***

- Definierte Cybersicherheitsrollen: Wer übernimmt welche Aufgaben im Bereich Cybersicherheit (bspw. CISO, IT Risk Officer)?
- Klare Verantwortlichkeiten: Jeder muss seine Aufgaben kennen, auch externe Partner.

***Wie erfüllt man die Anforderungen?***

- Ernennung von Schlüsselrollen: Der CISO übernimmt die Hauptverantwortung für die Cybersicherheit. In kleineren Unternehmen könnte der IT-Leiter zusätzliche Aufgaben wie Risikomanagement übernehmen.
- Dokumentation und Kommunikation: Verantwortlichkeiten müssen schriftlich festgelegt und kommuniziert werden, etwa durch NDAs, Arbeitsanweisungen und Schulungen. Alle Mitarbeiter, einschliesslich externer Partner, müssen ihre Rolle verstehen.
- Zusammenarbeit: Cybersicherheitsrollen müssen effektiv zusammenarbeiten. In kleineren Unternehmen teilen sich oft wenige Personen diese Aufgaben.
- Regelmässige Überwachung: Sicherheitsverantwortlichkeiten werden durch regelmässige Überprüfungen oder Audits überwacht.

***Wann werden die Anforderungen erfüllt?***

- Rollen sind definiert und zugewiesen (z. B. CISO für Koordination der Sicherheitsmassnahmen).
- Externe Partner halten sich an die Sicherheitsanforderungen und melden sicherheitsrelevante Änderungen (z. B. Personalwechsel).
- Regelmässige Anpassungen und Überprüfungen erfolgen.

***Was wird zur Umsetzung benötigt?***

- Rollenbeschreibungen: Klare Definition der Cybersicherheitsaufgaben (intern und extern).
- Regelmässige Schulungen für Mitarbeiter und Partner (siehe PR.AT-2).
- Regelmässige Audits zur Überprüfung der Einhaltung der Sicherheitsverantwortlichkeiten.
- Management-Support: Die Unternehmensleitung muss die Bedeutung der Cybersicherheit betonen und die Wahrnehmung der festgelegten Rollen und Verantwortlichkeiten sicherstellen.
- Verträge mit Partnern: Externe Anbieter sollten vertraglich (z. B. per NDA) zur Einhaltung der Sicherheitsrichtlinien verpflichtet werden.

## Governance (ID.GV)

| ID.GV-1 Festlegung und Kommunikation der Vorgaben | MS |
|---|---|
| Vorgaben zur Informationssicherheit sind im Unternehmen festgelegt und kommuniziert. | 3 |

***Worum geht es?***

Unternehmen müssen Informationssicherheitsrichtlinien entwickeln, genehmigen, kommunizieren und regelmässig aktualisieren. Diese Richtlinien konkretisieren die strategischen Entscheidungen und Unternehmensziele. Sie basieren auf dem Prinzip des Risikomanagements und legen die Mittel zur Erreichung der Ziele fest. Sie schützen sensible Informationen, Infrastrukturen sowie kritische Aktivitäten und sorgen für die Einhaltung von Gesetzen und Regulierungen.

***Was muss erfüllt werden?***

Informationssicherheitsrichtlinien müssen vorhanden und allen Mitarbeitern bekannt sein. Regelmässige Aktualisierungen sind nicht zwingend erforderlich, aber empfohlen, um neue Bedrohungen zu adressieren.

***Wie erfüllt man die Anforderungen?***

Als Mindestanforderung muss eine Informationssicherheitsstrategie erarbeitet, kommuniziert und verabschiedet werden.

Dabei sollten die folgenden Schritte berücksichtigt werden:

- Ziele und Risiken verstehen: Identifikation kritischer Prozesse, Informationen und Risiken.
- Gesetze, Vorschriften und Standards einhalten: Analyse muss durchgeführt werden. Die Zusammenarbeit mit dem Rechtsteam sollte bevorzugt werden.
- Informationssicherheitsrichtlinie entwickeln: Klare Ziele, Verantwortlichkeiten und Erwartungen festlegen.
- Kommunikation und Umsetzung: Die Richtlinie muss allen Mitarbeitern zugänglich sein (z. B. via Intranet) und klar kommuniziert werden. Schulungen sind empfehlenswert.
- Aktualisierung und Verbesserung: Regelmässige Überarbeitung der Richtlinie, basierend auf neuen Bedrohungen und dem PDCA-Zyklus.
- Beispielhafte Inhalte einer Sicherheitsrichtlinie:
  - Risikomanagement
  - Gesetzeskonformität
  - Sicherheitskontrollen, Verwaltung von Zugängen
  - Umgang mit Vorfällen, Reaktion auf Vorfälle
  - Sensibilisierung und Schulung
  - Datenschutz, Kryptografie, BYOD-Regelungen
  - Einsatz von künstlicher Intelligenz

***Wann werden die Anforderungen erfüllt?***

- Informationssicherheitsrichtlinien sind vorhanden und werden von den Mitarbeitern angewendet.
- Die Anforderungen an jeden Mitarbeiter sind klar und dokumentiert.

| ID.GV-2 Koordination von Rollen und Verantwortlichkeiten | MS |
|---|---|
| Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sind mit internen Rollen (z. B. aus dem Riskmanagement) sowie externen Partnern koordiniert. | 3 |

***Worum geht es?***

Die Anforderung zielt darauf ab, bereits festgelegte Sicherheitsrollen effektiv zu koordinieren. Alle relevanten Akteure müssen wissen, wie sie im Bereich der Informationssicherheit zusammenarbeiten, um eine schnelle und effiziente Reaktion auf Vorfälle zu gewährleisten.

***Was muss erfüllt werden?***

Unternehmen müssen die bereits definierten Rollen klar koordinieren, sodass jeder Akteur seine Aufgaben kennt und bei sicherheitsrelevanten Themen zusammenarbeitet.

***Wie kann es erfüllt werden?***

Die Anforderungen können mittels folgender Massnamen erfüllt werden:

- Zentrale Koordination sicherstellen: Der CISO (falls vorhanden) koordiniert alle Cybersicherheitsteams und sorgt für eine klare Kommunikation. Er tauscht sich mit den anderen Sicherheitsverantwortlichen (RM, BCM, ...) aus.
- Regelmässige Abstimmungen: Regelmässige Briefings über Risiken und Sicherheitsmassnahmen sorgen dafür, dass alle Beteiligten informiert sind und sich auf dem neuesten Stand halten.
- Effektive Vorfallsreaktion: Definierte Notfallpläne und klare Verantwortlichkeiten ermöglichen eine schnelle und koordinierte Reaktion auf Vorfälle.
- Klare Eskalationsprozesse: Gut etablierte und strukturierte Eskalationspläne garantieren eine Rasche und geordnete Weiterleitung kritischer Informationen.
- Einbindung externer Partner: Durch eine gute Kommunikation mit externen Dienstleistern kann die Reaktion auf Vorfälle vorbereitet und positiv beeinflusst werden.
- Regelmässige Überprüfung: Durch eine periodische Überprüfung der Koordination und Prozesse werden diese kontinuierlich an neue Herausforderungen angepasst.

***Wann gilt es als erfüllt?***

Die Anforderungen gelten als erfüllt, wenn alle Rollen innerhalb des Unternehmens, aber auch mit externen Dienstleistern, effektiv koordiniert sind und eine schnelle Reaktionsfähigkeit bei Sicherheitsvorfällen sichergestellt ist.

| ID.GV-3 Erfüllung der Vorgaben zur Cybersicherheit | MS |
|---|---|
| Stellen sie sicher, dass ihre Organisation alle gesetzlichen und regulatorischen Vorgaben im Bereich der Cybersicherheit erfüllt, inkl. Vorgaben zum Datenschutz. | 3 |

***Worum geht es?***

Die Einhaltung gesetzlicher und regulatorischer Vorgaben gewährleistet ein Mindestmass an Cybersicherheit, schützt kritische Infrastrukturen und minimiert Risiken wie Datenlecks und Systemeinbrüche. Zusätzlich reduziert die Compliance potenzielle Kosten und Schäden durch Strafen, Cyberangriffe oder Betriebsunterbrechungen und stärkt das Vertrauen von Kunden und Partnern.

***Was muss erfüllt werden?***

Unternehmen sollten alle relevanten Gesetze und Vorschriften in ihre Abläufe integrieren und deren Einhaltung nachweisen können. Dies betrifft insbesondere die Cybersicherheit und den Datenschutz von kritischen Infrastrukturen.

***Wie kann es erfüllt werden?***

Die Umsetzung von ID.GV-3 erfordert einen systematischen Ansatz zur Identifizierung und Einhaltung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen. Eine enge Zusammenarbeit zwischen den Rechts-, Compliance- und Sicherheitsteams ist notwendig, um die Richtlinien und Verfahren an externe Entwicklungen anzupassen. Folgende Schritte sind zu beachten:

- Identifikation der rechtlichen und regulatorischen Verpflichtungen: Geltende Gesetze, Normen und vertragliche Verpflichtungen analysieren, um ein vollständiges Verzeichnis zu erstellen.
- Definition interner Richtlinien und Verfahren: Compliance-Richtlinien entwickeln und Überwachungsverfahren zur kontinuierlichen Überprüfung einrichten.
- Schulung und Sensibilisierung: Schulungen für Mitarbeiter durchführen, um die Einhaltung der Vorgaben sicherzustellen (siehe PR.AT-1).
- Überwachung und Risikomanagement: Mechanismen implementieren, um Compliance-Risiken zu minimieren und das Risiko der Nichteinhaltung zu reduzieren.
- Regelmässige Aktualisierung: Richtlinien regelmässig überprüfen und an neue Vorschriften anpassen, um die Konformität aufrechtzuerhalten.
- Dokumentation und Kommunikation: Alle Compliance-Massnahmen dokumentieren und regelmässige Berichte für die Geschäftsführung und die Stakeholder erstellen.

***Wann gilt es als erfüllt?***

Die Anforderungen sind erfüllt, wenn das Unternehmen alle relevanten Vorschriften kennt, umsetzt und deren Einhaltung jederzeit nachweisen kann.

## Lieferketten-Risikomanagement (ID.SC)

| ID.SC-3 Verträge mit Lieferanten | MS |
|---|---|
| Verträge mit Lieferanten und Drittparteien verpflichten diese, Massnahmen, zur Erfüllung der Ziele des Cybersicherheitsprogramms und des Cyber-Lieferkettenrisikomanagementplans der Organisation umzusetzen und einzuhalten. | 3 |

***Worum geht es?***

Immer mehr Angriffe konzentrieren sich auf die Lieferkette. Die Folgen können schwerwiegend sein, da sie oft kritische Dienstleistungen zur Verfügung stellen. Die enge Beziehung zwischen Betreiber und Lieferant darf aber den Bedarf an Cybersicherheit nicht überdecken. Beide müssen auf die Widerstandsfähigkeit gegenüber Cyberangriffen hinarbeiten. Transparenz, Kommunikation und Zusammenarbeit sind Schlüsselelemente der Cybersicherheit.

***Was muss erfüllt werden?***

Betreiber und ihre Partner/Lieferanten müssen vertragliche Vereinbarungen treffen, um sicherzustellen, dass sie die Anforderungen an die Cybersicherheit erfüllen. Der Betreiber muss nachweisen können, dass alle notwendigen Massnahmen getroffen werden, um sich vor Cyberangriffen zu schützen. Der Anbieter wiederum muss die Ernsthaftigkeit seines Vorgehens nachweisen.

***Wie erfüllt man die Anforderungen?***

Um die Cybersicherheit in der Zusammenarbeit mit Lieferanten sicherzustellen, sollten folgenden Massnahmen betrachtet werden[8]:

- Lieferkettenrisiken identifizieren: Identifikation der kritischen Lieferanten, deren Produkte und Dienstleistungen und Bewertung der potenziellen Risiken und Auswirkungen.
- Bewertung der Lieferanten: Vor der Beauftragung eines neuen Lieferanten soll eine Prüfung durchgeführt werden. Spezifische Fragen zu Sicherheitsrichtlinien, Zertifizierungen, Schwachstellenmanagement, Datenhosting und Verschlüsselung sollten beantwortet werden. Diese Fragen betreffen unter anderem die Sicherheitsstandards der Systeme, die Handhabung von Daten sowie die Kontrollmechanismen zur Sicherstellung der Cybersicherheit.
- Cybersicherheitsanforderungen in Verträgen festlegen: Die Klauseln können Anforderungen, wie einzuhaltende Sicherheitsstandards (NIST, ISO, ...), Richtlinien zur Benachrichtigung bei Vorfällen oder Datenschutzverletzungen oder regelmässige Sicherheitsprüfungen enthalten.
- Planung der Geschäftskontinuität (BCM): Verpflichtung zur Einhaltung von Vorfallmanagementprozessen, einschliesslich klarer Benachrichtigungsfristen und Massnahmen bei Cyberangriffen. Zudem müssen Lieferanten über Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung nach Ereignissen verfügen, um die Auswirkungen auf ihre Dienste und die Organisation zu minimieren.

***Wann werden die Anforderungen erfüllt?***

Der Betreiber hat seine Ziele erfüllt, wenn er seine Lieferanten aufgefordert hat, ihm die geforderten Informationen zur Verfügung zu stellen, und wenn er überprüft hat, dass die Systeme und Anwendungen die Erfüllung der genannten Kriterien ermöglichen.

[8] Weitere Informationen über die Cybersicherheit in der Lieferkette können auf der Webseite des BACS abgerufen werden: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html

## Schützen (PR)

Die Kategorie „Schützen“ beschreibt geeignete Schutzmassnahmen, um die Leistungserbringung kritischer Infrastrukturdienste sicherzustellen und die Auswirkungen eines potenziellen Cybersicherheitsvorfalls zu begrenzen oder zu minimieren.

***Zugriffsmanagement und Steuerung (PR.AC)***

Stellen Sie sicher, dass der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte möglich ist und dass der Zugriff nur für als zulässig definierte Aktivitäten möglich ist. Dies wird in Übereinstimmung mit dem bewerteten Risiko eines unbefugten Zugangs zu autorisierten Aktivitäten und Transaktionen verwaltet.

***Sensibilisierung und Ausbildung (PR.AT)***

Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Cybersicherheit geschult und ausgebildet werden. Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner ihre sicherheitsrelevanten Aufgaben gemäss den zugehörigen Vorgaben, Vereinbarungen und Prozessen ausführen.

***Datensicherheit (PR.DS)***

Informationen, Daten und Datenträger werden so gehandhabt, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden können.

***Informationsschutzrichtlinien (PR.IP)***

Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln sind erstellt. Diese Richtlinien umfassen im Minimum den Zweck, den Umfang, die Rollen und die Verantwortlichkeiten sowie die Koordination innerhalb der Organisation. Diese Richtlinien werden genutzt, um die Informationssysteme und Betriebsmittel zu schützen.

***Unterhalt (PR.MA)***

Unterhalts- und Reparaturarbeiten an Komponenten von IT-Systemen und ICS werden gemäss den geltenden Richtlinien und Prozessen durchgeführt.

***Einsatz von Schutztechnologien (PR.PT)***

Technische Security-Lösungen sind installiert, um die Sicherheit und Resilienz der Systeme und Daten gemäss den Vorgaben und Prozessen zu garantieren.

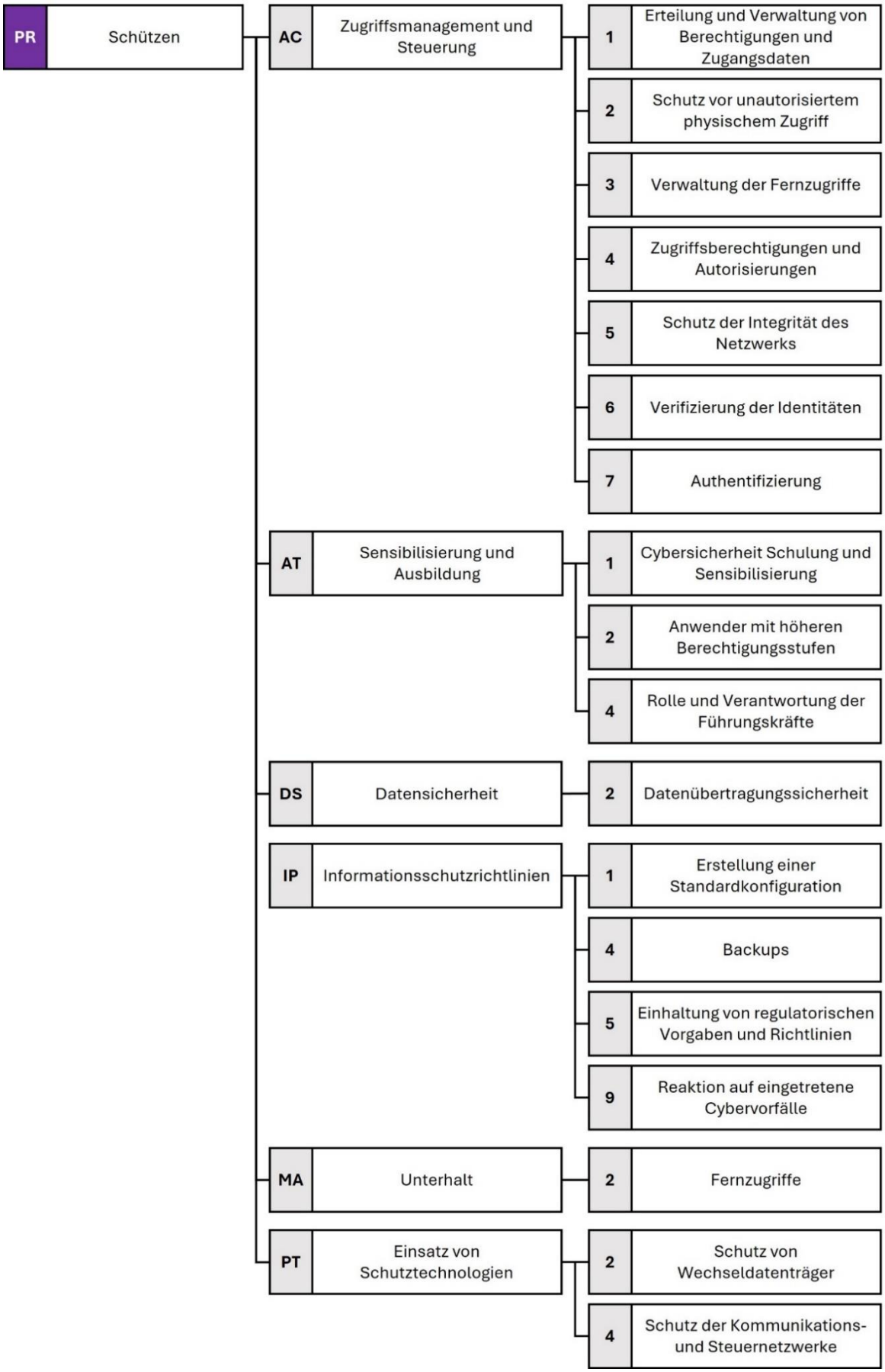



*Abbildung 8: Vorgeschriebene PR-Unterkategorien für Schutzniveau C*

## Zugriffsmanagement und -steuerung (PR.AC)

| PR.AC-1 Erteilung und Verwaltung von Berechtigungen und Zugangsdaten | MS |
|---|---|
| Etablieren sie einen klar definierten Prozess zur Erteilung und Verwaltung von Berechtigungen und Zugangsdaten für Benutzer, Geräte und Prozesse. | 2 |

***Worum geht es?***

Diese Massnahme stellt sicher, dass nur autorisierte Benutzende, Geräte und Prozesse Zugriff auf Ressourcen erhalten. Identitäten und Berechtigungen werden verwaltet, überprüft, entzogen und auditiert. Ziele sind die Einrichtung von Verfahren der Benutzerkontenverwaltung, die eindeutige Zuordnung von Identitäten sowie der rechtzeitige Entzug von Berechtigungen.

***Was muss erfüllt werden?***

Unternehmen sollten folgende Massnahmen implementieren:

- Führung einer aktuellen Benutzermatrix und zugehöriger Berechtigungen.
- Lebenszyklusmanagement für Berechtigungen implementieren.
- Mechanismen zur Identitätsüberprüfung und Berechtigungsvergabe.
- Nutzung von Zwei- oder Multi-Faktor-Authentifizierung (2FA/MFA).
- Festlegung von Verfahren zur Deaktivierung von Konten und dem Entzug von Berechtigungen.
- Sicherstellen, dass der Entzug rechtzeitig erfolgt, um unbefugten Zugriff zu verhindern.

***Wie kann es erfüllt werden?***

Folgende Schritte sollten unternommen werden:

- Richtlinien: Entwicklung und Durchsetzung von Richtlinien für das Management von Identitäten und Berechtigungen, inklusive 2FA/MFA und Passwortregeln.
- Mitarbeiterwechsel: Berechtigungen bei Austritt oder internem Wechsel anpassen. Laufblätter können dabei sehr hilfreich sein.
- Administration: Verwendung von speziellen Administratorkonten auf verschiedenen Ebenen (bspw. Domain, Server, Endgeräte).
- Audits: Regelmässige Überprüfung und Audits der Berechtigungen z. B. nach PS-CH 890[9].

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen gelten als erfüllt, wenn:

- Richtlinien und Verfahren dokumentiert und angewendet werden.
- Prozesse für Konten- und Berechtigungsmanagement schriftlich dokumentiert und nachweislich durchgeführt werden.
- Schulungen mit visierten Nachweisen durchgeführt werden.
- Empfehlung: Audits zur Anwendung der Richtlinien und Verfahren durchführen.

[9] Der Standard kann im Webshop von EXPERTSuisse heruntergeladen werden https://www.experts-uisse.ch/webshop (kostenpflichtig).

| PR.AC-2 Schutz vor unautorisiertem physischem Zugriff | MS |
|---|---|
| Stellen sie sicher, dass nur autorisierte Personen physischen Zugriff auf die IKT-Betriebsmittel haben. Sorgen sie mit (baulichen) Massnahmen dafür, dass die IKT-Betriebsmittel vor unautorisiertem physischem Zugriff geschützt sind. | 2 |

***Worum geht es?***

PR.AC-2 zielt darauf ab, den physischen Zugang zu kritischen Unternehmensressourcen zu kontrollieren und zu schützen. Dies minimiert Risiken durch physische Bedrohungen und unbefugte Manipulationen.

***Was muss erfüllt werden?***

Um die Anforderungen in PR.AC-2 zu erreichen, sollten Unternehmen folgende Massnahmen implementieren:

- Richtlinien und Verfahren für den physischen Zugang zu kritischen Infrastrukturen entwickeln.
- Sicherstellen, dass nur autorisierte Personen Zugang zu sensiblen Bereichen erhalten.
- Zutritte aufzeichnen, um Sicherheitsvorfälle nachvollziehen zu können.
- Regelmässige Überprüfung der physischen Zugangskontrollen, um sicherzustellen, dass sie weiterhin effektiv sind und den aktuellen Sicherheitsanforderungen entsprechen.

***Wie kann es erfüllt werden?***

- Richtlinien und Verfahren für den physischen Zugang zu kritischen Infrastrukturen erstellen, inkl. Zugangsberechtigungen, Schutzmassnahmen und Notfallzugangsverfahren.
- Elektronische Schliess- und Zutrittssysteme (bspw. RFID-Chips/-Schlüssel, biometrische Scanner, Zugangscodes) implementieren.
- Bauliche Sicherheitsmassnahmen (z. B. verstärkte Türen, Fenstersicherungen usw.) implementieren.
- Zugangsprotokolle regelmässig auf unbefugte Zugänge und Aktivitäten überprüfen.
- Jährliche Audits zu Vergabe, Nutzung und des Entzugs des physischen Zugangs durchführen. Das Audit kann z. B. nach PS-CH 890[10] erfolgen, wie es bei der jährlichen Wirtschaftsprüfung (Revision) teilweise verlangt wird.

***Wann werden die Anforderungen erfüllt?***

- Richtlinien und Verfahren sind dokumentiert, implementiert und angewendet.
- Je nach Grösse des Unternehmens werden Zugangsprotokolle überprüft und die Ergebnisse dokumentiert.
- Empfehlung: Mindestens jährlich wird die Anwendung der Richtlinien und Verfahren zu Vergabe, Nutzung und Entzugs des physischen Zugangs zu kritischen Infrastrukturen auditiert, dokumentiert und bestätigt.

[10] Der Standard kann im Webshop von EXPERTSuisse heruntergeladen werden https://www.expertsuisse.ch/webshop (kostenpflichtig).

| PR.AC-3 Verwaltung der Fernzugriffe | MS |
|---|---|
| Etablieren sie Prozesse zur Verwaltung der Fernzugriffe. | 3 |

***Worum geht es?***

PR.AC-3 hat zum Ziel, den Fernzugriff auf Systeme und Daten sicher zu verwalten, um die Integrität, Vertraulichkeit und Verfügbarkeit der Informationen zu schützen. Diese Massnahme stellt sicher, dass *Remote*-Benutzende sicher auf Ressourcen zugreifen können, während das Risiko von Sicherheitsbedrohungen minimiert wird.

***Was muss erfüllt werden?***

- Richtlinien und Verfahren für den Fernzugriff zu Systemen und Daten erstellen.
- Sichere Verfahren und Technologien zur Autorisierung des Fernzugriffs implementieren.
- Fernzugriffe überwachen und protokollieren, um unautorisierte und verdächtige Aktivitäten zu erkennen.
- Protokollierung von Fernzugriffen zur Nachverfolgbarkeit im Falle eines Sicherheitsvorfalls.
- Sensibilisierung und Schulung von Benutzenden.

***Wie kann es erfüllt werden?***

- Richtlinien und Verfahren für sichere Fernzugriffe entwickeln. Dabei sollte folgendes berücksichtigt werden:
  - Die Fernzugriffe müssen inventarisiert, beschrieben und auf ihre Kritikalität beurteilt werden.
  - Der Fernzugriff muss auf das Notwendigste beschränkt werden (*need-to-know*).
  - Zugriff nur nach Authentifizierung und Autorisierung, bspw. durch 2FA/MFA mit der vorzugsweisen Nutzung einer *Authenticator*-App für Mobiltelefone.
- Fernzugriffsverbindungen verschlüsseln und auf einer vertrauenswürdigen Fernzugriffskomponente enden, z. B. auf einem *Reverse-Proxy*, jedoch nicht direkt auf einem Zielsystem.
- Regelmässige Sicherheitsupdates für *Remote*-Zugangssoftware und Geräte installieren.
- Dienstleister vertraglich zu *Patch-Management*, Verschlüsselung, Zugriffsschutz und *Endpoint Protection* verpflichten. Das Unternehmen behält sich das Recht vor, die Einhaltung dieser Vorgaben selbst oder durch Dritte jederzeit zu überprüfen.
- Alle Fernzugriffe zentral aufzeichnen und auf verdächtige Aktivitäten kontrollieren.
- Schulungen über sichere Praktiken beim Fernzugriff, einschliesslich der Erkennung von *Phishing*-Versuchen und anderen *Social-Engineering*-Angriffen (siehe PR.AT-1).

***Wann werden die Anforderungen erfüllt?***

- Richtlinien und Verfahren sind dokumentiert, implementiert und werden angewendet.
- Mit Dienstleistern sind verbindliche, schriftliche Vorgaben über technische Anforderungen vereinbart.
- Fernzugriffe werden überwacht, protokoliert und auf verdächtige Aktivitäten überprüft.
- Empfehlung: Mindestens jährlich werden die Fernzugriffe auditiert, dokumentiert und bestätigt.
- Sensibilisierung und Schulung von Benutzenden über die sichere Verwendung von Fernzugriffen finden statt.

| PR.AC-4 Zugriffsberechtigungen und Autorisierungen | MS |
|---|---|
| Definieren sie Zugriffsberechtigungen und Autorisierungen unter Berücksichtigung der Grundsätze der geringsten Rechte und der Aufgabentrennung. | 2 |

***Worum geht es?***

Das Ziel von PR.AC-4 ist es, Sicherheitsrisiken zu minimieren, indem Benutzende nur die geringsten erforderlichen Berechtigungen für ihre Aufgaben erhalten. Durch die Prinzipien der geringsten Rechte (*least-privilege*) und der Rollentrennung (*seperation of duties*) wird das Risiko von Datenmissbrauch, unbeabsichtigten Änderungen und anderen sicherheitsrelevanten Problemen deutlich reduziert.

***Was muss erfüllt werden?***

Unternehmen können die Anforderungen dieser Unterkategorie erfüllen, indem sie:

- Richtlinien und Verfahren entwickeln, die Berechtigungen (u.a. Administratorenrechte) nach dem Prinzip der geringsten Rechte und des Bedarfs (*need-to-know*) vergeben.
- Rollentrennung einführen, sodass kritische Aufgaben von unterschiedlichen Personen ausgeführt werden. Beispiel: Bestimmung und Vergabe von Berechtigungen durch unterschiedliche Personen.

***Wie kann es erfüllt werden?***

Folgende Themen sollten berücksichtigt werden:

- Berechtigungen z. B. in einer Matrixtabelle erfassen und auf ihre Kritikalität beurteilen.
- Temporäre Berechtigungen nur in Ausnahmefällen gewähren und automatisch entziehen.
- Regelmässige Überprüfung und Anpassung der Berechtigungen.
- Übermässige Berechtigungen nach Aufgabenänderung entfernen.

Die Einführung folgender Instrumente wird empfohlen:

- Identität- und Zugriffsmanagement (IAM): Verwenden Sie Identitätsmanagementsysteme, um den Zugriff der Benutzer zentral zu erstellen, zu ändern und zu löschen.
- Rollenbasierter Zugriff (RBAC): Konfigurieren Sie Zugriffsebenen basierend auf spezifischen Rollen, anstatt jedem Benutzer individuelle Zugriffsrechte zu gewähren, um die Verwaltung der Berechtigungen zu vereinfachen.
- Multi-Faktor-Authentifizierung (MFA): Verwenden Sie die Multi-Faktor-Authentifizierung, um die Sicherheit des Zugriffs auf sensible Systeme zu erhöhen.

***Wann werden die Anforderungen erfüllt?***

- Richtlinien und Verfahren sind dokumentiert, implementiert und werden angewendet.
- Empfehlung: Mindestens jährlich werden die Benutzenden- und Zugriffsberechtigungen, auditiert, dokumentiert und bestätigt.

| PR.AC-5 Schutz der Integrität des Netzwerks | MS |
|---|---|
| Stellen sie sicher, dass die Integrität ihres Netzwerks geschützt ist. Segmentieren und Segregieren sie ihr Netzwerk logisch und physisch, wo notwendig und sinnvoll. | 2 |

***Worum geht es?***

Eine sichere und robuste Netzwerkarchitektur stellt eine der wichtigsten Voraussetzungen für einen erfolgreichen Schutz gegen Angriffe dar. Wo notwendig und sinnvoll, kann das Risiko von lateralen Bewegungen eines Angreifers im Falle eines Sicherheitsvorfalls durch eine Segmentierung der Netze verringert werden.

***Was muss erfüllt werden?***

Unternehmen müssen Massnahmen zur logischen und physischen Aufteilung des Netzwerks umsetzen, um es gegen interne und externe Bedrohungen zu schützen. Dabei wird betont, dass eine geeignete Segmentierung und Segregation des Netzwerks erforderlich sind, um dessen Integrität zu gewährleisten.

***Wie erfüllt man die Anforderungen?***

- Bestandsaufnahme und Risikobewertung:
  Eine vollständige Analyse aller Netzwerkkomponenten und -verbindungen ist notwendig. Dabei sollten potenzielle Schwachstellen oder kritische Bereiche identifiziert und priorisiert werden.
- Segmentierung des Netzwerks:
  - Logische Segmentierung (*Softwares*): VLANs (*Virtual Local Area Networks*) sollte verwendet werden, um das Netzwerk zu unterteilen und den Datenverkehr verschiedener Sicherheitsstufen trennen. Subnetting kann verwendet werden, um das Netzwerk in kleinere, leichter verwaltbare Subnetze zu unterteilen.
  - Physische Segmentierung (*Hardwares*): Dedizierte Hardware wie Router und Firewalls sorgen für eine physische Trennung zwischen den Netzwerken. Kritische Komponenten sollten in gesicherten Räumen oder Rechenzentren platziert werden, um den physischen Zugriff zu beschränken.
- Zugangskontrollen: *Network Access Control* (NAC) stellt sicher, dass nur autorisierte Geräte Zugang zum Netzwerk erhalten.
- Überwachung und Erkennung: *Intrusion Detection Systems* (IDS) und *Intrusion Prevention Systems* (IPS) ermöglichen es, ungewöhnliche Aktivitäten und potenzielle Angriffe in Echtzeit zu erkennen und zu verhindern. Kontinuierliche Überwachung und regelmässige Audits sichern die Netzwerkintegrität langfristig.

***Wann werden die Anforderungen erfüllt?***

- Richtlinien: Dokumentierte Sicherheitsrichtlinien legen fest, wie Netzwerke segmentiert und regelmässig überprüft und aktualisiert werden.
- Technische Aspekte: Je nach Unternehmensstrategie wird die am besten geeignete Netzwerkarchitektur gewählt und es werden risikobasiert die notwendigen Werkzeuge eingesetzt, um die Sicherheit des Netzwerks zu gewährleisten.

| PR.AC-6 Verifizierung der Identitäten | MS |
|---|---|
| Stellen Sie sicher, dass digitale Identitäten eindeutig verifizierten Personen oder Prozessen zugeordnet sind. | 2 |

***Worum geht es?***

PR.AC-6 bezieht sich auf die sorgfältige Zuweisung und Verifizierung digitaler Identitäten, um die Vertraulichkeit und Integrität digitaler Systeme zu gewährleisten. Digitale Identitäten umfassen alle digitalen Identifikatoren (Name, Geburtsdatum, Benutzername, E-Mail-Adresse, IP-Adressen, Benutzerverhalten, Jobtitel, ...), die mit einer Entität (natürliche oder juristische Person) oder einen Prozess verknüpft werden können. Diese Identitäten sind entscheidend für die Authentifizierung von Benutzern und den sicheren Zugriff auf internen Ressourcen.

***Was muss erfüllt werden?***

Digitale Identitäten sollten nur Personen und Prozessen zugewiesen werden, die im Voraus kontrolliert wurden und deren Identität verifiziert ist. Dies verhindert unberechtigten Zugriff, mindert das Risiko des Identitätsdiebstahls, sorgt für die Einhaltung von Vorschriften und schützt sensible Ressourcen vor externen und internen Bedrohungen.

***Wie erfüllt man die Anforderungen?***

- Vorab-Prüfung: Personen und Prozesse, die eine digitale Identität erhalten sollen, müssen überprüft werden. In manchen Fällen ist eine Sicherheitsprüfung der Person sinnvoll.
- Zero-Trust-Prinzip: Verfolgen Sie das Prinzip „Vertraue nie, überprüfe immer“ – jede Identität muss stets verifiziert werden.
- Identitätsmanagementsystem (IDM): Setzen Sie ein robustes IDM ein, das digitale Identitäten erstellt, verwaltet und überwacht. Es sollte Richtlinien für die Zuweisung und Verifizierung von Identitäten geben.
- Sicherheitsprüfung von Prozessen: Überprüfen Sie die Prozesse und Systeme auf potenzielle Sicherheitslücken, um Risiken durch unbefugte Zugriffe zu minimieren.

***Wann werden die Anforderungen erfüllt?***

- Überprüfung von Personen und Prozessen: Stellen Sie sicher, dass Personen und Prozesse Ihre Sicherheitsanforderungen erfüllen und mit den Behauptungen übereinstimmen.
- Zuordnung digitaler Identitäten: Stellen Sie sicher, dass die Zuweisung von digitalen Identitäten sorgfältig und richtig erfolgt.

Empfehlung: Kontinuierliche Überwachung und regelmässige Audits stellen sicher, dass alle Identitäten korrekt zugeordnet und aktiv sind. Zugriffsrechte sollten regelmässig überprüft werden, um sicherzustellen, dass sie den aktuellen Aufgaben und Verantwortlichkeiten entsprechen.

Notfallpläne sollten Massnahmen zur sofortigen Sperrung kompromittierter Identitäten und zur Wiederherstellung der Sicherheit umfassen.

| PR.AC-7 Authentifizierung | MS |
|---|---|
| Die Authentifizierung von Benutzern, Geräten und anderen Vermögenswerten (z. B. Ein-Faktor- oder Mehr-Faktor-Authentifizierung) erfolgt entsprechend dem Risiko der Transaktion (z. B. Sicherheits- und Datenschutzrisiken für Einzelpersonen und andere Unternehmensrisiken). | 2 |

***Worum geht es?***

Die Authentifizierung von Benutzern, Geräten und anderen Vermögenswerten ist entscheidend für die Sicherheit eines Unternehmens. Dieser Prozess ermöglicht es einem IT-System, sich der Identität des Antragstellers zu vergewissern.

***Was muss erfüllt werden?***

Die Wahl der Authentifizierungsmethode, ob Ein-Faktor oder Multi-Faktor-Authentifizierung (MFA), soll auf einer sorgfältigen Risikobewertung basieren. Ein höheres Risiko erfordert stärkere Authentifizierungsmechanismen.

***Wie erfüllt man die Anforderungen?***

Die Authentifizierungsstufe sollte risikoabhängig festgelegt werden. Für weniger kritische Vorgänge reicht eine einfache Authentifizierungsmethode (insb. Passwörter) aus, während bei sensiblen Transaktionen 2FA/MFA erforderlich ist. Dabei werden zwei oder mehr unabhängige Anmeldeinformationen wie Passwörter, biometrische Daten oder Sicherheitstoken kombiniert. Dies stellt sicher, dass sowohl die Sicherheit als auch der Datenschutz gewahrt bleiben.

Neben Benutzern sollten auch Geräte, die auf das Netzwerk zugreifen, authentifiziert werden. Dies unterstützt das *Zero-Trust*-Prinzip und schützt das System vor unbefugtem Zugriff. Adaptive Mechanismen, die Faktoren wie IP-Adresse oder Geolokalisierung einbeziehen, erhöhen die Sicherheit zusätzlich.

***Wann werden die Anforderungen erfüllt?***

Um die Anforderungen zu erfüllen, müssen folgende Massnahmen umgesetzt werden:

- Risikobewertung für jede Transaktion;
- Anpassung der Authentifizierungsstufe an das Risiko.

Auf diese Weise kann gewährleistet werden, dass die Authentifizierung den spezifischen Sicherheitsanforderungen entspricht und ein hohes Mass an Schutz für alle Unternehmensressourcen bietet.

Empfehlung: Eine kontinuierliche Überprüfung und Anpassung der Authentifizierungsverfahren sollen implementiert werden, um aktuellen Bedrohungen und technologischen Entwicklungen Rechnung zu tragen.

## Sensibilisierung und Ausbildung (PR.AT)

| PR.AT-1 Cybersicherheit Schulung und Sensibilisierung | MS |
|---|---|
| Stellen sie sicher, dass alle Mitarbeitenden bezüglich Cybersicherheit informiert und geschult sind. | 3 |

***Worum geht es?***

Technologische Sicherheitsmassnahmen reichen nicht mehr aus, um raffinierte Cyberangriffe abzuwehren. Daher ist es notwendig, alle Mitarbeitenden, einschliesslich externer Partner, regelmässig in der Informationssicherheit zu schulen, um das Sicherheitsbewusstsein zu stärken und die gesamte Sicherheitslage des Unternehmens zu verbessern.

***Was muss erfüllt werden?***

- Cybersicherheitsrisiken managen: Regelmässige Bedrohungsanalysen und Risikobewertungen.
- Dokumentierte Richtlinien: Sicherheitspraktiken müssen dokumentiert und standardisiert sein.
- Formalisierte Schulungsprozesse: Schulungsprogramme müssen regelmässig überprüft und aktualisiert werden.

***Wie kann es erfüllt werden?***

- Entwicklung eines Schulungsprogramms: Erstellen Sie ein detailliertes Schulungsprogramm, das alle relevanten Cybersicherheitsrichtlinien und -verfahren abdeckt.
- Regelmässige Schulungen: Alle Mitarbeitenden, inklusive neuer Mitarbeitender und externer Partner, müssen regelmässig geschult werden.
- Bewusstseinskampagnen: Führen Sie laufende Kampagnen zur Sensibilisierung durch.[11]
- Feedback und Verbesserung: Nutzen Sie das Feedback der Teilnehmenden zur Verbesserung des Schulungsprogramms. Prüfen Sie das Programm regelmässig auf Aktualität und Nutzen.

***Wann gilt es als erfüllt?***

- Dokumentation ist vorhanden.
- Regelmässige Schulungen werden durchgeführt und nachverfolgt.
- Bewusstseinskampagnen sind etabliert.
- Feedback wird zur Verbesserung genutzt.

***Was wird zur Umsetzung benötigt?***

Um die Schulungen erfolgreich umzusetzen, sollten Unternehmen mit *Awareness*-Trainings beginnen, die auf die Zielgruppen und relevanten Themen abgestimmt sind. Der Fortschritt wird durch regelmässiges Feedback und Schulungsnachweise dokumentiert und verbessert.

[11] Auf der Webseite des BACS finden Sie Informationen zu den letzten Sensibilisierungskampagnen: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sensibilisierung.html.

| PR.AT-2 Anwender mit höheren Berechtigungsstufen | MS |
|---|---|
| Stellen sie sicher, dass Anwender mit höheren Berechtigungsstufen sich ihrer Rolle und Verantwortung besonders bewusst sind. | 3 |

***Worum geht es?***

Diese Unterkategorie stellt sicher, dass privilegierte Benutzer, wie Administratoren und Benutzer mit erweiterten Zugriffsrechten, ihre spezifischen Sicherheitsverantwortungen kennen und verstehen. Da diese Benutzer Zugriff auf kritische Systeme und Daten haben, sind sie oft Ziel von Cyberangriffen. Regelmässige, spezialisierte Schulungen helfen ihnen, potenzielle Risiken zu erkennen, auf Sicherheitsvorfälle zu reagieren und das Gesamtrisiko für das Unternehmen zu senken.

***Was muss erfüllt werden?***

- Spezielle Rollen und Verantwortlichkeiten definieren und dokumentieren.
- Sicherheitspraktiken für privilegierte Benutzer festlegen, dokumentieren und regelmässig aktualisieren.
- Formalisierte Schulungsprogramme entwickeln, anwenden und aktualisieren. Sie sollen sicherstellen, dass privilegierte regelmässig geschult werden.

***Wie kann es erfüllt werden?***

- Rollen und Verantwortlichkeiten klar definieren: Rollenbeschreibung mit klaren Cybersicherheitsanforderungen und -erwartungen erstellen, einschliesslich der Zuweisung von Zugriffsrechten.
- Spezialisierte Schulungsprogramme entwickeln: Inhalte, die tiefere Kenntnisse (im Vergleich zu PR.AT-1) zur Bedrohungserkennung und Reaktion auf Sicherheitsvorfälle vermitteln.
- Regelmässige Schulungen durchführen: Erstellen Sie einen jährlichen Schulungskalender (siehe PR.AT-1) und stellen Sie so regelmässige Schulungen und Wiederholungen sicher.
- Bewusstseinskampagnen durchführen: Spezielle Kampagnen für privilegierte Benutzer gestalten.
- Feedback einholen und Programme verbessern: Holen Sie regelmässig Feedback von den Schulungsteilnehmenden ein und nutzen sie es zur kontinuierlichen Verbesserung ihrer Programme.

***Wann gilt es als erfüllt?***

- Dokumentation ist vorhanden und jederzeit zugänglich.
- Regelmässige Schulungen finden für privilegierte Benutzer nach definierten Regeln statt.
- Standardisierte Prozesse existieren und werden regelmässig aktualisiert.
- Bewusstseinskampagnen sind etabliert und finden laufend statt.
- Feedbackprozesse zur kontinuierlichen Verbesserung sind implementiert.

| PR.AT-4 Rolle und Verantwortung der Führungskräfte | MS |
|---|---|
| Stellen sie sicher, dass sich alle Führungskräfte ihrer besonderen Rolle und Verantwortung bewusst sind. | 3 |

***Worum geht es?***

PR.AT-4 stellt sicher, dass alle Schlüsselpersonen über ihre Rollen und Verantwortlichkeiten im Bereich Cybersicherheit informiert sind. Diese Massnahme ermöglicht eine bessere Umsetzung von Cybersicherheitsmassnahmen, indem die Aufgaben der einzelnen Personen klar definiert werden. Sie soll auch eine Kultur der Cybersicherheit schaffen, die von den oberen Ebenen und Führungskräften getragen wird.

***Was muss erfüllt werden?***

- Rollenverständnis: Führungskräfte müssen ihre Cybersicherheitsrollen kennen und sich ihrer Verantwortung bewusst sein.
- Sensibilisierung: Cybersicherheit geht alle an und muss von der Geschäftsleitung und dem Verwaltungsrat getragen werden. Diese müssen unbedingt für die Problematik sensibilisiert sein. Nur mit ihrer Unterstützung können proaktive Massnahmen zur Risikominderung ergriffen werden.

***Wie kann es erfüllt werden?***

- Dokumentation: Festlegung und Koordination der Rollen und Verantwortlichkeiten gemäss ID.AM-6 und ID.GV-2.
- Kommunikation: Die Rollen und Verantwortungen müssen klar und bei jeder Änderung kommuniziert werden.
- Sensibilisierung und Schulung: Führungskräfte werden für Cyberbedrohungen und Cyberrisiken sensibilisiert und entsprechend ihrer Rolle geschult (gesetzliche Verantwortung, Vorschriften, ...).

***Wann gilt es als erfüllt?***

- Dokumentation: Cybersicherheitsverantwortlichkeiten sind im Organigramm verankert.
- Kommunikation: Die Rollen und Verantwortlichkeiten der Führungskräfte sind klar kommuniziert.
- Sensibilisierung und Schulung: Führungskräfte kennen die Herausforderungen der Cybersicherheit und haben eine Cybersicherheitsschulung absolviert.
- Überprüfung: Cybersicherheitsrollen werden regelmässig überprüft und falls notwendig angepasst.

## Datensicherheit (PR.DS)

| PR.DS-2 Datenübertragungssicherheit | MS |
|---|---|
| Stellen sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind. | 2 |

***Worum geht es?***

Der Schutz von Informationen während der Übertragung ist ein kritischer Bestandteil der Sicherheitsstrategie eines Unternehmens. Diese Anforderung zielt darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen während der Übertragung zu gewährleisten, um Sicherheitsverletzungen zu verhindern.

***Was muss erfüllt werden?***

Um diese Anforderung zu erfüllen, ist es unerlässlich, starke Verschlüsselungsmethoden einzusetzen. Verschlüsselung stellt sicher, dass die Informationen während der Übertragung nur von autorisierten Empfängern gelesen werden können. Dazu sollten aktuelle und sichere Verschlüsselungsprotokolle wie TLS 1.3 (*Transport Layer Security*) verwendet werden, um die Informationen vor Abhörversuchen und Manipulation zu schützen.

***Wie erfüllt man die Anforderungen?***

- Verschlüsselung: Die Verschlüsselung zwischen Endpunkten schützt die Vertraulichkeit und Integrität der Informationen. Verwenden Sie Protokolle wie TLS 1.3.
- *Virtual Private Networks* (VPNs): VPNs können dazu beitragen, die Datenübertragung über öffentliche Netzwerke zu sichern. Diese Technologie schafft eine sichere, verschlüsselte Verbindung (IPsec) zwischen Endpunkten und schützt die Informationen vor unbefugtem Zugriff.
- Authentifizierung: Bevor Informationen übertragen werden, müssen die Identitäten der beteiligten Parteien gemäss PR.AC-7 eindeutig verifiziert werden.
- Datenintegrität: Verwenden Sie Hashfunktionen und digitale Signaturen, um die Integrität der Informationen während der Übertragung zu gewährleisten.
- Physische Sicherheit: Die Infrastruktur muss gegen physische Angriffe gemäss PR.AC-2 geschützt werden. Die Verfügbarkeit kann mithilfe der Redundanz von Diensten und Infrastruktur gewährleistet werden.
- Netzwerkschutz: Stellen Sie sicher, dass die Netzwerke gemäss PR.AC-5 und PR.PT-4 geschützt sind.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen sind erfüllt, wenn Mittel zum Schutz der Informationen während der Übertragung eingesetzt werden.

Zusätzlich sind die Überwachung und die Protokollierung der Datenübertragungen essenziell, um verdächtige Aktivitäten oder Anomalien frühzeitig zu erkennen und zeitnah zu beheben. Protokollierungen dienen zudem der lückenlosen Nachverfolgung aller Übertragungen und sind ein wichtiges Werkzeug für Audits und die Verbesserung der Sicherheitsmassnahmen.

Es ist wichtig, sicherzustellen, dass der Übertragungsdienstleister stets aktuelle und empfohlene Protokolle einsetzt.

## Informationsschutzrichtlinien (PR.IP)

| PR.IP-1 Erstellung einer Standardkonfiguration | MS |
|---|---|
| Erstellen sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur, sowie für die industriellen Kontrollsysteme. Stellen sie sicher, dass diese Standardkonfiguration typische Security-Prinzipien (z.B. N-1 Redundanz, Minimalkonfiguration, etc.) einhält. | 2 |

***Worum geht es?***

Die Erstellung einer Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur, sowie für industrielle Kontrollsysteme, ist ein grundlegender Schritt zur Sicherstellung der IT-Sicherheit und Effizienz. Dieser Punkt fordert, dass diese Standardkonfiguration typische Sicherheitsprinzipien einhält, wie N-1 Redundanz und Minimalkonfiguration.

***Was muss erfüllt werden?***

Eine Standardkonfiguration stellt sicher, dass alle Systeme und Geräte innerhalb der Infrastruktur einheitlich und sicher eingerichtet sind. Dies reduziert nicht nur die Angriffsfläche, sondern vereinfacht auch das Management und die Wartung der Systeme.

Um eine effektive Standardkonfiguration zu erstellen, müssen zunächst alle Komponenten der Informations- und Kommunikationsinfrastruktur sowie der industriellen Kontrollsysteme identifiziert und dokumentiert werden.

***Wie erfüllt man die Anforderungen?***

- Ziele definieren: Leistung, Sicherheit, Zuverlässigkeit und Skalierbarkeit sollten berücksichtigt werden.
- N-1 Redundanz: Dieses Prinzip stellt sicher, dass immer eine Reservekomponente vorhanden ist, die im Falle eines Ausfalls einspringen kann. Dies erhöht die Verfügbarkeit und Zuverlässigkeit der Systeme und minimiert das Risiko von Ausfallzeiten.
- Minimalkonfiguration: Systeme und Geräte werden nur mit den absolut notwendigen Funktionen und Diensten konfiguriert. Dadurch wird die Angriffsfläche reduziert und potenzielle Schwachstellen werden minimiert. Unnötige Software und Dienste sind zu entfernen und der Zugriff auf notwendige Funktionen ist einzuschränken.
- Netzwerkkonfiguration: IP-Adressierung, DNS-Konfiguration, Routing, ... gehören zu den grundlegenden Netzwerkparameter und -einstellungen.
- Sicherheitseinstellungen: Integrieren Sie Sicherheitsmassnahmen direkt in Ihre Standardkonfiguration.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen sind erfüllt, wenn die Systeme identifiziert sind, die Standardkonfiguration für jedes System festgelegt wurde und die oben genannten grundlegenden Sicherheitselemente enthalten sind.

Empfehlung: Um die Einhaltung der Prinzipien sicherzustellen, müssen regelmässige Überprüfungen und Aktualisierungen der Standardkonfiguration durchgeführt werden. Sicherheitsupdates und Patches sollten zeitnah eingespielt werden, und es sollten Mechanismen zur Überwachung und Durchsetzung der Standardkonfiguration eingerichtet werden. Dies kann durch automatisierte Tools und regelmässige Audits erreicht werden.

| PR.IP-4 Backups | MS |
|---|---|
| Stellen sie sicher, dass Sicherungen (*Backups*) ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der *Backups* testen). | 3 |

***Worum geht es?***

Die regelmässige Durchführung, Verwaltung und Prüfung von *Backups* ist ein entscheidender Aspekt der IT-Sicherheit und Geschäftskontinuität. *Backups* sind ein unverzichtbares Element der Cybersicherheit, um die Verfügbarkeit der Informationen und der Systeme zu schützen, die Kontinuität des Geschäftsbetriebs zu gewährleisten und sich gegen eine Vielzahl von Bedrohungen (z. B. *Ransomware*) abzusichern, indem sie die Wiederherstellung erleichtern.

***Was muss erfüllt werden?***

Es müssen regelmässig *Backups* von geschäftskritischen Informationen und Systemen erstellt, verwaltet und getestet werden. Dies stellt sicher, dass Datenverluste minimiert werden und schnelle sowie vollständige Wiederherstellungen möglich sind.

***Wie erfüllt man die Anforderungen?***

- Informationen und Systeme: Es geht darum, wichtige und kritische Informationen, Prozesse und Systeme zu erkennen und zu priorisieren. Die Wirksamkeit von *Backups* ist nur durch ihren überlegten Einsatz gewährleistet.
- Dokumentation: Die Umsetzung und die Verwaltung (Zuständigkeiten) von *Backups* muss dokumentiert werden.
- Durchführung von *Backups* unter Berücksichtigung folgender Aspekte:
  - *Backup*-Typ: vollständig (vollständige Sicherung), differenziell (nur Daten, die sich seit der letzten vollständigen Sicherung geändert haben), inkrementell (nur Daten, die sich seit der letzten vollständigen oder differenziellen Sicherung geändert haben, jedes neue *Backup* wird als inkrementelles Volumen gespeichert).
  - Medium: Kriterien wie Kosten, Zuverlässigkeit, Verfügbarkeit, Geschwindigkeit und Benutzbarkeit müssen bei der Auswahl eines Mediums (Festplatte, Flash-Laufwerke, Cloud, Hybrid, ...) berücksichtigt werden. Die *Backups* müssen an sicheren, redundanten Orten gespeichert werden.
  - Verschlüsselung: Sensible Daten müssen verschlüsselt werden. Das Masterpasswort darf nicht am selben Ort gespeichert werden.
  - 3-2-1: Es müssen drei verschiedene Kopien, auf zwei verschiedenen Speichertypen und eine separate Kopie (d. h. nicht am selben physischen Ort) aufbewahrt werden.
  - Zeitliche Dimension: *Backups* sollten gemäss einem definierten Zeitplan erstellt werden, abhängig von der Kritikalität der Daten und den geschäftlichen Anforderungen.
  - Dokumentation: Die *Backups* müssen ordnungsgemäss katalogisiert und leicht zugänglich sein.
- Tests: Die Wiederherstellung von *Backups* muss regelmässig getestet werden.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen sind erfüllt, wenn *Backups* regelmässig erstellt, verwaltet und durch Tests auf ihre Rückspielbarkeit überprüft werden. Diese Tests sollten in verschiedenen Szenarien durchgeführt werden, um sicherzustellen, dass die Wiederherstellung unter allen Umständen funktioniert.

| PR.IP-5 Einhaltung von regulatorischen Vorgaben und Richtlinien | MS |
|---|---|
| Stellen sie sicher, dass sie alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich der physischen Betriebsmittel erfüllen. | 3 |

***Worum geht es?***

Die gesetzlichen und regulatorischen Anforderungen an physischen Betriebsmitteln sind in der Regel dazu gedacht, ein Mindestmass an Sicherheit zu gewährleisten. Die physische Sicherheit spielt auch in der Cybersicherheit eine wichtige Rolle, zum Beispiel um die Beschädigung von Servern, die für *Backups* verwendet werden, zu vermeiden. Die Massnahme PR.IP-5 stellt sicher, dass diese Anforderungen eingehalten werden, um so Sanktionen oder Geldstrafen zu vermeiden und gleichzeitig ein grundlegendes Sicherheitsniveau zu gewährleisten.

***Was muss erfüllt werden?***

Ein Prozess zur Einhaltung von Vorschriften muss definiert, verabschiedet und umgesetzt werden. Dieser muss dazu dienen, sich über die geltenden Normen, Vorschriften und Gesetze zu informieren und die Anforderungen, denen das Unternehmen unterliegt, umzusetzen. Um über die Anforderungen hinauszugehen, wäre eine Rechts- und Regulierungsüberwachung erforderlich.

***Wie kann es erfüllt werden?***

Um die bestehenden Richtlinien und Vorschriften einzuhalten, muss jedes Unternehmen ein Inventar der geltenden Anforderungen durchführen. Diese umfassen unter anderem:

- Branchenspezifische Normen und Vorschriften
- Bundesgesetze
- Kantonale Gesetze

Diese Liste ist nicht abschliessend. Jedes Unternehmen ist dafür verantwortlich, die notwendigen Massnahmen zu ergreifen, um die Einhaltung der Vorschriften zu gewährleisten.

Technische Massnahmen zur Erhöhung der Resilienz physischer Systeme sind zum Beispiel:

- Verhinderung von unbefugtem Zugriff
- Schutz kritischer Mittel/Geräte
- Verhinderung von Datendiebstahl (physisch gespeicherte Daten)
- Schutz vor internen Angriffen
- Schutz vor Naturkatastrophen oder physischen Vorfällen

***Wann gilt es als erfüllt?***

Die Massnahmen PR.IP-5 gilt als erreicht, wenn alle bestehenden (regulatorischen) Anforderungen hinsichtlich der physischen Betriebsmittel vollständig erfüllt sind.

| PR.IP-9 Reaktion auf eingetretene Cybervorfälle | MS |
|---|---|
| Etablieren sie Prozesse zur Reaktion auf eingetretene Cybervorfälle. (*Incident Response Planning, Business Continuity Management, Incident Recovery, Disaster Recovery*). | 2 |

***Worum geht es?***

PR.IP-9 beschreibt die Entwicklung und Implementierung von Plänen zur Reaktion auf Sicherheitsvorfälle, die den gesamten Lebenszyklus eines Vorfalls abdecken – von der Identifizierung bis zur Wiederherstellung. Dazu zählen insbesondere die Bereiche *Incident Response, Business Continuity und Disaster Recovery*. Mit ihnen wird sichergestellt, dass ein Unternehmen auf Vorfälle effektiv reagiert, den Betrieb aufrechterhält und diesen nach einem Sicherheitsvorfall schnell wiederherzustellen.

***Was muss erfüllt werden?***

- *Incident Response*: Unternehmen müssen dokumentierte Richtlinien und Verfahren zur Vorfallsreaktion haben, Überwachungs- und Erkennungssysteme implementieren sowie Mitarbeitende regelmässig schulen. Kommunikationspläne und Nachbereitungsprozesse zur kontinuierlichen Verbesserung sind essenziell.
- *Business Continuity*: Es müssen Risikobewertungen durchgeführt und Kontinuitätspläne entwickelt werden, um kritische Geschäftsprozesse trotz eines Vorfalls aufrechtzuerhalten. Alle notwendigen Ressourcen müssen verfügbar sein, und regelmässige Schulungen und Übungen sind durchzuführen.
- *Disaster Recovery*: Unternehmen benötigen Notfallpläne zur Wiederherstellung von IT-Systemen und Daten. Regelmässige *Backups* sowie Tests und Übungen zur Überprüfung der Pläne und der Mitarbeitervorbereitung sind unerlässlich.

***Wie kann es erfüllt werden?***

- *Incident Response*: Detaillierte Richtlinien und Verfahren erstellen, Technologien zur Vorfallserkennung implementieren, regelmässige Schulungen und Simulationen organisieren sowie effektive Kommunikationsstrategien entwickeln.
- *Business Continuity*: Bedrohungsanalysen durchführen, Kontinuitätspläne entwickeln und sicherstellen, dass alle notwendigen Ressourcen verfügbar sind. Schulungen und Tests zur Planüberprüfung durchführen.
- *Disaster Recovery*: Notfallpläne erstellen, regelmässige Datensicherungen durchführen und klare Wiederherstellungsverfahren festlegen. Regelmässige Tests durchführen, um die Pläne zu verifizieren.

***Wann gilt es als erfüllt?***

- *Incident Response* Pläne: Dokumentiert, getestete Überwachungssysteme implementiert und Mitarbeitende geschult. Effektive Kommunikationsstrategien und Nachbereitungen sind etabliert.
- *Business Continuity*-Pläne: Dokumentiert, getestet und alle notwendigen Ressourcen sichergestellt. Mitarbeitende werden regelmässig geschult.
- *Disaster Recovery*-Pläne und *Backups*: Dokumentiert, erstellt und getestet. Wiederherstellungsverfahren sind erfolgreich.

## Unterhalt (PR.MA)

| PR.MA-2 Fernzugriffe | MS |
|---|---|
| Stellen sie sicher, dass Unterhaltsarbeiten an ihren Systemen, die über Fernzugriffe erfolgen, aufgezeichnet und dokumentiert werden. Stellen sie sicher, dass kein unautorisierter Zugriff möglich ist. | 2 |

***Worum geht es?***

Fernzugriffe auf Systeme stellen ein erhebliches Sicherheitsrisiko dar, da es von Angreifern ausgenutzt werden kann, um auf kritische Systeme zuzugreifen, ohne physisch anwesend zu sein. Dies ermöglicht Cyberangriffe wie den Diebstahl von Daten oder die Übernahme der Kontrolle über sensible Infrastrukturen. Ohne angemessene Sicherheitsmassnahmen sind die Systeme erheblichen Bedrohungen ausgesetzt.

***Was muss erfüllt werden?***

Alle ferngesteuerten Wartungsarbeiten an IKT-Systemen müssen aufgezeichnet und dokumentiert werden (Protokollierung). Zudem sollen Massnahmen eingeführt werden, die einen unberechtigten Zugriff verhindern.

***Wie kann es erfüllt werden?***

Die folgenden Massnahmen können ergriffen werden, um die Risiken im Zusammenhang mit unbefugtem Zugriff zu minimieren:

- Sichere Verbindungen: Einsatz von VPNs mit starker Verschlüsselung.
- Mehrfaktor-Authentifizierung (MFA): Sicherstellung der Identitätsprüfung.
- Zugangskontrolle: Rechte auf das Minimum beschränken und Einmalpasswörter verwenden.
- Überwachung und Protokollierung: Aktivität protokollieren und verdächtige Aktionen überwachen (*Firewalls*, IPS, IDS, SIEM usw.).
- Warnungen und Benachrichtigungen: Administratoren über ungewöhnliche Verbindungen oder unautorisierte Zugriffsversuche benachrichtigen.
- Anbieter-Management: Sicherstellen, dass Drittanbieter die Sicherheitsrichtlinien einhalten.
- Regelmässige Updates: Systeme und Software regelmässig aktualisieren.
- Schulung des Personals: Teams für Cybersicherheitspraktiken sensibilisieren.
- Klare Richtlinien: Definierte und kommunizierte Verfahren für den Fernzugriff.
- Endgerätesicherheit: Schutz der Geräte durch Antivirensoftware und *Firewalls*.
- Netzwerksegmentierung: Kritische Systeme isolieren.
- Datenverschlüsselung: Verschlüsseln sensibler Daten, um unbefugten Zugriff zu verhindern.
- Vorfallreaktionsplan: Erstellen Sie einen Aktionsplan, um im Falle eines sicherheitsrelevanten Vorfalls bei der Fernwartung schnell und effektiv zu reagieren.

***Wann gilt es als erfüllt?***

Das Unternehmen hat die Verfahren für die Wartung und den Fernzugriff vollständig definiert und angenommen. Es verfügt über eine klare Strategie, die darauf abzielt, unautorisierte Zugriffe zu verhindern. Die technischen Massnahmen und Werkzeuge zur Aufzeichnung und Protokollierung der Aktivitäten auf den Systemen sollten zumindest teilweise implementiert sein.

## Einsatz von Schutztechnologie (PR.PT)

| PR.PT-2 Schutz von Wechseldatenträger | MS |
|---|---|
| Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden. | 3 |

***Worum geht es?***

Wechseldatenträger sind ein wesentlicher Aspekt der Sicherheitsstrategie eines Unternehmens. Dies erfordert, dass Wechseldatenträger und ihre Informationen darauf geschützt werden.

***Was muss erfüllt werden?***

Wechseldatenträger wie USB-Sticks, externe Festplatten oder optische Medien müssen physisch und digital geschützt werden, um sicherzustellen, dass sie nicht unautorisiert genutzt oder manipuliert werden können. Dies kann durch die Verwendung von Verschlüsselungstechnologien erfolgen, um sicherzustellen, dass die auf den Datenträgern gespeicherten Informationen nur von autorisierten Personen gelesen werden können.

***Wie erfüllt man die Anforderungen?***

Um die Anforderungen zu erfüllen sind folgende Massnahmen notwendig:

- Richtlinien: Es sind klare Richtlinien und Verfahren für den Einsatz von Wechseldatenträgern festzulegen (Einsatz, Nutzung, Rückgabe, Entsorgung, ...) und sicherzustellen, dass alle Mitarbeiter darüber sensibilisiert und informiert sind.
- Verschlüsselung: Um den unbefugten Zugriff zu verhindern sollten die Daten verschlüsselt sein.
- Authentifizierung: Schützen Sie die Wechseldatenträger mit Passwörtern (oder MFA).
- *AutoRun/AutoPlay*: Verhindern Sie das automatische Ausführen von Dateien.
- *Data Loss Prevention* (DLP): Überwachen und kontrollieren Sie den Transfer sensibler Daten auf Wechseldatenträger.
- Physische Sicherheit: Bewahren Sie Wechseldatenträger an sicheren Orten auf.
- *Anti-Malware-Tools*: Scannen Sie Geräte regelmässig auf Malware.
- Gerätemanagement: Kontrollieren Sie den Zugriff auf USB-Ports und erlauben Sie nur autorisierte Geräte.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen werden erfüllt, wenn:

- Richtlinien gemäss ID.GV-1 festgelegt und durchgesetzt sind.
- Der Einsatz unter Einhaltung der Richtlinien erfolgt.
- Wechseldatenträger werden entsprechend ihrer Verwendung und den Risiken, denen sie ausgesetzt sind, geschützt.

Empfehlung: Die Überwachung und Kontrolle der Verwendung von Wechseldatenträgern ist unerlässlich, um sicherzustellen, dass die Richtlinien eingehalten werden und potenzielle Sicherheitsvorfälle erkannt werden können. Dies kann durch Technologien zur Überwachung von Datenzugriffen und durch Audits der Datenträgernutzung erreicht werden.

| PR.PT-4 Schutz der Kommunikations- und Steuernetzwerke | MS |
|---|---|
| Stellen sie sicher, dass ihre Kommunikations- und Steuernetzwerke geschützt sind. | 3 |

***Worum geht es?***

Für den Betreiber ist es von entscheidender Bedeutung, sein Netzwerk zu beherrschen. Dies umfasst die IT-Aspekte der Steuerung und Kontrolle sowie die Telekommunikation, die diese Netzwerke unterstützt.

***Was muss erfüllt werden?***

Die gesamte Netzwerktopologie sollte bekannt sein (ID.AM-3). Massnahmen zum Schutz der Kommunikations- und Steuernetzwerke müssen umgesetzt sein.

***Wie erfüllt man die Anforderungen?***

Die folgenden grundlegenden Prinzipien sind notwendig, um die Kontrolle über das Netzwerk zu behalten:

- Segmentierung: Siehe PR.AC-5.
- Kommunikationstechnik: Nicht sichere Services, wie Telnet, Remote Shell oder rlogin, müssen durch sichere Alternativen wie SSH ersetzt werden.
- *Firewalls*:
  - Überwachung und Kontrolle der Kommunikation an Aussengrenze und an wichtigen internen Schnittstellen.
  - Alle Regeln, die IT-Kommunikation durch die Firewall zulassen, müssen genehmigt werden.
  - Nicht zugelassene oder anfällige Dienste sind zu deaktivieren oder zu blockieren.
  - *Firewall*-Regeln müssen regelmässig aktualisiert werden, z. B. durch das Entfernen ungenutzter Dienste.
- Passwörtern: Standard-Passwörtern müssen geändert und generische Konten durch individuelle Benutzerkonten ersetzt werden.
- Die Verwaltungsschnittstelle muss durch starke Authentifizierung oder starke Passwörter gesichert und Benutzer nach mehreren fehlgeschlagenen Zugriffsversuchen gesperrt werden.
- Fernzugriff:
  - Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jede Art des zulässigen Fernzugriffs festlegen und dokumentieren.
  - Autorisierung jeder Art von Fernzugriff auf das System, bevor solche Verbindungen zugelassen werden.
  - Einsatz automatisierter Mechanismen zur Überwachung und Kontrolle von Fernzugriffsmethoden.

***Wann werden die Anforderungen erfüllt?***

Die Kommunikations- und Steuernetzwerke sind geschützt. Um die Sicherheitsmassnahmen zu prüfen kann ein Penetrationstest durchgeführt werden. Ausserdem sollte es nicht möglich sein, das Netzwerkmanagementsystem von einer Station aus zu steuern oder eine Station von einer anderen Station aus fernzusteuern.

Wenn der Fernzugriff nicht ausreichend gesichert werden kann, empfiehlt es sich, auf diesen Dienst zu verzichten.

## Erkennen (DE)

Die Kategorie „Erkennen“ definiert die geeigneten Massnahmen zur Identifizierung des Auftretens eines Cybersicherheitsereignisses und ermöglicht die rechtzeitige Erkennung von Anomalien.

***Überwachung (DE.CM):***

Das IKT-System inkl. aller Betriebsmittel wird in regelmässigen Intervallen überwacht, um einerseits Cybersicherheitsvorfälle zu entdecken und anderseits die Effektivität der Gegenmassnahmen sicherstellen zu können.

***Detektionsprozesse (DE.DP):***

Prozesse und Handlungsanweisungen zur Detektion von Cybersicherheitsvorfällen werden gepflegt, getestet und unterhalten, so dass Cybersicherheitsvorfälle erkannt werden.

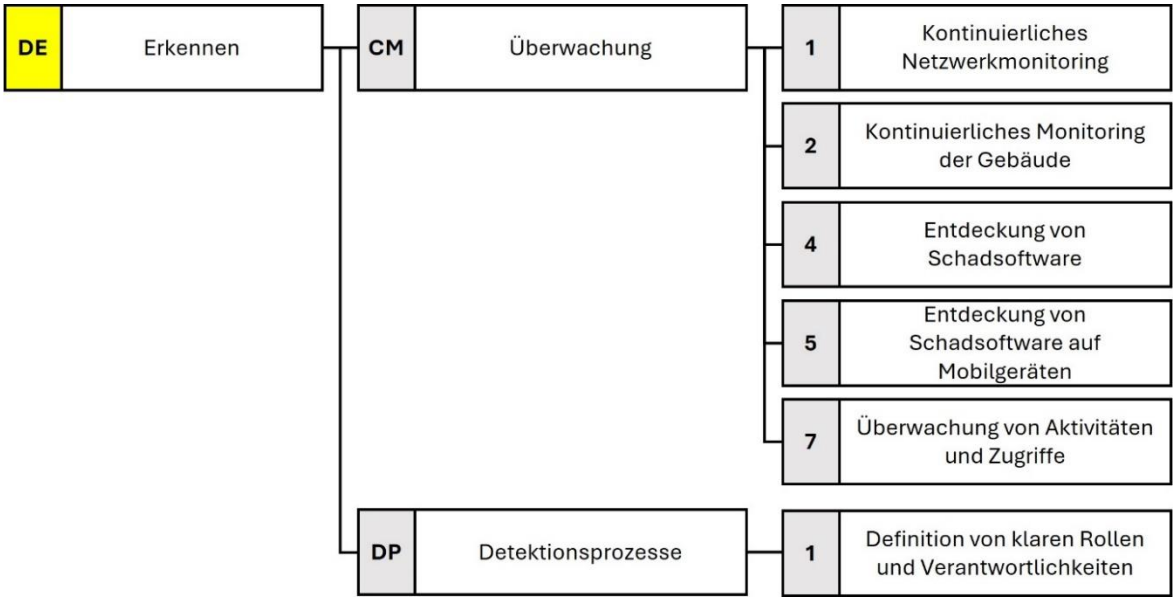



*Abbildung 9: Vorgeschriebene DE-Unterkategorien für Schutzniveau C*

## Überwachung (DE.CM)

| DE.CM-1 Kontinuierliches Netzwerkmonitoring | MS |
|---|---|
| Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potenzielle Cybersicherheitsvorfälle zu entdecken. | 2 |

***Worum geht es?***

Die Implementierung eines kontinuierlichen Netzwerkmonitorings ist entscheidend für die Früherkennung potenzieller Cybersicherheitsvorfälle.

***Was muss erfüllt werden?***

Mögliche Cyberangriffe, Anomalitäten oder verdächtige Aktivitäten sollen frühzeitig erkannt werden, um das Schadensausmass zu reduzieren. Es sollen entsprechende Verfahren erstellt und regelmässig getestet werden. Bei Wartungsarbeiten werden häufig Alarme ausgelöst, die mit denen eines Cyberangriffs identisch sind. Um eine schnelle Analyse durchführen zu können, müssen die Wartungspläne definiert und den Cyberspezialisten bekannt sein.

***Wie erfüllt man die Anforderungen?***

Das kontinuierliche Netzwerkmonitoring erfordert die permanente Überwachung von Netzwerkverkehr, Systemaktivitäten und Sicherheitsereignissen. Durch den Einsatz fortgeschrittener Technologien wie IDS, IPS und SIEM können Anomalien und verdächtige Aktivitäten erkannt werden.

Die Reaktionsfähigkeit auf erkannte Sicherheitsvorfälle ist ein zentraler Bestandteil des Monitorings. Unternehmen müssen über gut definierte *Incident Response* Pläne verfügen, die klare Verfahren zur Untersuchung, Behebung und Wiederherstellung nach einem Vorfall enthalten.

***Wann werden die Anforderungen erfüllt?***

Alle Beteiligten sollten die Bedeutung des Netzwerkmonitorings verstehen und wissen, wie sie auf erkannte Bedrohungen reagieren sollen. Regelmässige Schulungen halten das Wissen über aktuelle Bedrohungen und bewährte Praktiken auf dem neuesten Stand.

Empfehlung: Durch kontinuierliche Evaluierung und Verbesserung der Überwachungsstrategien können Unternehmen ihre Netzwerksicherheit ständig optimieren und auf neue Bedrohungen reagieren. Ein gut etabliertes Netzwerkmonitoring-System trägt dazu bei, die Integrität, Vertraulichkeit und Verfügbarkeit der IT-Infrastruktur zu schützen und die Auswirkungen von Sicherheitsvorfällen zu minimieren.

| DE.CM-2 Kontinuierliches Monitoring der Gebäude | MS |
|---|---|
| Etablieren Sie ein kontinuierliches Monitoring / Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersicherheitsvorfälle entdecken zu können. | 2 |

***Worum geht es?***

Ein kontinuierliches Monitoring der physischen Betriebsmittel und Gebäude ist entscheidend für die frühzeitige Erkennung potenzieller Cybersicherheitsvorfälle.

***Was muss erfüllt werden?***

Die kontinuierliche Überwachung von Gebäuden wird unter anderem durch physische Sicherheitsmassnahmen wie Zugangskontrollen, Überwachungskameras und Alarmanlagen gewährleistet. Ziel ist es, ungewöhnliche oder verdächtige Aktivitäten zu identifizieren, die auf mögliche Sicherheitsrisiken hinweisen könnten. Dies kann sowohl direkte physische Bedrohungen wie Einbrüche oder Sabotageversuche als auch indirekte Bedrohungen umfassen, die die IKT-Infrastruktur beeinträchtigen könnten.

***Wie erfüllt man die Anforderungen?***

Die Implementierung eines effektiven Monitoringsystems erfordert den Einsatz modernster Technologien und die Integration von Überwachungssystemen in ein zentrales Sicherheitsmanagement-System. Dies ermöglicht eine umfassende und kontinuierliche Überwachung physischer Sicherheitsereignisse.

Für eine schnelle Reaktion auf erkannte Sicherheitsvorfälle sind klare *Incident Response* Pläne unerlässlich. Diese Pläne sollten sicherstellen, dass Sicherheitsvorfälle schnell untersucht, behoben und die betroffenen Systeme wiederhergestellt werden können. Eine enge Zusammenarbeit zwischen dem physischen Sicherheitsverantwortlichen und dem IT-Sicherheitsverantwortlichen ist hierbei entscheidend.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen sind erfüllt, wenn unzulässige Zugriffe auf physische Ressourcen erkannt, gemeldet und entsprechend behandelt werden.

Die Schulung und Sensibilisierung der Mitarbeitenden sind von grosser Bedeutung. Alle Beteiligten sollten die Bedeutung des kontinuierlichen Monitorings verstehen und wissen, wie sie auf erkannte Bedrohungen reagieren müssen. Regelmässige Schulungen und Übungen können helfen, das Bewusstsein zu schärfen und die Reaktionsfähigkeit zu verbessern (siehe PR.AT-1).

| DE.CM-4 Entdeckung von Schadsoftware | MS |
|---|---|
| Stellen sie sicher, dass Schadsoftware entdeckt werden kann. | 2 |

***Worum geht es?***

Der Schutz gegen Schadsoftware ist eine kritische Komponente der Sicherheitsstrategie. Es soll ein Prozess für die effektive Erkennung und Entdeckung von Schadsoftware implementiert werden.

***Was muss erfüllt werden?***

Die Erkennung von Schadsoftware ist unerlässlich, um potenzielle Sicherheitsverletzungen frühzeitig zu identifizieren und angemessen zu reagieren. Schadsoftware kann in verschiedenen Formen auftreten, von Viren und Trojanern bis hin zu *Ransomware* und *Spyware*, die erhebliche Risiken für die IKT-Infrastruktur und die Datenintegrität darstellen.

***Wie erfüllt man die Anforderungen?***

Um eine effektive Erkennung von Schadsoftware sicherzustellen, setzen Unternehmen fortschrittliche Technologien ein, darunter Antivirensoftware, EDR-Lösungen, *Malware*-Analysetools IDS. Diese Systeme überwachen kontinuierlich den Netzwerkverkehr, die Systemaktivitäten und die Dateiintegrität, um ungewöhnliche Aktivitäten zu identifizieren, die auf eine Infektion hinweisen könnten.

Schnelle Reaktionen auf erkannte Schadsoftware sind entscheidend, um die Auswirkungen zu minimieren. Unternehmen sollten über gut durchdachte *Incident Response* Pläne verfügen, die klare Verfahren zur Untersuchung, Isolierung und Entfernung der Schadsoftware sowie zur Wiederherstellung der betroffenen Systeme definieren.

Schulung und Sensibilisierung der Mitarbeiter sind wesentlich, um die Erkennung von Schadsoftware zu verbessern. Mitarbeiter sollten über die Anzeichen und Symptome von Schadsoftware informiert sein und wissen, wie sie verdächtige Aktivitäten melden können. Regelmässige Schulungen helfen dabei, das Bewusstsein für aktuelle Bedrohungen zu schärfen und sicherheitsbewusstes Verhalten zu fördern.

***Wann werden die Anforderungen erfüllt?***

Empfehlung: Die regelmässige Überprüfung und Verbesserung der Erkennungssysteme sind wichtig, um auf neue Arten von Schadsoftware und veränderte Bedrohungslandschaften reagieren zu können. Durch regelmässige Tests, Audits und Updates der Sicherheitssoftware können Schwachstellen identifiziert und behoben sowie die Effektivität der Schadsoftware-Erkennung verbessert werden.

Die Implementierung eines effektiven Systems zur Erkennung von Schadsoftware ist entscheidend, um die Sicherheit der IKT-Infrastruktur zu gewährleisten. Durch proaktive Massnahmen und schnelle Reaktionen können Unternehmen potenzielle Schäden minimieren und die Integrität ihrer Daten schützen.

| DE.CM-5 Entdeckung von Schadsoftware auf Mobilgeräten | MS |
|---|---|
| Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten entdeckt werden kann. | 2 |

***Worum geht es?***

Die Gewährleistung der Entdeckung von Schadsoftware auf Mobilgeräten ist für die Sicherheitsstrategie eines Unternehmens wichtig.

***Was muss erfüllt werden?***

Die Erkennung von Schadsoftware auf Mobilgeräten ist essenziell, um potenzielle Sicherheitsverletzungen frühzeitig zu identifizieren und angemessen zu reagieren. Schadsoftware auf Mobilgeräten kann verschiedene Formen annehmen, darunter Malware, Spyware und unerwünschte Apps, die sensible Daten stehlen oder die Betriebsfähigkeit der Geräte beeinträchtigen können.

***Wie erfüllt man die Anforderungen?***

Um sicherzustellen, dass Schadsoftware effektiv erkannt wird, setzen Unternehmen fortschrittliche Technologien ein, wie *Mobile Device Management* (MDM), *Mobile Threat Detection Software* und Antivirus-Programme für Mobilgeräte. Diese Systeme überwachen kontinuierlich den Zustand der Mobilgeräte, scannen Apps und Daten auf Anomalien und führen regelmässige Sicherheitschecks durch.

Neben den technischen Möglichkeiten soll eine Richtlinie erstellt werden, wie die Mitarbeitenden mit dem Mobilgeräten umgehen müssen. In der Richtlinie soll auch geregelt sein, welche Apps genutzt werden dürfen und ob der Mitarbeitende selbst Apps installieren darf/kann.

***Wann werden die Anforderungen erfüllt?***

Schnelle Reaktionen auf erkannte Schadsoftware sind entscheidend, um potenzielle Schäden zu minimieren. Unternehmen sollten über gut durchdachte *Incident Response* Pläne verfügen, die klare Verfahren zur Untersuchung, Isolierung und Entfernung der Schadsoftware auf Mobilgeräten sowie zur Wiederherstellung der Geräte und Daten umfassen.

Schulung und Sensibilisierung der Mitarbeitenden sind wesentlich, um die Erkennung von Schadsoftware auf Mobilgeräten zu verbessern. Mitarbeitende sollen über die Anzeichen und Symptome von Schadsoftware informiert sein und wissen, wie sie verdächtige Aktivitäten melden können. Regelmässige Schulungen und *Awareness*-Kampagnen helfen dabei, das Bewusstsein für aktuelle Bedrohungen zu schärfen und sicherheitsbewusstes Verhalten zu fördern (siehe PR.AT-1).

| DE.CM-7 Überwachung von Aktivitäten und Zugriffe | MS |
|---|---|
| Überwachen Sie ihre Systeme laufend, um sicherzustellen, dass Aktivitäten / Zugriffe von unberechtigten Personen, Geräten und Software erkannt wird. | 2 |

***Worum geht es?***

Die kontinuierliche Überwachung von Systemen ist entscheidend, um sicherzustellen, dass alle Aktivitäten und Zugriffe von unberechtigten Personen, Geräten und Software rechtzeitig erkannt werden.

***Was muss erfüllt werden?***

Die Überwachung der Systeme erfolgt kontinuierlich, um verdächtige oder ungewöhnliche Aktivitäten zu identifizieren, die auf potenzielle Sicherheitsverletzungen hinweisen könnten. Dies beinhaltet die Überwachung von Netzwerkverkehr, Systemlogs, Benutzeraktivitäten und Zugriffsmustern.

***Wie erfüllt man die Anforderungen?***

Durch den Einsatz fortschrittlicher Technologien wie IDS, SIEM und *Log Management Tools* können Unternehmen diese Überwachung effektiv durchführen.

***Wann werden die Anforderungen erfüllt?***

Schnelle Reaktionen auf erkannte Sicherheitsvorfälle sind entscheidend, um potenzielle Schäden zu minimieren. Gut durchdachte *Incident Response* Pläne sollten klare Verfahren zur Untersuchung, Isolierung und Behebung von Sicherheitsvorfällen sowie zur Wiederherstellung der Systemintegrität umfassen.

Schulung und Sensibilisierung der Mitarbeitenden spielen eine wichtige Rolle, um die Überwachungseffizienz zu erhöhen. Mitarbeitenden sollen über die Bedeutung der Systemüberwachung informiert sein und wissen, wie sie verdächtige Aktivitäten melden können.

## Detektionsprozesse (DE.DP)

| DE.DP-1 Definition von klaren Rollen und Verantwortlichkeiten | MS |
|---|---|
| Definieren sie klare Rollen und Verantwortlichkeiten, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat. | 2 |

***Worum geht es?***

Die Erkennung von Cybersicherheitsereignissen muss strukturiert organisiert werden. Geräte müssen so konfiguriert werden, dass sie ihre Informationen an ein zentrales System (SIEM, syslog, ...) weiterleiten. Diese Systeme müssen durchsucht werden, um verdächtige Verhaltensweisen zu identifizieren. Ein interner oder externer Mitarbeiter überwacht Alarme, filtert Fehlalarme und entscheidet, welche Massnahmen zu ergreifen sind (z. B. Isolierung eines Systems im Alarmfall). Der Mitarbeiter muss über Wartungsarbeiten informiert sein, damit er zwischen betriebsbedingten und verdächtigen Alarmen sortieren kann.

Alle relevanten Rollen im Erkennungsprozess von (IT-Leiter, Systemadministrator, IT-Sicherheitsbeauftragter) müssen klar definiert und mit spezifischen Aufgaben und Entscheidungsbefugnisse versehen sein.

Neben den Personen, die eine definierte Verantwortung tragen, spielen alle Mitarbeiter des Unternehmens eine Rolle bei der Erkennung von Cyberangriffen. Alle verdächtigen Aktivitäten sollten gemeldet werden. Einfache Mittel zur Meldung von Vorfällen sollten zur Verfügung stehen.

***Was muss erfüllt werden?***

Ein Rollen- und Verantwortlichkeitsdokument muss erstellt und an alle relevanten Mitarbeiter verteilt werden, um sicherzustellen, dass alle ihre Aufgaben und Verantwortlichkeiten bei der Erkennung von Cybersicherheitsereignissen verstehen.

***Wie erfüllt man die Anforderungen?***

Schulung: Regelmässige Schulungen zur Erkennung von Cybersicherheitsereignissen, ergänzt durch Auffrischungskurse.

Überwachung: Kontrollmechanismen und regelmässige Berichte zur Einhaltung der Verantwortlichkeiten und dem Status der Erkennungsmassnahmen. Diese Berichte sollten regelmässig an die Geschäftsführung und relevante Führungskräfte weitergeleitet werden.

***Wann werden die Anforderungen erfüllt?***

Die definierten Rollen und Verantwortlichkeiten müssen regelmässig überprüft werden, um sicherzustellen, dass sie den aktuellen Bedrohungen und organisatorischen Anforderungen entsprechen. Bei Bedarf müssen die Rollenbeschreibungen und Verantwortlichkeiten angepasst werden, um Veränderungen in der IT-Infrastruktur, neuen Bedrohungen oder organisatorischen Änderungen Rechnung zu tragen.

## Reagieren (RS)

Die Kategorie „Reagieren“ umfasst geeignete Massnahmen, die bei einem erkannten Cybersicherheitsvorfall ergriffen werden sollten. Diese sind entscheidend, um Schäden schnell zu begrenzen, die Folgen eines Angriffs einzudämmen und die Resilienz der Organisation im Allgemeinen zu stärken.

***Reaktionsplanung (RS.RP):***

Reaktionsprozesse und -verfahren werden kontinuierlich ausgeführt und aufrechterhalten, um die Reaktion auf erkannte Cybersicherheitsvorfälle zu gewährleisten.

***Kommunikation (RS.CO)***

Bei einem Cybersicherheitsvorfall ist eine koordinierte Kommunikation zwischen allen internen und externen Stakeholdern von grösster Relevanz. Einerseits um den Vorfall möglichst effizient zu beheben, anderseits um alle relevanten Anspruchsgruppen kontinuierlich zu informieren.

***Schadensminderung (RS.MI)***

Es werden Massnahmen ergriffen, um die Ausbreitung eines Ereignisses zu verhindern, seine Auswirkungen abzuschwächen und den Vorfall zu beseitigen.

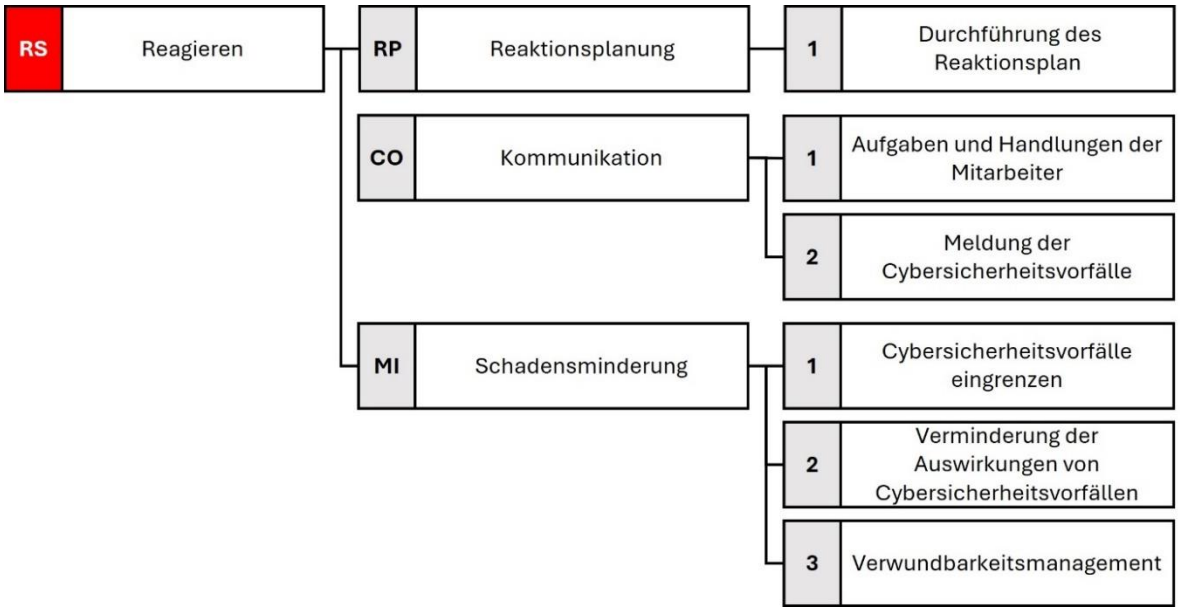



*Abbildung 10: Vorgeschriebene RS-Unterkategorien für Schutzniveau C*

## Reaktionsplanung (RS.RP)

| RS.RP-1 Durchführung des Reaktionsplan | MS |
|---|---|
| Stellen sie sicher, dass der Reaktionsplan während oder nach einem detektierten Cybersicherheitsvorfall korrekt und zeitnah durchgeführt wird. | 2 |

***Worum geht es?***

Im *Incident Response* Plan sind Massnahmen definiert, die während oder nach einem detektierten Cybersicherheitsvorfall zeitnah und korrekt umgesetzt werden.

***Was muss erfüllt werden?***

Ein effektiver *Incident Response* Plan definiert klare Verfahren und Verantwortlichkeiten für den Umgang mit Sicherheitsvorfällen. Er soll sicherstellen, dass Sicherheitsteams schnell reagieren können, um den Vorfall zu untersuchen, zu isolieren und zu beheben, um die Auswirkungen auf die Organisation zu minimieren.

***Wie erfüllt man die Anforderungen?***

Der *Incident Response* Plan sollte regelmässig überprüft, aktualisiert und durchgespielt werden, um sicherzustellen, dass alle Beteiligten mit den Verfahren vertraut sind und in der Lage sind, im Ernstfall effektiv zu handeln. Dieser Plan soll folgende Punkte beintragen:

- Wie Sie das Ausmass und die Tragweite des Vorfalls erkennen.
- Wie man kompromittierte Geräte eindämmt und isoliert.
- Wie man die Bedrohung beseitigt.
- Wie Sie Dienste wiederherstellen und zunächst auf ein minimales und dann auf ein normales Niveau zurücksetzen.

Schulungen und Übungen sind entscheidend, um die Reaktionsfähigkeit zu verbessern und sicherzustellen, dass alle Mitarbeitenden wissen, wie sie im Falle eines Vorfalls koordiniert vorgehen müssen.

Erstellen Sie Checklisten und halten Sie sich im Falle eines Cybervorfalls strikt an diese.

***Wann werden die Anforderungen erfüllt?***

Die Umsetzung eines robusten *Incident Response* Plans trägt dazu bei, die Resilienz der Organisation gegenüber Cyberangriffen zu stärken und potenzielle Schäden zu minimieren. Die Erwartungen werden erfüllt, wenn der Wiederherstellungsplan gemäss den festgelegten Prozessen, Rollen, Verantwortlichkeiten und Zielen umgesetzt wird. Im Falle eines Cyberangriffs ist es wichtig, sich auf die zuvor festgelegten Prozesse zu beziehen und diese zu befolgen, um nicht in Stress zu verfallen. Ein schnelles und koordiniertes Handeln im Ernstfall ist entscheidend, um die Sicherheit der IKT-Infrastruktur zu gewährleisten und das Vertrauen der Stakeholder zu behalten.

## Kommunikation (RS.CO)

| RS.CO-1 Aufgaben und Handlungen der Mitarbeiter | MS |
|---|---|
| Stellen Sie sicher, dass alle Personen ihre Aufgaben bezüglich der Reaktion und der Reihenfolge ihrer Handlungen auf eingetretene Cybersicherheitsvorfälle kennen. | 2 |

***Worum geht es?***

Bei einem Angriff kann der Stresspegel schnell ansteigen. Um bestmöglich reagieren zu können, ist eine vorherige Vorbereitung notwendig.

***Was muss erfüllt werden?***

Definieren Sie Angriffsszenarien und ermitteln Sie, welche Gegenmassnahmen zur Bekämpfung des Vorfalls am besten geeignet sind. Wenn beispielsweise ein Server beschädigt ist, ist es besser, ihn zu isolieren, indem Sie alle Netzwerkverbindungen entfernen, als ihn einfach abzuschalten. So können Experten für Cybersicherheit das System analysieren, um das Problem zu identifizieren.

Ein *Incident Response* Plan (RS.RP-1) enthält konkret Angaben, wie Netzwerkteile isoliert werden müssen, damit sich eine Malware nicht weiter ausbreitet.

***Wie erfüllt man die Anforderungen?***

Die folgenden Punkte sollten vorbereitet werden:

<u>Technik:</u>

- Ermittlung möglicher Angriffspfade und der zu ergreifenden technischen Gegenmassnahmen.
- Festlegung von Kriterien, die einen Cyberangriff vermuten lassen.

<u>Organisation:</u>

- Identifikation der Rollen: Bestimmen Sie die verschiedenen Rollen, die zur Verwaltung der Cybersicherheit in Ihrer Organisation erforderlich sind. Dazu gehören Sicherheitsverantwortliche, *Incident-Response-Teams*, *Backup*-Verantwortliche usw.
- Klare Verantwortlichkeiten: Beschreiben Sie die Verantwortlichkeiten jeder Rolle im Bereich der Cybersicherheit klar und deutlich.
- Dokumentierte Rollen: Überprüfen Sie, ob alle Rollen und Verantwortlichkeiten klar dokumentiert und die Dokumente zugänglich sind.

<u>Kommunikation:</u>

- Effektive Kommunikation: Stellen Sie sicher, dass die Informationen über Rollen und Verantwortlichkeiten ordnungsgemäss an alle Beteiligten kommuniziert wurden.

<u>Ausbildung:</u>

- Abgeschlossene Schulung: Bestätigen Sie, dass die Schulung zu Rollen und Verantwortlichkeiten durchgeführt wurde und die Mitarbeiter ihre Verantwortlichkeiten verstehen.

***Wann werden die Anforderungen erfüllt?***

Die Reaktion auf Vorfälle soll regelmässig getestet und überprüft werden. Schulen Sie Ihre Mitarbeitenden, wie sie auf mögliche Vorfälle reagieren sollen und implementieren Sie einen Meldekanal (Telefon, Teams-Kanal usw.).

| RS.CO-2 Meldung der Cybersicherheitsvorfälle | MS |
|---|---|
| Definieren sie Kriterien für Meldungen und stellen sie sicher, dass Cybersicherheitsvorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden. | 2 |

***Worum geht es?***

Es muss sichergestellt werden, dass die Kommunikation mit den relevanten Stakeholdern, unter anderem mit dem BACS (Bundesamt für Cybersicherheit) und mit dem EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) gewährleistet ist. Dabei sind Meldepflichten für kritische Infrastrukturen und die entsprechenden Fristen zu berücksichtigen. Unternehmen müssen hierfür einen Prozess definieren und die notwendigen Pläne und Dokumentationen dazu bereithalten. Ziel der Meldung ist, andere Unternehmen frühzeitig über neue Bedrohungen zu informieren und eine schweizweite Übersicht über Cyberangriffe zu erhalten.

Die Kriterien für die Meldepflicht werden in der Verordnung für die Cybersicherheit[12] (Cybersicherheitsverordnung, CSV) festgelegt.

***Was muss erfüllt werden?***

Organisationen sollten klare Richtlinien und Verfahren festlegen, die definieren, was als Cybersicherheitsvorfall[13] betrachtet wird und wie dieser gemeldet werden soll. Diese Kriterien sollten sowohl technische als auch geschäftliche Aspekte berücksichtigen, um sicherzustellen, dass alle relevanten Vorfälle erfasst und angemessen behandelt werden.

***Wie erfüllt man die Anforderungen?***

Organisationen sollten festlegen, welche Vorfälle zu melden sind (z. B. Meldung des Diebstahls von Kundendaten an EDÖB und die betroffenen Kunden).

Das Personal muss geschult werden, um zu wissen, wie bei einem Vorfall zu reagieren ist. Auch die Kommunikation muss klar definiert sein:

- Wer ist bei einem Vorfall zu benachrichtigen?
- Wie soll der Dienstleister oder Lieferant informiert werden?
- Umgekehrt: Wann und wie sollte der Dienstleister oder Lieferant das Unternehmen informieren?

***Wann werden die Anforderungen erfüllt?***

Die Kriterien zur Meldung von Vorfällen müssen klar kommuniziert und überprüft werden, um ihre Aktualität zu gewährleisten. Mitarbeiter sollten geschult sein, um Verdachtsfälle zu identifizieren und melden zu können.

Nach jedem Vorfall sollten Massnahmen zur Verbesserung der Abwehr, Verfahren, Sensibilisierung der Mitarbeiter und Kommunikation ergriffen werden.

Durch regelmässige Übungen zum Krisenmanagement, die auf die Grösse des Unternehmens abgestimmt sind, können sich die Teilnehmer auf den Umgang mit den verschiedenen Aspekten vorbereiten.

[12] Projekt, zurzeit in Vernehmlassung.
[13] Die Cybersicherheitsverordnung wird ein Teil dieser Massnahmen festlegen.

## Schadensminderung (RS.MI)

| RS.MI-1 Cybersicherheitsvorfälle eingrenzen | MS |
|---|---|
| Stellen Sie sicher, dass Cybersicherheitsvorfälle eingegrenzt werden können und die weitere Ausbreitung unterbrochen wird. | 2 |

***Worum geht es?***

Die Fähigkeit, Cybersicherheitsvorfälle wirksam einzudämmen und ihre weitere Ausbreitung zu unterbrechen, ist von entscheidender Bedeutung. Das Eingrenzen von Cybersicherheitsvorfällen erfordert ein schnelles und koordiniertes Handeln, um die Ausbreitung von Schadsoftware oder unautorisiertem Zugriff auf Systeme zu stoppen. Hierzu sollten Unternehmen klare Verfahren und Prozesse etablieren, die sicherstellen, dass Sicherheitsteams rasch auf Warnhinweise reagieren und die nötigen Massnahmen ergreifen können.

***Was muss erfüllt werden?***

Zu den Massnahmen gehören die Isolierung infizierter Systeme oder Netzwerkbereiche (siehe PR.AC-5), die Unterbrechung unerwünschter Netzwerkverbindungen und die vorübergehende Einschränkung des Zugriffs auf sensible Daten oder Ressourcen. Durch diese Massnahmen wird verhindert, dass sich ein Vorfall weiter ausbreitet und grössere Schäden verursacht.

Für die Suche nach einer Schadsoftware, empfiehlt es sich, das System aktiv, aber vollständig vom Netzwerk getrennt zu lassen. Dazu müssen die Kabel vor dem Abziehen korrekt beschriftet werden, damit die Inbetriebnahme vereinfacht wird, sobald das Problem im System behoben ist.

Eine effektive Reaktion auf Vorfälle erfordert eine enge Zusammenarbeit zwischen den IT- und Sicherheitsteams sowie klare Kommunikationswege, um schnell Entscheidungen treffen und Massnahmen umsetzen zu können. Regelmässige Schulungen und Übungen sind unerlässlich, um die Reaktionsfähigkeit zu verbessern und sicherzustellen, dass alle Beteiligten mit den Prozessen vertraut sind.

***Wie erfüllt man die Anforderungen?***

Die kontinuierliche Überprüfung und Optimierung der *Incident Response* Prozesse ist ebenfalls wichtig, um auf neue Bedrohungen und Technologien zu reagieren. Durch regelmässige Tests und Simulationen können Unternehmen ihre Fähigkeiten zur Eingrenzung von Cybersicherheitsvorfällen weiter verbessern und ihre Resilienz stärken.

***Wann werden die Anforderungen erfüllt?***

Die Implementierung eines robusten Systems zur Eingrenzung von Cybersicherheitsvorfällen trägt dazu bei, potenzielle Schäden zu minimieren und die Betriebskontinuität zu gewährleisten. Ein schnelles und effektives Eingreifen kann den Unterschied zwischen einer begrenzten Störung und einem schwerwiegenden Sicherheitsvorfall ausmachen.

| RS.MI-2 Verminderung der Auswirkungen von Cybersicherheitsvorfällen | MS |
|---|---|
| Stellen Sie sicher, dass die Auswirkungen von Cybersicherheitsvorfällen gemindert werden können. | 2 |

***Worum geht es?***

Ein wesentlicher Aspekt besteht darin, sicherzustellen, dass das Unternehmen in der Lage ist, Cybervorfälle effektiv zu bewältigen, um potenzielle Schäden zu minimieren.

***Was muss erfüllt werden?***

Ein gut strukturierter *Incident Response* Plan, der schnelle Erkennung, adäquate Reaktion und effiziente Wiederherstellungsmassnahmen umfasst sollte implementiert werden. Durch diese Massnahmen kann die Ausbreitung von Schadsoftware gestoppt, sensible Daten geschützt und die Betriebsfähigkeit schnell wiederhergestellt werden.

Zusätzlich spielt die transparente Kommunikation mit internen Teams, Stakeholdern und gegebenenfalls externen Partnern eine entscheidende Rolle. Ein klarer Informationsfluss während eines Vorfalls trägt dazu bei, Vertrauen zu wahren und eine effektive Zusammenarbeit sicherzustellen.

***Wie erfüllt man die Anforderungen?***

- Schnelle Reaktion und schnelles Eingreifen des Response-Teams.
- Klare Eskalationsprozesse damit Entscheidungsträger schnell informiert sind.
- Eingrenzung des Cybersicherheitsvorfalls gemäss RS.MI-1
- Priorität auf kritische Prozesse und Aktivitäten (OT) setzen.
- Schnelle Wiederherstellung (Daten + Systeme).
- Klare Kommunikation anhand eines Notfallkommunikationsplan um Mitarbeiter, Partner und Kunden rechtzeitig zu informieren.
- Externe Unterstützung von Fachleuten (Spezialisten) und/oder Behörden suchen (BACS, GovCERT, BFE).
- Einbeziehung der Strafverfolgungsbehörden, falls erforderlich.
- Cyber-Versicherung: Bewerten Sie die Möglichkeiten, die Ihnen zur Verfügung stehen.

Die kontinuierliche Verbesserung der *Incident Response* Prozesse durch eine gründliche Analyse nach jedem Vorfall ist ebenfalls von grosser Bedeutung. Dies ermöglicht es dem Unternehmen, aus Erfahrungen zu lernen, Schwachstellen zu identifizieren und die Sicherheitsstrategie kontinuierlich anzupassen, um zukünftige Vorfälle besser zu bewältigen.

***Wann werden die Anforderungen erfüllt?***

Durch die Implementierung eines robusten Ansatzes zur Reduzierung der Auswirkungen von Cyber-Vorfällen kann das Unternehmen seine Widerstandsfähigkeit gegenüber Sicherheitsbedrohungen stärken und die Integrität seiner Systeme und Daten schützen. Die ergriffenen Massnahmen sind je nach Vorfall unterschiedlich. Es ist jedoch wichtig, dass sie vorher in verschiedenen Szenarien festgelegt werden und ihre Umsetzung bis zur vollständigen Wiederherstellung methodisch verfolgt wird.

| RS.MI-3 Verwundbarkeitsmanagement | MS |
|---|---|
| Stellen sie sicher, dass neu identifizierte Verwundbarkeiten reduziert oder als akzeptierte Risiken dokumentiert werden. | 2 |

***Worum geht es?***

Die Identifizierung und Bewertung von Verwundbarkeiten ist ein Bestandteil einer umfassenden Sicherheitsstrategie. Anhand einer kontinuierlichen Analyse der Risiken muss das Unternehmen über seine Strategie zum Schwachstellenmanagement entscheiden.

***Was muss erfüllt werden?***

Organisationen sollten regelmässig Schwachstellenanalysen durchführen, um potenzielle Sicherheitslücken zu erkennen, bevor sie von Angreifern ausgenutzt werden können. Es ist möglich und empfehlenswert, Informationen von externen Dienstleistern und Partnern oder vom Bund einzuholen (Cyber Security Hub CSH[14], MISP, ...).

***Wie erfüllt man die Anforderungen?***

Für neu identifizierte Verwundbarkeiten müssen Unternehmen geeignete Massnahmen ergreifen, um das Risiko zu mindern. Dies kann durch die Implementierung von Sicherheitspatches, Konfigurationsänderungen oder anderen Kontrollen geschehen, die die Sicherheitslücke schliessen oder ihre Auswirkungen reduzieren.

In Fällen, in denen es nicht möglich ist, die Verwundbarkeit sofort zu beheben oder zu eliminieren, sollte eine dokumentierte Risikoakzeptanz erfolgen. Dies bedeutet, dass das Management die Risiken bewertet hat, die mit der Verwundbarkeit verbunden sind, und bewusst entschieden hat, sie vorübergehend oder dauerhaft zu tolerieren.

***Wann werden die Anforderungen erfüllt?***

Die Dokumentation dieses Prozesses ist entscheidend, um Transparenz zu gewährleisten und sicherzustellen, dass die Risikobewertung auf fundierten Informationen basiert. Dies erleichtert auch die Überwachung und das Management der Verwundbarkeiten über die Zeit hinweg.

Durch die Implementierung eines strukturierten Ansatzes können Organisationen die Sicherheitslage verbessern, indem sie potenzielle Schwachstellen proaktiv adressieren und Risiken effektiv managen. Dies trägt dazu bei, die Resilienz zu stärken und das Risiko von Cyberangriffen zu minimieren.

[14] Fragen zum CSH oder zu anderen Dienstleistungen des BACS sollten an info@ncsc.admin.ch gerichtet werden.

## Wiederherstellen (RC)

Die Kategorie „Wiederherstellen“ identifiziert geeignete Massnahmen zur Erstellung und Aufrechterhaltung von Plänen zur Widerstandsfähigkeit und zur Wiederherstellung von Funktionen oder Diensten, die aufgrund eines Cybersicherheitsvorfalls beeinträchtigt wurden. Dies unterstützt die rechtzeitige Wiederherstellung des normalen Betriebs, um die Auswirkungen eines Cybersicherheitsvorfalls zu verringern.

***Wiederherstellungsplanung (RC.RP):***

Wiederherstellungsprozesse und -verfahren werden ausgeführt und aufrechterhalten, um die Wiederherstellung von Systemen oder Anlagen zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind.


*Abbildung 11: Vorgeschriebene RC-Unterkategorie für Schutzniveau C*

## Wiederherstellungsplanung (RC.RP)

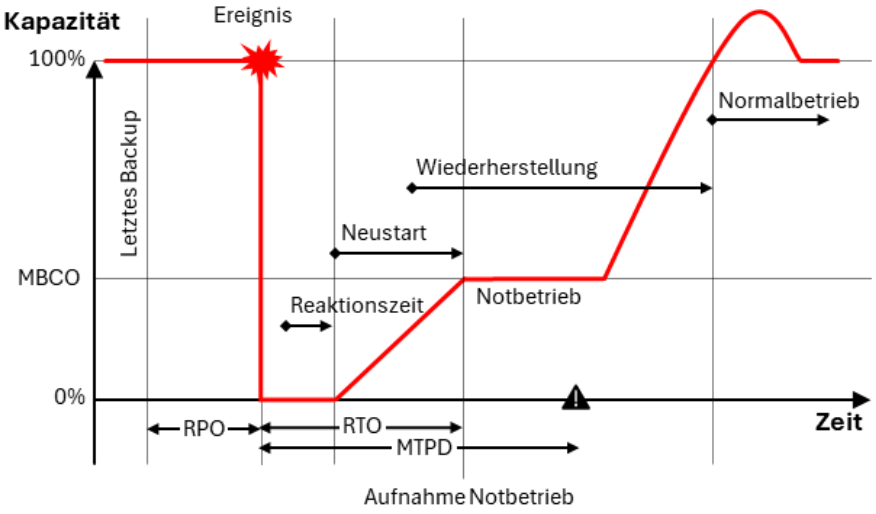
| RC.RP-1 Korrekte Durchführung des Wiederherstellungsplan | MS |
|---|---|
| Stellen Sie sicher, dass der Wiederherstellungsplan nach einem eingetretenen Cybersicherheitsvorfall korrekt durchgeführt werden kann. | 2 |

***Worum geht es?***

Um die ordnungsgemässe Durchführung eines Wiederherstellungsplans nach einem Cybersicherheitsvorfall zu gewährleisten, sind mehrere wichtige Schritte erforderlich. Nur eine angemessene Vorbereitung und die sorgfältige Durchführung des Wiederherstellungsplans ermöglichen eine schnelle Rückkehr zum normalen Betrieb und die Verringerung der Auswirkungen des Vorfalls.

***Was muss erfüllt werden?***

Der Wiederherstellungsplan sollte klare Anweisungen enthalten, wie mit verschiedenen Arten von Sicherheitsvorfällen umzugehen ist, um eine schnelle Reaktion zu ermöglichen. Regelmässige Aktualisierungen sind unerlässlich, um sicherzustellen, dass der Plan aktuelle Bedrohungen und Technologien berücksichtigt.




**RPO**: Recovery Point Objective. Ab diesem Zeitpunkt sind die Daten verloren.

**RTO**: Recovery Time Objective. Wie lange dauert es, bis der Betrieb wieder aufgenommen wird? Ist Ersatzmaterial verfügbar? Gibt es genug Ressourcen und Support vom Dienstleister?

**MBCO**: Minimum Business Continuity Objective. Welche Systeme sind für den Notbetrieb erforderlich (BCM)?

**MTPD**: Maximum Tolerable Period of Disruption

*Abbildung 12: Wiederherstellungsprozess*

***Wie erfüllt man die Anforderungen?***

Eine klare Aufteilung der Verantwortlichkeiten, definierte Eskalationswege und klare Kommunikationskanäle sind entscheidend, um die Auswirkungen zu minimieren. Die Verwendung von Checklisten hilft, die Schritte des Wiederherstellungsplans strukturiert zu verfolgen und Fehler/Versehen zu vermeiden.

***Wann werden die Anforderungen erfüllt?***

Die Anforderungen sind erfüllt, wenn das Unternehmen den Prozess zur Wiederherstellung in klaren Etappen definiert hat. Die Durchführung soll schrittweise erfolgen und kann durch Hilfsmittel (z. B. Checkliste) unterstützt werden. Nach jedem Vorfall ermöglicht eine präzise Dokumentation die Verbesserung des Plans. Konsistenz in diesen Massnahmen gewährleistet die Betriebskontinuität und stärkt das Vertrauen.

# Abbildungsverzeichnis



# Abkürzungsverzeichnis

| | |
|---|---|
| 2FA | Zwei-Faktor-Authentifizierung |
| Abs. | Absatz |
| Art. | Artikel |
| BACS | Bundesamt für Cybersicherheit |
| BCM | *Business Continuity Management* (Betriebliches Kontinuitätsmanagement) |
| BFE | Bundesamt für Energie |
| BSI | Bundesamt für Sicherheit in der Informationstechnik (DE) |
| BWL | Bundesamt für wirtschaftliche Landesversorgung |
| BYOD | *Bring Your Own Device* (Mitbringen eigener Geräte zum Arbeitsplatz) |
| CISO | *Chief Information Security Officer* (Leiter der Informationssicherheit) |
| COBIT | *Control Objectives for Information and Related Technology* |
| CSF | *Cybersecurity Framework* (Cybersicherheitsrahmen) |
| CSH | *Cybersecurity Hub* |
| CSV | Cybersicherheitsverordnung |
| DLP | *Data Loss Prevention* (Datenverlustprävention) |
| DNS | *Domain Name System* |
| DSG | Datenschutzgesetz |
| DSGVO | Datenschutz-Grundverordnung (EU) |
| DSV | Datenschutzverordnung |
| EDÖB | Eidegenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| EDR | *Endpoint Detection and Response* (Endpunkterkennung und -reaktion) |
| EU | Europäische Union |
| GovCERT | *Government Computer Emergency Response Team* (Computer-Notfallteam des Bundes) |
| IAM | *Identity and Access Management* (Identitäts- und Zugriffsmanagement) |
| ICS | *Industrial Control System* (industrielle Steuerungssysteme) |
| IDM | *Identity Management* (Identitätsmanagement) |
| IDS | *Intrusion Detection System* (System zur Erkennung von Ereignissen) |
| IKS | Internes Kontrollsystem |
| IKT | Informations- und Kommunikationstechnologie |
| IoT | *Internet of Things* (Internet der Dinge) |
| IP | *Internet Protocol* |

| | |
|---|---|
| IPS | *Intrusion Prevention System* (System zur Prävention von Ereignissen) |
| IPsec | *Internet Protocol Security* |
| ISO | *International Organization for Standardization* (Internationale Organisation für Normung) |
| IT | *Information Technology* (Informationstechnologie) |
| KI | Kritische Infrastruktur |
| KMU | Kleine und mittlere Unternehmen |
| MBCO | *Minimum Business Continuity Objective* (Mindestziel für die Geschäftskontinuität) |
| MDM | *Mobile Device Management* (Verwaltung mobiler Endgeräte) |
| MFA | Multi-Faktor-Authentifizierung |
| MISP | *Malware Information Sharing Platform* (Plattform zum Austausch von Informationen über Schadsoftware) |
| MS | Maturitätsstufe |
| MTPD | *Maximum Tolerable Period of Disruption (*Maximal tolerierbare Ausfallzeit) |
| NAC | *Network Access Control* (Netzwerkzugangskontrolle) |
| NDA | *Non-Disclosure Agreement* (Verschwiegenheitserklärung) |
| NERC | *North American Electric Reliability Corporation* |
| NIST | *National Institute of Standards and Technology* |
| OT | *Operational Technology* (Betriebstechnologie) |
| PDCA | *Plan-Do-Check-Act* (Planen – Umsetzen – Überprüfen – Handeln) |
| RBAC | *Role-Based Access Control* (Rollenbasierte Zugriffskontrolle) |
| RFID | *Radio Frequency Identification* |
| Rlogin | *Remote Login* |
| RLSV | Rohrleitungssicherheitsverordnung |
| RM | Risk Management |
| RPO | *Recovery Point Objective* (Maximal zulässiger Datenverlust) |
| RTO | *Recovery Time Objective* (Wiederanlaufzeit) |
| SIEM | *Security Information and Event Management* (Verwaltung von Sicherheitsinformationen und -ereignissen) |
| SR | Systematische Rechtssammlung |
| SSH | *Secure Shell* |
| SYSLOG | *System Logging* |
| Telnet | *Teletype Network Protocol* |
| TLS | *Transport Layer Security* |
| USB | *Universal Serial Bus* |
| VLAN | *Virtual Local Area Network* (Virtuelles Lokales Netzwerk) |
| VPN | *Virtual Private Network* (Virtuelles Privates Netzwerk) |
| WLAN | *Wireless Local Area Network* |

# Anhang

## Anhang 1: Glossar

Nachfolgend werden Begriffe aufgelistet, welche im Rahmen dieses Dokumentes eine spezifische Bedeutung haben. Auf das Auflisten von im IKT-Kontext allgemein gebräuchlichen Begriffen (z.B. Hardware, Software, Backup, etc.) wird verzichtet.

| Begriff | Bedeutung |
|---|---|
| Cyberangriffe | Cyberangriffe umfassen sämtliche bewussten Aktivitäten, die zum Ziel haben die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten zur verletzen. |
| EDR | Ein EDR (*Endpoint Detection and Response*) ist ein Cybersicherheits-Tool, das kontinuierlich die Aktivitäten auf Endgeräten (wie Computern, Servern oder mobilen Geräten) überwacht und analysiert, um Bedrohungen zu erkennen, zu verhindern und darauf zu reagieren, indem es Echtzeit-Einblicke und Abhilfemassnahmen bietet. |
| *Hardware Lifecycle Management* | Hardware Lifecycle Management ist ein umfassender Ansatz zur Bewirtschaftung von IKT-Hardware über deren gesamte Einsatzdauer hinweg. |
| IKT-Infrastruktur | Sämtliche Elemente der Informations- und Telekommunikationsausrüstung, die eine Organisation zur Erfüllung ihrer Geschäftsprozesse benötigt. Z.B. Desktop-PCs, Mobiltelefone, Rechenzentren, etc. |
| Industrielle Kontrollsysteme | «Industrielle Kontrollsysteme» ist ein Überbegriff für all diejenigen Elemente, die zur Steuerung und Überwachung von Anlagen oder Industrieprozessen eingesetzt werden. Ein industrielles Kontrollsystem umfasst typischerweise Sensoren, Rechenzentren, Leitstellen, Leitungen und Anlagen. Die englischen Begriffe «Industrial Control System/ICS» und «Supervisory Control and Data Aqcuisition System/SCADA» werden synonym verwendet. |
| IDS | Ein IDS (*Intrusion Detection System*) ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Netzwerk gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachendes Computersystem laufen. |
| Kompromittierung | Ein System, eine Datenbank oder auch nur ein einzelner Datensatz wird als kompromittiert betrachtet, wenn Daten manipuliert sein könnten und wenn der Eigentümer (oder Administrator) des Systems keine Kontrolle über die korrekte Funktionsweise oder den korrekten Inhalt mehr hat. |
| Kritische Infrastruktur | Das Spektrum der kritischen Infrastrukturen (KI) umfasst neun Sektoren, unterteilt in 27 Teilsektoren (Branchen). Die vollständige Übersicht ist online verfügbar, unter:<br>https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html |
| *Least Privilege* | Die Mitarbeiter haben nur die für sie unbedingt notwendigen und keine zusätzlichen Berechtigungen für ihre Aktivitäten. |

| Begriff | Bedeutung |
|---|---|
| MDM | Ein MDM (*Mobile Device Management*) ist ein Verwaltungstool, das die Konfiguration und Nutzung von Mobilgeräten harmonisiert und gleichzeitig ein hohes Mass an Sicherheit gewährleistet, z. B. durch Backups, Fernsperrung und Update-Management. |
| *Need-to-know* | Das *Need-to-know*-Prinzip besagt, dass die Nutzer nur Zugang zu den Informationen haben, die für ihre Arbeit unbedingt erforderlich sind. |
| *Phishing* | Unter dem Begriff *Phishing* versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Anwenders zu gelangen und damit Identitätsdiebstahl zu begehen. |
| *Security Awareness Programm* | Ein *Security Awareness Programm* hat zum Ziel, das Bewusstsein für Sicherheitsthemen und entsprechendes Verhalten bei Mitarbeitern, Partnern, Lieferanten, usw. zu verbessern. |
| *Security by default* | *Security by Default* bedeutet, dass Systeme, Anwendungen oder Geräte standardmässig so konfiguriert sind, dass sie das höchstmögliche Sicherheitsniveau bieten, ohne dass der Benutzer eingreifen muss. Dies stellt sicher, dass nur die notwendigen Funktionen aktiviert sind, wodurch das Risiko einer Bedrohung verringert wird. |
| *Security by design* | *Security by Design* bedeutet, dass Sicherheit von Anfang an in die Konzeption eines Produkts oder Systems integriert wird. Sicherheitsaspekte werden während des gesamten Entwicklungsprozesses berücksichtigt, um eine sichere und widerstandsfähige Architektur gegen Angriffe zu gewährleisten. |
| *Security Monitoring* | *Security Monitoring* beschreibt den Prozess, mit dem laufend die Datenflüsse und Netzwerkaktivitäten im eigenen Netz beobachtet werden. Das Ziel ist es, auffälliges Verhalten frühzeitig zu entdecken. Zu diesem Zweck werden dedizierte *Security-Monitoring*-Systeme eingesetzt. |
| SIEM | Ein SIEM (*Security Information and Event Management*) ist ein System, das in Echtzeit Sicherheitsdaten aus verschiedenen Quellen (wie Logs von Anwendungen, Servern oder Netzwerkgeräten) sammelt, analysiert und korreliert, um Bedrohungen zu erkennen, Teams zu alarmieren und bei der Verwaltung von Sicherheitsvorfällen zu helfen. |
| System | Eine organisierte Zusammenstellung von Ressourcen und Verfahren, die durch Interaktion oder Interdependenz vereint und geregelt werden, um eine Reihe spezifischer Funktionen zu erfüllen. Diese können zum Beispiel das Messen, Kontrollieren, Verarbeiten, Übertragen, Speichern, Benutzen und die Sicherheit von Daten ermöglichen. |
| VPN | Ein VPN (*Virtual Private Network*) ist ein privates Netzwerk, das eine sichere Verbindung über öffentliche Netzwerke ermöglicht. Eine VPN-Verbindung schafft einen Tunnel, durch welchen verschlüsselte Daten kommuniziert werden können. |

| Begriff | Bedeutung |
| --- | --- |
| *Zero Trust* | *Zero Trust* ist ein Sicherheitsgrundsatz, der besagt, dass man einem Benutzer oder System niemals standardmässig vertrauen sollte, auch wenn sie sich innerhalb des Netzwerks befinden, und dass man jeden Zugriff und jede Aktion immer durch strenge Authentifizierung und Kontrolle überprüfen und validieren sollte. |

## Anhang 2: Weiterführende Informationen

Die folgenden Listen enthalten Beispiele für Ressourcen, die bei der Umsetzung von Cybersicherheitsmassnahmen helfen können.

**Hilfsmittel des BACS**

| Thema | Link |
|---|---|
| Cyberangriffe gegen Firmen | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html |
| Cybersicherheit in der Lieferkette | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html |
| Empfehlung für die Zusammenarbeit mit IT-Providern | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html |
| Krisenkommunikation | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/krisenkommunikation.html |
| Massnahmen im Falle eines Cyberangriffs | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/checkliste-ciso.html |
| Massnahmen im Falle eines Datenabfluss | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/datenabfluss.html |
| Massnahmen im Falle eines Ransomware-Angriffs | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html |
| Massnahmen zum Schutz von ICS | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ics.html |
| Ransomware | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-bedrohungen/ransomware.html |
| Sicherer Umgang mit Fernzugriffen | https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/homeoffice.html |

**Dokumentation aus der EU**

| Thema | Link |
|---|---|
| Awareness Campaign – Fuel for Cyber | https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/fuel-for-cyber |
| Cyber Insurance: Recent Advances, Good Practices and Challenges | https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges |
| Cyber Security Culture in Organisations | https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations |
| Cybersecurity Guide for SMEs – 12 Steps to Securing your Business | https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes |

| | |
|---|---|
| Cybersecurity Maturity Assessment for Small and Medium Enterprises | https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/ |
| Good Practices for Supply Chain Cybersecurity | https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity |
| Mapping of Security Measures for Operators of Essential Services | https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services |
| Raising Awareness of Cybersecurity | https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity |

**Andere Hilfsmittel (UK/USA/AU)**

| Thema | Link |
|---|---|
| Advice & Guidance (46 topics) | https://www.ncsc.gov.uk/section/advice-guidance/all-topics |
| Cyber-Physical Security Considerations for the Electricity Sub-Sector | https://www.cisa.gov/resources-tools/resources/sector-spotlight-cyber-physical-security-considerations-electricity-sub-sector |
| Cybersecurity Capability Maturity Model (C2M2) | https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 |
| Cybersecurity Framework Profile for Liquefied Natural Gas | https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-liquefied-natural-gas |
| Device Security Guidance | https://www.ncsc.gov.uk/collection/device-security-guidance |
| Electricity Substation Physical Security | https://www.cisa.gov/resources-tools/resources/sector-spotlight-electricity-substation-physical-security |
| Energy Sector Cybersecurity Preparedness | https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness |
| Infographics of NCSC guidance | https://www.ncsc.gov.uk/section/infographics/home |
| Information for Small & Medium Sized Organisations | https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations |
| Operational Technology Guidance | https://www.ncsc.gov.uk/collection/operational-technology |
| Principles of Operational Technology Cyber security | https://www.cyber.gov.au/about-us/view-all-content/publications/principles-operational-technology-cyber-security?utm_source=international_partner&utm_medium=social&utm_campaign=critical_infrastructure |
| SCADA in the Cloud | https://www.ncsc.gov.uk/blog-post/scada-cloud-new-guidance-ot-organisations |
| Smartphone Security Checker | https://www.fcc.gov/smartphone-security |

**NIST-Veröffentlichungen**

| Dokument | Link |
|---|---|
| NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* | https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final |

| | |
|---|---|
| NIST SP 800-82 Rev. 3, *Guide to Operational Technology (OT) Security* | https://csrc.nist.gov/pubs/sp/800/82/r3/final |
| NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* | https://csrc.nist.gov/pubs/sp/800/83/r1/final |
| NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* | https://csrc.nist.gov/pubs/sp/800/84/final |
| NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* | https://csrc.nist.gov/pubs/sp/800/86/final |
| NIST SP 800-92, *Guide to Computer Security Log Management* | https://csrc.nist.gov/pubs/sp/800/92/final |
| NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* | https://csrc.nist.gov/pubs/sp/800/94/final |
| NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* | https://csrc.nist.gov/pubs/sp/800/115/final |
| NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* | https://csrc.nist.gov/pubs/sp/800/128/upd1/final |
| NIST SP 1800-2, *Identity and Access Management for Electric Utilities* | https://csrc.nist.gov/pubs/sp/1800/2/final |
| NIST SP 1800-22, *Mobile Device Security: Bring Your Own Device (BYOD)* | https://csrc.nist.gov/pubs/sp/1800/22/final |
| NIST SP 1800-23, *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry* | https://csrc.nist.gov/pubs/sp/1800/23/final |