CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

CYBER-SECURITY und RESILIENZ

in Supply Chains mit Fokus auf KMU

FH Oberösterreich

Logistikum

FH Salzburg

Technische Hochschule Deggendorf

universität innsbruck

Universität Passau

IMPRESSUM

Stand / Version April 2026

Förderhinweis Diese Publikation wurde im Rahmen Projektes „Cyber Security und Resilienz in Supply Chains mit Fokus auf KMU (CySeReS-KMU)“ erstellt.
Das Projekt wird gefördert durch das Programm Interreg VI-A Bayern–Österreich 2021–2027, kofinanziert von der Europäischen Union.

Publisher FH OÖ Forschungs & Entwicklungs GmbH
Roseggerstraße 15, 4600 Wels, Österreich • Tel: +43 (0) 5 0804 33200
https://fh-ooe.at/forschung/ueber-die-forschung-entwicklung

Gestaltung Werbeagentur Hauer-Heinrich GmbH, Passau • https://www.hauer-heinrich.de

Bildlizenz https://www.freepik.com/

Urheberrecht © 2026 FH Oberösterreich – Logistikum. Alle Rechte vorbehalten.
Die Inhalte sind urheberrechtlich geschützt. Nutzung/Vervielfältigung/Verbreitung nur im Rahmen der geltenden urheberrechtlichen Bestimmungen.

Haftungsausschluss Keine Gewähr für Richtigkeit, Vollständigkeit und Aktualität. Haftung für Schäden aus der Nutzung – soweit rechtlich zulässig – ausgeschlossen.

Hinweis zu externen Links Für Inhalte externer Websites Dritter wird keine Haftung übernommen; verantwortlich ist jeweils der/die Betreiber*in der verlinkten Seiten.

Projektteam Amar Almaini[3], Stefan Anthuber[3], Gottfried Egger[3], Daniel Grabner[1], Amelie Gutbrod[1], Michael Herburger[1], Laura Holzer[1], Abdurrahman Icyer[3], Stefan Katzenbeisser[5], Manuel Kraxberger[1], Sven Kufner[3], Karoline Langner[1], Bjarne Lill[4], Nico Mexis[5], Julia Pichler[1], Michael Plasch[1], Clemens Sauerwein[4], Martin Schramm[3], Daniel Szilagyi[1], Carina Wagner[1], Alexander Zeisler[2]

Projektkonsortium

[1] FH Oberösterreich, Campus Steyr / Logistikum
Wehrgrabengasse 1-3 • A-4400 Steyr • michael.plasch@fh-steyr.at

[2] FH Salzburg
Urstein Süd 1 • A-5412 Puch / Salzburg • alexander.zeisler@fh-salzburg.ac.at

[3] TH Deggendorf, Technologie Campus Vilshofen
Aidenbacher Straße 32 • D-94474 Vilshofen an der Donau • amar.almaini@th-deg.de

[4] Universität Innsbruck
Innrain 52 • A-6020 Innsbruck • clemens.sauerwein@uibk.ac.at

[5] Universität Passau
Innstraße 41 • D-94032 Passau • nico.mexis@uni-passau.de

INHALT

Tabellenverzeichnis VII
Abbildungsverzeichnis VIII
Abstract IX

1 Cyber-Security Grundschutz für KMU 1

Einleitung 2
1.1 Bedeutung von Cyber-Security für KMU 2
1.1.1 Was sind die größten Herausforderungen und Chancen? 2
1.2 Schritte vor der Umsetzung eines Cyber-Security-Projektes 3
1.2.1 IST-Zustand identifizieren 3
1.2.2 Zielsetzung festlegen 5
1.2.3 Verantwortlichkeiten festlegen 5
1.2.4 Priorisierung der Projektinhalte und Festlegung eines Projektplanes 5
1.3 Vorgehensweise zur Umsetzung eines Cyber-Security Projektes 5
1.3.1 Plan: Unternehmensinfrastruktur und Cybersicherheitsmaßnahmen analysieren 6
1.3.2 Do: Umsetzung von geplanten Cybersicherheitsmaßnahmen 6
1.3.3 Check: Überprüfung der Sicherheitsmaßnahmen 6
1.3.4 Act: Anpassen 6
1.4 Cyber-Security Grundschutz Maßnahmen 7
1.4.1 Zugangskontrolle 7
1.4.2 Sicherung des Unternehmensumfelds 8
1.4.3 Sicherheitsbewusstsein 9
1.4.4 Sichere Konfiguration 9
1.4.5 Patches und Updates 10
1.4.6 Datensicherung und Wiederherstellung 10
1.4.7 Malware und Antivirus-Software 11
1.4.8 Zugangsmanagement 11
1.4.9 Feststellen von Angriffen 12
1.4.10 Mitarbeiterschulungen 12
1.4.11 Konfigurationsmanagement 13

1.4.12 Reaktion auf Zwischen- und Notfälle 13
1.4.13 Überwachung und Protokollierung 14
1.4.14 Cyber-Versicherung 14
1.4.15 Lieferkettensicherheit & OT-Security 15
1.5 Kontinuierliche Verbesserung 15
1.6 Auswahl von Cybersicherheits-Frameworks 15
1.7 Anlagen zu Cyber-Security Grundschutz für KMU 16
1.7.1 Anlage 1: Projektzeitplan Vorschlag 16
1.7.2 Anlage 2: Inventarisierungslisten Muster 17
Kritikalitätsskala 18

2 Handbuch Supply Chain Cyber-Security für KMU 19

Einleitung 20
2.1 Bedeutung und Relevanz von Supply Chain Cyber-Security für kleine und mittlere Unternehmen 20
2.2 Identifikation von relevanten Supply Chain Partnern 20
2.3 Schritte vor der Umsetzung eines Supply Chain Cyber-Security-Projektes 21
2.3.1 Zielsetzung festlegen 21
2.3.2 Verantwortlichkeiten festlegen 21
2.3.3 Priorisierung der Projektinhalte und Festlegung eines Projektplanes 22
2.4 Vorgehensweise zur Umsetzung eines Supply Chain Cyber-Security-Projektes 22
2.4.1 AP1: Bestehende Supply Chain Partner identifizieren 23
2.4.2 AP2: Supply Chain Partner klassifizieren/bewerten 24
2.4.3 AP3: Risikobasierte Maßnahmen für Supply Chain Partner festlegen 26
2.5 Kontinuierliche Verbesserung 29
2.6 Fazit 30
2.7 Anlagen zu Supply Chain Cyber-Security 31
2.7.1 Anlage 1: Projektzeitplan Vorschlag 31
2.7.2 Anlage 2: Excel Template zur Klassifizierung von SC-Partnern 32
2.7.3 Anlage 3: Fragen zur Bewertung von SC-Partnern 34
2.7.4 Anlage 4: Risikomanagement aufbauen/integrieren 35
2.7.5 Anlage 5: Beispielhafte Vertragsklauseln 42

3 Handbuch Cyber-Security Awareness & Kultur für KMU 50
Einleitung 51
3.1 Der Dreiklang: Skillset – Mindset – Toolset 51
3.2 Security-First-Kultur im Unternehmen verankern 52
3.2.1 Vorbildfunktion der Führungsebene 52
3.2.2 Geteilte Verantwortung – Cybersicherheit ist Teamarbeit 52
3.2.3 Investitionen in Schulung und Sensibilisierung – Schulung stärkt die Sicherheit 53
3.2.4 Offene Kommunikations- und Fehlerkultur 53
3.2.5 Dynamische Anpassungsfähigkeit – Sicherheit braucht ständige Anpassung 53
3.3 Zero-Trust: Sicherheit durch konsequentes Misstrauen 54
3.3.1 Strikte Identitätsprüfung – jeder Zugriff wird überprüft 54
3.3.2 Prinzip der minimalen Rechtevergabe (Least Privilege) 54
3.3.3 Kontinuierliche Überwachung und Analyse 55
3.3.4 Mikrosegmentierung 55
3.3.5 Sichere Endgeräte und Zero-Trust-Network-Access 55
3.4 Praxisfokus: Serious Games als Schulungstool 56
3.5 Fazit: Der Weg zur sicheren Unternehmenskultur 56
3.6 Anlage: Serious Games als Schulungstool 57
4 Handbuch Cyber-Notfallkonzept für KMU 58
Einleitung 59
4.1 Grundlagen: Was ist ein Cyber-Notfall? 60
4.1.1 Definition Cyber-Notfall 60
4.1.2 Typische Bedrohungsszenarien 60
4.1.3 Auswirkungen eines Cyber-Notfalls auf KMU 60
4.2 Bestandteile des Cyber-Notfallkonzepts 61
4.2.1 Vorbereitung: „Nach dem Vorfall ist vor dem Vorfall“ 61
4.2.2 Bereitschaft: Reaktionsfähigkeit sicherstellen 63
4.2.3 Bewältigung: Incident Response Plan 64
4.2.4 Nachbereitung: Optimierung des Notfallkonzepts 68
4.3 Checklisten & Vorlagen 69
4.3.1 Notfall-Kontaktliste 69
4.3.2 Maßnahmen-Checkliste für KMU 70
4.3.3 Vorlage: Incident Response Plan (IRP) 70

4.4 Fazit & Ausblick 71
4.4.1 Wichtige Erkenntnisse aus dem Handbuch 71
4.4.2 Ausblick und zukünftige Maßnahmen 72
4.4.3 Abschließende Empfehlung 72
4.5 Ressourcen & weiterführende Informationen 72
4.5.1 Wichtige Anlaufstellen und Behörden 72
4.5.2 Kostenlose Tools für Incident Management 73
4.5.3 Standards und Frameworks für Cyber-Resilienz 73
4.5.4 Fazit 74
4.6 Anlage: Cyber-Notfallplan 75

5 Handbuch OT-Security für KMU 84

Einleitung 85
5.1.1 Warum ist OT-Sicherheit für kleine und mittlere Unternehmen wichtig? 85
5.1.2 Was sind die größten Pitfalls? 86
5.2 Schritte vor der Erhöhung der OT-Security-Posture 86
5.2.1 Zielsetzung festlegen 86
5.2.2 Verantwortlichkeiten festlegen 87
5.2.3 Priorisierung der Projektinhalte und Festlegung eines Projektplanes 87
5.3 Vorgehensweise zur Umsetzung eines OT-Security- Projektes 87
5.3.1 Plan: Bestehende OT-Security bewerten und Verbesserungs- 87
potenzial identifizieren 87
5.3.2 Do: Testweise Verbesserung der OT-Security an einem Gerät 95
5.3.3 Check: Überprüfung der Funktionalität 96
5.3.4 Act: Anwendung des Best Practices in allen relevanten Bereichen 96
5.4 Kontinuierliche Verbesserung 96
5.5 Anlage: Projektzeitplan Vorschlag 97

Glossar 98

Begriffe in 1 Cyber-Security Grundschutz für KMU 98
Begriffe in 2 Supply Chain Cyber-Security 100
Begriffe in 4 Cyber-Notfallkonzept für KMU 102
Begriffe in 5 OT-Security für KMU 107

Quellen und weiterführende Literatur 109

Tabellenverzeichnis

Tabelle 1: Überblick über empfohlene Maßnahmen pro Klassifizierungskategorie 28
Tabelle 2: Notfall-Kontaktliste.....69
Tabelle 3: Kritische IT-Systeme 75
Tabelle 4: Notfallteam-Struktur 75
Tabelle 5: Externe Notfallkontakte.....76
Tabelle 6: Incident-Klassifizierung 77
Tabelle 8: Quellen und weiterführende Literatur..... 114

Abbildungsverzeichnis

Abbildung 1: Excel Gantt-Chart Projektzeitplan Handbuch 1 16
Abbildung 2: Inventarisierungsliste Muster Assets 17
Abbildung 3: Inventarisierungsliste Muster Prozess 17
Abbildung 4: Inventarisierungsliste Muster Informationen und Daten 17
Abbildung 5: Inventarisierungslisten Vorschlag Kritikalitätsskala 18
Abbildung 6: Übersicht zur Vorgehensweise bei der Umsetzung eines Supply Chain Cyber-Security-Projekts 22
Abbildung 7: Excel Gantt-Chart Projektzeitplan Handbuch 2 31
Abbildung 8: Excel-Lieferantenklassifizierungstool Tabellenblatt Bewertung Kritikalität 32
Abbildung 9: Excel-Lieferantenklassifizierungstool Tabellenblatt Bewertung Integration 32
Abbildung 10: Excel-Lieferantenklassifizierungstool Tabellenblatt Gesamtbewertung 33
Abbildung 11: Excel-Lieferantenklassifizierungstool Tabellenblatt Umsetzungsmaßnahmen 33
Abbildung 12: Serious Games als Schulungstool 57
Abbildung 14: Grafische Oberfläche von LARS ICS. 92
Abbildung 15: Grafische Oberfläche von CSET am Beispiel des NIST SP 800-82r3-Standards 93
Abbildung 16: Excel Gantt-Chart Projektzeitplan Handbuch 5 97

Abstract

Dieser Best Practice Guide zeigt, wie kleine und mittlere Unternehmen (KMU) ihre Cyber-Resilienz umfassend stärken können, von der technischen Basis über Lieferketten und Unternehmenskultur bis hin zu Notfallmanagement und OT-Security. Da Cyberangriffe zunehmend komplexer werden und menschliches Verhalten weiterhin in über 80 % der Vorfälle eine entscheidende Rolle spielt, reicht technische Absicherung allein nicht aus. Entscheidend ist ein integrierter Ansatz, der Mindset (sicherheitsbewusste Haltung), Skillset (praktisches Wissen und regelmäßige Schulungen) und Toolset (adäquate technische Lösungen) miteinander verbindet.

Der Cyber-Security Grundschutz vermittelt KMU praxisnahe Schritte zur Identifikation des IST-Zustands, zur Priorisierung von Schutzmaßnahmen und zur Einführung eines kontinuierlichen Verbesserungsprozesses nach dem PDCA-Modell. Das Supply Chain Cyber-Security Handbuch verdeutlicht, wie digital vernetzte Lieferketten zu kritischen Angriffspunkten werden können und unterstützt Unternehmen dabei, relevante Partner zu identifizieren, zu klassifizieren und risikobasierte Maßnahmen zu implementieren. Das Awareness- & Kultur-Handbuch zeigt, wie eine „Security-First"-Kultur entsteht, die Cybersicherheit als Teamaufgabe begreift und über Zero-Trust-Prinzipien, klare Verantwortlichkeiten und moderne Lernformate wie Serious Games nachhaltig verankert.

Das Cyber-Notfallkonzept bietet KMU einen strukturierten Leitfaden zur Vorbereitung, Reaktion und Wiederherstellung bei Sicherheitsvorfällen - inklusive Checklisten, Rollenmodellen und Incident-Response-Plänen, um Ausfallzeiten zu minimieren und handlungsfähig zu bleiben. Ergänzend vermittelt das OT-Security Handbuch die Besonderheiten industrieller Systeme und zeigt, wie KMU ihre Produktionsumgebungen schützen können - von der Bewertung kritischer Anlagen über sichere Konfigurationen bis zur schrittweisen Umsetzung praxistauglicher OT-Security-Maßnahmen.

Gemeinsam bilden die fünf Handbücher ein ganzheitliches Rahmenwerk, das KMU befähigt, Cybersicherheit als festen Bestandteil des Arbeitsalltags zu verankern, Risiken entlang der gesamten Wertschöpfungskette zu reduzieren und die eigene Widerstandsfähigkeit gegenüber Cyberbedrohungen systematisch zu erhöhen.

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

1

CYBER-SECURITY GRUNDSCHUTZ FÜR KMU

Leitfaden zur Verbesserung Ihrer Cyber-Security

FH Oberösterreich

Logistikum Challenge Accepted

FH Salzburg

Technische Hochschule Deggendorf THD

universität innsbruck

Universität Passau

Einleitung

Dieses Handbuch bietet einen Leitfaden für die Umsetzung von Cybersicherheitsmaßnahmen im Rahmen des Cyber-Security Grundschutz. Der Cyber-Security Grundschutz soll Unternehmen dabei unterstützen, ihre Cybersicherheitslandschaft im Unternehmen zu etablieren, Cybersicherheit stärker als ganzheitliche Unternehmensaufgabe zu verstehen und schrittweise zu stärken. Es richtet sich besonders an kleine und mittelständische Unternehmen (KMU). Im Handbuch werden die verschiedenen Vorbereitungsschritte auf ein Cyber-Security Projekt kurz vorgestellt und anschließend auf die konkreten Cybersicherheitsmaßnahmen für KMU eingegangen. Das Handbuch ist dabei in mehrere Kapitel gegliedert. Kapitel 1.1 geht kurz auf die Bedeutung von Cyber-Security für KMU im Allgemeinen ein und beleuchtet die Herausforderungen aber auch Chancen des Themas. Kapitel 1.2 steigt dann direkt in die Vorbereitung eigener Cybersicherheitsprojekte und Maßnahmen basierend auf einer Analyse des IST-Zustandes des eigenen Unternehmens ein. Kapitel 1.3 beschreibt die allgemeine Vorgehensweise bei der Umsetzung von Cybersicherheitsprojekten auf Basis der Plan-Do-Check-Act (PDCA) Methode und Kapitel 1.4 beinhaltet eine Zusammenstellung von grundlegenden Cyber-Security Maßnahmen auf Basis von etablierten Standards, Interviews und dem Austausch mit Experten. Kapitel 1.5 befasst sich mit der Notwendigkeit, Cybersicherheit nicht als einmalige Aktivität, sondern als kontinuierlichen Verbesserungsprozess zu verstehen. Abgeschlossen wird das Handbuch mit einer Auflistung von etablierten Standards in Kapitel 1.6, sowie weiteren hilfreichen Quellen.

1.1 Bedeutung von Cyber-Security für KMU

Die fortschreitende Verknüpfung und Digitalisierung von Unternehmensprozessen und Lieferketten bewirkt, dass kleine und mittelständische Unternehmen immer effizienter vernetzt sind, Waren und Informationen im eigenen Unternehmen und mit anderen Unternehmen austauschen und Geschäftsprozesse digitalisieren und automatisieren. Dies führt zu einer gesteigerten Geschäftseffizienz, aber eröffnet gleichzeitig auch viele Möglichkeiten für Cyberangriffe. Cyberangriffe können dabei besonders für KMU gefährlich sein, da schon kurze Unterbrechungen in unternehmenskritischen Abläufen zu großen finanziellen Schäden, Imageverlust und sogar zum Konkurs des Unternehmens führen können. KMU sind dabei oftmals besonders anfällig, da sie aufgrund ihrer kleinen und schlanken Strukturen über weniger Ressourcen für die Cybersicherheit verfügen. Sie können sich den Luxus eines dedizierten Cybersicherheitsbeauftragten nicht leisten. Dies führt häufig dazu, dass in diesen Unternehmen weniger Fachwissen über Cybersicherheit vorhanden ist, was sie zu einer leichten Beute für Angreifer macht. Die Liste der Cyber-Angriffe ist dabei lang und neue Angriffe werden tagtäglich aufgedeckt.

KMU sollten daher ihre Cybersicherheit gezielt stärken, um sich selbst und ihre Geschäftspartner vor Schaden zu bewahren. Ein kompetenter Umgang mit dem Thema Cybersicherheit kann dabei wesentlich dazu beitragen, Angriffen vorzubeugen und Ausfallzeiten bei Cyberangriffen zu verkürzen. Dadurch kann die Wettbewerbsfähigkeit der Unternehmen gestärkt und erhalten werden.

1.1.1 Was sind die größten Herausforderungen und Chancen?

Eine der größten Herausforderungen für KMU sind die oft sehr begrenzten Ressourcen und in einigen Fällen auch das fehlende Fachwissen in diesem Bereich. Aufgrund ihrer oft schlanken und kleinen Unternehmensstrukturen sind die Ressourcen für Cybersicherheit begrenzt und die Unternehmen können häufig nicht auf Fachwissen im Bereich der Informationstechnologie und speziell der Cybersicherheit zurückgreifen. Dies erschwert die Entwicklung einer soliden Cybersicherheitsstrategie sowie die Umsetzung und Durchführung von Maßnahmen.

Auf der anderen Seite können die schlanken und flachen Strukturen dieser Unternehmen auch als Chance gesehen werden, da sie Veränderungen hin zu mehr Cybersicherheit begünstigen. KMU können aufgrund ihrer Größe oft flexibler und schneller auf Herausforderungen der Cybersicherheit reagieren als Großunternehmen. Außerdem haben viele KMU bereits einige Ad-hoc-Maßnahmen zur Cybersicherheit umgesetzt, müssen aber noch weiter gehen. Von einem fragmentierten Ansatz hin zu einer koordinierten Gesamtstrategie für Cybersicherheit. Eine gut aufgestellte Cybersicherheit kann auch als Wettbewerbsvorteil im Rahmen von Regulierung und Wettbewerb dienen, da insbesondere Initiativen wie der Cyber Resilience Act und die NIS 2 Richtlinie der Europäischen Union (siehe 4.5.3) die Cybersicherheit auch in kleinen und mittleren Unternehmen in den Fokus rücken.

Zur Unterstützung dieses Ansatzes ist eine solide Wissensbasis und Umsetzungsstrategie von Vorteil.

1.2 Schritte vor der Umsetzung eines Cyber-Security-Projektes

Die erfolgreiche Umsetzung eines jeden Projektes erfordert eine klare Zielsetzung vor Beginn eines solchen Projektes. Da die Anforderungen je nach Unternehmen, Branche und regulatorischen Vorgaben variieren, sollten die Projektinhalte flexibel an die individuellen Bedürfnisse angepasst werden. Die folgenden Überlegungen helfen, diese Aspekte zielgerichtet zu strukturieren und eine fundierte Basis für ein Cybersicherheits-Projekt zu schaffen.

1.2.1 IST-Zustand identifizieren

Die Basis für alle Cybersicherheitsbestreben bildet eine fundierte und gründliche Analyse und Bestandsaufnahme des IST-Zustandes im Unternehmen. Dies beinhaltet sich einen Überblick über unter anderem die folgenden Themenfelder zu verschaffen:

1. **Informationen und Daten**
2. **Inventarisierung von Hardware und Software-Assets**
3. **Unternehmensprozesse und Datenverarbeitung**
4. **Wissensstand im Bereich der Cybersicherheit**
5. **Bisher umgesetzte Cybersicherheitsmaßnahmen**
6. **Definition von kritischen Unternehmensprozessen und Assets**

Als Hilfestellung steht Ihnen eine Excel Muster_Prozess_Inventar_Listen als Referenz und Startpunkt für Ihre eigenen Inventarisierungsaktivitäten zur Verfügung. Abbildungen hierzu finden Sie in Anlage 1.7.2.

1.2.1.1 Informationen und Daten

Ermitteln Sie, welche Informationen im Unternehmen im Umlauf sind. Es gibt dabei viele verschiedene Arten von Informationen, die unterschiedlich gehandhabt werden müssen, z. B. öffentliche Informationen, persönliche Daten, Kundendaten, Produktionsdaten, etc. Besonderes Augenmerk sollte auf sensible Daten im Bezug zu kritischen Unternehmensprozessen und Kundendaten gelegt werden.

1.2.1.2 Inventarisierung von Hardware und Software-Assets

Eine vollständige Inventarliste von verwendeter Hardware und Software im Unternehmen erleichtert die Auswahl und Priorisierung von Maßnahmen anhand der vorhandenen Strukturen und Assets. Hierbei sollte ein Augenmerk auf möglicherweise veraltete und nicht mehr unterstützte Hardware und Software gelegt werden, da diese keine Sicherheitsupdates und Patches von Hersteller mehr erhalten. Inventarlisten können sowohl physisch wie auch digital geführt werden, wobei bei einer digitalen Speicherung der Zugriff im Notfall sichergestellt werden sollte.

1.2.1.3 Unternehmensprozesse und Datenverarbeitung

Verschaffen Sie sich einen Überblick über die verschiedenen Produktions- und Verwaltungsprozesse sowie die Datenflüsse innerhalb und außerhalb des Unternehmens. Achten Sie dabei auf die unterschiedlichen Informationen, die in den jeweiligen Prozessen benötigt, verarbeitet und weitergegeben werden. Von besonderer Bedeutung sind die Datenflüsse über die Unternehmensgrenzen hinweg (Internetschnittstellen, Schnittstellen zu Dienstleistern und Kunden etc.).

1.2.1.4 Wissensstand im Bereich der Cybersicherheit

Finden Sie heraus, wie es um das Wissen über Cybersicherheit im Unternehmen bestellt ist. Dies kann über Rücksprache mit den verschiedenen Unternehmensparteien wie der IT-Abteilung, Produktion, etc. geschehen. Sollte nur wenig Expertise vorhanden sein, kann es sich lohnen, sich vorab grundlegend über das Thema Cybersicherheit zu informieren. Viele Regierungen und Organisationen bieten hierzu Materialien an (z.B. BSI, ENISA, NIST, etc.). Auch die verschiedenen Leitfäden des CySeReS-KMU Projekts bieten hier gebündelte Informationen. Darüber hinaus werden zahlreiche Beratungen und Förderungen zum Thema Cybersicherheit angeboten. Es kann sich lohnen, sich hier einen Überblick zu verschaffen. Beispielsweise bietet die österreichische Regierung verschiedene Beratungsangebote und Förderungen an.[1] Weitere hilfreiche Informationsquellen finden Sie in Kapitel 1.6 und den Quellen.

1.2.1.5 Bisher umgesetzte Cybersicherheitsmaßnahmen

Bei der Analyse des Ist-Zustandes im Unternehmen sollten auch bereits geplante und umgesetzte Cybersicherheitsmaßnahmen berücksichtigt und dokumentiert werden. Dies hilft später bei der Entwicklung und Umsetzung einer umfassenderen Cybersicherheitsstrategie für das Unternehmen und sollte auch bei der Priorisierung von Maßnahmen im Rahmen der Projektplanung berücksichtigt werden.

1.2.1.6 Definition von kritischen Unternehmensprozessen und Assets

Die im Rahmen der IST-Zustand Analyse des Unternehmens gesammelten Informationen, Inventarlisten und Prozessaufstellung werden zur Definition von kritischen Unternehmensprozessen und Assets herangezogen. Dabei sollten die Prozesse und Assets in verschiedene Kritikalitätslevel eingestuft werden (z.B. niedrig, mittel, hoch) basierend auf den Auswirkungen bei einem Ausfall (siehe 4.1.3). Grundlage hierfür ist im Wesentlichen eine Risikobewertung der einzelnen Assets und Prozesse auf Basis der zu erwartenden negativen Auswirkungen im Falle eines Ausfalls.

Die im Verlauf der IST-Zustandsanalyse gesammelten Informationen, Inventarlisten und Risikobewertungen bilden die unerlässliche Basis für die weitere Planung und Umsetzung eines Cybersicherheits-Projektes.

[1] https://www.onlinesicherheit.gv.at/Services/News/KMU-Beratung-Foerderungen-Cybersicherheit.html

1.2.2 Zielsetzung festlegen

Als nächsten Schritt sollten klare Ziele für das Cybersicherheitsprojekt definiert werden, da die Projektinhalte variabel an die eigenen Bedürfnisse angepasst werden können. Folgende Überlegungen können dabei hilfreich sein:

- **Ziele definieren:** Was soll erreicht werden? Welche Schutzziele sollen erreicht werden?
- **Erforderliche Standards prüfen:** Strebt das Unternehmen eine Zertifizierung oder die Einhaltung einer Norm an? Müssen gesetzliche Vorschriften eingehalten werden? Einen Überblick über geeignete Regularien findet sich in Abschnitt 1.6.
- **Ressourcen planen:** Wie viele personelle und finanzielle Ressourcen stehen für das Projekt zur Verfügung? Welche Daten liegen bereits zum Thema Cybersicherheit und der Unternehmensinfrastruktur vor?
- **Interne Kooperation und Abstimmung**
  Wer ist/sollte in das Projekt involviert sein? Hierbei sollte darauf geachtet werden, verschiedene Ansprechpartner in die Planung und Abstimmung mit einzubeziehen (z.B. nicht nur das Fachpersonal, sondern auch Personal, welches in die Prozesse involviert ist). Diese können oftmals wertvolle Einblicke in die bisherigen Arbeitsabläufe und Hürden für das geplante Projekt beitragen.
- **Zeitrahmen festlegen:** Liegt der Schwerpunkt auf kurz- oder langfristigen Projektinhalten? Wie schnell sollen Resultate sichtbar sein, bzw. können sie sichtbar werden?

1.2.3 Verantwortlichkeiten festlegen

Ein oder zwei zentrale Ansprechpartner im Unternehmen sollten für die Umsetzung der Cybersicherheitsmaßnahmen verantwortlich sein. Bei der Auswahl dieser Personen sollte darauf geachtet werden, dass sie mindestens ein grundlegendes Verständnis von Cybersicherheit haben (siehe 2.3.2).

1.2.4 Priorisierung der Projektinhalte und Festlegung eines Projektplanes

Bevor mit der Umsetzung der im Handbuch beschriebenen Inhalte begonnen werden kann, ist eine Priorisierung und strukturierte Planung auf Basis der Projektziele erforderlich.
Als Hilfestellung steht Ihnen ein anpassbares Gantt-Diagramm zur Verfügung, das die in Abschnitt 1.3 beschriebene Vorgehensweise sowie eine grobe Aufwandsschätzung bereits enthält. Es soll Ihnen helfen, die Projektinhalte vor Projektbeginn individuell auf Ihr Unternehmen abzustimmen und zu priorisieren. Es sollte während der Projektlaufzeit regelmäßig aktualisiert werden, um den Projektfortschritt nachvollziehbar zu dokumentieren. Weitere Informationen finden Sie in Anhang 1.7.1 und den beigelegten Excel-tabellen.

1.3 Vorgehensweise zur Umsetzung eines Cyber-Security Projektes

Dieses Handbuch bietet vier Phasen zur Umsetzung von Maßnahmen im Bereich Cyber-Security. Diese sind an den Plan-Do-Check-Act-Zyklus (PDCA) angelehnt und daher nicht in der Reihenfolge veränderbar. Jedoch kann frei gewählt werden, in welcher Reihenfolge die Maßnahmen oder Best Practices implementiert werden sollen. Der PDCA-Zyklus kann und sollte dabei regelmäßig überprüft und gegebenenfalls wiederholt werden, da sich die Cybersicherheitsanforderungen laufend weiterentwickeln.

1.3.1 Plan: Unternehmensinfrastruktur und Cybersicherheits-maßnahmen analysieren

In der Planungsphase ist es wichtig, sich wie bereits genauer in Kapitel 1.2 der Projektvorbereitung beschrieben, den IST-Zustand der Unternehmens-Cybersicherheit zu dokumentieren und zu analysieren. Hierdurch entsteht ein Gesamtüberblick über die vorhandenen Strukturen und Cybersicherheitsmaßnahmen, welcher genutzt wird, um das weitere Projektvorgehen zu definieren und die Priorisierung von Maßnahmen festzulegen. Die somit etablierten oder aktualisierten Informationen bezüglich Asset Inventarlisten, Prozessabläufen und bereits umgesetzten Cybersicherheitsmaßnahmen werden als Basis für die Kritikalitätsbewertung (siehe 1.2.1.6) und Zielsetzung genutzt (siehe 1.2.2) und bildet die Grundlage für die weitere Projektumsetzung.

Die Priorisierung von Maßnahmen erfolgt danach anhand der Kritikalität von Assets für die Unternehmensinternen Prozesse und Wertschöpfungsabläufe. Das CySeRes-KMU Projekt hat in Kapitel 1.4 eine Übersicht über die KMU Grundschutz Best Practices auf Basis von Praxisinput und literarischen Quellen zusammengestellt. Diese basieren auf etablierten Standards (z.B. NIST, ENISA, BSI, etc.), Interviews und dem Austausch mit Experten.

1.3.2 Do: Umsetzung von geplanten Cybersicherheitsmaßnahmen

Nachdem der Projektrahmen festgelegt und die Sicherheitsziele und -Maßnahmen definiert wurden, kann mit der Umsetzung der Maßnahmen begonnen werden. Dabei kann auf die Standards und Maßnahmen aus Kapitel 1.4 zurückgegriffen werden. In diesem Schritt muss die konkrete Umsetzung und Implementierung der Maßnahmen an die eigene Unternehmensinfrastruktur und die vorhandene Systemlandschaft angepasst werden. Dabei ist es oft sinnvoll, in kleinen, inkrementellen Schritten vorzugehen, da eine abrupte Umstellung von vielen Einzelmaßnahmen erfahrungsgemäß zu Problemen führen kann. Durch die kontinuierliche Umsetzung kleinerer Maßnahmenpakete kann die Umsetzung reibungsloser erfolgen. Die Umsetzung von Maßnahmen sollte dabei fortlaufend mit dem involvierten Fach- und Prozesspersonal abgestimmt werden.

1.3.3 Check: Überprüfung der Sicherheitsmaßnahmen

Anschließend an die Umsetzung von Cybersicherheitsmaßnahmen sollte deren korrekte Funktionalität und / oder Effekt auf Arbeitsabläufe und das Sicherheitslevel überprüft werden. Hierbei sollte darauf geachtet werden, dass die Arbeitsabläufe weiterhin reibungslos funktionieren und keine Informationen irrtümlicherweise verloren gehen oder abgewandelt werden. Diese Phase kann durchaus mehrere Wochen dauern, da so viele Daten wie möglich über die neuen Prozessabläufe und Auswirkung der neuen Sicherheitsmaßnahme gesammelt werden sollten (vor allem in Richtung Zuverlässigkeit, Schutzwirkung und reibungsloser Abläufe).

1.3.4 Act: Anpassen

Im Anschluss an die Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen aus dem vorherigen Prozessschritt sollte abschließend überprüft werden, ob die Schutz- und Umsetzungsziele wie gewünscht erreicht wurden. Ist dies der Fall, können weitere Verbesserungsmaßnahmen eingeleitet werden. Wurden Schutzziele nicht erreicht und/oder Prozesse und Abläufe im Rahmen der Umsetzung gestört, sollte mit Korrekturmaßnahmen und weiteren Verbesserungen reagiert werden, um eine reibungslose Integration der Maßnahmen in die Unternehmensprozesse zu erreichen.

1.4 Cyber-Security Grundschutz Maßnahmen

In diesem Kapitel werden die grundlegenden Basismaßnahmen für Cyber-Security kurz vorgestellt. Es dient besonders zur Bewertung und Identifikation von Verbesserungspotentialen im eigenen Unternehmen und kann für die Planung und Durchführung von Maßnahmen zur Etablierung eines gesamtheitlichen Cybersicherheitskonzeptes im Unternehmen herangezogen werden. Die Maßnahmen sind immer in eine „Hauptmaßnahme" (siehe 1.4.1 Zugangskontrolle) mit mehreren Aktionsfeldern (siehe 1.4.1.1 Benutzerauthentifizierung, 1.4.1.2, etc.) zur Umsetzung gegliedert. Dies soll dabei helfen, über die Hauptmaßnahmen einen Überblick über die wichtigsten Cybersicherheitsfelder zu erhalten und diese dann im Zuge der Aktionsfelder für die Umsetzung weiter zu konkretisieren. Hierbei muss gesagt werden, dass die Liste keinesfalls allumfassend ist und in jedem Gebiet für sehr fortgeschrittene Unternehmen auch weitere Maßnahmen und Techniken existieren. Aufgrund der begrenzten Ressourcen von KMU sind die „Best Practices" für KMU basierend auf etablierten Standards zusammengefasst. Weiterhin finden Sie eine Auswahl von etablierten Standards zu diesem Thema in Kapitel 1.6 angehängt und die Quellen am Ende des Dokuments können zusätzlich zur genaueren Umsetzung und Informationsbeschaffung zu dedizierten Maßnahmen konsultiert werden. Die präsentierten Maßnahmen sind dabei „locker" nach Ressourcenaufwand und Komplexität in aufsteigender Reihenfolge angeordnet (leichteste Maßnahmen zuerst). Diese spiegelt die generelle Einschätzung zu Aufwand und Umsetzungskomplexität in KMU wider, kann allerdings aufgrund von verschiedenen Faktoren wie vorhandenen Unternehmens- und Prozessstrukturen und Expertise abweichen.

1.4.1 Zugangskontrolle

Regulieren und kontrollieren Sie den Zugriff auf Ihre Daten, Netzwerke, Dateien und Systeme. Implementieren Sie Mechanismen zur Zugangskontrolle, damit nur befugtes Personal auf Geschäftsdaten zugreifen, Systeme nutzen und Änderungen vornehmen kann. Dies gilt für alle Laptops, Computer, Tablets und Smartphones, Systeme und Netzwerke. Achten Sie besonders auf Home-Office-Accounts und Accounts mit administrativen Rechten, da diese besondere Aufmerksamkeit erfordern.

1.4.1.1 Benutzerauthentifizierung

Schützen Sie alle Ihre Geräte durch eine Form der Benutzerauthentifizierung. Legen Sie ein starkes Passwort (Satzstruktur) für die Bildschirmsperre, eine PIN oder eine andere Authentifizierungsmethode wie Fingerabdruck oder Gesichtserkennung fest. Verwenden Sie Zwei-Faktor-Authentifizierung, wo immer dies möglich ist, insbesondere für Konten mit administrativen Rechten. Diese zusätzliche Authentifizierungsmethode bietet eine weitere Sicherheitsebene.

1.4.1.2 Least-Privilege-Prinzip

Geben Sie jedem Benutzer nur die minimalen Zugriffsrechte, die er für seine Arbeit benötigt (siehe 3.3.2). Schränken Sie außerdem administrative Rechte so weit wie möglich ein und schützen Sie administrative Konten immer zusätzlich durch eine mehrstufige Authentifizierung. Achten Sie darauf, dass Konten und Passwörter nicht von mehreren Mitarbeitern gemeinsam genutzt werden.

1.4.1.3 Passwortrichtlinie

Erstellen Sie eine konsistente Passwortrichtlinie, die die allgemeinen Anforderungen an Passwörter festlegt (Länge, Sonderzeichen, Regeln für die Wiederverwendung, Passwortmanager und Intervalle für Passwortänderungen). Stellen Sie sicher, dass Passwörter immer geändert werden, wenn der Verdacht besteht, dass ein Konto kompromittiert wurde.

1.4.1.4 Verschlüsselung

Verwenden Sie anerkannte kryptografische Methoden, um alle sensiblen Geschäftsdaten, E-Mails und Dokumente zu verschlüsseln. Dies gilt auch für Speicherlaufwerke, Sicherungskopien, mobile Geräte und alle Formen des Datenaustausch. Achten Sie darauf, Kodierungsschlüssel niemals über dieselbe Kommunikationsmethode auszutauschen.

1.4.1.5 Physische Zugangskontrolle

Verhindern Sie, dass Unbefugte Zugang zu Ihren Einrichtungen und Geräten erhalten. Schützen Sie alle Geräte durch Bildschirmsperren oder andere Sperrmechanismen.

1.4.1.6 Inventarisierung von Hardware und Software

Inventarisieren Sie alle verwendeten Assets und Software im Unternehmen. Stellen Sie sicher, dass unbekannte oder unautorisierte Assets und Software isoliert und aus dem Netzwerk entfernt werden.

1.4.1.7 Trennung von Geräten für Private und Geschäftliche Nutzung

Führen Sie keine persönlichen Aktivitäten wie Chats, E-Mails usw. auf Ihrem Geschäftsgerät durch und umgekehrt. Wenn Sie ein Gerät zur Ausführung anderer Aufgaben verwenden, stellen Sie sicher, dass alle geschäftlichen Daten von den persönlichen Daten getrennt und verschlüsselt sind.

1.4.2 Sicherung des Unternehmensumfelds

Erlauben Sie nur autorisierten Personen den Zugang zu Ihrem Unternehmen. Verhindern Sie, dass unbefugte oder unbekannte Personen oder Software in Ihre Geschäftsumgebung eindringen.

1.4.2.1 Mehrstufiger Schutz

Verwenden Sie Proxys, Firewalls, VPNs und Filter, um Ihr internes Netzwerk vor externen Bedrohungen zu schützen. Verhindern Sie die Kommunikation mit unbekannten und bösartigen Websites durch White- und Blacklisting und lassen Sie nur vertrauenswürdige und autorisierte Protokolle die Netzwerkgrenzen überschreiten. Darüber hinaus wird empfohlen, eine DNS-Firewall-Lösung (Domain Name System) zu implementieren, um die Verbindung zu bekannten bösartigen Webdomänen zu verhindern.

1.4.2.2 WLAN sichern

Sichern Sie Ihr WLAN, indem Sie Standardpasswörter ändern und den Sicherheitsstandard WPA 2 oder höher verwenden. Trennen Sie Ihr WLAN durch eine Firewall vom Rest des internen Netzwerks. Wenn Besuchern ein öffentlicher WLAN-Zugang geboten wird, darf dieser nicht mit dem internen Netzwerk und anderen Systemen der Organisation verbunden sein. Inventarisieren Sie die Zugangspunkte und Geräte des Netzwerkes und verhindern Sie, dass nicht autorisierte Geräte Zugang zum Netzwerk erhalten.

1.4.2.3 Kontrolle von mobilen Geräten und Hardware

Unbekannte Hardware darf nicht in den Unternehmensbereich gelangen. Verhindern Sie, dass unbekannte Hardware beim Einstecken automatisch Aktivitäten ausführt, indem Sie die Autostart-Funktion deaktivieren, und informieren Sie Ihre Mitarbeiter über die Risiken, damit diese Hardware gar nicht erst verbunden wird. Untersagen Sie die gemeinsame Nutzung von USB-Sticks und externen Festplatten für private und geschäftliche Zwecke.

1.4.2.4 Physische Zugangskontrolle

Unbefugte Personen sollten nicht in der Lage sein, Ihre Büroräume ohne Kontrolle oder Befragung zu betreten. Dazu gehört auch die Überwachung von Wartungsarbeiten und externen Mitarbeitern, um böswillige Aktivitäten zu verhindern. Sperren Sie Ihre Computerbildschirme und andere Geräte, wenn Sie abwesend sind, um zu verhindern, dass andere Personen unbefugt auf Informationen zugreifen können.

1.4.3 Sicherheitsbewusstsein

Sicherheitsbewusstsein und aktuelles Wissen über Bedrohungen und Angriffsmuster sind wichtige Bestandteile für Ihre Informationssicherheit. Stellen Sie Ihren Mitarbeitern aktuelle Informationen über Sicherheitsbedrohungen und das Vorgehen bei Vorfällen zur Verfügung, um das Sicherheitsbewusstsein zu schärfen (siehe 3.2).

1.4.3.1 Sensibilisierung für Sicherheitsfragen

Versorgen Sie Ihre Mitarbeiterinnen und Mitarbeiter mit aktuellen Informationen über Sicherheitsbedrohungen und Angriffsmuster wie Malware und Phishing-E-Mails. Idealerweise wird dieser Prozess im Rahmen des Onboardings für neue Mitarbeiter gestartet und anschließend über E-Mails, Broschüren oder auch spezielle Informationsveranstaltungen in die tägliche Geschäftskommunikation integriert. Machen Sie das Thema Sicherheit zu einem Teil Ihres Geschäftsalltags. Überprüfen und aktualisieren Sie die Informationen regelmäßig.

1.4.3.2 Einführung von Sicherheitsrichtlinien und -verfahren

Definieren Sie anerkannte Geschäftspraktiken und -erwartungen, an die sich die Mitarbeiter halten können. Welche Regeln gelten fürs Home-Office, wie ist mit sensiblen Kundendaten umzugehen und wo kann man sich bei Fragen Hilfe holen? Stellen Sie Informationen und Anleitungen zur Verfügung wie Sicherheitsvorfälle erkannt und wie darauf reagiert werden muss. Einer der wichtigsten Aspekte ist es, klar zu kommunizieren, was im Falle eines Sicherheitsverstoßes zu tun ist und wer die Ansprechpartner sind. Beispielsweise hat das Bundesamt für Sicherheit in der Informationstechnik eine kurze Guideline.[2]

1.4.4 Sichere Konfiguration

Stellen Sie sicher, dass alle Geräte, Systeme und Software ordnungsgemäß konfiguriert sind. Dazu gehören die Änderung von Standardpasswörtern, die Überprüfung auf Unternehmens- und Software-Updates, die Aktivierung oder Installation von Anti-Malware-Software sowie die Überwachung und Protokollierung der Aktivitäten.

1.4.4.1 Authentifizierung einrichten

Verwenden Sie eine Passphrase oder eine andere Authentifizierungsmethode (Fingerabdruck, PIN, etc.), um das Gerät vor unbefugter Nutzung zu schützen. Dazu gehört auch, alle Standardpasswörter in neuen Geräten und neuer Software zu ändern, da diese oft leicht geknackt werden können.

1.4.4.2 Anti-Malware-Software und Logs

Installieren oder aktivieren Sie Anti-Malware-Lösungen und System-Firewalls, wo immer dies möglich ist. Auf vielen Geräten können Sie vorinstallierte Lösungen verwenden. Achten Sie jedoch darauf, diese richtig zu konfigurieren, da die Standardkonfigurationen der Hersteller oft eher auf Benutzerfreundlichkeit als auf Sicherheit ausgerichtet sind. Aktivieren Sie auch Protokollierungsfunktionen. Dies kann Ihnen helfen, verdächtige Aktivitäten zu erkennen und den Diagnose- und Wiederherstellungsprozess im Falle eines Sicherheitsvorfalls beschleunigen (siehe 1.4.12.1).

[2] https://www.bsi.bund.de/dok/13824824

1.4.4.3 Deaktivieren nicht benötigter Funktionen

Deaktivieren Sie alle nicht benötigten Funktionen und Anwendungen auf Ihren Geräten, da diese ein Sicherheitsrisiko darstellen können.

1.4.5 Patches und Updates

Halten Sie alle Geräte und Software in Ihrem Unternehmen auf dem neuesten Stand. Dazu gehört die regelmäßige Überprüfung auf neue Updates und deren Installation, die Sicherstellung des kontinuierlichen Herstellersupport und eine Routine für die Einrichtung von neuen Geräten.

1.4.5.1 Installieren Sie Updates so schnell wie möglich

Prüfen Sie regelmäßig, ob es neue Updates gibt, und installieren Sie diese entweder manuell oder fügen Sie sie den automatischen Update-Prozessen hinzu. Es kann Sinn ergeben, einen bestimmtes Zeitfenster (einen halben / einen Tag im Monat) für den Updateprozess und die Patchaufspielung zu reservieren.

1.4.5.2 Automatische Updates aktivieren

Aktivieren oder konfigurieren Sie automatische Updates und Patches, wo immer dies möglich ist (siehe Kapitel 5). Viele Geräte und Anwendungen verfügen über eingebaute automatische Patching-Funktionen, die genutzt werden können.

1.4.5.3 Gewährleistung eines kontinuierlichen Supports

Achten Sie darauf, dass Geräte und Software kontinuierlich aktualisiert werden. Geräte, die vom Hersteller nicht mehr unterstützt werden, sollten generell entfernt und durch eine moderne Alternative ersetzt werden. Installieren und warten Sie nur Geräte und Software, die vom Hersteller unterstützt werden.

1.4.6 Datensicherung und Wiederherstellung

Sichern Sie regelmäßig Ihre wichtigen Geschäftsdaten und überprüfen Sie, ob diese korrekt wiederhergestellt werden können. Auf diese Weise können Verluste und Störungen durch Datenverlust aufgrund von Feuer, Diebstahl oder Malware-Angriffen minimiert werden und das Unternehmen schneller in den Normalbetrieb zurückkehren.

1.4.6.1 Identifikation und Sicherung wichtiger Geschäftsinformationen

In der Regel handelt es sich dabei um wichtige Dokumente, Fotos, Systemdaten und vieles mehr. Je nachdem, wie kritisch diese Daten für Ihr Unternehmen sind, sollten Sie das Sicherungsintervall sorgfältig abwägen. Dies kann von täglichen Backups für sensible Daten bis zu monatlichen, vierteljährlichen oder jährlichen Backups für weniger sensible Systeme reichen.

1.4.6.2 Automatische Datensicherung

Aktivieren oder konfigurieren Sie automatische Sicherungen, wo immer dies möglich ist. Viele Geräte und Anwendungen verfügen über eingebaute automatische Sicherungsfunktionen, die genutzt werden können.

1.4.6.3 Backups von der Quelle trennen

Trennen Sie das Backup-Medium von seiner ursprünglichen Quelle. Es darf weder physisch noch über ein Netzwerk angeschlossen bleiben und darf dem Personal während des täglichen Betriebs nicht zugänglich sein. Beispiele hierfür können ausgelagerte Server, Cloud-Lösungen und Festplatten sein.

1.4.6.4 Physische Sicherheit und Datenverschlüsselung

Bewahren Sie eine Kopie der Sicherungskopie an einem anderen physischen Ort auf, idealerweise an einem externen Standort. Dies verhindert einen vollständigen Verlust im Falle eines Brandes, einer Überschwemmung oder anderer physischer Schäden. Verschlüsseln Sie außerdem alle Sicherungskopien, um sie im Falle von Verlust oder Diebstahl zusätzlich zu schützen.

1.4.6.5 Testen der Sicherheitskopien

Führen Sie regelmäßige Tests durch, bei denen eine Stichprobe von Daten auf einem System wiederhergestellt wird, um die Funktionsfähigkeit und Integrität sicherzustellen.

1.4.7 Malware und Antivirus-Software

Installieren Sie Anti-Malware-Software auf allen Geräten. Achten Sie darauf, dass diese stets auf dem neuesten Stand ist.

1.4.7.1 Aktivierung von Anti-Malware-Software

Installieren oder aktivieren Sie auf allen Geräten Anti-Malware-Lösungen, Firewalls und Intrusion-Detektion-Systeme. Häufig ist die Software bereits vom Hersteller vorinstalliert. Vergewissern Sie sich, dass sie sicher konfiguriert ist, und führen Sie regelmäßig Virenscans und vollständige Systemprüfungen durch, um Malware zu erkennen.

1.4.7.2 Kontrolle von Software und Hardware

Ihre Mitarbeiter sollten nur Software aus vom Hersteller genehmigten Shops herunterladen dürfen, um nicht vertrauenswürdige Downloads aus unbekannten Quellen zu vermeiden. Es besteht die Möglichkeit, die Download-Berechtigungen für Benutzerkonten zu entziehen, um das Risiko weiter zu verringern. Schulen Sie Ihre Mitarbeiterinnen und Mitarbeiter, keine unbekannte Hardware wie USB-Sticks anzuschließen und zu verwenden, da diese Schadsoftware enthalten können.

1.4.8 Zugangsmanagement

Das Zugangsmanagement erweitert die Maßnahme 1.4.1 Zugangskontrolle um fortgeschrittenere und aufwendigere Aktionsmaßnahmen.
Führen Sie eine aktive Bestands- und Softwarekontrolle sowie eine Benutzerkontenverwaltung durch. Erstellen Sie eine hierarchische Struktur von Datensicherheitskategorien für verschiedene Vertraulichkeitsstufen und passen Sie die Sicherheitsmaßnahmen dementsprechend an.

1.4.8.1 Accountverwaltung und Überwachung

Behalten Sie die Konten von der Einrichtung bis zur Deaktivierung im Auge. Löschen Sie die Accounts, wenn Mitarbeiter das Unternehmen verlassen. Dies gilt auch für Auftragnehmer und Testaccounts. Deaktivieren Sie Accounts automatisch nach einer bestimmten Zeit der Inaktivität und behalten Sie den Überblick über alle vergebenen Benutzerrechte.

1.4.8.2 Daten klassifizieren und Netzwerke segmentieren

Sortieren Sie Ihre Daten in verschiedene Sicherheitskategorien (z. B. vertraulich, nicht vertraulich usw.) und segmentieren Sie sie entsprechend mit zusätzlichen Sicherheitsmaßnahmen. Segmentieren Sie

auch die verschiedenen Teile des Netzwerks, indem Sie zusätzliche Firewalls oder Proxys einrichten, um laterale Bewegungen innerhalb des Netzwerks zu verhindern. Nur autorisierte Systeme sollten miteinander kommunizieren können. Sperren Sie alle anderen Zugänge.

1.4.8.3 Mobilität absichern

Da mobile Geräte wie Laptops, Smartphones oder Tablets häufig die „Sicherheit" des Unternehmens verlassen, erfordern sie besondere Sorgfalt. Verschlüsseln Sie alle Daten auf den Geräten und schützen Sie sie mit einer Multi-Faktor-Authentifizierung. Verbinden Sie sich nicht mit unbekannten WLAN-Hotspots, da man nie weiß, wer sie wirklich kontrolliert. Deaktivieren Sie die automatische Verbindung zu unbekannten Netzwerken. Nutzen Sie stattdessen Ihr Mobilfunknetz, Tethering oder einen WLAN-Dongle für den Internetzugang. Schränken Sie außerdem die Verwendung von Bluetooth und anderen NFC-Protokollen für den Austausch sensibler Daten ein und verlangen Sie immer die Verwendung eines VPN, wenn Sie remote arbeiten. Schaffen Sie die Möglichkeit, verlorene Geräte aus der Ferne zu orten, zu sperren und zu löschen, um sensible Geschäftsdaten zu schützen. Der Zugriff auf eine Sicherungskopie des Geräts kann hilfreich sein.

1.4.9 Feststellen von Angriffen

Gewähren Sie nur autorisierten Personen Zugang zu Ihrem Unternehmen. Verhindern Sie, dass unbefugte oder unbekannte Personen oder Software in Ihre Geschäftsumgebung eindringen. Überwachen Sie den externen Datenverkehr und entwickeln Sie die Fähigkeit, unbekannte Angreifer aufzuspüren und innerhalb Ihres Netzwerks einzudämmen, um die laterale Bewegung und den durch Angreifer verursachten Schaden zu minimieren.

1.4.9.1 Erkennungssysteme

Konfigurieren Sie ein Überwachungs- und Protokollierungssystem, um den netzwerkübergreifenden Datenverkehr aufzuzeichnen, und verwenden Sie ein netzwerkbasiertes Intrusion Detection System (IDS), um zu verhindern, dass unbefugte und schädliche Software-Zugang zu Ihren internen Netzwerken erhält. Überprüfen Sie die gesammelten Daten regelmäßig auf Anomalien, um Sicherheitsvorfälle zu erkennen.

1.4.9.2 Interne Netzwerksegmentierung

Bewerten und klassifizieren Sie Ihre verschiedenen Datensicherheitsstufen sorgfältig. Segmentieren Sie Ihre internen Netzwerke entsprechend mit Hilfe von Proxys, Firewalls und Intrusion Detection Systemen sowie unterschiedlichen Benutzerzugriffsrechten, um sie gegen laterale Bewegungen von Angreifern abzusichern und sensible Geschäftsdaten zu schützen.

1.4.10 Mitarbeiterschulungen

Sicherheitsübungen und Mitarbeiterschulungen sind ein wichtiger Bestandteil der Informationssicherheit des Unternehmens. Identifizieren Sie die spezifischen Kenntnisse und Fähigkeiten, die Ihre Mitarbeiter benötigen, um ihre Arbeit sicher ausführen zu können, und bieten Sie entsprechende Schulungen und Anleitungen an, um das Verständnis und die Koordination bei einem Sicherheitsvorfall zu fördern.

1.4.10.1 Kennen Sie Ihre Mitarbeiter

Bestimmen Sie die spezifischen Kenntnisse, Fähigkeiten und Fertigkeiten, die für alle funktionalen Rollen in Ihrem Unternehmen erforderlich sind. Beginnen Sie mit den wichtigsten Rollen und arbeiten Sie sich von oben nach unten vor. Identifizieren Sie Wissenslücken und stellen Sie gezielte Ressourcen und Schulungen bereit, um diese zu schließen.

1.4.10.2 Sicherheitsschulungen

Organisieren Sie regelmäßig Schulungen und Szenarien (jährlich bis zu monatlich), um Ihr Personal für relevante Sicherheitsbedrohungen zu sensibilisieren und zu schulen. Dies fördert eine bessere Kommunikation und eine schnellere Reaktion auf Zwischenfälle und kann dazu beitragen, Schwachstellen in der Reaktionskette zu identifizieren.

1.4.11 Konfigurationsmanagement

Entwickeln Sie einen systematischen Ansatz für die Konfiguration und Einrichtung Ihrer Geräte. Dies beinhaltet die Entwicklung eines Standardkonfigurations-Images, das für alle Geräte gilt. Dazu gehört auch die aktive Überwachung aller Sicherheitskonfigurationen, um Abweichungen von der definierten Standardkonfiguration zu erkennen und zu korrigieren.

1.4.11.1 Startkonfiguration

Anstatt die Konfiguration für jedes Gerät manuell zu ändern, sollten Sie ein initiales sicheres Konfigurationssetup entwickeln und dokumentieren, das auf das jeweilige Gerät oder System angewendet wird. Orientieren Sie sich an öffentlich entwickelten und anerkannten Sicherheitsstandards und ergänzen Sie diese, um sie an die Bedürfnisse Ihres Unternehmens anzupassen. Überarbeiten Sie diese regelmäßig.

1.4.11.2 Sicherheitskonfigurationen überwachen

Überwachen Sie alle Sicherheitskonfigurationen durch Konfigurationsmanagement und Änderungsüberwachung, um sicherzustellen, dass eine sichere Konfiguration implementiert und aufrechterhalten wird. Dies kann durch automatisierte Tools erfolgen, die Standardkonfigurationen überprüfen und Änderungen erkennen und dann automatisch darüber informieren.

1.4.12 Reaktion auf Zwischen- und Notfälle

Erstellen Sie einen detaillierten Aktionsplan für Maßnahmen, die bei einem Sicherheitsvorfall zu ergreifen sind. Dies kann bei Bränden, medizinischen Notfällen, Einbrüchen oder Naturkatastrophen der Fall sein. Er sollte Maßnahmen, definierte Rollen, Schulungen und Kommunikation beinhalten, um schnell auf einen Vorfall reagieren zu können. Weitere Informationen hierzu finden Sie auch unter Kapitel 4.

1.4.12.1 Definition eines Sicherheitsvorfalls

Es ist sehr wichtig, klar zu definieren, welche Art von Aktivitäten oder Ereignissen einen Sicherheitsvorfall darstellen und eine Reaktion erfordern. Beispiele hierfür sind Systemausfälle, erhebliche Ausfallzeiten der Unternehmenswebsite und vieles mehr. Dies ist sehr relevant, da jede Reaktion auf einen Sicherheitsvorfall negative Auswirkungen auf den täglichen Betrieb haben kann, z. B. wenn Systeme heruntergefahren, Computer gesperrt oder Informationen aus Sicherheitsgründen an einen Backup-Standort verschoben werden müssen.

1.4.12.2 Rollen und Verantwortlichkeiten

Definition der Verantwortlichkeiten für jede Rolle während des Vorfalls. Dabei kann es sich um Verantwortlichkeiten für die Datenerfassung, die Entscheidungsfindung, rechtliche Verantwortlichkeiten sowie eine allgemeine Kommunikationsstrategie und Koordination handeln. Legen Sie fest, wer für die Durchführung von Aufgaben wie die Meldung des Vorfalls und die Einleitung des Wiederherstellungsprozesses verantwortlich ist und wer Entscheidungen über das weitere Vorgehen nach einem Sicherheitsvorfall trifft. Jede Rolle sollte einem bestimmten Mitarbeiter zugewiesen werden, und für den Fall, dass dieser nicht verfügbar ist, sollte ein Stellvertreter benannt werden.

1.4.12.3 Dokumentation der Verfahren und Reaktionen auf Zwischenfälle

Erstellen Sie ein schriftliches Dokument mit Informationen über den Aktionsplan für Zwischenfälle, Verfahrensbeschreibungen sowie Rollen und Verantwortlichkeiten. Fügen Sie Kontaktinformationen für weitere Anlaufstellen, sowie Strafverfolgungs- und Justizbehörden hinzu, die im Falle eines Zwischenfalls kontaktiert werden müssen. Stellen Sie außerdem sicher, dass der gesamte Reaktionsprozess auf einen Vorfall dokumentiert wird, damit er später analysiert und wertvolle Erkenntnisse zur Prozessverbesserung und Aufarbeitung gewonnen werden können.

1.4.12.4 Schulungen zur Reaktion auf Zwischenfälle durchführen

Trainieren und optimieren Sie die Reaktion auf Zwischenfälle durch spezielle Trainingsszenarien.

1.4.13 Überwachung und Protokollierung

Protokollieren und überwachen Sie Geräte- und Netzwerkaktivitäten, um verdächtige Aktivitäten zu erkennen und Bereiche für Sicherheitsverbesserungen zu identifizieren. Die Protokollierung und Überwachung verbessert die Fähigkeit Ihres Unternehmens, Vorfälle zu erkennen, festzustellen, welche Daten und Systeme angegriffen wurden, und den Untersuchungs- und Wiederherstellungsprozess zu beschleunigen, nachdem ein Sicherheitsvorfall entdeckt wurde.

1.4.13.1 Logging

Aktivieren Sie die Protokollierungsfunktionen auf allen Geräten wie Laptops, Telefonen, Netzwerkgeräten, Firewalls, Antivirensoftware und VPNs. Zeichnen Sie detaillierte Informationen wie Ereignisquelle, Datum, Benutzer, Zeitstempel und andere nützliche Informationen auf. Dies kann Ihrem Unternehmen bei der Erkennung von Anomalien sowie bei der Untersuchung und Wiederherstellung im Falle eines Vorfalls sehr helfen. Sorgen Sie für ausreichende Speicherkapazität für Protokollaktivitäten (mindestens ein Jahr).

1.4.13.2 Regelmäßige Log-Überprüfungen

Sammeln, verwalten und analysieren Sie regelmäßig Log Daten aus allen verfügbaren Quellen. Dies kann bei der Identifizierung von Sicherheitslücken helfen. Die Überprüfung kann manuell durch geschultes Personal für Informationssicherheit erfolgen und/oder durch automatisierte Tools zur Loganalyse unterstützt werden.

1.4.13.3 Überwachung der Systemlandschaft

Überwachen Sie Datenflüsse, Netzwerkverkehr und Asset-Aktivitäten, um unbefugten Zugriff und Systemnutzung zu erkennen. Achten Sie auf Datenströme, die die Außengrenzen Ihres Unternehmens überschreiten. Überwachen Sie auch die Zugriffsrechte von Benutzern und deren Änderungen, insbesondere bei administrativen Konten, da diese ein Indikator für verdächtige Aktivitäten sein können. Beispiele hierfür sind fehlgeschlagene administrative Anmeldungen oder Benutzer, die versuchen, auf Informationen zuzugreifen, ohne über die entsprechenden Rechte zu verfügen.

1.4.14 Cyber-Versicherung

Beschäftigen Sie sich mit der Risikominimierung im Falle eines Cyberangriffs durch den Abschluss einer dedizierten Cyber-Versicherung, da herkömmliche Versicherungsverträge dies oftmals nicht abdecken.

1.4.15 Lieferkettensicherheit & OT-Security

Zwei weitere für KMU relevante Themen sind die Operational Technology-Security (OT) und die Sicherheit der Lieferkette. Hierzu wurde vom CySeReS-KMU Projekt jeweils ein dediziertes Handbuch ausgearbeitet, welches Ihnen hilft, diese Themen im Detail zu verstehen und umzusetzen (siehe Kapitel 2 und 5)

1.5 Kontinuierliche Verbesserung

Die dargestellten Maßnahmen und Umsetzungsschritte auf Basis des PDCA-Zyklus sind nicht als einmalige Umsetzungsanweisung zu verstehen. Vielmehr ist das Thema Cybersicherheit als ein kontinuierlicher Verbesserungs- und Weiterentwicklungsprozess in Unternehmen anzusehen. Die Cybersicherheitslandschaft und die damit verbundenen Bedrohungspotenziale für Unternehmen und ihre Geschäftspartner entwickeln sich ständig weiter. Daher ist eine ständige Neubewertung und Reaktion auf neue Bedrohungen und Angriffsmuster erforderlich. Cybersicherheit ist kein einmaliger Vorgang. Vielmehr erfordert sie kontinuierliche Aktivitäten und Anpassungen, um auf dem neuesten Stand zu bleiben. Aus diesem Grund wurde der Plan-Do-Check-Act-Zyklus, eine iterative Managementmethode zur kontinuierlichen Verbesserung, als Grundlage für dieses Handbuch verwendet. Die in Kapitel 1.3 dargestellten PDCA-Schritte sollten regelmäßig wiederholt, aktualisiert und überprüft werden, um die Wirksamkeit bestehender Maßnahmen weiter zu validieren und die Cybersicherheitsmaßnahmen des Unternehmens an interne Veränderungen sowie neu auftretende Bedrohungen und Sicherheitsanforderungen anzupassen.

1.6 Auswahl von Cybersicherheits-Frameworks

Eine Auswahl von Cybersicherheits-Frameworks, auf denen auch die Maßnahmen in Kapitel 1.4 maßgeblich aufbauen, finden Sie im folgenden Abschnitt:

Cybersicherheit für KMU – TOP 14 Fragen – Broschüre des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit leicht verständlichen Informationen zu den Grundlagen der KMU-Cybersicherheit.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cybersicherheit_KMU.pdf?__blob=publicationFile&v=15

ENISA Cyber-Security Guide for SME – Das Framework der European Union Agency for Cyber-Security (ENISA) stellt 12 Schritte zur Absicherung von KMU vor.
https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Cyber-Security%20guide%20for%20SMEs-online-single_page.pdf

NIST Cyber-Security Framework 2.0: Small Business Quick Starter Guide – eine Zusammenfassung des NIST Cyber-Security Frameworks mit Maßnahmen – besonders für KMU mit keiner bis leicht fortgeschrittener Cybersicherheit.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

THE NIST Cyber-Security Framework (CSF) 2.0 – ein sehr umfangreiches Cybersicherheitsdokument zum Thema Cybersicherheit für Unternehmen (nicht dediziert auf KMU zugeschnitten).
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CIS Critical Security Controls Version 8.1 – Eine detaillierte Zusammenstellung von Cybersicherheitsmaßnahmen für Unternehmen jeder Größe (das Framework unterscheidet zwischen drei verschiedenen Unternehmensklassen – eine davon angelehnt an KMU).
https://www.cisecurity.org/controls/v8-1

ISO 27000 Reihe – eine Reihe von Cybersicherheitszertifizierungen, welche prominent im Cybersicherheitsbereich sind (eher für fortgeschrittene Unternehmen geeignet, welche eine weitreichende Cybersicherheitszertifizierung anstreben oder vorweisen müssen). Hier sind besonders die ISO 27001 / 27002 hervorzuheben.
Weitere hilfreiche Informationen zu verschiedenen Frameworks und Sicherheitsmaßnahmen finden Sie in den Quellen. Viele der hier aufgelisteten Webseiten bieten eine Vielzahl von relevanten und informativen Unterkategorien zu bestimmten Feldern der Cybersicherheit.

1.7 Anlagen zu Cyber-Security Grundschutz für KMU

1.7.1 Anlage 1: Projektzeitplan Vorschlag

Firmenname	Max Mustermann	**Projektanfang:**	7.4.2026
Projektleiter	Max Mustermann	**Projektende (Prognose) :**	16.6.2026

Arbeitspaket		Tasks	Verant-wortl.	Beteiligt	Status	Dauer (Wochen)	Start	Ende
AP0	**PLAN - Vorbereitung**	0.1 IST-Zustand identifizieren	Name	Namen	noch nicht begonnen	1	7.4.26	14.4.26
		0.2 Zielsetzung festlegen	Name	Namen	in Arbeit	0,5	14.4.26	17.4.26
		0.3 Verantwortlichkeiten festlegen	Name	Namen	Abgeschlossen	0,5	17.4.26	21.4.26
		0.4 Priorisierung und Festlegung des Projektplanes	Name	Namen	noch nicht begonnen	1	21.4.26	28.4.26
AP1	**DO - Umsetzung**	1.1 Projekt / Maßnahme	Name	Namen	im Review	1	28.4.26	5.5.26
		1.2 z.B. Sicherung des Unternehmensumfeldes	Name	Namen	in Arbeit	1	5.5.26	12.5.26
		1.3 Einfüllen geplanter Maßnahm.	Name	Namen	noch nicht begonnen	1	12.5.26	19.5.26
AP2	**CHECK - Prüfung**	2.1 Wirkung der Maßnahmen prüfen	Name	Namen		0,5	19.5.26	22.5.26
		2.2 Reibungslose Arbeitsabläufe prüfen	Name	Namen		0,5	22.5.26	26.5.26
AP3	**ACT - Anpassung**	3.1 Finale Überprüfung und Nachsteuern	Name	Namen		1	26.5.26	2.6.26
AP4	**Kontinuierliche Verbeserung**	4.1 Prozess für kontinuierliche Verbesserung einführen	Name	Namen		2	2.6.26	16.6.26

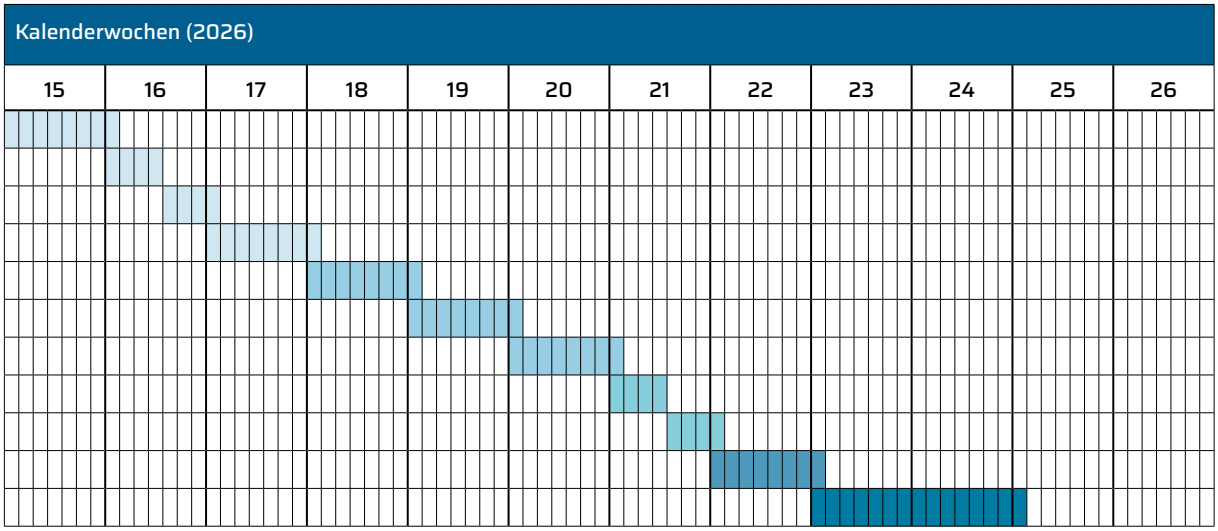


Abbildung 1: Excel Gantt-Chart Projektzeitplan Handbuch 1

1.7.2 Anlage 2: Inventarisierungslisten Muster

Asset_ID	Bezeichnung	Typ	Standort	Betriebs/- System-informationen	Serien-/ Lizenznr.
A001	Dispositionsserver	Server	Raum B15	Windows Server 2022	C17891-4
A002	Produktionsrouter	Router	Produktionshalle West	Firmware v3.2	P2341234
A003	PC Buchhaltung	Arbeitsplatzrechner	Buchhaltung	Windows 10	P2134213

Wartungs-intervall	Updatestatus	Backup Status	Kritikalität	Verantwortlicher	Anmerkung
6 Monate	Updated	Verfügbar	Hoch	Max Mustermann	/
12 Monate	Nicht Updated	Nicht Verfügbar	Kritisch	Petra Musterfrau	Backup erstellen
Keiner	Updated	Verfügbar	Sehr gering	Max Mustermann	/

Abbildung 2: Inventarisierungsliste Muster Assets

Prozess ID	Prozess-name	Beschreibung	Prozess-art	Abhängig-keiten	Kritikalität	Verantwortlicher	Anmer-kung
P001	Disposition	Ablaufprozess Disposition	Intern	P002	Hoch	Max Mustermann	/
P002	Einkauf	Einkaufsprozess	Extern	P00X, P00Y	Gering	Petra Musterfrau	/
P003	Produktion	Produktionsprozess	Intern	P001	Kritisch	Max Mustermann	/

Abbildung 3: Inventarisierungsliste Muster Prozess

Info_ID	Bezeichnung	Typ	Quelle	Backup Status	Kritikalität	Verantwortlicher	Anmer-kung
I001	Kundendaten	Vertraulich	ERP_System	Verfügbar	Hoch	Max Mustermann	/
I002	Produktdaten	Öffentlich	ERP_System	Nicht Verfügbar	Gering	Petra Musterfrau	/
I003	Rechnungsliste	Vertraulich	Buchhaltung	Verfügbar	Kritisch	Max Mustermann	/

Abbildung 4: Inventarisierungsliste Muster Informationen und Daten

Kritikalitätsskala

Stufe	Kritikalität	Beschreibung	Beispiele
1	**Sehr gering**	Geringe Bedeutung – Ausfall oder Beeinträchtigung hat kaum Auswirkung auf den Geschäftsbetrieb oder Sicherheitsanforderungen.	Unkritische Verwaltungssoftware, Peripheriegeräte ohne sensiblen Datenbezug
2	**Gering**	Geringe Auswirkungen – Es besteht ein gewisser Nutzen, jedoch führt ein Ausfall zu kleinen operativen Einschränkungen, die schnell behoben werden können.	Standardbürosoftware, weniger kritische Netzwerkkomponenten
3	**Mittel**	Moderate Bedeutung – Ein Ausfall oder Fehler hat spürbare Auswirkungen auf die Betriebsabläufe und kann zu Verzögerungen führen, jedoch nicht zu einem kompletten Stillstand.	Interne Kommunikationssysteme, Produktionsmaschinen (bei Ausfall nicht sofort kritisch, aber langfristig problematisch)
4	**Hoch**	Hohe Bedeutung – Der Ausfall oder die Beeinträchtigung hat gravierende Auswirkungen auf den Betrieb, führt zu erheblichen Verzögerungen oder Produktionsausfällen und muss mit hoher Priorität behandelt werden.	IT-Systeme, die zentrale Unternehmensfunktionen unterstützen, kritische Prozessschritte in der Produktion
5	**Kritisch**	Höchste Bedeutung – Ein Ausfall oder Sicherheitsvorfall hat unmittelbare, katastrophale Auswirkungen auf den Geschäftsbetrieb, womit der fortlaufende Betrieb ohne schnelle Wiederherstellung nicht gewährleistet ist.	Kernsysteme der IT-Infrastruktur, kritische Prozesskomponenten oder Assets, deren Kompromittierung zu ernsthaften Sicherheitslücken führt.

Dieser Vorschlag für die Kritikalitätsskala kann auch abgeändert werden, es kann z.B. je nach Unternehmensgröße und Komplexität erforderlich sein, diese zu erweitern bzw. auch auf z.B. (Hoch, Mittel, Niedrig) zu reduzieren.

Abbildung 5: Inventarisierungslisten Vorschlag Kritikalitätsskala

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

2

HANDBUCH SUPPLY CHAIN CYBER-SECURITY FÜR KMU

Leitfaden zur Sicherung Ihrer Lieferkette

FH OBERÖSTERREICH

LOGISTIKUM CHALLENGE ACCEPTED

FH Salzburg

TECHNISCHE HOCHSCHULE DEGGENDORF THD

universität innsbruck

UNIVERSITÄT PASSAU

Einleitung

Dieses Handbuch bietet einen Leitfaden für die Umsetzung von Cybersicherheitsmaßnahmen in der Lieferkette, insbesondere für kleine und mittlere Unternehmen (KMU). Es zeigt, wie Unternehmen ihre Lieferketten vor Cyberangriffen schützen können, um finanzielle Schäden, Betriebsunterbrechungen und Vertrauensverlust zu vermeiden.
Das Handbuch ist in mehrere Kapitel gegliedert. Kapitel 2.1 und 2.2 bieten allgemeine Informationen zur Cybersicherheit in der Lieferkette und erläutern die spezifischen Risiken für KMU. Kapitel 2.3 beschreibt die notwendigen Schritte, um ein Projekt aufzusetzen, einschließlich der Festlegung von Zielen, Standards, Ressourcen und Zeitrahmen. Kapitel 2.4 widmet sich der Projektdurchführung und bietet einen strukturierten Ansatz zur Implementierung von Cybersicherheitsmaßnahmen, unterstützt durch ein Excel-Tool zur Bewertung und Priorisierung von Partnern. Kapitel 2.5 befasst sich mit Aktivitäten nach Abschluss des Projekts, um Cybersicherheit als festen Bestandteil in der Organisation zu verankern und kontinuierlich zu verbessern. Kapitel 2.7 enthält einen Anhang mit weiterführenden Informationen und Ressourcen.

2.1 Bedeutung und Relevanz von Supply Chain Cyber-Security für kleine und mittlere Unternehmen

Die Digitalisierung macht Lieferketten effizienter, aber auch anfälliger für Cyberangriffe. Angreifer nutzen Schwachstellen in Unternehmen oder digitale Verbindungen zwischen Supply Chain Partnern (SC-Partnern) aus, um Zugang zu sensiblen Daten und IT-Systemen zu erhalten. Solche Angriffe können zu finanziellen Schäden, Betriebsunterbrechungen, Imageverlust und sogar zum Konkurs von Unternehmen führen. KMU sind besonders anfällig für Cyberangriffe, da sie oft über weniger Ressourcen für Cybersicherheit verfügen. Ein Beispiel ist der Angriff auf einen IT-Dienstleister in Oberösterreich im Jahr 2021, bei dem 34 Unternehmen betroffen waren.

Solche Angriffe führen nicht nur zum Verlust sensibler Daten, sondern auch zum Vertrauensverlust bei Kunden und Partnern. KMU sollten daher ihre Sicherheitsmaßnahmen verstärken und ihre Lieferkette regelmäßig auf Schwachstellen überprüfen. Ein sicherer Umgang mit Cyber-Risiken schützt nicht nur das eigene Unternehmen, sondern die gesamte Lieferkette.

2.2 Identifikation von relevanten Supply Chain Partnern

KMU sind oft Teil komplexer Lieferketten, in denen viele Unternehmen zusammenarbeiten. Um den Überblick zu behalten und Entscheidungen schneller treffen zu können, setzen Unternehmen zunehmend auf digitale Verbindungen. Diese Verbindungen sollten aber auch kritisch hinterfragt werden: Stellen sie ein potenzielles Risiko für mein Unternehmen dar? Viele denken dabei vor allem an Software-Lieferanten – aber auch andere Partner, die Zugriff auf sensible Daten oder Systeme haben, stellen ein Risiko dar. Daher sollten alle relevanten Lieferanten und Dienstleister in die Cybersicherheitsstrategie einbezogen werden. Die wichtigsten Partner, die berücksichtigt werden sollten, sind:

- **Hersteller von IT- und OT-Produkten:** Diese Unternehmen entwerfen, entwickeln und produzieren Soft- und Hardware für die Informationsverarbeitung und die Produktionsautomatisierung. Dabei verwenden sie häufig Komponenten anderer Hersteller. Da ihre Produkte in vielen Branchen eingesetzt werden, spielen sie eine kritische Rolle für die Cybersicherheit und sollten sorgfältig geprüft werden.

- **Dienstleister in Bezug auf IT- und OT-Produkte:** IT- und OT-Dienstleister sind für die Installation, den Betrieb und die Wartung von Systemen zuständig und haben oft weitreichenden Zugriff auf kritische Daten. Sie arbeiten häufig aus der Ferne und sind für viele Unternehmen schwer zu ersetzen, da ein Anbieterwechsel teuer sein kann. Daher ist es wichtig, ihre Sicherheitsstandards regelmäßig zu überprüfen, um Cyber-Risiken zu minimieren.

- **Lieferanten von Rohmaterialien und Halbfertigprodukten sowie sonstige Dienstleister und Kunden:** Diese SC-Partner werden oft von vornherein kategorisch ausgeschlossen, da ihre Produkte keinen direkten Einfluss auf die Systeme des Unternehmens haben. Es ist jedoch zu hinterfragen, wie kritisch die Daten sind, die SC-Partner erhalten und welchen digitalen und physischen Zugang sie zu unternehmensinternen Systemen haben.

2.3 Schritte vor der Umsetzung eines Supply Chain Cyber-Security-Projektes

Die erfolgreiche Umsetzung von Cyber-Security Maßnahmen in der Supply Chain erfordert eine klare Zielsetzung vor Beginn eines solchen Projektes. Da die Anforderungen je nach Unternehmen, Branche und regulatorischen Vorgaben variieren, sollten die Projektinhalte flexibel an die individuellen Bedürfnisse angepasst werden. Die folgenden Überlegungen helfen, diese Aspekte zielgerichtet zu strukturieren und eine fundierte Basis für ein Supply Chain Cyber-Security Projekt zu schaffen.

2.3.1 Zielsetzung festlegen

Zunächst sollten klare Ziele für die Umsetzung von Supply Chain Cyber-Security definiert werden, da die Projektinhalte variabel an die eigenen Bedürfnisse angepasst werden können. Folgende Überlegungen können dabei hilfreich sein

- **Ziele definieren:** Was soll erreicht werden? Soll ein Überblick über die gesamte Supply Chain erstellt werden oder sollte ein bestimmter Teilbereich beleuchtet werden?
- **Erforderliche Standards prüfen:** Strebt das Unternehmen eine Zertifizierung oder die Einhaltung einer Norm an? Müssen gesetzliche Vorschriften, wie z. B. NIS-2, eingehalten werden?
- **Ressourcen planen:** Wie viele personelle und finanzielle Ressourcen stehen für das Projekt zur Verfügung? Welche Daten liegen bereits über die SC-Partner vor?
- **Zeitrahmen festlegen:** Liegt der Schwerpunkt auf kurz- oder langfristigen Projektinhalten? Wie schnell sollen Resultate sichtbar sein bzw. an die SC-Partner kommuniziert werden?

2.3.2 Verantwortlichkeiten festlegen

Ein oder zwei zentrale Ansprechpartner im Unternehmen sollten für die Umsetzung der Cybersicherheitsmaßnahmen verantwortlich sein. Bei der Auswahl dieser Personen sollte darauf geachtet werden, dass sie ein grundlegendes Verständnis von Cybersicherheit und den Prozessen mit SC-Partnern haben. Zur Unterstützung können weitere Rollen integriert werden:

- IT-Verantwortliche und Produktionsleiter: Technische Expertise.
- Einkauf/Vertrieb: Prozesswissen im Umgang mit SC-Partnern.

2.3.3 Priorisierung der Projektinhalte und Festlegung eines Projektplanes

Bevor mit der Umsetzung der inhaltlichen Arbeitspakete (AP) begonnen werden kann, ist eine Priorisierung und strukturierte Planung auf Basis der Projektziele erforderlich.
Als Hilfestellung steht Ihnen ein anpassbares Gantt-Diagramm (siehe 2.7.1) zur Verfügung, das die in Kapitel 2.4 beschriebene Vorgehensweise sowie eine grobe Aufwandsschätzung bereits enthält. Es soll Ihnen helfen, die Projektinhalte vor Projektbeginn individuell auf Ihr Unternehmen abzustimmen und zu priorisieren. Es sollte während der Projektlaufzeit regelmäßig aktualisiert werden, um den Projektfortschritt nachvollziehbar zu dokumentieren.

2.4 Vorgehensweise zur Umsetzung eines Supply Chain Cyber-Security-Projektes

In diesem Kapitel werden nun die inhaltlichen Themen zur Umsetzung eines Supply Chain Cyber-Security Projektes beschrieben. Die folgende Abbildung 6: Übersicht zur Vorgehensweise bei der Umsetzung eines Supply Chain Cyber-Security-Projekts zeigt die vier zentralen AP, die in den folgenden Unterkapiteln näher erläutert werden. Diese Arbeitspakete sind modular aufgebaut, so dass die Reihenfolge beliebig gewählt werden kann. Grundsätzlich wird jedoch empfohlen, die Reihenfolge der APs einzuhalten.

Abbildung 6: Übersicht zur Vorgehensweise bei der Umsetzung eines Supply Chain Cyber-Security-Projekts

2.4.1 AP1: Bestehende Supply Chain Partner identifizieren

Vor der Implementierung von Sicherheitsmaßnahmen muss klar sein, welche SC-Partner als relevant identifiziert wurden. Nicht alle SC-Partner sind im Hinblick auf Cyber-Security relevant. Diese Auswahl bildet die Grundlage für die weiteren Bewertungen und Maßnahmen. Zur Einschätzung der Relevanz können sich Unternehmen folgende Fragen stellen:

- Kann der SC-Partner Einfluss auf meine IT- und OT-Systeme nehmen?
- Hat er teilweisen oder vollständigen Zugriff auf sensible Assets meines Unternehmens (= Vermögenswerte des Unternehmens, wie z. B. Software, Konfigurationen, Daten, Prozesse, Hard-ware, Personen, Räumlichkeiten)

In den folgenden Kapiteln werden drei mögliche Herangehensweisen zur Identifikation von relevanten SC-Partnern für die Cyber-Security beschrieben.

2.4.1.1 Kreditoren- und Debitorenliste als Basis

Die Daten der SC-Partner werden in vielen Fällen bereits über verschiedene Systeme (z. B.: ERP-System) erfasst. Diese Daten können meist in Form einer Kreditorenliste (für Lieferanten) und einer Debitorenliste (für Kunden) exportiert werden. Im Idealfall werden diese Listen dann mit den zuständigen internen Personen besprochen und die obigen Fragen beantwortet. Wenn eine dieser Fragen mit „Ja“ beantwortet wird, sollte diese als relevant eingestuft werden.

Der Vorteil dieser Methodik ist, dass man bereits eine Liste von SC Partnern hat, die man dann auf ihre Cybersicherheitsrelevanz überprüfen kann. Der Nachteil ist, dass die Bewertung der Cybersicherheitsrelevanz auf breiter Basis zu aufwendig sein kann. Dies kann dazu führen, dass häufiger SC-Partner als nicht relevant eingestuft werden, da eine detaillierte Auseinandersetzung mit den einzelnen SC-Partnern fehlt.

2.4.1.2 Assets als Basis

Beim zweiten Ansatz bilden die unternehmensinternen Assets die Grundlage für die Identifikation relevanter SC-Partner. Dabei muss geklärt werden, welche Assets mein Unternehmen benötigt und welche SC-Partner diese bereitstellen bzw. Zugriff darauf haben. Dies ist eine qualitative Erhebung der relevanten SC-Partner und sollte in Zusammenarbeit mit verschiedenen Rollen im Unternehmen erfolgen.

Beispiele für kritische Assets:

- **IT-Systeme:** Server, Netzwerke oder Anwendungen, die mit SC-Partnern geteilt werden.
- **OT-Systeme:** Produktionsmaschinen und Steuerungssoftware, die von externen Dienstleistern gewartet werden (siehe Kapitel 5).
- **Daten:** Kundendaten, Produktdesigns oder technische Spezifikationen, die von Dritten verarbeitet werden.
- **Logistikinfrastruktur:** Transportmanagementsysteme und digitale Lieferkettenplattformen.

Der Vorteil dieser Methode liegt darin, dass bereits eine qualitative Bewertung einfließen kann, die die Einstufung im nächsten Schritt erleichtert. Der Nachteil besteht darin, dass möglicherweise SC-Partner übersehen werden und die Liste nicht vollständig ist.

2.4.1.3 Kombinierter Ansatz

Der kombinierte Ansatz zur Identifikation relevanter SC-Partner nutzt beide zuvor beschriebenen Ansätze, indem sowohl die kritischen Assets betrachtet als auch die Liste der Kreditoren und Debitoren herangezogen werden. Durch die Betrachtung der Assets (siehe 2.4.1.2) können die SC-Partner identifiziert werden, die mit den wichtigsten Assets in Verbindung stehen. Anhand der Kreditoren- und Debitorenliste (siehe 2.4.1.1) wird anschließend überprüft, ob noch relevante SC-Partner übersehen wurden.

2.4.2 AP2: Supply Chain Partner klassifizieren/bewerten

Sobald eine Liste der relevanten SC-Partner vorliegt, kann mit der systematischen Klassifizierung dieser Partner begonnen werden. Hierzu steht ein Excel-Tool in Anhang 2 zur Verfügung, mit dem die Bedeutung und das Risiko der relevanten SC-Partner klassifiziert werden können. Dieses Tool steht zusätzlich unter folgendem Link zum Download zur Verfügung: https://cyseres-kmu.eu/a2_template-zur-sc-partner-klassifizierung-2/

Das Excel-Tool ermöglicht es Unternehmen, ihre SC-Partner anhand vordefinierter Kriterien in den beiden Kategorien Kritikalität und Integration zu bewerten. Diese Kriterien werden durch zwei Hauptfragen in den Arbeitsblättern „Bewertung Kritikalität" und „Bewertung Integration" definiert.

Die Ergebnisse der Bewertung werden als Liste und grafisch in einer Matrix im Tabellenblatt „Gesamtbewertung" dargestellt, um eine schnelle Interpretation und Priorisierung zu ermöglichen. Idealerweise wird die Klassifizierung jährlich überprüft bzw. durchgeführt. In den folgenden Unterkapiteln wird die Anwendung des Excel-Tools kurz beschrieben.

2.4.2.1 Vorbereitung des Excel-Tools

Zunächst müssen die Namen der SC-Partner im Tabellenblatt „Bewertung Kritikalität" eingetragen werden. Im Template befinden sich derzeit vordefinierte Namen mit „SC-Partner 1", „SC-Partner 2", usw. Diese Einträge werden dann automatisch in die weiteren Tabellenblättern übertragen.

Sowohl bei der Bewertung der Kritikalität als auch bei der Bewertung der Integration gibt es weiterführende Fragen, die ausgefüllt werden können. Diese weiterführenden Fragen können die automatische Bewertung noch weiter spezifizieren, der Mehraufwand ist jedoch zu berücksichtigen. Alle weiterführenden Fragen sind im Excel-Tool als ausgeblendete Spalten hinterlegt.

2.4.2.2 Bestimmung der Kritikalität

Nachdem das Excel-Tool vorbereitet wurde, erfolgt die Bewertung der Kritikalität der SC-Partner im Reiter „Bewertung Kritikalität". Bei der Kritikalität wird bestimmt, wie kritisch relevante SC-Partner für mein Unternehmen sind. Beispielhaft dienen dabei unter anderem die folgenden zwei Fragen zur automatischen Berechnung der Kritikalität:

- Wie leicht ist der SC-Partner ersetzbar?
- Wie zeitkritisch sind die Lieferungen/Dienstleistungen für das Unternehmen?

Zu allen Fragen wurden jeweils selbsterklärende Antwortmöglichkeiten hinzugefügt, um die Beantwortung für die Anwender*innen so einfach wie möglich zu gestalten. Aus dieser Beantwortung errechnet sich dann eine automatische Klassifizierung des SC-Partners im Bereich Kritikalität in den vier Stufen:

- Geringe/keine Kritikalität
- Moderate Kritikalität
- Hohe Kritikalität
- Sehr hohe Kritikalität

Zusätzlich zur automatischen Bewertung kann eine manuelle Bewertung durchgeführt werden. Diese hat immer Vorrang vor der automatischen Bewertung. Damit ist sichergestellt, dass der Anwender auch punktuell in die Bewertung eingreifen kann. Diese Entscheidung muss folglich begründet und im Excel-Tool dokumentiert werden, so dass diese Entscheidung nachvollziehbar ist.

2.4.2.3 Bestimmung der Integration

Nachdem die Kritikalität der SC-Partner bewertet wurde, ist der nächste Schritt die Bestimmung ihres Integrationsgrades im Reiter „Bewertung Integration". Die Vorgehensweise hier ist gleich aufgebaut wie die Bewertung der Kritikalität, fokussiert sich jedoch auf die Zusammenarbeit und Einbindung der Partner in unternehmensinternen Abläufen und Systemen. Auch hier werden beispielhaft zwei der zugrunde liegenden Bewertungsfragen aufgeführt:

- Wie sensibel und vertraulich sind die Daten, die Sie mit diesem SC-Partner austauschen?
- Hat der SC-Partner Zugriff bzw. Fernwartungszugriff auf Ihre Systeme?

Die Bewertung dieser Fragen erfolgt nach dem gleichen Schema wie bei der Bestimmung der Kritikalität.

2.4.2.4 Überprüfung der Ergebnisse

Im letzten Schritt der Klassifizierung werden die Ergebnisse der SC-Partner zusammengefasst und übersichtlich dargestellt. Auf dem Tabellenblatt „Gesamtbewertung" bietet das Excel-Tool zwei wesentliche Darstellungsformen: eine grafische Matrix und eine tabellarische Auflistung. Beide Ansätze helfen Unternehmen dabei, die Kritikalität und Integration ihrer Partner auf einen Blick zu erfassen und passende Maßnahmen abzuleiten, die im nächsten Arbeitspaket genauer beschrieben werden.

Die Matrix und ihre Bedeutung

Die Matrix ordnet die Partner basierend auf den Ergebnissen der Kritikalitäts- und Integrationsbewertung in vier Kategorien ein. Diese Kategorien geben Aufschluss über die Relevanz und die damit verbundenen Risiken der jeweiligen Partner:

Unkritische SC-Partner:

- Partner mit geringer Kritikalität und Integration.
- Diese Partner sind nicht entscheidend für die betrieblichen Abläufe.

Geschäftskritische SC-Partner:

- Partner mit hoher Kritikalität, aber geringem Integrationslevel.
- Diese Partner sind essenziell für bestimmte Geschäftsprozesse, jedoch sind sie wenig in die Systeme des Unternehmens eingebunden.

Integrationskritische SC-Partner:

- Partner mit hoher Integration, aber geringerer Kritikalität.
- Diese Partner sind eng in die Systeme eingebunden, tragen jedoch keine geschäftskritische Verantwortung.

Unternehmenskritische SC-Partner:

- Partner mit hoher Kritikalität und Integration.
- Diese Partner stellen die höchste Priorität dar, da ihr Ausfall oder Fehlverhalten gravierende Folgen für das Unternehmen haben könnte.

Die Klassifizierung sollte so erfolgen, dass möglichst viele SC-Partner in die Kategorie der unkritischen Partner fallen und nur wenige in die Kategorie der unternehmenskritischen Partner, um den späteren Aufwand zu minimieren. Falls sehr viele Partner in die Kategorie der unternehmenskritischen Partner fallen, sollten gegebenenfalls zusätzliche Kriterien aufgenommen werden.

2.4.3 AP3: Risikobasierte Maßnahmen für Supply Chain Partner festlegen

Ein effektives Management von Cyberrisiken in der Supply Chain erfordert einen systematischen und risikobasierten Ansatz. Da nicht alle SC-Partner gleich kritisch für das Unternehmen sind, sollten Maßnahmen gezielt auf die jeweilige Risikoklasse abgestimmt werden.

Der risikobasierte Ansatz basiert auf zwei wesentlichen Faktoren: dem potenziellen Schadensausmaß eines Sicherheitsvorfalls und der Eintrittswahrscheinlichkeit. Während ein Angriff auf einen weniger kritischen Partner nur geringe Auswirkungen haben kann, kann eine Sicherheitslücke bei einem unternehmenskritischen Partner schwerwiegende Folgen für die gesamte Lieferkette haben. Daher müssen Maßnahmen je nach Partnerkategorie angepasst und in ihrer Intensität skaliert werden.

Für eine strukturierte Umsetzung werden zunächst unternehmensinterne Maßnahmen vorgestellt, die als Basis für eine sichere Zusammenarbeit mit SC-Partnern dienen. Darauf folgen Maßnahmen, die eine direkte Interaktion mit den Partnern erfordern, um sowohl die Transparenz als auch das Sicherheitsbewusstsein innerhalb der Lieferkette zu erhöhen. Abschließend wird eine Methodik zur Maßnahmenzuordnung auf Basis der Klassifizierung der SC-Partner vorgestellt. Es bildet die Grundlage für eine zielgerichtete und effiziente Umsetzung von Sicherheitsmaßnahmen und ist ebenfalls in das Excel-Tool integriert.

2.4.3.1 Unternehmensinterne Maßnahmen im Umgang mit Supply Chain Partnern

Unternehmensinterne Maßnahmen bilden die Grundlage für eine sichere Zusammenarbeit mit SC-Partnern. Durch präventive Strategien können Risiken minimiert und eine stabile Basis für die Absicherung der Lieferkette geschaffen werden.

Folgende Maßnahmen können ergriffen werden:

- **Kompetenzen aufbauen**
  Aufbau interner, redundanter Kapazitäten für kritische Prozesse,
  um Abhängigkeiten von externen Partnern zu reduzieren –
  durch den Fokus auf eigene Expertise (z. B. Mitarbeiterschulungen),
  Schaffung redundanter Kapazitäten (z. B. Lagerbestände)
  und die Erstellung von Backups.

- **Mehrlieferantenstrategie prüfen**
  Die Beschaffung von Produkten und Dienstleistungen von mehreren SC-Partnern
  verringert das Risiko von Engpässen oder Störungen im Falle eines Cyberangriffs.

- **Need-to-Know Prinzip einführen/überprüfen**
  Beschränkung des Zugriffs auf Daten und Systeme auf das unbedingt Notwendige,
  um sensible/vertrauliche Daten zu schützen und Auswirkungen von Cyberangriffen
  beim SC-Partner auf ein Minimum zu reduzieren. Dies umfasst sowohl physische Zutritte
  als auch digitale Zugriffe. Dies muss regelmäßig überprüft werden.

2.4.3.2 Maßnahmen für die Bewertung von Supply Chain Partnern

Neben unternehmensinternen Maßnahmen sollten auch Maßnahmen ergriffen werden, die die Interaktion mit den SC-Partner fordern, um einerseits Informationen aus erster Hand zu erhalten und andererseits die Awareness zum Thema Cyber-Security beim SC-Partner zu steigern. Folgende Maßnahmen können diesbezüglich gesetzt werden:

- **Verantwortliche benennen**
  Jeder SC-Partner sollte einen Ansprechpartner für Cyber-Security Fragen benennen. Diese Person koordiniert die Sicherheitsanforderungen und dient als Kontaktpunkt für eventuelle Rückfragen. Klare Verantwortlichkeiten verbessern die Zusammenarbeit und fördern die Transparenz.

- **Fragebogen Cyber-Security-Praktiken**
  Unternehmen sollten die Sicherheitspraktiken ihrer Partner punktuell hinterfragen und gemeinsam mögliche Schwachstellen identifizieren. Mögliche Fragen dazu finden sich in 2.7.3 Anlage 3, die als Anregung dienen und je nach Schwerpunkt und Relevanz angepasst werden können. Sie können entweder durch eine Selbstauskunft des SC-Partners oder durch ein Gespräch mit dem SC-Partner vor Ort erhoben werden.

- **Zertifizierungen abfragen**
  Zertifikate wie ISO 27001 oder TISAX belegen, dass die Partner grundlegende Sicherheitsstandards einhalten. Unternehmen sollten gezielt nach solchen Nachweisen fragen, um sicherzustellen, dass die Partner etablierte Cybersicherheitsprotokolle implementiert haben.

- **Zusammenarbeit bei Cyberangriffen klären**
  Ein definiertes Vorgehen im Falle eines Cyber-Angriffs ist entscheidend, um Reaktionszeiten zu minimieren. Unternehmen und Partner sollten im Vorfeld Meldewege und Zuständigkeiten klären, um im Ernstfall effizient handeln zu können.

- **Verträge anpassen**
  Die Aufnahme von Sicherheitsanforderungen in Verträge schafft Rechtsverbindlichkeit und stellt sicher, dass die Partner bestimmte Standards einhalten. Solche vertraglichen Anforderungen können regelmäßige Sicherheitsaudits, die Aktualisierung von IT-Systemen oder die Verpflichtung zur Meldung von Vorfällen umfassen. Eine sofortige Anpassung der Verträge ist jedoch nur in den seltensten Fällen praktikabel. Daher sollte die Vertragslaufzeit überprüft und entschieden werden, ob der Vertrag in den nächsten Jahren neu verhandelt werden kann oder ob der Zeitraum bis dahin für das Unternehmen zu lang ist. Vorschläge für Cybersicherheitsrelevante Vertragsklauseln finden sich unter 2.7.5 Anlage 5.

2.4.3.3 Maßnahmen für Partnerklassifizierung festlegen

Je nach Klassifizierung der SC-Partner sind Standardmaßnahmen abzuleiten, die im Umgang mit ihnen berücksichtigt werden. Dabei gilt: Je höher das Risiko, desto umfangreichere Maßnahmen sind erforderlich. Aus diesem Grund wurde eine Ableitung von Maßnahmen auf Basis der Klassifizierung aus Kapitel 2.4.2 vorgeschlagen, die in das beiliegende Excel-Tool im Tabellenblatt „Umsetzungsmaßnahmen“ integriert wurde (siehe Tabelle 1).

	Unkritische SC-Partner	Geschäftskritische SC-Partner	Integrationskritische SC-Partner	Unternehmenskritische SC-Partner
Kompetenzen aufbauen		X		X
Multiple Sourcing forcieren		X		X
Need-to-Know Prinzip einführen/überprüfen			X	X
Verantwortliche benennen	X	X	X	X
Fragebogen				X
Zertifizierungen abfragen			X	X
Zusammenarbeit klären		X	X	X
Vertragsanpassungen	**Nur bei neuen SC-Partner**		**Bei neuen SC-Partner, bei bestehenden SC-Partnern prüfen**	

Tabelle 1: Überblick über empfohlene Maßnahmen pro Klassifizierungskategorie

Im beiliegenden Excel-Tool im Tabellenblatt „Umsetzungsmaßnahmen" werden automatisch die empfohlenen Maßnahmen für die jeweiligen SC-Partner angezeigt. Diese sind standardmäßig mit der Kennzeichnung „Umsetzung prüfen" versehen. Felder, in denen keine direkte Empfehlung ausgesprochen wurde, sind mit einem „-" markiert und grau hinterlegt. Dies zeigt an, dass die jeweilige Maßnahme nicht explizit erforderlich ist, aber dennoch in das Monitoring einbezogen werden kann.

Jede Maßnahme sollte je nach Fortschritt über ein Dropdown-Menü aktualisiert werden.
Dabei stehen folgende Optionen zur Verfügung:

- „Nicht erforderlich" (grau) ➔ Keine Maßnahme notwendig
- „Umsetzung prüfen" (gelb) ➔ Standardvorgabe, Maßnahme muss geprüft werden
- „Umsetzung planen" (gelb) ➔ Maßnahme befindet sich in der Planungsphase
- „In Bearbeitung" (gelb) ➔ Maßnahme wird derzeit umgesetzt
- „Umgesetzt" (grün) ➔ Umsetzung der Maßnahme erfolgreich abgeschlossen

Diese Farbcodierung erleichtert das Monitoring und die Fortschrittskontrolle.

AP4: PROZESS FÜR NEUE SUPPLY CHAIN PARTNER IMPLEMENTIEREN

Ein Prozess für das Onboarding neuer SC-Partner ist essenziell, um Sicherheitsrisiken bereits vor Vertragsabschluss zu minimieren. Dieser Prozess ermöglicht es, neue Partner systematisch zu bewerten und gezielt in bestehende Prozesse zu integrieren.

Folgende Prozessschritte sollten diesbezüglich beachtet werden:

1. **Initiale Identifikation und Bewertung neuer Partner**
   Der erste Schritt ist eine Bewertung, ob der potenzielle SC-Partner Einfluss auf IT- und OT-Systeme nehmen kann oder Zugriff auf sensible Assets hat.
   Dazu sollte die Person Auskunft geben können, die den SC-Partner angefragt hat.

2. **Klassifizierung und Bewertung**
   Danach kann das Excel-Tool verwendet werden, um die Kritikalität und Integration des SC-Partners zu bewerten. Das Ergebnis dient als Ausgangsbasis für die Vertragsgestaltung.

3. **Risikobasierte Maßnahmen festlegen**
   Auf Basis der Klassifizierung sollte danach festgelegt werden, welche Maßnahmen erforderlich sind, um Cyberrisiken in Bezug auf den SC-Partner zu minimieren.
   Ein wichtiger Teil davon sind auch Vertragsvorbereitungen. Verträge mit neuen Partnern sollten klare Sicherheitsanforderungen auf Basis der Klassifizierung beinhalten.
   Zudem sollte definiert werden, wie die kontinuierliche Überwachung und Zusammenarbeit gestaltet werden sollen. Dazu können die Beispiele aus Anhang 5 herangezogen werden.

4. **Kontinuierliche Überwachung und Zusammenarbeit**
   Basierend auf den festgelegten Maßnahmen gilt es nun über die Vertragslaufzeit den SC-Partner zu überwachen. Dies beinhaltet auch die Prüfung, ob sich in Bezug auf den SC-Partner Änderungen bei der Risikoeinschätzung ergeben haben (z. B. aufgrund der Leistungs- und Umfangsänderung, geänderte Rahmenbedingungen, etc.).
   Zudem sollte ein kontinuierlicher Austausch über Cyber-Security-Themen erfolgen.

Indem diese Schritte systematisch angewendet werden, können KMUs sicherstellen, dass sie bei der Aufnahme neuer SC-Partner gut aufgestellt sind, um Cyber-Security-Risiken zu minimieren und eine sichere Zusammenarbeit zu gewährleisten. Standardisierte Vorlagen und Checklisten erleichtern dabei eine konsistente Bewertung neuer SC-Partner und sparen Zeit.

2.5 Kontinuierliche Verbesserung

Supply Chain Cyber-Security sollte nicht nur als einmaliges Projekt betrachtet werden, sondern fest in der Organisation verankert sein. Die kontinuierliche Anpassung von Maßnahmen ist entscheidend, um auf dynamische Herausforderungen und neuartige Cyberrisiken reagieren zu können. Kurzfristige Maßnahmen können sofort umgesetzt werden, um schnell Verbesserungen in der Supply Chain Cyber-Security zu erreichen. Schulungen und einfache Richtlinien helfen Mitarbeitenden, sicher mit Systemen umzugehen, ohne selbst Experten sein zu müssen. Für nachhaltige Sicherheit müssen diese jedoch in einen kontinuierlichen Verbesserungsprozess eingebettet werden. Im Folgenden werden erprobte Maßnahmen aufgelistet, um die Supply Chain Cyber-Security von Unternehmen über einen längeren Zeitraum sicherzustellen.

KURZFRISTIGE MASSNAHMEN:

- **Schulungen einsetzen und erweitern**
  Mitarbeitende und relevante Abteilungen sollten regelmäßig Schulungen zu aktuellen Cybersicherheitsbedrohungen erhalten. Diese sind idealerweise auf den jeweiligen Aufgabenbereich zugeschnitten und beinhalten auch die Auswirkungen von Cyber-Security-Verletzungen in Lieferketten.

- **Zusätzliche Tools recherchieren und einsetzen**
  Um zusätzliche Informationen in die Bewertung von SC-Partnern integrieren zu können, kann angedacht werden, weitere Tools von verschiedenen Anbietern im Unternehmen zu nutzen. Diese Tools sammeln und analysieren Daten zu verschiedenen Unternehmen und bieten detaillierte Einblicke in deren Cyber-Security-Standards und -Praktiken.
  Sie können beispielsweise Informationen über Sicherheitsvorfälle, Compliance mit Sicherheitsstandards und allgemeine Sicherheitsbewertungen liefern. Solche Tools helfen dabei, fundierte Entscheidungen zu treffen, potenzielle Risiken besser zu bewerten und die Cyber-Security der gesamten Lieferkette zu stärken.

MITTELFRISTIGE MASSNAHMEN:

- **Richtlinien festlegen**
  Um die Vorgehensweise des Unternehmens klar zu dokumentieren und festzulegen, wird idealerweise eine Richtlinie zum Thema „Umgang mit SC-Partnern in Bezug auf Cyber-Security" verfasst und regelmäßig aktualisiert. Eine solche Richtlinie ist auch häufig Voraussetzung für etablierte Standards in der Cyber-Security (z. B. ISO 27001) oder einiger Regulativen (z. B. NIS-2), die auch für KMU relevant sein können.

- **Zusammenarbeit mit SC-Partner intensivieren**
  Die Sicherheitsmaßnahmen der SC-Partner sollten regelmäßig überprüft und aktualisiert werden. Gemeinsame Workshops oder Cyber-Security Übungen fördern den Austausch von Best Practices und erhöhen das Sicherheitsniveau in der gesamten Lieferkette.

LANGFRISTIGE MASSNAHMEN:

- **Weiterentwicklung der Methodik**
  Um die kontinuierliche Verbesserung der Supply Chain Cyber-Security für KMU voranzutreiben, ist es entscheidend, die Methodik regelmäßig zu überprüfen und weiterzuentwickeln. Dies beinhaltet die Erweiterung des Betrachtungsumfangs, insbesondere wenn der ursprüngliche Fokus eingegrenzt war. Darüber hinaus können zusätzliche Kriterien in die Klassifizierung von SC-Partnern aufgenommen werden, um eine präzisere Risikobewertung zu ermöglichen (Mögliche Fragen dazu befinden sich in 2.7.3 Anlage 3). Bestehende Maßnahmen sollten regelmäßig evaluiert und bei Bedarf erweitert werden, um neu auftretenden Bedrohungen effektiv zu begegnen.

- **Feedback- und Optimierungsprozesse etablieren**
  Erkenntnisse aus vergangenen Sicherheitsvorfällen und Rückmeldungen von SC-Partnern sollten systematisch genutzt werden, um bestehende Maßnahmen kontinuierlich zu verbessern. Ein strukturierter Feedbackprozess hilft, Best Practices zu identifizieren und nachhaltig in die Sicherheitsstrategie zu integrieren.

2.6 Fazit

Dieses Handbuch bietet eine umfassende Anleitung zur Implementierung von Cybersicherheitsmaßnahmen in der Lieferkette, speziell für KMU. Die zunehmende Digitalisierung und Vernetzung von Lieferketten bringt nicht nur Effizienzgewinne, sondern auch neue Herausforderungen im Bereich der Cybersicherheit mit sich. KMU stehen vor der Aufgabe, ihre Lieferketten gegen Cyberangriffe zu schützen, um finanzielle Schäden, Betriebsunterbrechungen und Vertrauensverlust zu vermeiden.

In den kommenden Jahren wird die Bedeutung von Supply Chain Cyber-Security weiter zunehmen. Unternehmen müssen sich kontinuierlich an neue Bedrohungen und sich verändernde Rahmenbedingungen anpassen. Die im Handbuch beschriebenen Maßnahmen und Methoden bieten eine solide Grundlage, um die Cybersicherheit in der Lieferkette zu stärken. Die kontinuierliche Verbesserung und Anpassung der Sicherheitsmaßnahmen werden dabei eine zentrale Rolle spielen.

Dieses Handbuch soll Ihnen dabei helfen, eine nachhaltige Cybersicherheitsstrategie zu entwickeln und Ihre Lieferkette gegen die zunehmenden Cyberbedrohungen zu wappnen. Indem Sie die beschriebenen Schritte umsetzen und kontinuierlich weiterentwickeln, können Sie die Sicherheit und Resilienz Ihrer Lieferkette gewährleisten.

2.7 Anlagen zu Supply Chain Cyber-Security

2.7.1 Anlage 1: Projektzeitplan Vorschlag

Firmenname	Max Mustermann	**Projektanfang:**	2.4.2026
Projektleiter	Max Mustermann	**Projektende (Prognose) :**	17.6.2026

Arbeitspaket		Tasks	Verant-wortl.	Beteiligt	Status	Dauer (Wochen)	Start	Ende
AP0	**Vorprojekt**	0.1 Zielsetzung festlegen	Name	Namen	Abgeschlossen	0,5	2.4.26	5.4.26
		0.2 Verantwortlichkeiten festlegen	Name	Namen	Abgeschlossen	0,5	5.4.26	9.4.26
		0.3 Festlegung Projektplan	Name	Namen	im Review	0,5	9.4.26	12.4.26
AP1	**SC-Partner identifizieren**	1.1 Kreditoren-/Debitorenliste Basis	Name	Namen	im Review	1	12.4.26	19.4.26
		1.2 Assets als Basisfestlegen	Name	Namen	in Arbeit	1	19.4.26	26.4.26
		1.3 Kombinierter Ansatz	Name	Namen	noch nicht begonnen	2	26.4.26	10.5.26
AP2	**SC-Partner klassifizieren**	2.1 Vorbereitung des Excel-Tools	Name	Namen		0,2	10.5.26	11.5.26
		2.2 Bestimmung der Kritikalität	Name	Namen		1	11.5.26	18.5.26
		2.3 Bestimmung der Integration	Name	Namen		1	18.5.26	25.5.26
		2.4 Überprüfung der Ergebnisse	Name	Namen		0,2	25.5.26	27.5.26
AP3	**Risiko-maßnahmen definieren**	3.1 Maßnahmen für Partnerklassifizierung festlegen	Name	Namen		1	27.5.26	3.6.26
AP4	**Neue Partner implementieren**	4.1 Prozess für neue Supply Chain Partner implementieren	Name	Namen		2	3.6.26	17.6.26

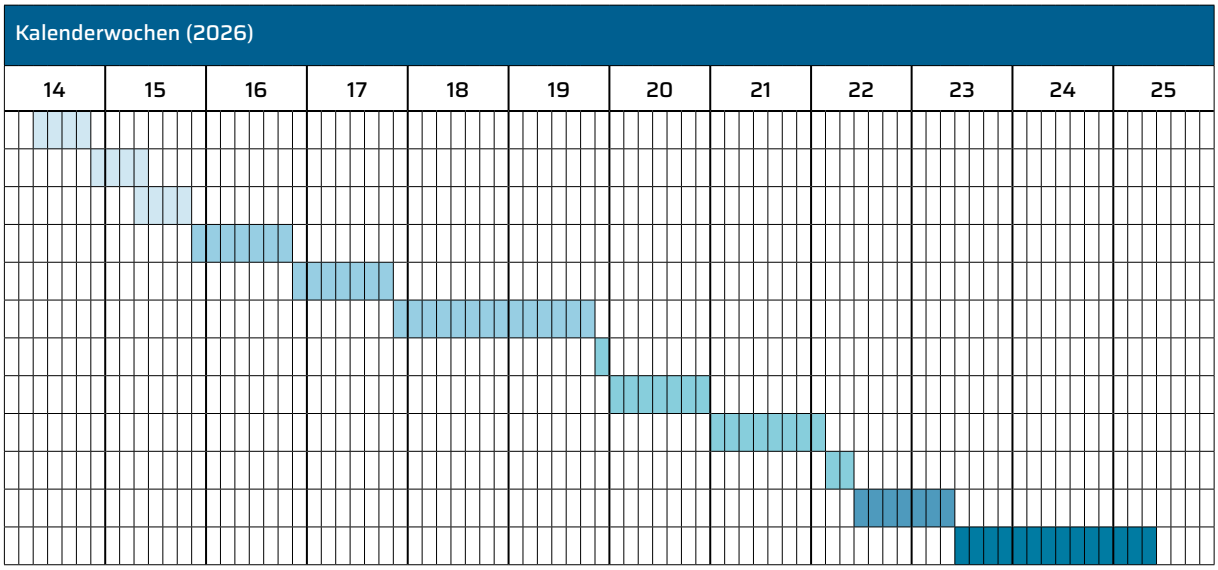


Abbildung 7: Excel Gantt-Chart Projektzeitplan Handbuch 2

2.7.2 Anlage 2: Excel Template zur Klassifizierung von SC-Partnern

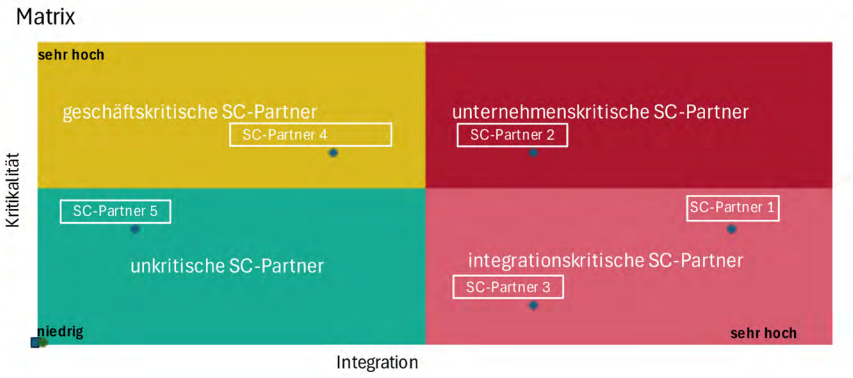
Die eingetragenen SC-Partner-Namen aus Spalte A werden automatisch auf alle anderen Tabellenblätter übertragen.	Wie leicht ist der SC Partner ersetzbar?	Wie zeitkritisch sind die Lieferungen/Dienstleistungen für das Unternehmen?	Automatische Kritikalitätsbewertung	Manuelle Kritikalitätsbewertung
SC-Partner 1	Nicht ersetzbar (es gibt keinen anderen Lieferanten)	moderat (kritisch nach einem Monat)	hohe Kritikalität	moderate Kritikalität
SC-Partner 2	Ersetzbar, aber mit hohem Aufwand	sehr zeitkritisch (sofortige Ausfälle)	hohe Kritikalität	
SC-Partner 3	nicht relevant	nicht zeitkritisch (keine Beeinträchtigung von Geschäftstätigkeiten)	geringe/keine Kritikalität	
SC-Partner 4	Nicht ersetzbar (Alternativen sind nicht relevant)	nicht relevant	hohe Kritikalität	
SC-Partner 5	Nicht ersetzbar (es gibt keinen anderen Lieferanten)	nicht relevant	sehr hohe Kritikalität	moderate Kritikalität
SC-Partner 6				
SC-Partner 7				

Abbildung 8: Excel-Lieferantenklassifizierungstool Tabellenblatt Bewertung Kritikalität

Aus dem Tabellenblatt "Bewertung Kritikalität" übertragen.	Wie sensibel sind die Daten, die Sie mit diesem SC-Partner austauschen?	Hat der SC-Partner einen Fernwartungszugriff auf Ihre Systeme?	Automatische Integrationsbewertung	Manuelle Integrationsbewertung
SC-Partner 1	wenig sensibel (geringfügig vertrauliche Daten)	Ja, einen dauerhaften Zugriff ohne Überwachung	hohe Integration	sehr hohe Integration
SC-Partner 2	nicht relevant	Ja, einen dauerhaften Zugriff mit automatisierten Monitoring	hohe Integration	
SC-Partner 3	nicht sensibel (keine vertraulichen oder geschäftskritischen Daten)	Ja, einen dauerhaften Zugriff ohne Überwachung	hohe Integration	
SC-Partner 4	nicht relevant	Ja, einen terminierten Zugriff mit Monitoring	mittlere Integration	
SC-Partner 5	nicht sensibel (keine vertraulichen oder geschäftskritischen Daten)	nicht relevant	keine/geringe Integration	
SC-Partner 6				
SC-Partner 7				

Abbildung 9: Excel-Lieferantenklassifizierungstool Tabellenblatt Bewertung Integration

Aus dem Tabellenblatt "Bewertung Kritikalität" übertragen.	Bewertung Kritikalität	Bewertung Integration	Gesamtbeurteilung
SC-Partner 1	moderate Kritikalität	sehr hohe Integration	integrationskritische SC-Partner
SC-Partner 2	hohe Kritikalität	hohe Integration	unternehmenskritische SC-Partner
SC-Partner 3	geringe/keine Kritikalität	hohe Integration	integrationskritische SC-Partner
SC-Partner 4	hohe Kritikalität	mittlere Integration	geschäftskritische SC-Partner
SC-Partner 5	moderate Kritikalität	keine/geringe Integration	unkritische SC-Partner
SC-Partner 6			
SC-Partner 7			



Art der SC-Partner	Anzahl
unternehmenskritische SC-Partner	1
integrationskritische SC-Partner	2
geschäftskritische SC-Partner	1
unkritische SC-Partner	1

Abbildung 10: Excel-Lieferantenklassifizierungstool Tabellenblatt Gesamtbewertung

Aus dem Tabellenblatt "Bewertung Kritikalität" übertragen.	Gesamtbewertung	Vertragsanpassungen bestehender SC-Partner (...)	Kompetenzen aufbauen	Multiple Sourcing forcieren	Need-to-Know Prinzip einführen/überprüfen	Verantwortliche benennen	Fragebogen	Zertifizierungen abfragen	Zusammenarbeit klären
SC-Partner 1	integrationskritische SC-Partner	Umsetzung prüfen	-	-	Umsetzung prüfen	Umsetzung prüfen	-	Umsetzung prüfen	Umsetzung prüfen
SC-Partner 2	unternehmenskritische SC-Partner	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen	Umsetzung prüfen
SC-Partner 3	integrationskritische SC-Partner	Umsetzung prüfen	-	-	Umsetzung prüfen	Umsetzung prüfen	-	Umsetzung prüfen	Umsetzung prüfen
SC-Partner 4	geschäftskritische SC-Partner	-	Umsetzung prüfen	Umsetzung prüfen	-	Umsetzung prüfen	-	-	Umsetzung prüfen
SC-Partner 5	unkritische SC-Partner	-	-	-	-	Umsetzung prüfen	-	-	-
SC-Partner 6									
SC-Partner 7									

Abbildung 11: Excel-Lieferantenklassifizierungstool Tabellenblatt Umsetzungsmaßnahmen

2.7.3 Anlage 3: Fragen zur Bewertung von SC-Partnern

B RATING – BASISANFORDERUNGEN AN CYBERSICHERHEIT

1. Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?
2. Schulen Sie Ihre Mitarbeiter regelmäßig in Informationssicherheit?
3. Gibt es in Ihrem Unternehmen eine oder mehrere benannte Personen, die für das Thema Informationssicherheit zuständig sind?
4. Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services (inkl. Cloud-Dienste) sowie der damit verbundenen Verantwortlichkeiten?
5. Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?
6. Verlangen Sie von Ihren Mitarbeitern, für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?
7. Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?
8. Überprüfen Sie – sofern vorhanden – individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?
9. Aktualisieren Sie alle IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?
10. Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von außen ab?
11. Überwachen Sie Ihre IT-Systeme auf Malware?
12. Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?
13. Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?
14. Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?

A RATING – ERHÖHTE SICHERHEITSANFORDERUNGEN (ZUSÄTZLICH ZU B RATING)

Überprüfen Sie IT-Systeme in Ihrem Netzwerk auf Sicherheitslücken?

1. Haben Sie Mechanismen im Einsatz, die bei der Erstellung bzw. dem Erwerb von individuell entwickelter Software deren Sicherheit überprüfen?
2. Führen Sie in Ihrer Systemlandschaft Penetration Tests durch?
3. Überwachen Sie Ihre Systemlandschaft auf ungewöhnliche Aktivitäten und Anomalien?
4. Haben Sie Whitelisting und Cloud Access Security Broker (CASB) im Einsatz, um die Ausführung nicht autorisierter Prozesse und Anwendungen zu unterbinden?
5. Schützen Sie Identitäten, Zugriffe und Berechtigungen in geeigneter und nachvollziehbarer Weise?
6. Haben Sie Technologie im Einsatz, die die Log Files Ihrer Systeme automatisiert korreliert und analysiert?
7. Haben oder nutzen Sie ein Security Operations Team?
8. Können Sie bei einem schwerwiegenden Sicherheitsvorfall auf qualifizierte Ressourcen zurückgreifen?
9. Stellen Sie über ein getestetes Resilienzkonzept oder eine resiliente Architektur Ihre Betriebskontinuität sicher?
10. Haben Sie einen Prozess zum Management Ihrer SC-Partner-risiken?

WEBRISK INDICATOR – PRÜFUNG VON EXTERNEN IT-SICHERHEITSFAKTOREN: Gibt es Hinweise auf Malwareverteilung über Ihre Domains? Wurde Ihre Website durch Defacements verändert oder manipuliert? Nutzen Sie eine sichere SSL-Verschlüsselung (SSL-Ciphersuite, Gültigkeit, Hostname, Trustlevel)?

1. Sind auf Ihrer Website Security-Header korrekt implementiert?
2. Befinden sich Ihre Domains oder Domains, auf die Ihre Seiten verlinken, auf Blacklists?

BEISPIELHAFTE FRAGEN ZUR CYBERSICHERHEITSBEWERTUNG EINES SC-PARTNERS AUS ANDEREN QUELLEN

1. Ist Ihr Unternehmen bereits nach dem Cyber Risk Rating oder einem vergleichbaren Standard bewertet worden?
2. Wie stellen Sie sicher, dass Ihre Cyber-Security-Maßnahmen transparent und nachvollziehbar sind?

Hinweis zur Anwendung der nachfolgenden Inhalte
Die nachfolgenden Abschnitte enthalten umfassende Informationen zu Risikomanagement, Cybersicherheit und regulatorischen Anforderungen, die sich an Unternehmen unterschiedlicher Größen und Branchen richten. Sie wurden auf Basis gängiger Standards und bewährter Methoden zusammengestellt. Da diese Inhalte **nicht speziell auf die Strukturen und Ressourcen von KMU ausgerichtet** sind, sollte jedes Unternehmen individuell prüfen, welche Maßnahmen relevant, wirtschaftlich sinnvoll und umsetzbar sind. Die Anwendung einzelner Konzepte oder Prozesse hängt von Branche, Unternehmensgröße und regulatorischen Vorgaben ab.

2.7.4 Anlage 4: Risikomanagement aufbauen/integrieren

Ein strukturiertes Risikomanagement ist essenziell, um Unternehmen vor unerwarteten Gefahren zu schützen und langfristige Stabilität zu gewährleisten. Dieser Leitfaden basiert auf wissenschaftlichen Quellen und zeigt Schritt für Schritt, wie ein effektives Risikomanagement aufgebaut wird.

1. GRUNDLAGEN SCHAFFEN

Ein effektives Risikomanagement erfordert eine solide Basis, die durch klare Strukturen, Verantwortlichkeiten und die Einhaltung regulatorischer Vorgaben geschaffen wird. Dies stellt sicher, dass Risiken frühzeitig erkannt, analysiert und gesteuert werden können.

1.1 VERANTWORTLICHKEITEN FESTLEGEN

Um ein wirksames Risikomanagementsystem zu etablieren, müssen klare Verantwortlichkeiten festgelegt werden. Dies umfasst:

Benennung eines Risikomanagement-Beauftragten oder Teams

- Je nach Unternehmensgröße kann die Funktion Risikomanagement von einer Einzelperson (z. B. „Risiko-Champion“) oder einer ganzen Abteilung übernommen werden.
- Der Beauftragte sollte Erfahrung mit Risikomanagement-Prozessen haben und strategisch sowie operativ arbeiten.

Einbindung der Geschäftsleitung für strategische Entscheidungen

- Die Unternehmensspitze ist verantwortlich für die regelmäßige Durchführung des Risikomanagement-Prozesses.

- Sie muss sicherstellen, dass die wichtigsten Risikofelder identifiziert werden. Beispiele hierfür sind Elementarrisiken, wie Brände oder Personalrisiken durch den Weggang von Schlüsselpersonen.
- Das Management sollte regelmäßig Risikomanagement-Sitzungen einberufen und die Gesamtrisikoposition (=aktuellen Stand) überprüfen.

1.2 REGULATORISCHE ANFORDERUNGEN PRÜFEN

Unternehmen müssen gesetzliche Rahmenbedingungen beachten, um ein regelkonformes Risikomanagementsystem zu implementieren.

Gesetzliche Pflichten identifizieren

- **NIS-2-Richtlinie (EU-Richtlinie zur Netz- und Informationssicherheit):** Unternehmen aus kritischen und wichtigen Sektoren müssen angemessene Cybersicherheitsmaßnahmen umsetzen und Meldepflichten für Sicherheitsvorfälle einhalten.
- **Cyber Resilience Act (CRA):** Der CRA legt Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen fest. Unternehmen, die solche Produkte herstellen oder verwenden, müssen deren Sicherheitsrisiken bewerten und Schwachstellenmanagement betreiben.
- **Österreichisches Unternehmensrecht:** Das Unternehmensgesetzbuch (UGB) und das Bankwesengesetz (BWG) schreiben für bestimmte Unternehmen die Etablierung interner Kontroll- und Risikomanagementsysteme vor.

NIST als Leitlinie nutzen

- **NIST CSF (National Institute of Standards and Technology Cyber-Security Framework):** Dieses Framework beschreibt fünf Kernfunktionen – Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen – die Unternehmen bei der strukturierten Risikosteuerung unterstützen.
- **Risikobasierter Ansatz:** Das NIST-Framework ermöglicht eine schrittweise Einführung von Risikomanagementprozessen und kann an bestehende Sicherheitsmaßnahmen angepasst werden.
- **Integration in bestehende Managementsysteme:** Unternehmen können das NIST CSF nutzen, um bestehende Prozesse zu ergänzen oder eine eigenständige Sicherheitsstrategie aufzubauen.

1.3 RISIKOMANAGEMENT ALS STRATEGISCHES ZIEL FESTLEGEN

Risikomanagement muss fest in der Unternehmenskultur und den Geschäftsprozessen verankert sein.

Verankerung im Unternehmensleitbild

- Eine schriftlich definierte Risikopolitik, die von der Geschäftsführung genehmigt wurde, ist der erste Schritt.

- Die Risikopolitik legt Organisation, Kompetenzen und Verantwortlichkeiten für verschiedene Risikoarten/Risikokategorien fest, die im Punkt 2.2 weiter definiert werden.

Integration ins bestehende Controlling und Reporting

- Risikomanagement sollte mit dem bestehenden Controllingsystem verknüpft werden, um eine einheitliche Bewertung finanzieller und operationeller Risiken zu ermöglichen.
- Eine regelmäßige Berichterstattung an die Geschäftsleitung und den Verwaltungsrat ist erforderlich.

2. RISIKOIDENTIFIKATION UND ANALYSE

Um Risiken effektiv zu steuern, müssen sie zunächst systematisch erfasst, kategorisiert und bewertet werden. Dieser Prozess ermöglicht es Unternehmen, relevante Bedrohungen frühzeitig zu erkennen und entsprechende Maßnahmen abzuleiten.

2.1 RISIKEN SYSTEMATISCH ERFASSEN

Bevor Unternehmen Maßnahmen zur Risikobewältigung ergreifen können, müssen sie alle potenziellen Risiken identifizieren. Hierfür gibt es verschiedene Methoden:

Interviews mit Abteilungen durchführen

- Einzel- oder Gruppeninterviews mit Mitarbeitern verschiedener Unternehmensbereiche helfen dabei, Schwachstellen und spezifische Risiken frühzeitig zu erkennen.
- Interviews sollten strukturiert geführt werden, beispielsweise mit einem Fragenkatalog zu bisherigen Schadensfällen oder operativen Herausforderungen.
- In kleineren Unternehmen, in denen Abteilungen oft nicht klar getrennt sind, können informelle Gespräche oder kurze Feedbackrunden ebenfalls wertvolle Erkenntnisse liefern.

Workshops zur Risikoerkennung organisieren

- Workshops bringen verschiedene Perspektiven zusammen und ermöglichen eine umfassendere Risikobetrachtung.
- Es können Methoden wie Brainstorming, die Delphi-Methode oder Ursachen-Wirkungs-Diagramme eingesetzt werden.
- In den Workshops werden auch Szenarien entwickelt, die helfen, mögliche zukünftige Risiken abzuleiten.
- Eine strukturierte Moderation sorgt dafür, dass die Diskussion zielgerichtet bleibt und konkrete Maßnahmen abgeleitet werden.
- Beispiel: Ein Handwerksbetrieb organisiert einen Workshop, um Risiken in der Lieferkette zu analysieren. Dabei werden mögliche Störungen, wie Materialengpässe oder steigende Rohstoffpreise, identifiziert. Anschließend werden praktikable Lösungen, wie alternative Lieferanten oder größere Lagerbestände, entwickelt.

Schadensfalldatenbanken nutzen

- Eigene Erfahrungswerte und vergangene Vorfälle sind oft die beste Quelle für die Risikoanalyse. Eine einfache Tabelle zur Dokumentation von Schäden, Fehlern oder Produktionsausfällen kann bereits wertvolle Muster aufzeigen.
- Branchenberichte, Handelskammern oder Versicherungen bieten oft wertvolle Daten zu häufigen Schadensfällen in bestimmten Wirtschaftszweigen.
- Der Austausch mit anderen Unternehmen – z. B. in regionalen Netzwerken oder Verbänden – kann zusätzliche Erkenntnisse über branchenspezifische Risiken liefern.

2.2 RISIKOKATEGORIEN FESTLEGEN

Nicht alle Risiken sind gleichartig. Unternehmen sollten daher Risiken in verschiedene Kategorien einteilen, um eine gezielte Analyse und Bewältigung zu ermöglichen. Typische Risikokategorien sind:

- Strategische Risiken (z. B. Marktveränderungen, Wettbewerbsdruck)
- Finanzielle Risiken (z. B. Währungsrisiken, Kreditausfälle)
- Operationelle Risiken (z. B. Produktionsausfälle, IT-Systemfehler)
- Externe Risiken (z. B. Naturkatastrophen, regulatorische Änderungen)

2.3 RISIKEN BEWERTEN

Nachdem Risiken identifiziert und kategorisiert wurden, müssen sie bewertet werden. Dies erfolgt anhand zweier Faktoren:

Eintrittswahrscheinlichkeit und Schadenshöhe bestimmen

- Die Bewertung erfolgt oft mit qualitativen oder quantitativen Methoden.
- Häufig wird eine Skala verwendet, um die Wahrscheinlichkeit von „sehr unwahrscheinlich" bis „sehr wahrscheinlich" und den Schaden von „gering" bis „katastrophal" einzuordnen.
- Speziell für finanzielle oder sicherheitskritische Risiken können größere Unternehmen Methoden wie Monte-Carlo-Analysen oder Value-at-Risk-Berechnungen nutzen, für KMU sind jedoch meist strukturierte Einschätzungen und standardisierte Bewertungsmethoden ausreichend.

Erstellung einer Risikomatrix

- Eine Risikomatrix visualisiert die Bewertung der Risiken und hilft, Prioritäten festzulegen.
- Risiken mit hoher Eintrittswahrscheinlichkeit und hoher Schadenshöhe sollten zuerst behandelt werden.

3. MASSNAHMEN ABLEITEN UND UMSETZEN

Sobald Risiken identifiziert und bewertet wurden, müssen gezielte Strategien zur Risikobewältigung entwickelt und in die Unternehmensabläufe integriert werden. Dabei geht es nicht nur um die Auswahl geeigneter Maßnahmen, sondern auch um deren nachhaltige Implementierung in Geschäftsprozesse und Notfallkonzepte.

3.1 RISIKOBEWÄLTIGUNGSSTRATEGIEN DEFINIEREN

Unternehmen können verschiedene Strategien zur Bewältigung von Risiken anwenden. Je nach Risikoart und Unternehmensstrategie sind folgende Ansätze möglich:

Risiken vermeiden (z. B. Prozesse anpassen)

- Risikoquellen werden eliminiert oder Geschäftsprozesse so geändert, dass bestimmte Risiken nicht mehr entstehen.
- Unternehmen sollten systematisch analysieren, welche Prozesse geändert oder welche Aktivitäten nicht weiterverfolgt werden sollten.
- Beispiel: Ein Online-Shop entscheidet sich gegen die Annahme von Kreditkartenzahlungen, um das Risiko von Zahlungsbetrug und damit verbundenen Compliance-Anforderungen zu vermeiden. Stattdessen setzt er auf Direktüberweisung und sichere Zahlungsanbieter mit Betrugsprävention.

Risiken reduzieren (z. B. Notfallpläne, technische Maßnahmen)

- Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit oder der Schadenshöhe können technische, organisatorische oder personelle Verbesserungen umfassen. (Schulungen werden im Abschnitt „Schulungen und Sensibilisierung sicherstellen" ausführlicher behandelt.)
- Interne Kontrollsysteme und vorbeugende Wartungsmaßnahmen sind häufig genutzte Methoden.
- Beispiel: Ein Produktionsunternehmen führt regelmäßige Datensicherungen ein und schult seine Mitarbeitenden in sicherer E-Mail-Kommunikation, um Cyberangriffe und Datenverluste zu minimieren.

Risiken akzeptieren (wenn Kosten der Vermeidung zu hoch sind)

- Unternehmen akzeptieren ein Risiko, wenn die Kosten für dessen Vermeidung oder Transfer den potenziellen Schaden übersteigen.
- Dies geschieht oft bei Restrisiken, die durch andere Maßnahmen nicht weiter reduziert werden können.
- Beispiel: Ein mittelständisches Unternehmen mit begrenztem IT-Budget entscheidet sich bewusst gegen den Einsatz einer hochpreisigen, rund um die Uhr besetzten Security Operations Center (SOC)-Lösung, da die laufenden Kosten für Personal und Infrastruktur den potenziellen Schaden durch einen Cyberangriff übersteigen würden.
  Stattdessen akzeptiert das Unternehmen das Restrisiko eines möglichen Cyberangriffs und setzt auf kosteneffizientere Maßnahmen, wie regelmäßige Software-Updates, Mitarbeiterschulungen und eine grundlegende Firewall- und Antivirus-Lösung.
  Die Entscheidung basiert auf einer Kosten-Nutzen-Analyse, bei der festgestellt wurde, dass eine vollständige Vermeidung des Risikos wirtschaftlich nicht tragbar ist.
  Sollte dennoch ein Sicherheitsvorfall eintreten, wird dieser durch vorbereitete Notfallmaßnahmen (z. B. Backup-Systeme und Reaktionsprotokolle) abgefedert.

3.2 MASSNAHMEN IN GESCHÄFTSPROZESSE INTEGRIEREN

Um das Risikomanagement nachhaltig im Unternehmen zu verankern, müssen die abgeleiteten Maßnahmen in bestehende Prozesse eingebunden werden.

Anpassung von internen Richtlinien und Prozessen

- Unternehmen sollten neue Sicherheitsrichtlinien erstellen oder bestehende Verfahren überarbeiten.
- Beispiel: Ein Unternehmen überarbeitet seine Passwortrichtlinie, um Sicherheitsrisiken zu minimieren. Statt einfacher Passwörter mit festen Ablauffristen werden nun längere, komplexe Passwörter ohne regelmäßige Änderungspflicht, aber mit Multi-Faktor-Authentifizierung (MFA) eingeführt, um die IT-Sicherheit zu erhöhen.
- Dazu gehören klare Zuständigkeiten für Risikoüberwachung und Entscheidungsprozesse.

Technische Unterstützung (IT-Systeme, Monitoring-Tools) nutzen

- Softwarelösungen können helfen, Risiken in Echtzeit zu überwachen und rechtzeitig Warnungen auszugeben.
- Beispiel: Ein Unternehmen setzt ein SIEM-System (Security Information and Event Management) ein, das verdächtige Aktivitäten in der IT-Infrastruktur in Echtzeit analysiert und bei Anomalien, wie unbefugten Zugriffsversuchen oder ungewöhnlichem Datenverkehr, sofort eine Warnung an das IT-Sicherheitsteam sendet.
- Automatisierte Risikoberichte und Dashboards erleichtern das Management komplexer Risikoumfelder.

3.3 NOTFALL- UND KRISENPLÄNE ERSTELLEN

Für kritische Risiken müssen Notfallmaßnahmen definiert und regelmäßig getestet werden, um auf unerwartete Ereignisse vorbereitet zu sein.

Reaktionsstrategien für verschiedene Szenarien entwickeln

- Notfallpläne sollten für verschiedene Arten von Bedrohungen (z. B. Naturkatastrophen, Cyberangriffe, Lieferkettenausfälle) existieren. (Die Umsetzung und Tests dieser Pläne erfolgen im Rahmen der regelmäßigen Überprüfung und Anpassung, (siehe Abschnitt „Überwachung und kontinuierliche Verbesserung").
- Unternehmen sollten Verantwortlichkeiten klar festlegen und Abläufe dokumentieren.

4. ÜBERWACHUNG UND KONTINUIERLICHE VERBESSERUNG

Risikomanagement ist kein einmaliger Prozess, sondern erfordert eine laufende Überprüfung und Anpassung. Durch regelmäßige Analysen, gezielte Schulungen und eine transparente Berichterstattung kann sichergestellt werden, dass das System wirksam bleibt und auf neue Herausforderungen reagiert.

4.1 RISIKOMANAGEMENT REGELMÄSSIG ÜBERPRÜFEN

Risikomanagement ist ein kontinuierlicher Prozess, der regelmäßig überprüft und an neue Gegebenheiten angepasst werden muss.

Quartalsweise oder jährliche Risiko-Reviews durchführen

- Eine regelmäßige Wiederholung der Risikoanalyse ermöglicht es Unternehmen, Veränderungen frühzeitig zu erkennen.
- Die Häufigkeit der Reviews hängt von der Risikobewertung ab. Kritische Bereiche sollten mindestens quartalsweise überprüft werden, während weniger dynamische Risikofelder auch jährlich bewertet werden können.
- Zusätzlich müssen Notfallpläne regelmäßig getestet werden, um ihre Wirksamkeit sicherzustellen. Unternehmen sollten Simulationen oder praktische Übungen durchführen, um Abläufe zu optimieren und mögliche Schwachstellen zu identifizieren.

Externe Audits oder interne Kontrollen etablieren

- Externe Audits durch Wirtschaftsprüfer oder branchenspezifische Prüfstellen helfen, die Einhaltung gesetzlicher Vorgaben sicherzustellen.
- Interne Revisionen sollten regelmäßig durchgeführt werden, um Prozesslücken oder Kontrollschwächen frühzeitig aufzudecken.

4.2 SCHULUNGEN UND SENSIBILISIERUNG SICHERSTELLEN

Ein effektives Risikomanagement erfordert eine gut geschulte Belegschaft und eine Unternehmenskultur, die Risikobewusstsein fördert.

Mitarbeiterschulungen zu Risikobewusstsein und -management

- Schulungen sind ein entscheidender Bestandteil, um Risiken zu minimieren. Dazu gehören allgemeine Schulungen zum Risikomanagement sowie spezifische Weiterbildungen für kritische Unternehmensbereiche.
- IT-Sicherheits-Trainings, Compliance-Schulungen oder Erste-Hilfe-Kurse zählen zu den häufig eingesetzten Maßnahmen.

Aufbau einer Risikokultur im Unternehmen

- Risikomanagement sollte nicht als reine Kontrollinstanz wahrgenommen werden, sondern als integraler Bestandteil der Unternehmenskultur aus Mitarbeitersicht verstanden werden.
- Transparente Kommunikation über Risiken und Maßnahmen stärkt das Bewusstsein in der Belegschaft.

4.3 DOKUMENTATION UND BERICHTERSTATTUNG OPTIMIEREN

Eine klare und strukturierte Berichterstattung ist essenziell, um Risiken transparent zu machen und notwendige Maßnahmen schnell einzuleiten.

Risikoberichte für Geschäftsleitung und Stakeholder bereitstellen

- Regelmäßige Berichterstattung hilft Führungskräften, fundierte Entscheidungen zu treffen.
- Berichte sollten standardisiert sein und sowohl qualitative als auch quantitative Risikoanalysen beinhalten.

Laufende Anpassungen an neue Risiken und Entwicklungen vornehmen

- Neue Technologien, Marktveränderungen und regulatorische Anforderungen erfordern eine kontinuierliche Anpassung des Risikomanagements.
- Prozessanpassungen erfolgen basierend auf den Erkenntnissen aus Krisenanalysen und Best Practices (siehe Abschnitt „Lernen aus Vorfällen und neuen Entwicklungen“).

5. INTEGRATION IN DIE UNTERNEHMENSSTRATEGIE

Ein wirkungsvolles Risikomanagement darf nicht als isolierter Prozess betrachtet werden, sondern muss in strategische und operative Entscheidungen integriert werden. Dies ermöglicht eine proaktive Steuerung von Unsicherheiten und stärkt die langfristige Stabilität des Unternehmens.

5.1 RISIKOMANAGEMENT IN ENTSCHEIDUNGSPROZESSE EINBINDEN

Ein effektives Risikomanagement sollte nicht isoliert betrachtet werden, sondern direkt in die strategischen und operativen Entscheidungen des Unternehmens einfließen.

Risikoanalysen in Investitionsentscheidungen einfließen lassen

- Investitionsentscheidungen unterliegen Unsicherheiten, weshalb verschiedene Methoden zur Risikoanalyse angewendet werden sollten.

- Dazu gehören Sensitivitätsanalysen, die untersuchen, wie stark eine Investition auf Änderungen zentraler Faktoren reagiert, sowie Monte-Carlo-Simulationen, die verschiedene Szenarien modellieren.
- Einbindung von Risikomanagement in Kapitalwertberechnungen und Cashflow-Analysen, um Risiken quantifizierbar zu machen.

Langfristige Risikoanalysen in die Unternehmensstrategie integrieren

- Unternehmen sollten eine regelmäßige strategische Risikoanalyse durchführen, um langfristige Trends wie technologische Disruptionen oder regulatorische Veränderungen zu berücksichtigen.
- Strategische Risikoanalysen helfen dabei, Entscheidungen antizyklisch zu treffen, also in Krisenzeiten Wachstumspotenziale zu nutzen.
- Integration des Risikomanagements in Balanced Scorecards und Management-by-Objectives-Systeme, um Risiken auf allen Unternehmensebenen zu erfassen.

5.2 LERNEN AUS VORFÄLLEN UND NEUEN ENTWICKLUNGEN

Die kontinuierliche Weiterentwicklung des Risikomanagements basiert auf Erfahrungswerten aus vergangenen Krisen und Best Practices der Branche.

Reaktionen auf Krisen analysieren und Prozesse anpassen

- Nach jeder größeren Störung oder Krise sollte eine Post-Mortem-Analyse durchgeführt werden, um Ursachen und Fehlerquellen zu identifizieren.
- Basierend auf diesen Erkenntnissen sollten Unternehmen ihre Notfallpläne, Berichterstattungsprozesse und operativen Abläufe kontinuierlich anpassen.

Best Practices aus der Branche berücksichtigen

- Unternehmen sollten sich regelmäßig mit Branchenbenchmarks vergleichen, um bewährte Risikomanagement-Praktiken zu übernehmen.
- Der Austausch mit anderen Unternehmen in Fachgremien oder über Branchenverbände kann helfen, neue Risikomanagement-Ansätze frühzeitig zu erkennen und zu adaptieren.

2.7.5 Anlage 5: Beispielhafte Vertragsklauseln

Hinweis zur Verwendung der Mustervertragsklauseln

Die in diesem Anhang enthaltenen Mustervertragsklauseln dienen ausschließlich als allgemeine Orientierungshilfe und Beispielvorlagen zur Regelung von Informationssicherheit und Cybersicherheitsanforderungen in vertraglichen Vereinbarungen. Sie wurden sorgfältig auf Basis einschlägiger Standards und Best Practices erstellt, stellen jedoch keine verbindliche Rechtsberatung dar. Es wird ausdrücklich darauf hingewiesen, dass die rechtliche Wirksamkeit und Angemessenheit der Klauseln von den individuellen Umständen eines Unternehmens, dem geltenden nationalen Recht sowie den spezifischen Vertragsbeziehungen abhängt. Die Verwendung der Musterklauseln erfolgt daher ausschließlich auf eigene Verantwortung des jeweiligen Unternehmens oder Vertragspartners. **Es wird keine Haftung für die inhaltliche Richtigkeit, Vollständigkeit oder rechtliche Durchsetzbarkeit der hier aufgeführten Klauseln übernommen.** Unternehmen wird dringend empfohlen, die Musterklauseln vor einer Verwendung durch

einen qualifizierten Rechtsbeistand prüfen und anpassen zu lassen, um sicherzustellen, dass sie den individuellen Anforderungen sowie den geltenden gesetzlichen Vorschriften entsprechen. Durch die Nutzung oder Integration der vorliegenden Vertragsklauseln erkennen die Vertragsparteien an, dass der Herausgeber dieser Mustertexte nicht für etwaige rechtliche oder wirtschaftliche Konsequenzen haftet, die aus deren Anwendung entstehen könnten.

1. GRUNDLEGENDE SICHERHEITSANFORDERUNGEN UND STANDARDS

In diesem Abschnitt wird sichergestellt, dass alle beteiligten Parteien hohe Sicherheitsstandards einhalten. Es geht um die Verpflichtung zur Umsetzung von Maßnahmen, die den Schutz von Informationen, Systemen und Daten gewährleisten. Dazu zählen internationale Sicherheitsstandards, ein strukturiertes Management der Informationssicherheit sowie Geheimhaltungs- und Datenschutzregelungen.

- **Verpflichtung zur Einhaltung anerkannter Standards (ISO/IEC 27001, IEC 62443, DSGVO)**
  „Der Auftragnehmer hat angemessene organisatorische und technische Maßnahmen nach dem aktuellen Stand der Technik zu treffen, um die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit des Betriebs des Lieferanten sowie seiner Lieferungen und Leistungen sicherzustellen. Diese Maßnahmen sollen branchenüblich sein und ein angemessenes Managementsystem für Informationssicherheit in Übereinstimmung mit Standards wie ISO/IEC 27001 oder IEC 62443 (soweit anwendbar) beinhalten."

- **Implementierung eines Informationssicherheits-Managementsystems (ISMS)**
  „Der Auftragnehmer muss Informationssicherheitsmanagementprozesse (ISMS) nach einem anerkannten Sicherheitsstandard aufsetzen. Diese Prozesse sowie entsprechende Rollen und Verantwortlichkeiten müssen als Teil seiner Informationssicherheitsrichtlinien dokumentiert sein. Die Richtlinien müssen seiner Belegschaft bekannt sein und regelmäßig auf Aktualität und Richtigkeit überprüft werden."

- **Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit**
  „Der Lieferant wird angemessene, branchenübliche Standards, Prozesse und Methoden in Übereinstimmung mit Standards wie ISO/IEC 27001 oder IEC 62443 (soweit anwendbar) implementieren, um jegliche Schwachstellen, Schadcode und sicherheitsrelevante Ereignisse in den Lieferungen und Leistungen zu verhindern, zu identifizieren, zu bewerten und zu beheben."

- **Verpflichtung zur Geheimhaltung vertraulicher Informationen (auch nach Vertragsende)**
  „Die Parteien verpflichten sich, die VERTRAULICHEN INFORMATIONEN ausschließlich zu dem Zweck zu verwenden, zu welchem sie offengelegt wurden (d. h. ausschließlich zur Durchführung des PROJEKTS) und sie insbesondere nicht Dritten gegenüber preiszugeben oder offen zu legen oder sie anderweitig zu verwerten."

2. IT- UND OT-SICHERHEIT SOWIE SCHWACHSTELLENMANAGEMENT

Dieser Abschnitt stellt sicher, dass IT- und OT-Systeme vor Angriffen geschützt werden. Unternehmen müssen bekannte Sicherheitslücken aktiv schließen und Maßnahmen ergreifen, um neue Schwachstellen frühzeitig zu erkennen und zu beheben. Dazu gehört auch ein strukturiertes Schwachstellenmanagement.

- **Schutz der IT- und OT-Systeme nach aktuellem Stand der Technik**
  „Der Leistungserbringer verpflichtet sich, seine Informatikmittel (d.h. Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen) mit potenzieller Berührung zum vorliegenden Vertragsgegenstand nach dem jeweils aktuellen Stand der Technik vor Cyberangriffen dem Risiko angemessen zu schützen."

- **Verpflichtung zur Identifikation und Behebung von Schwachstellen (inkl. Vulnerability-Management)**
  „Auftragnehmer müssen ihre Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, bspw. in Form eines sogenannten Vulnerability-Managements, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Das Vulnerability-Management basiert auf der Transparenz der Funktionalität, der technischen Architektur und von Unterkomponenten einschließlich der Betriebssysteme, Datenbanken, Server (z. B. Web, Telnet, SSH), Middleware und Bibliotheken. Ziel ist es, neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen."
  „Der Leistungserbringer behebt vor, während oder nach einem Cyberangriff entdeckte Schwachstellen (d.h. Schwächen oder Fehler in Informatikmitteln mit dem Potenzial, einen Cyberangriff zu ermöglichen) umgehend und auf eigene Kosten."

3. ZUGRIFFS- UND BERECHTIGUNGSMANAGEMENT

Dieser Abschnitt regelt den sicheren Zugriff auf IT-Systeme und Daten. Es wird sichergestellt, dass nur autorisierte Personen Zugang zu sensiblen Informationen haben. Aber auch Maßnahmen wie starke Authentifizierungsmethoden, regelmäßige Überprüfung von Zugriffsrechten und Vermeidung unkontrollierter Fernzugriffe verpflichtend sind.

- **Dokumentation und Verwaltung von Zugriffsrechten sowie deren Weitergabe**
  „Es wird allgemein erwartet, dass jeder Nutzer ein persönliches Nutzerkonto bereitgestellt bekommt. Der Auftraggeber akzeptiert Ausnahmen, sollten Umstände auftreten (Unternehmen mit mehreren Supportcentern und einer großen Anzahl an Personal), die dies erschweren. Solche Ausnahmen müssen vorab dokumentiert und in einem SLA (Service Level Agreement) festgehalten werden. In diesem Fall wird der Auftragnehmer die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festhalten (im besten Fall revisionssicher) und diese dem Auftraggeber mindestens einmal jährlich und zusätzlich auf Verlangen aushändigen. Authentisierungsmerkmale (Passwörter, PINs) dürfen nur verschlüsselt über das Netzwerk übermittelt werden."

- **Einsatz von Mindeststandards für Authentifizierung (z. B. Multi-Faktor-Authentifizierung)**
  „Für Fernzugänge sollte mindestens eine Zwei-Faktor-Authentifizierung eingesetzt werden."

- **Regelmäßige Überprüfung und Entzug von Zugriffsrechten**
  „Sollte die Situation auftreten, dass der Auftragnehmer ein Nutzerkonto nicht mehr benötigt, muss der Auftraggeber darüber unverzüglich informiert werden, so dass das entsprechende Konto gesperrt werden kann. Der Auftraggeber kann durch eine Betriebsfunktion oder eine alternative Service-Management-Funktion repräsentiert werden. Derartige Kontakte sind im SLA zu definieren."
  „Es wird vom Auftragnehmer erwartet, Nutzerkonten mit Fernzugangsfunktion alle XXX Monate zu überprüfen und den Auftraggeber über notwendige Änderungen zu informieren."

- **Keine unautorisierten Fernzugriffe auf kritische Systeme**
  „Fernzugänge von Drittanbietern zum Netzwerk des Auftraggebers und/oder dessen zugehörigen Unternehmen wird unter den nachfolgend beschriebenen Bedingungen gestattet. Prozess und Funktion dieses Zugriffs werden allein vom Auftraggeber definiert."
  „Zugänge zur XXX sollten nie direkt, sondern immer über Sprungserver oder vergleichbare Funktionalität in die geschützten Zonen hinein und auf XXX erfolgen."
  „Fernzugänge sollten nur zeitbeschränkt geöffnet werden bzw. automatisch geschlossen werden."

4. MELDEPFLICHTEN FÜR SICHERHEITSVORFÄLLE UND INCIDENT-RESPONSE

Dieser Abschnitt stellt sicher, dass Sicherheitsvorfälle frühzeitig erkannt und an den Auftraggeber gemeldet werden. Dazu gehören klare Fristen für die Meldung, Anforderungen an den Inhalt der Meldung sowie das Recht des Auftraggebers, Untersuchungen durchzuführen und relevante Daten einzusehen.

- **Verpflichtung zur Meldung von Sicherheitsvorfällen innerhalb von XXX Stunden**
  „Der Leistungserbringer meldet potenziell erfolgreiche Cyberangriffe, wenn also die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen des Bundes direkt oder indirekt gestört oder gefährdet sind oder solches beabsichtigt wurde."
  „Der Leistungserbringer meldet Art und Ausführung einen solchen Cyberangriff spätestens innert XXX Stunden nach Entdeckung."

- **Inhalt der Meldung: Art, Ausmaß und Gegenmaßnahmen**
  „Die Parteien tauschen sich dann laufend über Art und Ausführung, mögliche und tatsächliche Auswirkungen, geplante und getroffene Maßnahmen aus."

- **Dokumentation der Schadensermittlung, Sofortmaßnahmen und langfristigen Maßnahmen**
  „Der Auftragnehmer wird in solchen Fällen neben selbstverständlichen Zwischeninformationen einen finalen Abschlussbericht bereitstellen."
  „Der Lieferant hat ein Meldeformular für Informationssicherheitsereignisse auszufüllen. Es müssen die folgenden Punkte enthalten sein:
  - Allgemeine Angaben zum Vorfall (Lieferantenname, Datum, betroffener Zeitraum)
    - Beschreibung des Vorfalls (betroffene Systeme, Ursache, Auswirkungen)
    - Reaktionen und Zustand des Systems (Quickfix und langfristige Maßnahmen zur Vermeidung des erneuten Auftretens)
  - Art des Vorfalls (z. B. Datenverlust, Vertraulichkeitsverletzung, Systemfehlfunktion)
    - Eingeleitete und geplante Maßnahmen zur Behebung"

- **Auftraggeber hat Recht auf Untersuchungen und Zugriff auf Systemprotokolle**
  „Sofern der Leistungsbezüger oder das BACS es zum Schutz der Daten und Informationen des Bundes für notwendig erachten, gewährt der Leistungserbringer ihnen und von ihnen für die Vorfallbearbeitung beigezogenen Dritten unverzüglich Zugang zu Analysen, Untersuchungsberichten und anderen Feststellungen und Informationen (Dokumente, Daten, Log-Daten, Gegenstände etc.), die es erlauben, den Cyberangriff und dessen Auswirkungen zu analysieren und abzuwehren."

5. NACHWEISPFLICHTEN UND AUDITRECHTE

Dieser Abschnitt stellt sicher, dass der Auftraggeber regelmäßig prüfen kann, ob der Leistungserbringer alle Sicherheitsanforderungen einhält. Dazu gehören die Verpflichtung zur Bereitstellung von Sicherheitsnachweisen, das Recht auf Audits und die Kostenübernahme durch den Leistungserbringer, falls erhebliche Sicherheitsmängel festgestellt werden.

- **Vorlage regelmäßiger Nachweise zur Cybersicherheit**
  „Der Leistungserbringer erbringt dem Leistungsbezüger halbjährlich unaufgefordert und ohne separate Verrechnung Nachweise zu seiner Cybersicherheit in Form von (Form konkretisieren und einfügen)."

„Zur Erfüllung der Verpflichtungen unter Punkt XXX gewährleistet der Partner ein geeignetes Sicherheitskonzept, welches der WiG zur Prüfung vorzulegen und mit dieser abzustimmen ist. Die Einhaltung geeigneter Sicherheitsstandards kann auch durch die Vorlage geeigneter Zertifikate (z. B. ISO/IEC 27001 oder ISO 27001 auf Basis IT-Grundschutz), einer Testierung nach dem VDA-Modell TISAX (Trusted Information Security Assessment Exchange) oder anderer adäquater Sicherheitsnachweise nachgewiesen werden."

- **Durchführung von Audits durch den Auftraggeber**
  „Sofern diese Nachweise als ungenügend erachtet werden oder wenn Hinweise auf Lücken in der Cybersicherheit bestehen, kann der Leistungsbezüger (oder ein Dritter in seinem Auftrag) beim Leistungserbringer und von ihm beigezogenen Dritten Audits zur Cybersicherheit durchführen."

- **Kostenübernahme bei gravierenden Sicherheitsmängeln**
  „Sollten jedoch im Rahmen eines Audits wesentliche Mängel der Cybersicherheit festgestellt werden, trägt der Leistungserbringer neben den eigenen Kosten und den Aufwänden zur Behebung zusätzlich die Audit-Kosten des Leistungsbezügers."

6. PHYSISCHE SICHERHEIT UND SCHUTZ SENSIBLER INFORMATIONEN

Dieser Abschnitt stellt sicher, dass sensible Informationen und Systeme nicht durch unkontrollierten physischen Zugang oder unautorisierte Weitergabe gefährdet werden. Dazu gehören Zutrittsbeschränkungen, der Schutz sensibler Daten vor unberechtigtem Zugriff und Vorgaben zur sicheren Speicherung und Verarbeitung von vertraulichen Dokumenten.

- **Zugangsbeschränkungen zu sensiblen Bereichen**
  „Zutritt zu Bereichen mit Informationen oder Systemen mit Schutzbedarf muss auf den autorisierten Personenkreis beschränkt werden. Dazu gehören auch die Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokoll und Sicherung gegen Einbruch u. a."

- **Schutz vor unautorisierten Aufnahmen oder Weitergabe sensibler Informationen**
  „Besonders sensible Informationen sind ausschließlich auf einer Bedarfsgrundlage mit zusätzlichen Sicherheitskontrollen bezüglich Lagerung, Zugriff und Entsorgung weiterzugeben. Für die Weitergabe dieser Informationen ist eine Geheimhaltungsvereinbarung erforderlich."

- **Klassifizierung und sichere Speicherung vertraulicher Dokumente**
  „Markieren Sie alle Informationen von XXX mit der richtigen Dokumentenklassifizierung. Halten Sie die Richtlinien für die Dokumentenklassifizierung von XXX ein.
  Gilt für: Informationen in jedweder Form. Gibt an: XXXs Eigentum am Dokument, seine Sensibilität und wie damit umzugehen ist."

7. SICHERHEITSANFORDERUNGEN FÜR SOFTWARE, IT-PRODUKTE UND CLOUD-DIENSTE

Dieser Abschnitt stellt sicher, dass alle eingesetzten Software- und IT-Produkte hohen Sicherheitsstandards entsprechen. Es geht darum, dass Software und Hardware keine bekannten Sicherheitslücken enthalten, regelmäßige Updates bereitgestellt werden und Cloud-Dienste nur mit nachweislich sicheren Maßnahmen genutzt werden dürfen. Auch Drittanbieter und Unterauftragnehmer müssen diese Anforderungen einhalten.

- **Keine bekannten Schwachstellen oder Schadcode in Software und Hardware**
  „Sofern Lieferungen oder Leistungen Software, Firmware oder Chipsätze beinhalten:
  - Wird der Lieferant angemessene, branchenübliche Standards, Prozesse und Methoden in Übereinstimmung mit Standards wie ISO/IEC 27001 oder IEC 62443 (soweit anwendbar) implementieren, um jegliche Schwachstellen, Schadcode und sicherheitsrelevante Ereignisse in den Lieferungen und Leistungen zu verhindern, zu identifizieren, zu bewerten und zu beheben.
  - Ist der Auftraggeber berechtigt, jedoch nicht verpflichtet, die Lieferungen und Leistungen jederzeit selbst oder durch Dritte auf Schadcode und Schwachstellen zu testen, wobei der Lieferant den Auftraggeber in angemessener Weise unterstützen wird."

- **Bereitstellung von Sicherheitsupdates während des gesamten Produktlebenszyklus**
  „Wird der Lieferant für den Zeitraum einer angemessenen Lebensdauer der Lieferungen und Leistungen Reparatur-, Update-, Upgrade- und sonstige Pflegeleistungen anbieten und Patches zur Verfügung stellen, um Schwachstellen zu beheben."
  „Sollte es zu der Situation kommen, in der der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen, etc.) das Ende des Lifecycles verkündet, wird vom Auftragnehmer erwartet, dass er angemessene Alternativlösungen anbietet und/oder gemeinsam mit dem Auftraggeber nach Lösungsansätzen sucht und diese anbietet. Anderenfalls müssen offene Sicherheitslücken durch Maßnahmen vor Ort kompensiert werden."

- **Dokumentation der verwendeten Drittanbieter-Software**
  „Wird der Lieferant eine Stückliste zur Verfügung stellen, aus der sich alle Softwarekomponenten Dritter ergeben, die in den Lieferungen und Leistungen verwendet werden. Softwarekomponenten Dritter müssen zum Zeitpunkt der Lieferung auf dem aktuellen Stand sein."
  „Der gebräuchliche Umfang einer derartigen Dokumentation inkludiert:
  - Liste der Hardware
  - Liste der Software (inklusive Betriebssystem und Patch-Level)
  - Überblick über die Systemarchitektur
  - Kommunikationsmatrix
  - Überblick über die Datenflüsse (Datenflussschemata)
  - Existierende Benutzerkonten und Rollen sowie deren Berechtigungen."

- **Nutzung sicherer Cloud-Dienste und Nachweis der Sicherheitsmaßnahmen**
  „Bei Clouddiensten ist eine individuelle Anpassung von Sicherheitsmaßnahmen aufgrund der Standardisierung der Cloudservices für einzelne Kunden in der Regel nur schwer möglich. Umso wichtiger ist es, dass die für den Clouddienst implementierten Sicherheitsmaßnahmen auf einem so hohen Stand der Technik laufen und regelmäßig und im Bedarfsfall angepasst werden, dass sie die Anforderungen aus der Perspektive XXX erfüllen. Ein geeigneter Cloud Diensteanbieter muss angemessene Sicherheitsmaßnahmen zur Verfügung stellen können." „Es ist notwendig, vorhandene Zertifikate des Clouddienst-

leisters bei der Bewertung des Sicherheitsniveaus mit einzubeziehen. Beispielsweise werden beim Standard C5 (Cloud Computing Compliance Criteria Catalogue) des BSI alle in Kapitel 2 aufgelisteten Anforderungen an den Clouddienstleister mit betrachtet."

- **Verpflichtung zur Einhaltung von Sicherheitsanforderungen durch Unterauftragnehmer**
  „Der Auftragnehmer muss Sicherheitsanforderungen mit seinen Dienstleistern/Subunternehmern, die Teile der Dienstleistung erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben, schriftlich vereinbaren. Die Sicherheitsanforderungen an die Subunternehmer müssen mindestens in dem vereinbarten Umfang weitergereicht bzw. definiert werden, damit der Auftragnehmer sicherstellen kann, dass seine Verpflichtungen gegenüber dem Auftraggeber vollständig erfüllt werden."

- **Möglichkeit der Auditierung und Kontrolle von Cloud-Diensten durch den Auftraggeber**
  „Bei Cloud-Dienstleistungen ist eine direkte Zuordnung von Infrastruktur und Service oft nicht möglich. In solchen Fällen kann ein Nachweis oder eine Kontrolle nur über die Dokumentation und Zertifizierungen erfolgen."
  „Die Einhaltung muss überwacht und je nach Kritikalität auch durch Lieferantenaudits nachweisbar sein."

8. SICHERHEITSBEWUSSTSEIN UND SCHULUNGEN

Dieser Abschnitt stellt sicher, dass alle beteiligten Mitarbeiter ausreichend über Sicherheitsrisiken informiert sind und regelmäßig geschult werden (siehe 1.4.3). So sollen potenzielle Sicherheitslücken durch menschliches Fehlverhalten minimiert und ein hohes Sicherheitsniveau langfristig sichergestellt werden.

- **Verpflichtung zur regelmäßigen Schulung von Mitarbeitern zu Sicherheitsrisiken**
  „Security-Awareness-Trainings für die Mitarbeiter müssen periodisch durchgeführt werden. Die Inhalte der Schulungen müssen entsprechend den aktuellen Erkenntnissen regelmäßig aktualisiert werden."
  „Der Auftragnehmer verpflichtet sich, seine Mitarbeiter regelmäßig zu schulen, um sicherzustellen, dass diese die Anforderungen an die Informationssicherheit verstehen und einhalten."

- **Aufklärung über Social-Engineering-Risiken und Phishing**
  „Der Auftragnehmer stellt sicher, dass seine Mitarbeiter regelmäßig über Bedrohungen wie Social Engineering, Phishing-Angriffe und andere Cyberrisiken informiert werden und geeignete Schutzmaßnahmen kennen."

9. VERTRAGSGESTALTUNG UND RECHTLICHE ANFORDERUNGEN

Dieser Abschnitt stellt sicher, dass Sicherheitsanforderungen nicht nur technisch, sondern auch vertraglich verbindlich festgelegt sind. Dazu gehören die Einhaltung von Datenschutzvorgaben (z. B.: DSGVO), branchenspezifische Sicherheitsanforderungen sowie das Recht des Auftraggebers auf Kontrolle und Auditierung.

- **Berücksichtigung von DSGVO-Anforderungen für personenbezogene Daten**
  „Jede Partei ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz, insbesondere die EU-Datenschutzgrundverordnung (DSGVO) bei der Ausführung der Vereinbarung zu beachten und die Einhaltung dieser Bestimmungen ihren Mitarbeitern aufzuerlegen. Jede Partei verarbeitet etwa erhaltene personenbezogene Daten der anderen Partei (z. B. Namen und Kontaktdaten der jeweiligen Ansprechpartner) ausschließlich zur Erfüllung dieser Vereinbarung und wird diese durch technische Sicherheitsmaßnahmen (Art. 32 DSGVO) schützen, die an den aktuellen Stand der Technik angepasst sind."

„Sollte eine Partei im Rahmen der Vertragsdurchführung für die andere Partei personenbezogene Daten im Auftrag verarbeiten, werden die Parteien hierüber eine Vereinbarung über die Auftragsverarbeitung nach Art. 28 DSGVO schließen. Eine zusätzliche Verarbeitung für eigene Zwecke, auch in anonymisierter Form, ist ausgeschlossen."

- **Einhaltung branchenspezifischer und nationaler Sicherheitsanforderungen**
  „Zusätzlich muss ein Eskalationsprozess vereinbart werden, um Verstöße gegen Vereinbarungen und Sicherheitsfragen zu behandeln. Die Kontaktinformationen sollen Teil der Vertrags- /Projektdokumentation zwischen dem Auftraggeber und dem Auftragnehmer sein."
  „Es können Situationen auftreten, die die Anpassung von verwendeten und/oder vereinbarten Sicherheitsstandards fordern (beachte den All-Gefahren-Ansatz). Mit dem Auftragnehmer sollte geklärt und dokumentiert werden, wie dieser konstruktiv auf diese Veränderungen reagiert, sich an den neuen Standards und Anforderungen orientiert und proaktiv Trends in der Sicherheit verfolgt, umsetzt und nutzt (Changemanagement)."

- **Aufnahme von Sicherheitsstandards und Auditrechten in Verträge**
  „Der Auftragnehmer muss Sicherheitsanforderungen mit seinen Dienstleistern/Subunternehmern, die Teile der Dienstleistung erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben, schriftlich vereinbaren. Die Sicherheitsanforderungen an die Subunternehmer müssen mindestens in dem vereinbarten Umfang weitergereicht bzw. definiert werden, damit der Auftragnehmer sicherstellen kann, dass seine Verpflichtungen gegenüber dem Auftraggeber vollständig erfüllt werden."
  „Die Einhaltung muss überwacht und je nach Kritikalität auch durch Lieferantenaudits nachweisbar sein."

10. VERTRAGSSTRAFEN, HAFTUNG UND KONSEQUENZEN BEI SICHERHEITSVERSTÖSSEN

Dieser Abschnitt legt fest, welche Konsequenzen der Leistungserbringer zu tragen hat, wenn er gegen die vertraglichen Sicherheitsanforderungen verstößt. Dazu gehören finanzielle Sanktionen, Haftungsregelungen für Schäden und die Möglichkeit zur außerordentlichen Kündigung des Vertrags bei schwerwiegenden Verstößen.

- **Vertragsstrafe bei Verstößen gegen Sicherheitsvorgaben**
  „Der Leistungserbringer schuldet eine Konventionalstrafe, sofern er seinen Meldepflichten aus den Ziffern XXX – XXX gegenüber dem Leistungsbezüger nicht oder nicht fristgerecht nachkommt oder entdeckte Schwachstellen bzw. festgestellte Mängel nicht umgehend behebt. Diese beträgt je Verletzungsfall XXX % der gesamten Vergütung, mindestens jedoch XXX.-- € je Fall."

- **Haftung für Schäden durch Sicherheitsmängel oder Cyberangriffe**
  „Der Leistungserbringer haftet für den Schaden, welcher dem Leistungsbezüger durch Cyberangriffe und die Nichteinhaltung der Bestimmungen in Ziff. XXX entsteht, sofern er nicht beweist, dass ihn kein Verschulden trifft."

- **Möglichkeit zur außerordentlichen Kündigung bei gravierenden Verstößen**
  „Im Vertrag ist bei den Kündigungsvoraussetzungen darauf zu achten, dass die Nichteinhaltung der Bestimmungen betreffend Cyberangriffen als Kündigungsgrund für den Leistungsbezüger festgelegt wird (als außerordentlicher Kündigungsgrund oder als Kündigung aus wichtigem Grund)."

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

3

HANDBUCH CYBER-SECURITY AWARENESS & KULTUR FÜR KMU

FH Oberösterreich

Logistikum

FH Salzburg

Technische Hochschule Deggendorf THD

universität innsbruck

Universität Passau

Einleitung

Dieses Handbuch erklärt die Relevanz von Cyber-Security Awareness sowie einer dafür ausgerichteten Unternehmenskultur, um als KMU resilient in turbulenten, herausfordernden Zeiten agieren zu können. Es zeigt, worauf Unternehmen achten sollen, und gibt Anleitung, wie eine entsprechende Kultur entwickelt werden kann.

Cyber-Security-Vorfälle sind zu einem Großteil auf den menschlichen Faktor zurückzuführen – Studien zufolge bis zu > 80%. Angreifer nutzen gezielt Verhaltensweisen und Interaktionen aus, wodurch technische Sicherheitsmaßnahmen allein nicht ausreichen, um eine umfassende Cyber-Resilienz zu gewährleisten. Die wirksamste Strategie besteht in der Kombination von technologischen Schutzmaßnahmen und einer starken Sicherheitskultur innerhalb eines Unternehmens.

Die zunehmende Komplexität und Häufigkeit von Cyberangriffen verdeutlichen die Notwendigkeit einer Security-First-Kultur in Unternehmen. Eine sicherheitsorientierte Unternehmenskultur beeinflusst maßgeblich die Einstellungen und Verhaltensweisen der Mitarbeiter*innen und stellt sicher, dass Cybersicherheit als integraler Bestandteil aller Unternehmensprozesse wahrgenommen wird. Cybersicherheit ist dabei nicht allein eine technische Herausforderung, sondern auch eine kulturelle und organisatorische Aufgabe. Unternehmen, die Cybersicherheit als festen Bestandteil ihrer Unternehmenskultur begreifen, profitieren von einer besseren Resilienz gegen Bedrohungen und geringeren Risiken durch menschliche Fehler.
Das Zero-Trust-Prinzip basiert auf der Maxime „Never trust, always verify“ und stellt sicher, dass jeder Zugriff – unabhängig von Standort oder Identität – kontinuierlich authentifiziert und autorisiert wird, um Sicherheitsrisiken zu minimieren.
„Security First“ und „Zero-Trust” sind wesentliche Elemente einer resilienten Unternehmenskultur.

3.1 Der Dreiklang: Skillset – Mindset – Toolset

Im Artikel „Es kommt auf die menschliche Firewall an“ wird die wachsende Bedrohung durch Phishing Angriffe für Unternehmen in Deutschland beschrieben. Laut einer Bitkom-Studie nutzen Cyberkriminelle gezielt den „Faktor Mensch“ als vermeintlich schwächstes Glied in der Sicherheitskette. Dabei werden Mitarbeiter*innen durch professionell gefälschte E-Mails manipuliert – etwa im Namen von Vorgesetzten oder Geschäftspartnern – und so zur Preisgabe sensibler Daten oder zum Öffnen schädlicher Anhänge verleitet.

Der Autor betont, dass technischer Schutz allein nicht ausreicht. Entscheidend ist eine ganzheitliche IT-Sicherheitskultur, die auf dem Dreiklang **Mindset – Skillset – Toolset** basiert.

- **Mindset bedeutet:** Mitarbeiter*innen müssen verstehen, dass sie selbst eine wichtige Rolle für die Sicherheit spielen – als „menschliche Firewall“. Ein Umdenken ist nötig, um nicht blind auf Technik zu vertrauen, sondern potenzielle Gefahren bewusst zu erkennen.
- **Skillset** umfasst das nötige Wissen und die praktischen Fähigkeiten, um verdächtige E-Mails zu identifizieren und richtig zu reagieren. Regelmäßige Schulungen, praxisnahe Übungen und interaktive Formate wie Serious Games fördern das Sicherheitsbewusstsein nachhaltig.
- **Toolset** steht für die technischen Werkzeuge und Systeme, die Phishing-Mails erkennen, Angriffe abwehren und Vorfälle dokumentieren – etwa E-Mail-Filter, sichere Authentifizierungsverfahren und Monitoring-Lösungen. Nur wenn alle drei Bereiche zusammenspielen, können Unternehmen wirksam gegen Cyberangriffe gewappnet sein.

3.2 Security-First-Kultur im Unternehmen verankern

Eine sicherheitsorientierte Unternehmenskultur ist essenziell, um das Sicherheitsbewusstsein der Mitarbeiter*innen zu fördern und Cyber-Bedrohungen aktiv zu begegnen. Eine Security-First-Kultur stellt Cybersicherheit als zentrale Komponente aller Geschäftsprozesse und Entscheidungen in den Fokus. Dabei wird Sicherheit nicht als rein technisches Problem betrachtet, sondern als gemeinschaftliche Verantwortung aller Beschäftigten.

Der Aufbau einer Security-First-Kultur erfordert ein Umfeld, in dem Cybersicherheit nicht nur eine Priorität ist, sondern auch aktiv verstanden und in die Struktur des täglichen Betriebs integriert wird.

Eine erfolgreiche Sicherheitskultur zeichnet sich durch kollektives Engagement (alle Mitarbeiter*innen und Führungskräfte tragen gleichermaßen Verantwortung für die Sicherheitsstrategie bei), Anpassungsfähigkeit (Strategien zur Cybersicherheit sollten auf den kulturellen Kontext des Unternehmens abgestimmt sein, um eine hohe Akzeptanz und Einhaltung sicherer Praktiken zu gewährleisten), und Führungsverantwortung (Führungskräfte setzen Standards für Cybersicherheit, indem sie sie in strategische Entscheidungsprozesse integrieren und vorleben) aus.

Eine auf Sicherheit ausgerichtete Unternehmenskultur beeinflusst direkt das Verhalten der Mitarbeiter*innen und ihre Einstellung zu Cybersicherheitspraktiken. Sie sorgt dafür, dass Sicherheitsrichtlinien nicht als Bürde, sondern als selbstverständlicher Bestandteil der Arbeitsweise angesehen werden.

Zur erfolgreichen Implementierung einer Security-First-Kultur in KMU sind mehrere Faktoren ausschlaggebend, welche im Folgenden kurz ausgeführt werden.

3.2.1 Vorbildfunktion der Führungsebene

Führungskräfte haben großen Einfluss darauf, wie wichtig Cybersicherheit im Unternehmen genommen wird. Wenn sie das Thema ernst nehmen und aktiv ansprechen, wirkt sich das direkt auf das Verhalten der Mitarbeitenden aus. Wenn Cybersicherheit regelmäßig in Besprechungen, E-Mails oder bei Entscheidungen mitgedacht wird, merken alle: Das ist kein Nebenthema, sondern ein fester Bestandteil der Unternehmenskultur.

- **Beispiel aus dem Alltag:** Thema Gesundheit: Wenn die Geschäftsleitung selbst auf gesunde Ernährung achtet und an Gesundheitstagen teilnimmt, motiviert das auch andere, mitzumachen. Genauso ist es mit IT-Sicherheit – wer als Führungskraft bewusst sichere Passwörter nutzt oder beim Thema Phishing aufmerksam ist, sendet ein starkes Signal: Sicherheit geht uns alle an.

3.2.2 Geteilte Verantwortung – Cybersicherheit ist Teamarbeit

Cybersicherheit ist Teamarbeit. Cybersicherheit ist nicht nur Aufgabe der IT-Abteilung. Alle im Unternehmen tragen Verantwortung dafür, Daten zu schützen und Risiken zu verringern. Jede einzelne Person kann – bewusst oder unbewusst – ein Einfallstor für Angriffe sein. Umso wichtiger ist es, dass alle Mitarbeitenden wachsam sind, verdächtige Aktivitäten melden und sicher mit digitalen Werkzeugen umgehen.

- **Beispiel aus dem Alltag:** Brandschutz: Zwar gibt es Feuerwehrleute (die IT-Abteilung), aber auch alle anderen achten darauf, keine Kerzen unbeaufsichtigt brennen zu lassen oder Notausgänge freizuhalten. Genauso funktioniert es bei der Cybersicherheit – sie gelingt nur, wenn alle mitdenken und mithelfen.

3.2.3 Investitionen in Schulung und Sensibilisierung – Schulung stärkt die Sicherheit

Regelmäßige Schulungen und Info-Angebote helfen Mitarbeiter*innen dabei, Cyber-Bedrohungen früh zu erkennen und im Ernstfall richtig zu reagieren. Denn wer weiß, worauf er achten muss, kann Gefahren besser vermeiden. Besonders erfolgreich sind interaktive Formate wie Workshops oder sogenannte „Serious Games" – also Lernspiele, bei denen man spielerisch typische Situationen aus dem Arbeitsalltag durchspielt. So bleibt das Wissen besser hängen und macht obendrein mehr Spaß als trockene Vorträge (siehe auch 4.2.1.3).

- **Beispiel aus dem Alltag:** Erste-Hilfe-Kurs: Man hofft, das Gelernte nie zu brauchen – aber im Notfall kann es entscheidend sein. Wer regelmäßig übt, einen Feuerlöscher zu benutzen oder Verbände richtig anzulegen, fühlt sich sicherer und reagiert im Ernstfall souveräner. Genauso ist es mit IT-Sicherheit: Übung macht den Unterschied.

3.2.4 Offene Kommunikations- und Fehlerkultur

In einem Unternehmen sollte es ganz normal sein, Sicherheitsvorfälle oder mögliche Schwachstellen offen anzusprechen – ohne Angst vor Schuldzuweisungen oder negativen Konsequenzen. Nur so lassen sich Probleme frühzeitig erkennen und schnell beheben. Wenn Mitarbeiter*innen wissen, dass sie auch kleine Fehler oder Verdachtsmomente melden dürfen, ohne dafür „an den Pranger gestellt" zu werden, steigt die Bereitschaft, ehrlich und schnell zu handeln. Anonyme Meldesysteme können zusätzlich helfen, die Hemmschwelle zu senken.

- **Beispiel aus dem Alltag:** Melden von Beinahe-Unfällen – etwa in einer Werkstatt: Wenn jemand sagt „Da wäre ich fast gestolpert, weil ein Kabel im Weg lag", kann man sofort handeln, bevor wirklich etwas passiert. Genauso kann auch eine frühzeitige Meldung in der IT – zum Beispiel bei einem seltsamen E-Mail-Anhang – Schlimmeres verhindern. Offenheit schützt alle.

3.2.5 Dynamische Anpassungsfähigkeit – Sicherheit braucht ständige Anpassung

Im Bereich Cybersicherheit gibt es ständig neue Bedrohungen – deshalb reicht es nicht, einmal eine Strategie festzulegen und dann dabei zu bleiben. Sicherheitsmaßnahmen müssen regelmäßig überprüft und weiterentwickelt werden. Durch regelmäßige Sicherheitsüberprüfungen (Audits) und das Sammeln von Rückmeldungen aus dem Unternehmen lässt sich erkennen, was gut funktioniert – und wo nachgebessert werden muss. So bleibt die Strategie wirkungsvoll und aktuell.

- **Beispiel aus dem Alltag:** Das ist wie beim Auto: Nur weil es beim Kauf sicher war, heißt das nicht, dass es ewig so bleibt. Man bringt es regelmäßig zur Inspektion, tauscht bei Bedarf Teile aus und passt die Fahrweise an Wetter oder Straßenbedingungen an. Genauso muss sich auch die Cybersicherheit ständig weiterentwickeln, um mit neuen Gefahren Schritt zu halten.

3.3 Zero-Trust: Sicherheit durch konsequentes Misstrauen

Das Zero-Trust-Modell basiert auf dem Grundsatz „Never trust, always verify". Es stellt einen fundamentalen Paradigmenwechsel in der Cybersicherheit dar, indem es davon ausgeht, dass kein Benutzer, Gerät oder System – unabhängig davon, ob es sich innerhalb oder außerhalb des Unternehmensnetzwerks befindet – automatisch als vertrauenswürdig gilt. Dies erfordert eine kontinuierliche Authentifizierung und Autorisierung aller Zugriffe und Aktivitäten. In Kombination mit einer starken Cyber-Security Awareness und Sicherheitskultur kann Zero-Trust dazu beitragen, die Resilienz von Organisationen gegenüber Cyberbedrohungen erheblich zu erhöhen.

Zero-Trust und Awareness ergänzen sich gegenseitig, da beide Ansätze darauf abzielen, Sicherheitslücken durch menschliche Fehler zu minimieren. Mitarbeiter*innen müssen verstehen, dass sie selbst eine kritische Rolle im Sicherheitsgefüge eines Unternehmens spielen. Ein gut implementiertes Zero-Trust-Modell kann dabei unterstützen, Sicherheitsbewusstsein zu schärfen, indem es den Mitarbeiter*innen regelmäßig sicherheitskritische Entscheidungen abverlangt, beispielsweise durch Multi-Faktor-Authentifizierung (MFA) oder regelmäßige Sicherheitsprüfungen.

Eine Sicherheitskultur entsteht nicht durch einmalige Maßnahmen, sondern durch kontinuierliche Sensibilisierung und konsequente Sicherheitspraktiken. Zero-Trust kann zur Etablierung einer solchen Kultur beitragen, indem es sicherheitsbewusstes Verhalten zur Routine macht. Wenn Mitarbeiter*innen regelmäßig Sicherheitsmaßnahmen umsetzen müssen, entwickelt sich ein Bewusstsein für die Notwendigkeit dieser Praktiken.

3.3.1 Strikte Identitätsprüfung – jeder Zugriff wird überprüft

Im Zero-Trust-Modell wird niemand automatisch als vertrauenswürdig eingestuft – auch nicht innerhalb des eigenen Firmennetzwerks. Jeder Zugriff auf Daten oder Systeme muss zuerst eindeutig geprüft werden. Das bedeutet: Mitarbeiter*innen müssen sich regelmäßig durch Sicherheitsverfahren wie die Zwei-Faktor-Authentifizierung (2FA, MFA) ausweisen – zum Beispiel mit einem Passwort und einem Bestätigungscode auf dem Smartphone. Diese konsequente Überprüfung sorgt dafür, dass nur berechtigte Personen Zugang bekommen – auch dann, wenn ein Passwort mal in falsche Hände gerät. Außerdem stärkt sie das Bewusstsein dafür, wie wichtig Schutzmaßnahmen im digitalen Alltag sind.

- **Beispiel aus dem Alltag:** Online-Banking: selbst, wenn man Benutzername und Passwort kennt, reicht das nicht aus – man muss zusätzlich einen Code eingeben, der per App oder SMS kommt. Genauso schützt Zero-Trust sensible Unternehmensdaten: Nur wer sich eindeutig ausweisen kann, darf weiter. Das macht Angreifern das Leben deutlich schwerer.

3.3.2 Prinzip der minimalen Rechtevergabe (Least Privilege)

Nach dem Prinzip der minimalen Rechtevergabe sollen Mitarbeiter*innen nur auf die Informationen und Systeme zugreifen können, die sie wirklich für ihre tägliche Arbeit brauchen – nicht mehr und nicht weniger. Je weniger Zugriff jemand hat, desto geringer ist das Risiko, dass Daten versehentlich weitergegeben oder missbraucht werden – ob absichtlich oder unbeabsichtigt. So lassen sich interne Sicherheitsrisiken deutlich verringern.

- **Beispiel aus dem Alltag:** Schlüssel in einem Unternehmen: Eine Reinigungskraft braucht den Schlüssel für den Putzmittelraum – aber nicht für das Personalarchiv. Umgekehrt braucht jemand aus der Personalabteilung keinen Zutritt zur Technikzentrale. Jede*r bekommt nur die Schlüssel, die er oder sie wirklich braucht. Das erhöht die Sicherheit und macht allen bewusst, wie wichtig es ist, sorgfältig mit Zugriffsrechten umzugehen.

3.3.3 Kontinuierliche Überwachung und Analyse

Durch die ständige Überwachung (Monitoring) und Protokollierung (Logging) von Aktivitäten im System kann auffälliges oder ungewöhnliches Verhalten frühzeitig erkannt werden – zum Beispiel, wenn jemand zu ungewöhnlichen Zeiten auf sensible Daten zugreift. Solche Hinweise helfen, mögliche Sicherheitsverstöße oder Cyberangriffe schnell zu entdecken und zu stoppen. Gleichzeitig erkennen Mitarbeiter*innen, wie wichtig es ist, sich verantwortungsvoll und sicher im digitalen Arbeitsumfeld zu verhalten.

- **Beispiel aus dem Alltag:** Bürogebäude mit Überwachungskameras: Wenn jemand nachts um drei Uhr versucht, in ein Archiv zu gehen, obwohl er dort nichts zu suchen hat, fällt das auf. Genauso funktionieren digitale Überwachungssysteme – sie schlagen Alarm, wenn etwas vom normalen Verhalten abweicht.

3.3.4 Mikrosegmentierung

Mikrosegmentierung bedeutet, dass ein Netzwerk in viele kleine, voneinander getrennte Bereiche unterteilt wird. So kann ein Angreifer, der sich Zugang zu einem Teil verschafft, nicht automatisch auf alle anderen Bereiche zugreifen.

- **Beispiel aus dem Alltag:** Ein modernes Bürogebäude: Jede Abteilung – etwa Buchhaltung, Personal und IT – hat ihr eigenes Büro mit Zugangskontrolle. Wenn jemand unerlaubt in das Büro der Buchhaltung eindringt, kommt er trotzdem nicht automatisch ins IT-Büro oder zum Personalarchiv, weil jede Tür einzeln gesichert ist. Genauso funktioniert Mikrosegmentierung im Netzwerk: Selbst wenn ein Angreifer in einen Bereich gelangt, etwa durch eine infizierte E-Mail, bleibt der Zugriff auf andere kritische Daten und Systeme blockiert. So wird verhindert, dass sich der Angriff unkontrolliert ausbreitet.

3.3.5 Sichere Endgeräte und Zero-Trust-Network-Access

Im Arbeitsalltag nutzen viele Mitarbeiterinnen und Mitarbeiter verschiedene Geräte – etwa Laptop, Smartphone oder Tablet –, um auf Unternehmensdaten zuzugreifen. Das Zero-Trust-Modell verlangt, dass nur geprüfte und sichere Geräte diesen Zugriff bekommen. Ein infiziertes oder veraltetes Gerät kann ein Einfallstor für Angreifer sein. Deshalb ist es entscheidend, dass nur autorisierte Geräte mit aktueller Sicherheitssoftware zugelassen werden.

Wissen schützt: Regelmäßige Schulungen helfen dabei, die Belegschaft im sicheren Umgang mit ihren Geräten zu schulen – zum Beispiel beim Erkennen von Phishing-Versuchen oder dem sicheren Umgang mit Passwörtern. So entsteht ein gemeinsames Sicherheitsbewusstsein.

- **Beispiel aus dem Alltag:** Das ist vergleichbar mit einem Firmenparkplatz, auf den nur Fahrzeuge mit einer gültigen Parkkarte dürfen. Ein unbekanntes Auto ohne Genehmigung bleibt draußen – selbst wenn der Fahrer einen Firmenausweis hat. Genauso prüft das System bei Zero-Trust nicht nur den Nutzer, sondern auch das Gerät. Nur wenn beides vertrauenswürdig ist, gibt es Zugang.

3.4 Praxisfokus: Serious Games als Schulungstool

Serious Games sind interaktive Anwendungen, die spielerische Elemente mit ernsthaften Bildungs- oder Trainingszielen kombinieren. Sie werden zunehmend in verschiedenen Bereichen wie Bildung, Gesundheitswesen und Unternehmensschulungen eingesetzt, um Wissen zu vermitteln, Problemlösungskompetenzen zu fördern und Verhaltensweisen positiv zu beeinflussen. Besonders im Bereich der IT-Sicherheit und Awareness-Schulungen gewinnen Serious Games an Bedeutung, da sie Mitarbeiter*innen ermöglichen, reale Bedrohungsszenarien in einer sicheren Umgebung zu erleben und darauf zu reagieren.

Serious Games bieten eine innovative und effektive Möglichkeit, Wissen zu vermitteln und das Bewusstsein für sicherheitskritische Themen zu schärfen. Die Evaluierung solcher Spiele anhand von Kriterien wie Benutzerfreundlichkeit, Lernerfolg, Aktualität, Integration in den Arbeitsalltag und Praxisbezug hilft dabei, qualitativ hochwertige Schulungstools auszuwählen. Unternehmen sollten darauf achten, dass Serious Games nicht nur unterhaltsam, sondern auch praxisrelevant sind, um einen nachhaltigen Lerneffekt zu gewährleisten. So können Mitarbeiter*innen spielerisch auf Bedrohungsszenarien vorbereitet werden und im Ernstfall angemessen reagieren.
Ein Überblick über eine Auswahl an kostengünstigen und analogen Serious Games befindet sich im Anhang.

3.5 Fazit: Der Weg zur sicheren Unternehmenskultur

Cybersicherheit ist längst nicht mehr nur ein technisches Thema, sondern eine gesamtunternehmerische Aufgabe, die Kultur, Kommunikation und kontinuierliche Weiterbildung vereint. Dieses Handbuch hat gezeigt, dass eine resiliente Sicherheitskultur vor allem auf drei Säulen basiert: Mindset, Skillset und Toolset. Nur wenn alle Mitarbeitenden die Bedeutung ihrer Rolle im Sicherheitsgefüge verstehen, das nötige Wissen besitzen und auf geeignete technische Werkzeuge zurückgreifen können, lässt sich eine starke und nachhaltige Abwehr gegen Cyberbedrohungen aufbauen.

Gerade für kleine und mittlere Unternehmen (KMU), die oft mit begrenzten Ressourcen arbeiten, bietet ein strukturierter, kulturorientierter Ansatz einen effektiven und machbaren Weg zur Stärkung der Cyber-Resilienz. Sicherheitsbewusstsein lässt sich nicht durch einmalige Maßnahmen verankern – es braucht stetige Schulung, gelebte Vorbilder in der Führungsebene und eine offene Kommunikationskultur.

Der Blick nach vorne:

Die Bedrohungslage wird sich weiterentwickeln, ebenso wie die Angriffsmethoden. Daher müssen Unternehmen flexibel bleiben, ihre Strategien regelmäßig prüfen und anpassen. Zukünftig werden Themen wie Künstliche Intelligenz in der Angriffserkennung, automatisiertes Monitoring und spielerische Schulungsformate (z. B. Serious Games) noch stärker an Bedeutung gewinnen. Auch hybride Arbeitsmodelle erfordern neue Sicherheitskonzepte, die ortsunabhängig greifen.

Ein starkes Sicherheitsfundament entsteht nicht über Nacht – aber es wächst mit jeder bewussten Entscheidung für eine „Security-First"-Mentalität. Wer heute beginnt, in Kultur, Kompetenz und Technologie zu investieren, schafft die besten Voraussetzungen für eine sichere digitale Zukunft.

3.6 Anlage: Serious Games als Schulungstool

Name	Beschreibung
Backdoors & Breaches Kartenspiel – Analog **Inhalt:** Angriffstaktiken, Tools, Methoden	Ein kooperatives Kartenspiel rund um Incident Response. Aus vier Angriffskategorien entstehen tausende mögliche Vorfallszenarien. Die Spieler analysieren Angriffe, identifizieren Taktiken und entwickeln geeignete Gegenmaßnahmen. Dabei trainieren sie strategisches und intuitives Denken. Besonders geeignet für Teams, die praxisnah und spielerisch ihr Verständnis für Cyberangriffe und Verteidigungsstrategien vertiefen möchten.
Potatopirates - Enter the Spudnet Brettspiel – Analog **Inhalt:** Computernetzwerke, Cyberangriffe	Ein unterhaltsames Brettspiel über Cybersicherheit und Netzwerke. Die Spieler bauen Infrastrukturen auf, schließen Allianzen und wehren Angriffe ab – oder hintergehen sich gegenseitig. Je nach Modus kooperativ oder kompetitiv spielbar. Das Spiel vermittelt grundlegende Netzwerk- und Sicherheitskonzepte und eignet sich sowohl für Schulungen als auch für Spieleabende – unabhängig vom technischen Vorwissen.
Cyber Threat Defender Kartenspiel – Analog **Inhalt:** Cybersicherheitsgrundlagen, Netzwerkinfrastruktur, Angriffs- und Verteidigungsstrategien	Ein strategisches Mehrspieler-Kartenspiel, das an Pokemon erinnert und Grundlagen der Cybersicherheit vermittelt. Die Spielendr schützen ihre Netzwerke, reagieren auf Angriffe und lernen zentrale Fachbegriffe sowie Zusammenhänge zwischen Bedrohungen und Verteidigungsmaßnahmen kennen. Einfach zugänglich und motivierend gestaltet, fördert es spielerisch das Verständnis für technische und historische Hintergründe der Cyberwelt.
Data Heist Kartenspiel – Analog **Inhalt:** Datenschutz, persönliche Cyberhygiene, Angriffssimulation	Ein interaktives Kartenspiel, das Datenschutz und persönliche Cyberhygiene vermittelt. Die Spieler übernehmen die Rolle von Hackern und nutzen typische Angriffsarten, um Daten zu „stehlen". Dabei werden reale Bedrohungsszenarien simuliert und Sicherheitslücken aufgezeigt. Erweiterte Regeln ermöglichen unterschiedliche Schwierigkeitsstufen und machen das Spiel sowohl für Einsteiger als auch für erfahrene Teilnehmende geeignet.
[DOX3D!] Brettspiel – Analog **Inhalt:** Netzwerksicherheit, Angriffs- und Verteidigungsmechanismen, Datenschutz	Ein kooperatives Brettspiel zur Einführung in die Netzwerksicherheit. Die Spieler lernen Fachbegriffe, Sicherheitsmechanismen und Schutzmaßnahmen kennen. Mit modularem Spielbrett und Aktionspunktesystem simuliert es reale Netzwerktopologien. Ideal für Einsteigergruppen, um Grundlagen der Cybersicherheit praxisnah zu verstehen und sichere Verhaltensweisen im Unternehmenskontext zu entwickeln.
Hacker Brettspiel – Analog **Inhalt:** Programmierlogik, Angriffs-szenarien, Schutzmechanismen	Ein herausforderndes Brettspiel mit 40 Missionen in drei Phasen. Die Spieler programmieren ihre Agenten, sammeln Datenchips und vermeiden Viren oder Alarme. Dabei erleben sie, wie Angriffe funktionieren und wie Programme geschützt werden können. Geeignet für Workshops und Schulungen, fördert es logisches Denken sowie praxisnahes Verständnis für IT-Sicherheit.
OWASP Cornucopia Kartenspiel – Analog **Inhalt:** Sicherheitsanforderungen, Bedro-hungsmodelle, Webanwendungssicherheit	Ein Team-Kartenspiel zur Identifikation von Sicherheitsanforderungen und Schwachstellen in Webanwendungen. Es unterstützt die Entwicklung sicherheitsbezogener User Stories und führt in die Bedrohungsmodellierung ein. Besonders geeignet für Entwicklungs- und Projektteams, um Sicherheitsaspekte strukturiert in Prozesse zu integrieren und das Bewusstsein für Datenschutzrisiken zu stärken.
Perihack Brettspiel – Analog **Inhalt:** Red-Team-/Blue-Team-Szenarien, Datenschutz, Angriffserkennung	Ein rundenbasiertes Brettspiel, in dem ein Angreifer-Team versucht, Sicherheitslücken auszunutzen, während das Verteidiger-Team das Netzwerk schützt. Die Spieler lernen Fachbegriffe, Angriffsmuster und typische Betrugsstrategien kennen. Durch Teamarbeit wird das Bewusstsein für Cyberbedrohungen gestärkt und praxisnahes Sicherheitsdenken gefördert.
ALARM - Serious Games Brettspiel – Analog **Inhalt:** Awareness-Training, Cyber-sicherheitsgrundlagen, Sensibilisierung	Ein Serious Game als Bestandteil eines ganzheitlichen Awareness-Konzepts. Es kann einzeln oder kombiniert mit weiteren Spielen im Stationenlernen eingesetzt werden. Das Spiel dient als Einstieg oder Auflockerung in Schulungen und fördert spielerisch das Bewusstsein für sicherheitsrelevante Themen im Unternehmensalltag.

Abbildung 12: Serious Games als Schulungstool

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

HANDBUCH CYBER-NOTFALLKONZEPT FÜR KMU

Ein praktischer Leitfaden zur Krisenbewältigung

FH Oberösterreich

Logistikum

FH Salzburg

Technische Hochschule Deggendorf

universität innsbruck

Universität Passau

Einleitung

ZWECK UND NOTWENDIGKEIT DES CYBER-NOTFALLKONZEPTS

Die zunehmende Digitalisierung bringt nicht nur zahlreiche Vorteile, sondern auch erhebliche Sicherheitsrisiken mit sich. Cyberangriffe sind längst zu einer der größten Bedrohungen für Unternehmen geworden, unabhängig von ihrer Größe oder Branche. Besonders kleine und mittlere Unternehmen (KMU) stehen vor der Herausforderung, ihre IT-Sicherheitsmaßnahmen kontinuierlich zu verbessern, da sie häufig nicht über die gleichen Ressourcen wie Großunternehmen verfügen.

Untersuchungen zeigen, dass KMU gezielt ins Visier von Cyberkriminellen geraten, da Angreifer oft davon ausgehen, dass deren Sicherheitsvorkehrungen weniger ausgereift sind. Ein erfolgreicher Cyberangriff kann schwerwiegende Folgen für ein Unternehmen haben. Neben finanziellen Verlusten und Betriebsunterbrechungen kann ein solcher Vorfall auch erhebliche rechtliche und reputationsbezogene Konsequenzen mit sich bringen. Laut Security-Insider verzeichneten KMU im Jahr 2023 die meisten Cyberangriffe mit durchschnittlich 40 Angriffsversuchen pro Benutzer.

Eine Untersuchung ergab zudem, dass Cyberangriffe deutsche Unternehmen im Jahr 2022 wirtschaftliche Schäden in Höhe von 203 Milliarden Euro verursachten, wobei insbesondere mittelständische Unternehmen betroffen waren. Eine Statista-Umfrage aus 2021 ergab, dass 26,6 Prozent der befragten Mittelstandsunternehmen in den letzten zwei Jahren Opfer eines erfolgreichen Cyberangriffs wurden. Die konkreten Auswirkungen eines Cyber-Notfalls werden in Kapitel 4.1.3 näher beschrieben. Ohne eine strukturierte Vorgehensweise zur Prävention und Reaktion auf solche Bedrohungen sind Unternehmen im Ernstfall meist schlecht vorbereitet, was den Schaden erheblich vergrößern kann.

Ein gut durchdachtes Cyber-Notfallkonzept ist daher essenziell, um die Widerstandsfähigkeit eines Unternehmens gegenüber Cyberangriffen zu erhöhen. Ein solches Konzept umfasst sowohl präventive Maßnahmen zur Risikominimierung als auch klare Handlungsanweisungen für den Ernstfall. Ziel ist es, den Geschäftsbetrieb trotz eines Angriffs aufrechtzuerhalten oder schnellstmöglich wiederherzustellen.

Dieses Handbuch bietet eine praxisorientierte Anleitung zur Implementierung eines Cyber-Notfallkonzepts, das auf die spezifischen Bedürfnisse von KMU zugeschnitten ist. Die strukturierte Vorgehensweise basiert auf vier zentralen Phasen der Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung. Unternehmen erhalten hiermit eine systematische Methodik, um sich auf Cyber-Bedrohungen vorzubereiten, Notfallsituationen effizient zu bewältigen und aus Vorfällen zu lernen, um ihre Sicherheitsmaßnahmen kontinuierlich zu verbessern.

ZIELGRUPPE

Das Handbuch richtet sich an Geschäftsführer, IT-Verantwortliche und Sicherheitsbeauftragte von KMU, die eine systematische Vorgehensweise zur Absicherung gegen Cyber-Bedrohungen entwickeln möchten. Die beschriebenen Maßnahmen sind praxisorientiert und berücksichtigen die oft begrenzten Ressourcen in kleinen und mittleren Unternehmen. Auch für Unternehmen ohne eigene IT-Abteilung stellt dieses Handbuch eine wertvolle Unterstützung dar, indem es praxisnahe und umsetzbare Maßnahmen beschreibt.

4.1 Grundlagen: Was ist ein Cyber-Notfall?

4.1.1 Definition Cyber-Notfall

Ein Cyber-Notfall ist ein Sicherheitsvorfall, der die Integrität, Vertraulichkeit oder Verfügbarkeit von IT-Systemen, Netzwerken oder Daten in einem Unternehmen erheblich beeinträchtigt. Solche Notfälle können durch gezielte Cyberangriffe oder unbeabsichtigte Sicherheitslücken entstehen und erfordern eine sofortige Reaktion, um Schäden zu minimieren. Ein Cyber-Notfall unterscheidet sich von alltäglichen IT-Problemen dadurch, dass er den normalen Geschäftsbetrieb erheblich stört und kein sofortiges oder routinemäßiges Eingreifen zur Lösung ausreicht. Unternehmen müssen daher klare Prozesse zur Erkennung und Bewältigung solcher Notfälle definieren.

4.1.2 Typische Bedrohungsszenarien

Cyber-Notfälle können durch eine Vielzahl von Angriffsformen und technischen Fehlern verursacht werden. Die häufigsten Bedrohungsszenarien für KMU sind:

- **Ransomware-Angriffe:** Schadsoftware verschlüsselt Daten und verlangt ein Lösegeld für die Wiederherstellung.
- **Datenlecks und Insider-Bedrohungen:** Sensible Daten gelangen durch interne oder externe Einflüsse unbefugt an Dritte.
- **Denial-of-Service (DoS)-Angriffe:** Gezielte Überlastung eines Systems, sodass es für legitime Nutzer nicht mehr zugänglich ist.
- **Phishing und Social Engineering:** Mitarbeiter werden durch gefälschte E-Mails oder Anrufe zur Preisgabe sensibler Informationen verleitet.
- **Schwachstellen in IT-Systemen:** Sicherheitslücken in Software oder Hardware, die von Angreifern ausgenutzt werden.
- **Unbefugter Zugriff:** Hacker oder böswillige Akteure verschaffen sich Zugriff auf Netzwerke und Systeme eines Unternehmens.

4.1.3 Auswirkungen eines Cyber-Notfalls auf KMU

Die Folgen eines Cyber-Notfalls können für KMU besonders gravierend sein, da sie meist weniger finanzielle und technische Ressourcen haben, um schnell auf Angriffe zu reagieren. Zu den wichtigsten Auswirkungen zählen:

- **Finanzielle Verluste:** Direkte Kosten für die Behebung des Schadens, Zahlung von Lösegeld bei Ransomware, Vertragsstrafen oder entgangene Umsätze.
- **Rechtliche Konsequenzen:** Verstöße gegen Datenschutzbestimmungen wie die DSGVO können Bußgelder und juristische Konsequenzen nach sich ziehen.
- **Betriebliche Unterbrechung:** Produktions- und Geschäftsausfälle, die sich negativ auf Lieferketten und Kundenbeziehungen auswirken.
- **Reputationsschäden:** Kunden und Partner verlieren das Vertrauen in das Unternehmen, was langfristige finanzielle Einbußen zur Folge haben kann.

Diese Bedrohungen verdeutlichen, warum KMU nicht nur reaktive Maßnahmen ergreifen, sondern auch präventive Strategien umsetzen sollten, um ihre IT-Sicherheit zu stärken und Notfälle effektiv zu managen.

4.2 Bestandteile des Cyber-Notfallkonzepts

Ein Cyber-Notfallkonzept setzt sich aus mehreren essenziellen Bestandteilen zusammen, die sicherstellen, dass Unternehmen sowohl präventive Maßnahmen ergreifen als auch angemessen auf Cyber-Vorfälle reagieren können. Diese Struktur hilft dabei, Cyber-Risiken frühzeitig zu erkennen, im Notfall schnell zu handeln und aus Vorfällen zu lernen. Das Konzept umfasst vier zentrale Phasen:
Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung. Jede dieser Phasen spielt eine entscheidende Rolle für die Cybersicherheit eines Unternehmens.

4.2.1 Vorbereitung: „Nach dem Vorfall ist vor dem Vorfall“

4.2.1.1 Risikoanalyse und Identifikation kritischer Systeme

Die Grundlage für ein funktionierendes Cyber-Notfallkonzept ist eine gründliche Risikoanalyse. Unternehmen müssen zunächst ihre kritischen IT-Systeme identifizieren und bewerten, welche Auswirkungen ein Cyber-Vorfall auf den Geschäftsbetrieb hätte. Dazu gehören Server, Netzwerke, ERP-Systeme, Kundendatenbanken sowie E-Mail-Kommunikation. Eine umfassende Inventarisierung und Bewertung dieser Systeme ermöglicht es, gezielt Sicherheitsmaßnahmen zu ergreifen und Prioritäten für den Notfall zu setzen. Die Risikoanalyse sollte auch potenzielle Bedrohungen berücksichtigen. Unternehmen müssen bewerten, welche Schwachstellen bestehen und welche Angriffsszenarien realistisch sind. Typische Gefahrenquellen sind ungesicherte Zugangsdaten, veraltete Software oder fehlende Netzwerksicherungen. Regelmäßige Sicherheitsbewertungen helfen dabei, potenzielle Schwachstellen frühzeitig zu identifizieren und zu beheben (siehe auch 2.7.4).

4.2.1.2 Erstellung eines Cyber-Notfallplans

Ein Cyber-Notfallplan definiert die konkreten Maßnahmen und Verantwortlichkeiten, die im Falle eines Cyberangriffs zu ergreifen sind. Der Plan sollte alle möglichen Angriffsszenarien abdecken, von Ransomware-Angriffen bis hin zu Datenlecks. Er sollte außerdem festlegen, welche Systeme zuerst wiederhergestellt werden müssen und wie die Kommunikation während eines Vorfalls erfolgt. Ein Notfallplan sollte klare Eskalationsstufen enthalten: Wann handelt die IT-Abteilung, wann wird die Geschäftsführung informiert und wann müssen externe Stellen wie Strafverfolgungsbehörden oder Datenschutzbeauftragte eingeschaltet werden? Die Dokumentation eines solchen Plans sorgt für eine koordinierte und effektive Reaktion im Ernstfall.

4.2.1.3 Schulung und Sensibilisierung der Mitarbeitenden

Mitarbeitende sind oft die erste Verteidigungslinie gegen Cyber-Bedrohungen, aber gleichzeitig auch eine der größten Schwachstellen in der IT-Sicherheit. Viele erfolgreiche Angriffe, insbesondere durch Phishing und Social Engineering, nutzen menschliche Fehler aus. Daher ist es essenziell, dass alle Mitarbeitenden regelmäßig geschult und für Cyber-Bedrohungen sensibilisiert werden (siehe 3.2.3).

Ein effektives Schulungsprogramm sollte sich auf folgende Kernbereiche konzentrieren:

- **Erkennung von Cyber-Bedrohungen:** Wie Mitarbeitende Phishing-E-Mails, verdächtige Links und Social-Engineering-Taktiken identifizieren können.
- **Sicherer Umgang mit Passwörtern und Authentifizierungsmechanismen:** Die Nutzung von starken, eindeutigen Passwörtern und Multi-Faktor-Authentifizierung (MFA).
- **Meldepflichten und Reaktionsstrategien:** Wie und wann ein Sicherheitsvorfall gemeldet werden muss, um Schäden zu minimieren.
- **Sichere Nutzung von Unternehmenssystemen:** Umgang mit Cloud-Diensten, Speichermedien und mobilen Geräten, um Sicherheitslücken zu vermeiden.

Zusätzlich zu klassischen Schulungsmaßnahmen kann das Awareness- und Kultur-Handbuch als ergänzende Ressource genutzt werden. Dieses bietet weiterführende Informationen und konkrete Maßnahmen, wie Unternehmen eine Sicherheitskultur etablieren können. Ein nachhaltiger Sicherheitsansatz erfordert nicht nur regelmäßige Schulungen, sondern auch eine Kultur der Wachsamkeit innerhalb der Organisation. Unternehmen sollten daher sicherstellen, dass Cybersicherheit als fester Bestandteil der Unternehmenskultur verstanden wird und dass alle Mitarbeitenden in ihrem täglichen Handeln Verantwortung für IT-Sicherheit übernehmen.

4.2.1.4 Technische Schutzmaßnahmen und regelmäßige Updates

Technische Schutzmaßnahmen sind essenziell, um Angriffe frühzeitig abzuwehren. Dazu gehört die regelmäßige Aktualisierung aller Systeme und die Implementierung moderner Sicherheitstechnologien. Alle sicherheitsrelevanten Updates sollten automatisiert oder innerhalb definierter Zeiträume durchgeführt werden, um Schwachstellen in Software und Betriebssystemen zu schließen.

Zusätzlich sollte jedes Unternehmen über regelmäßige Backups verfügen, um im Ernstfall schnell reagieren zu können. Backups sollten:

- Automatisiert und regelmäßig erfolgen.
- An einem sicheren, externen Standort gespeichert werden.
- Getestet werden, um sicherzustellen, dass die Wiederherstellung tatsächlich funktioniert.

4.2.1.5 Business Continuity Planning (BCP)

Ein Cyberangriff kann schwerwiegende Auswirkungen auf den Geschäftsbetrieb haben, insbesondere wenn kritische IT-Systeme betroffen sind. Business Continuity Planning (BCP) beschreibt die Maßnahmen, die ergriffen werden, um den Geschäftsbetrieb während oder nach einem Cyber-Notfall aufrechtzuerhalten.

Ein gut ausgearbeiteter BCP stellt sicher, dass Unternehmen auch im Falle eines IT-Ausfalls arbeitsfähig bleiben und sich so schnell wie möglich wieder vollständig erholen. Der Plan sollte Folgendes enthalten:

- **Identifikation geschäftskritischer Prozesse:** Welche Abläufe müssen in jedem Fall aufrechterhalten werden (z. B. Finanztransaktionen, Produktionssteuerung, Kundensupport)?
- **Alternative Betriebsabläufe:** Wie kann das Unternehmen weiterarbeiten, wenn zentrale IT-Systeme nicht verfügbar sind? Dazu gehören Notfalllösungen wie Cloud-basierte Systeme oder manuelle Arbeitsprozesse.
- **Rollen und Verantwortlichkeiten:** Wer ist für welche Maßnahmen verantwortlich?
- **Notfall-IT-Ressourcen:** Gibt es Backup-Systeme oder Ersatzhardware, um kritische Arbeitsabläufe fortzuführen?
- **Kommunikationsstrategie:** Wie wird intern und extern kommuniziert, wenn Systeme ausfallen?

Zur besseren Veranschaulichung enthält das Handbuch in der Anlage 4.6 einen Beispielplan für Business Continuity Planning, der als Vorlage für die Erstellung eines eigenen BCPs verwendet werden kann. Unternehmen sollten diesen Plan regelmäßig testen und aktualisieren, um sicherzustellen, dass er im Ernstfall funktioniert.

4.2.2 Bereitschaft: Reaktionsfähigkeit sicherstellen

4.2.2.1 Einrichtung eines Cyber-Notfallmanagementteams

Ein Cyber-Notfallmanagementteam koordiniert die Maßnahmen im Falle eines Angriffs. Es sollte aus Vertretern der IT-Abteilung, Geschäftsleitung, Datenschutzbeauftragten und externen Sicherheitsberatern bestehen. Jedes Mitglied sollte genau wissen, welche Aufgaben es zu erfüllen hat.

4.2.2.2 Pflege und Aktualisierung einer Notfall-Kontaktliste

Eine aktuelle und vollständige Notfall-Kontaktliste ist essenziell, um im Falle eines Cyber-Vorfalls schnell reagieren zu können. Sie sollte regelmäßig überprüft und aktualisiert werden, damit alle relevanten internen und externen Ansprechpartner jederzeit erreichbar sind. Die Notfall-Kontaktliste sollte mindestens folgende Informationen enthalten:

- **Interne Ansprechpartner**, darunter IT-Verantwortliche, Geschäftsleitung und Datenschutzbeauftragte
- **Externe Partner**, wie IT-Dienstleister und Cyber-Security-Spezialisten
- **Behördliche Anlaufstellen**, darunter Strafverfolgungsbehörden und Datenschutzaufsichtsbehörden

Da sich Zuständigkeiten, Kontaktdaten oder externe Dienstleister im Laufe der Zeit ändern können, muss die Liste regelmäßig überprüft und angepasst werden. Es empfiehlt sich, eine vierteljährliche Aktualisierung durchzuführen sowie eine physische Kopie bereitzuhalten, um im Notfall auch bei einem IT-Ausfall Zugriff zu haben. Eine Beispiel-Notfall-Kontaktliste mit allen wesentlichen Elementen ist in Kapitel 4.3.1 zu finden und kann als Vorlage für die Erstellung einer eigenen Unternehmensliste genutzt werden.

4.2.2.3 Festlegen sicherer Kommunikationswege

Im Notfall kann es vorkommen, dass reguläre Kommunikationssysteme wie E-Mail oder interne Chats kompromittiert sind. Unternehmen sollten daher alternative Kommunikationskanäle festlegen. Dazu gehören verschlüsselte Messenger oder Notfalltelefone, die unabhängig vom Unternehmensnetzwerk betrieben werden.

4.2.2.4 Durchführung regelmäßiger Planspiele zur Notfallbewältigung

Durch Planspiele können Unternehmen ihre Notfallreaktion trainieren. Diese Simulationen helfen, Schwachstellen in den bestehenden Abläufen zu identifizieren.
Typische Szenarien sind:

- Ein plötzlicher Ransomware-Angriff auf das Firmennetzwerk.
- Ein erfolgreicher Phishing-Angriff, bei dem ein Mitarbeitender sensible Zugangsdaten weitergibt.
- Ein gezielter Angriff auf kritische IT-Systeme, der den Betrieb lahmlegt.

4.2.2.5 Sicherheitsaudits und IT-Penetrationstests

Sicherheitsaudits und Penetrationstests sind essenziell, um Angriffsvektoren frühzeitig zu identifizieren und Sicherheitsmaßnahmen zu verbessern. Externe Sicherheitsprüfer können Lücken aufdecken, die intern möglicherweise übersehen wurden.

4.2.3 Bewältigung: Incident Response Plan

Die Bewältigung eines Cyber-Notfalls erfordert ein strukturiertes Vorgehen, um Schäden zu minimieren, schnell wieder arbeitsfähig zu sein und gesetzliche Vorgaben einzuhalten. Ein Incident Response Plan (IRP) beschreibt die konkreten Schritte, die im Falle eines Cyberangriffs durchgeführt werden müssen. Dieser Plan sorgt dafür, dass alle Beteiligten wissen, was zu tun ist und keine wertvolle Zeit durch Unsicherheit oder chaotische Abläufe verloren geht.

4.2.3.1 Erkennung und Einstufung von Cyber-Vorfällen

Die frühzeitige Erkennung eines Cyber-Vorfalls ist entscheidend, um rechtzeitig angemessene Gegenmaßnahmen einzuleiten. Unternehmen müssen in der Lage sein, zwischen harmlosen Systemfehlern und schwerwiegenden Cyberangriffen zu unterscheiden. Dabei hilft eine strukturierte Einstufung des Vorfalls, um die Dringlichkeit und den erforderlichen Handlungsbedarf zu bestimmen.

4.2.3.1.1 Früherkennung von Sicherheitsvorfällen

Sicherheitsvorfälle können auf verschiedene Weise erkannt werden. Unternehmen sollten ihre IT-Systeme kontinuierlich überwachen und auf folgende Indikatoren achten:

- **Ungewöhnliche Systemaktivitäten**, z. B. plötzliche Performance-Einbrüche, unerklärlicher Datenverlust oder unerwartete Systemneustarts.
- **Alarme von Sicherheitssystemen**, wie Firewalls, Intrusion Detection Systeme (IDS), Endpoint Protection oder SIEM-Lösungen, die verdächtige Aktivitäten melden.
- **Meldungen von Mitarbeitenden**, die verdächtige E-Mails, unbekannte Softwareinstallationen oder ungewöhnliches Systemverhalten bemerken.

Wenn einer oder mehrere dieser Indikatoren auftreten, sollte der Vorfall sofort untersucht und anhand eines Einstufungsschemas bewertet werden.

4.2.3.1.2 Einstufung von Cyber-Vorfällen

Cyber-Vorfälle lassen sich in verschiedene Schweregrade unterteilen, um die Dringlichkeit und den erforderlichen Handlungsbedarf zu bestimmen:

- **Geringfügige Vorfälle:** Beispielsweise verdächtige E-Mails oder ungewöhnliche Login-Versuche, die keinen unmittelbaren Schaden verursachen.
- **Mittelschwere Vorfälle:** Einschränkungen in IT-Systemen, beispielsweise Malware-Infektionen oder erfolgreiche Phishing-Angriffe auf einzelne Mitarbeitende.
- **Kritische Vorfälle:** Schwere Beeinträchtigungen des Geschäftsbetriebs, wie Ransomware-Angriffe, Datenlecks oder ein kompletter IT-Ausfall.

4.2.3.1.3 Ziel der Einstufung und Reaktionspläne

Die Einstufung dient nicht nur dazu, die Dringlichkeit auf einer zwischenmenschlichen Ebene klar zu kommunizieren, sondern auch um festzulegen, welche Maßnahmen ergriffen werden müssen und wer dafür zuständig ist. Unternehmen sollten daher für verschiedene Schweregrade von Vorfällen unterschiedliche Reaktionspläne vorbereiten, um im Ernstfall effizient handeln zu können. Für geringfügige Vorfälle genügt es oft, interne IT-Sicherheitsrichtlinien zu befolgen, etwa das Sperren verdächtiger E-Mail-Absender oder das Zurücksetzen kompromittierter Passwörter. Mittelschwere Vorfälle erfordern oft eine Untersuchung durch das IT-Team, beispielsweise die Analyse infizierter Systeme oder die Durchführung von forensischen Untersuchungen.

Kritische Vorfälle hingegen machen eine Eskalation an die Geschäftsleitung, externe IT-Sicherheitsdienstleister oder Behörden erforderlich und müssen nach einem detaillierten Incident Response Plan gehandhabt werden. Unternehmen sollten daher sicherstellen, dass für jede Einstufung klare Handlungsanweisungen existieren, die genau beschreiben, wer was tun muss und wie die Kommunikation intern sowie extern ablaufen soll. Ein klar definierter Eskalationsprozess stellt sicher, dass schwerwiegende Vorfälle nicht unterschätzt und unkritische Ereignisse nicht überreagiert behandelt werden.

4.2.3.2 Sofortmaßnahmen und Eindämmung

Sobald die Einstufung erfolgt ist, müssen Sofortmaßnahmen zur Eindämmung des Schadens ergriffen werden. Diese umfassen:

- **Trennen des betroffenen Systems vom Netzwerk,** um eine weitere Ausbreitung zu verhindern.
- **Deaktivieren oder Sperren betroffener Benutzerkonten,** falls verdächtige Aktivitäten festgestellt wurden.
- **Isolierung kompromittierter Server oder Arbeitsplätze,** um weitere Schäden zu vermeiden.

In Fällen von Ransomware-Angriffen sollte keine Lösegeldzahlung erfolgen, da dies nicht garantiert, dass die Daten tatsächlich entschlüsselt werden. Stattdessen müssen gesicherte Backups geprüft werden.

4.2.3.3 Kommunikation mit Behörden, Partnern und Kunden

Ein Cyber-Vorfall kann nicht nur technische und betriebliche, sondern auch kommunikative Herausforderungen mit sich bringen. Unternehmen müssen sicherstellen, dass alle relevanten internen und externen Stakeholder informiert werden, ohne Panik auszulösen oder sensible Informationen unkontrolliert weiterzugeben.

Die Kommunikation sollte klar geregelt sein, um Fehlinformationen und rechtliche Probleme zu vermeiden. Dazu gehört eine frühzeitige Meldung an Behörden, wenn dies gesetzlich vorgeschrieben ist, sowie eine transparente, aber kontrollierte Information an Partner und Kunden, falls deren Daten oder Geschäftsprozesse betroffen sind.

4.2.3.3.1 Meldepflichten und Kommunikation mit Behörden

In vielen Fällen sind Unternehmen gesetzlich verpflichtet, Cyber-Vorfälle an zuständige Behörden zu melden. Dazu gehören:

- **Datenschutzbehörden** (z. B. im Falle eines Datenschutzverstoßes gemäß DSGVO)
- **Strafverfolgungsbehörden** (z. B. wenn ein Angriff zu wirtschaftlichem Schaden oder Erpressung führt)
- **Branchenverbände oder Regulierungsstellen,** falls branchenspezifische Sicherheitsvorgaben existieren

Unternehmen sollten im Vorfeld klären, welche Behörden für sie zuständig sind und wie eine Meldung erfolgen muss. Die Notfall-Kontaktliste (siehe 4.3.1) enthält eine Übersicht relevanter Ansprechstellen.

4.2.3.3.2 Kommunikation mit Geschäftspartnern und Kunden

Falls ein Vorfall Auswirkungen auf Partner oder Kunden hat, muss das Unternehmen eine klare und professionelle Kommunikationsstrategie verfolgen. Hierbei hilft ein strategischer Kommunikationsplan, der definiert, wer wann welche Informationen erhält.

EIN STRATEGISCHER KOMMUNIKATIONSPLAN FÜR KMU BEANTWORTET DREI ZENTRALE FRAGEN:

1. **Wer muss informiert werden?**
   - Interne Stakeholder (z. B. Geschäftsführung, IT-Team, Datenschutzbeauftragter)
   - Externe Partner (z. B. Lieferanten, Dienstleister, Banken)
   - Kunden (falls deren Daten oder Dienstleistungen betroffen sind)

2. **Wann wird kommuniziert?**
   - Direkt nach Feststellung des Vorfalls
   - Nach einer ersten Einschätzung des Schadens
   - Sobald Maßnahmen zur Schadensbegrenzung eingeleitet wurden
   - Nach der vollständigen Wiederherstellung

3. **Wie wird kommuniziert?**
   - **Interne Kommunikation:** Über Meetings, E-Mail oder sichere Messaging-Tools (z. B. Signal oder Threema)
   - **Externe Kommunikation mit Partnern und Kunden:** Offizielle E-Mails oder Pressemitteilungen, um Vertrauen zu wahren
   - **Öffentlichkeitsarbeit:** Falls notwendig, abgestimmte Statements für Presse oder Social Media

4.2.3.3.3 Praxisbeispiel für KMU: Wie ein Kommunikationsplan aussehen kann

Szenario: Ein Ransomware-Angriff hat das Rechnungswesen lahmgelegt, sodass Kunden keine Rechnungen erhalten können.

1. **Interne Kommunikation:**
   - IT-Abteilung und Geschäftsleitung werden informiert.
   - Sofortiges Krisenmeeting zur Lageeinschätzung.
   - Mitarbeiter werden angewiesen, keine externen Informationen herauszugeben.

2. **Meldung an Behörden:**
   - Falls personenbezogene Daten betroffen sind, wird die Datenschutzbehörde informiert.
   - Falls ein finanzieller Schaden oder eine Erpressung vorliegt, wird die Polizei eingeschaltet.

3. **Externe Kommunikation:**
   - Kunden erhalten eine E-Mail mit der Information, dass es technische Probleme gibt, aber die Rechnungsstellung bald wieder möglich ist.
   - Geschäftspartner und Lieferanten werden informiert, dass es temporäre Verzögerungen geben kann.
   - Falls Medienanfragen eintreffen, wird ein vorbereitetes Statement genutzt, um Spekulationen zu vermeiden.

Ein solcher Plan hilft KMU, klar und professionell zu kommunizieren, ohne vorschnelle Aussagen zu treffen, die Panik auslösen oder rechtliche Probleme verursachen könnten.

4.2.3.4 Beweissicherung und forensische Analyse

Nach einem Cyber-Vorfall ist es entscheidend, alle relevanten Beweise zu sichern, um die Ursachen des Angriffs zu analysieren, rechtliche Schritte vorzubereiten und zukünftige Angriffe zu verhindern. Die digitale Forensik befasst sich mit der Untersuchung des Vorfalls und der Identifikation der genauen Eintrittspunkte und Methoden der Angreifer.

Ein zentraler Aspekt der Analyse ist die Identifikation des Angriffsvektors. Der Angriffsvektor beschreibt die Methode, über die der Angreifer in das System eingedrungen ist.
Typische Angriffsvektoren sind:

- **Phishing:** Mitarbeitende wurden durch gefälschte E-Mails dazu gebracht, auf schädliche Links zu klicken oder Zugangsdaten preiszugeben.
- **Schwachstellen in Software:** Veraltete oder ungepatchte Programme wurden genutzt, um sich Zugriff auf Systeme zu verschaffen.
- **Gestohlene Zugangsdaten:** Hacker haben sich durch kompromittierte Passwörter oder unsichere Authentifizierungsmethoden Zugriff verschafft.
- **Externe Speichergeräte oder USB-Sticks:** Schadsoftware wurde über infizierte Geräte ins System eingeschleust.

Die Beweissicherung sollte so erfolgen, dass alle Spuren des Angriffs erhalten bleiben und nicht durch übereilte Maßnahmen verloren gehen. Dazu gehören:

- **Sicherung von Log-Dateien,** insbesondere von Firewalls, Servern und Netzwerküberwachungssystemen.
- **Forensische Sicherung der betroffenen Systeme** (z. B. durch Abbildungen des RAM-Speichers und Festplattenkopien).
- **Dokumentation aller auffälligen Aktivitäten** einschließlich Zeitpunkt, betroffene Systeme und erste Reaktionsmaßnahmen.

Falls das Unternehmen nicht über eigene forensische Expertise verfügt, sollte ein externer IT-Forensik-Dienstleister hinzugezogen werden. Die gesicherten Daten helfen nicht nur bei der internen Untersuchung, sondern können auch als Beweismittel für Strafverfolgungsbehörden dienen, falls eine Anzeige erstattet wird.

4.2.3.5 Entscheidungsfindung und Wiederherstellungsoptionen

Sobald die Eindämmung und Beweissicherung abgeschlossen sind, müssen Unternehmen entscheiden, wie sie zur Normalität zurückkehren. Dabei gibt es zwei Hauptoptionen:

1. **Wiederherstellung aus Backups:** Falls vollständige und aktuelle Backups vorhanden sind, können Systeme aus diesen wiederhergestellt werden.
2. **Neuaufsetzen der betroffenen Systeme:** Falls kein sauberes Backup existiert, muss das betroffene System vollständig neu aufgesetzt werden.

Während der Wiederherstellung müssen sämtliche Schwachstellen behoben werden, die den Angriff ermöglicht haben, um zukünftige Vorfälle zu verhindern.

4.2.4 Nachbereitung: Optimierung des Notfallkonzepts

Nach der Bewältigung eines Cyber-Notfalls darf der Vorfall nicht als abgeschlossen betrachtet werden. Vielmehr ist es essenziell, dass Unternehmen die Situation analysieren und daraus lernen, um zukünftige Sicherheitsvorfälle besser handhaben oder sogar verhindern zu können.

4.2.4.1 Dokumentation und Lessons Learned

Jeder Sicherheitsvorfall sollte detailliert dokumentiert werden, um Erfahrungen für zukünftige Vorfälle nutzbar zu machen. Diese Dokumentation sollte enthalten:

- **Was ist passiert?** (Art des Angriffs, betroffene Systeme).
- **Wie wurde der Vorfall entdeckt?** (Sicherheitsalarme, Meldung von Mitarbeitenden).
- **Welche Maßnahmen wurden ergriffen?** (Reaktion, Kommunikation, Wiederherstellung).
- **Welche Schäden oder Verluste sind entstanden?** (Finanziell, rechtlich, operativ).
- **Welche Maßnahmen müssen ergriffen werden, um eine Wiederholung zu vermeiden?**

Die Dokumentation hilft auch, rechtliche Anforderungen zu erfüllen, falls externe Stellen eine Untersuchung durchführen.

4.2.4.2 Regelmäßige Überprüfung und Aktualisierung des Notfallkonzepts

Basierend auf den Erkenntnissen aus vergangenen Vorfällen muss das Cyber-Notfallkonzept regelmäßig überarbeitet und aktualisiert werden. Dabei sollten folgende Fragen geklärt werden:

- **Funktionierten die Reaktionsmaßnahmen wie geplant?**
- **Gibt es technische oder organisatorische Verbesserungsmöglichkeiten?**
- **Müssen neue Bedrohungen in den Plan aufgenommen werden?**

Besonders nach großen Sicherheitsvorfällen sollte eine vollständige Überarbeitung des Notfallplans erwogen werden.

4.2.4.3 Verstärkung des Monitorings nach einem Angriff

Nach einem Cyber-Vorfall ist das Unternehmen besonders anfällig für weitere Angriffe. Angreifer testen oft verschiedene Schwachstellen und könnten nach einem ersten erfolgreichen Angriff erneut versuchen, in das System einzudringen. Daher ist es essenziell, das Monitoring der IT-Systeme zu intensivieren, um ungewöhnliche Aktivitäten frühzeitig zu erkennen. Dazu gehören Maßnahmen wie:

- **Erweiterte Überwachung von Systemlogs,** um verdächtige Anmeldeversuche oder ungewöhnliche Datenbewegungen schneller zu identifizieren.
- **Häufigere Sicherheitsaudits und Penetrationstests,** um sicherzustellen, dass keine weiteren Schwachstellen existieren.
- **Neue Sicherheitslösungen zu implementieren,** falls der Vorfall zeigt, dass bestehende Maßnahmen nicht ausgereicht haben.

Ein Beispiel für eine neue Sicherheitslösung nach einem Vorfall wäre die Einführung eines Intrusion Detection Systems (IDS), falls der Angriff unbemerkt über eine ungesicherte Netzwerkverbindung erfolgte. Ebenso könnte ein Unternehmen nach einem Phishing-Angriff mit gestohlenen Zugangsdaten eine verpflichtende Multi-Faktor-Authentifizierung (MFA) für alle sensiblen Systeme einführen.

4.2.4.4 Anpassung der Schulungsmaßnahmen

Erfahrungen aus realen Cyber-Vorfällen sollten genutzt werden, um zukünftige Schulungen praxisnäher zu gestalten. Falls ein Unternehmen beispielsweise Opfer eines Ransomware-Angriffs wurde, sollte eine Schulung zu Erkennung und Vermeidung von Ransomware durchgeführt werden.
Die Schulungsstrategie sollte regelmäßig überprüft und angepasst werden, um aktuelle Bedrohungen abzudecken.

4.3 Checklisten & Vorlagen

Die folgenden Checklisten und Vorlagen bieten Unternehmen eine praktische Unterstützung bei der Umsetzung des Cyber-Notfallkonzepts. Sie helfen dabei, wichtige Maßnahmen zu planen, Verantwortlichkeiten zu definieren und Notfallszenarien systematisch zu bewältigen. Diese Dokumente sollten regelmäßig überprüft und aktualisiert werden, um sie an neue Bedrohungslagen anzupassen.

4.3.1 Notfall-Kontaktliste

Eine aktuelle und schnell zugängliche Notfall-Kontaktliste ist essenziell, um im Falle eines Cyber-Vorfalls unverzüglich reagieren zu können. Sie sollte alle internen und externen Ansprechpartner enthalten, die im Ernstfall eingebunden werden müssen.

Funktion	Name	Telefon	E-Mail	Verantwortlichkeit
IT-Sicherheits-beauftragter	**Max Mustermann**	+49 123 456789	max.mustermann@firma.de	Koordination IT-Sicherheitsmaßnahmen
Geschäftsleitung	**Lisa Beispiel**	+49 987 654321	lisa.beispiel@firma.de	Entscheidungsträger für kritische Maßnahmen
Datenschutz-beauftragter	**Anna Datenschutz**	+49 234 567890	anna.datenschutz@firma.de	Meldepflichten und rechtliche Bewertung
Externer IT-Sicherheits-dienstleister	**IT-Response GmbH**	+49 111 222333	support@it-response.de	Forensik und Vorfallsanalyse
Zentrale Ansprechstelle Cybercrime (ZAC)	**Polizei**	+49 800 1234567	cybercrime@polizei.de	Strafverfolgung und Beratung

Tabelle 2: Notfall-Kontaktliste

Diese Liste sollte ausgedruckt und physisch aufbewahrt werden, damit sie auch im Falle eines Systemausfalls zur Verfügung steht.

4.3.2 Maßnahmen-Checkliste für KMU

Die nachfolgende Checkliste enthält alle essenziellen Maßnahmen, die ein KMU vor, während und nach einem Cyber-Vorfall umsetzen sollte.

PRÄVENTIVE MASSNAHMEN (VORBEREITUNG AUF EINEN CYBER-VORFALL)

- ○ Dokumentation aller IT-Systeme und Netzwerke ist aktuell.
- ○ Sicherheitsupdates für alle Systeme werden regelmäßig durchgeführt.
- ○ Firewall, Virenscanner und Intrusion Detection Systeme sind eingerichtet und aktiv.
- ○ Regelmäßige Backups werden erstellt und deren Wiederherstellung wurde getestet.
- ○ Multi-Faktor-Authentifizierung ist für alle kritischen Systeme aktiviert.
- ○ Mitarbeitende erhalten regelmäßige Schulungen zu Cybersicherheit.
- ○ Ein Cyber-Notfallplan existiert und ist allen relevanten Mitarbeitenden bekannt.

MASSNAHMEN IM AKUTEN NOTFALL (REAKTION AUF EINEN CYBER-VORFALL)

- ○ Sofortige Erkennung und Klassifizierung des Vorfalls (z. B. Ransomware, Datenleck, DDoS-Angriff)
- ○ Betroffene Systeme vom Netzwerk trennen, um eine weitere Ausbreitung zu verhindern.
- ○ Interne IT-Abteilung oder externer IT-Sicherheitsdienstleister wurde informiert.
- ○ Erste Maßnahmen zur Schadensbegrenzung wurden ergriffen (z. B. Passwortänderung, Sperrung betroffener Zugänge).
- ○ Beweissicherung wurde eingeleitet (Logdateien sichern, Netzwerkanalysen durchführen).
- ○ Meldung an die zuständige Datenschutzbehörde (bei personenbezogenen Daten erforderlich).
- ○ Kommunikation mit betroffenen Kunden und Partnern wurde eingeleitet.

MASSNAHMEN NACH DEM VORFALL (ANALYSE & OPTIMIERUNG)

- ○ Betroffene Systeme wurden analysiert und bereinigt.
- ○ Sicherheitsmaßnahmen wurden überprüft und verbessert.
- ○ Lessons Learned wurden dokumentiert, um künftige Vorfälle zu verhindern.
- ○ Schulungen für Mitarbeitende wurden angepasst, um erneute Fehler zu vermeiden.
- ○ Das Notfallkonzept wurde auf Basis der Erkenntnisse aktualisiert.

Diese Checkliste hilft Unternehmen, sich vor Cyber-Bedrohungen zu schützen, Notfallmaßnahmen gezielt umzusetzen und aus vergangenen Vorfällen zu lernen.

4.3.3 Vorlage: Incident Response Plan (IRP)

Ein Incident Response Plan (IRP) beschreibt die konkreten Schritte, die ein Unternehmen im Falle eines Cyber-Vorfalls unternehmen muss. Dieses Dokument dient als Vorlage, die an die spezifischen Anforderungen des Unternehmens angepasst werden kann.

1. Erkennung und Bewertung des Vorfalls

Datum und Uhrzeit des Vorfalls: _____
Betroffene Systeme oder Abteilungen: _____
Art des Vorfalls (z. B. Ransomware, Datenleck, DDoS): _____
Beschreibung der ersten beobachteten Anzeichen: _____
Erste Einschätzung der Auswirkungen auf den Geschäftsbetrieb: _____

2. SOFORTMASSNAHMEN ZUR EINDÄMMUNG DES SCHADENS

- Betroffene Systeme wurden vom Netzwerk getrennt, um eine weitere Ausbreitung zu verhindern.
- Zugriff auf kompromittierte Benutzerkonten wurde gesperrt.
- Externe IT-Forensiker oder Sicherheitsexperten wurden kontaktiert.
- Beweissicherung wurde eingeleitet (Logfiles, Netzwerkanalyse, Speicherabbilder).
- Mitarbeitende und relevante Stakeholder wurden informiert.
- Vorläufige Risikobewertung zur Einschätzung des potenziellen Schadens durchgeführt.

3. KOMMUNIKATION & MELDEPFLICHTEN

- Interne IT-Teams und Geschäftsleitung informiert.
- Datenschutzbehörde informiert (falls erforderlich, z. B. bei personenbezogenen Daten).
- Kunden und Partner informiert (falls deren Daten betroffen sind).
- Polizei oder Strafverfolgungsbehörden informiert (falls erforderlich).
- Öffentlichkeitsstrategie definiert, falls öffentliche Kommunikation erforderlich ist.

4. WIEDERHERSTELLUNG & SICHERHEITSVERBESSERUNG

- Entscheidung über Wiederherstellung aus Backups getroffen.
- Betroffene Systeme überprüft, bereinigt und ggf. neu aufgesetzt.
- Sicherheitsmaßnahmen verbessert, um erneute Angriffe zu verhindern.
- Lessons Learned dokumentiert und Schulungen aktualisiert.
- Der Incident Response Plan wurde überarbeitet und optimiert.

Diese Vorlage dient als Leitfaden für Unternehmen, um schnell und effizient auf Cyber-Vorfälle zu reagieren. Durch eine strukturierte Vorgehensweise kann der Schaden minimiert und die Wiederherstellung beschleunigt werden.

4.4 Fazit & Ausblick

Die zunehmende Digitalisierung und die wachsende Bedrohung durch Cyberangriffe erfordern von kleinen und mittleren Unternehmen (KMU) ein gezieltes Vorgehen, um sich gegen IT-Sicherheitsvorfälle zu schützen. Dieses Handbuch stellt eine praxisnahe Anleitung zur Entwicklung und Umsetzung eines Cyber-Notfallkonzepts dar. Die strukturierte Vorgehensweise in den vier Phasen – Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung – ermöglicht es KMU, ihre Cybersicherheitsmaßnahmen systematisch zu verbessern und ihre Widerstandsfähigkeit gegenüber Cyber-Bedrohungen zu stärken.

4.4.1 Wichtige Erkenntnisse aus dem Handbuch

1. **Vorbereitung ist der Schlüssel zur Sicherheit:** Unternehmen, die präventive Maßnahmen wie regelmäßige Sicherheitsaudits, Mitarbeiterschulungen und aktuelle IT-Sicherheitsrichtlinien umsetzen, sind deutlich widerstandsfähiger gegenüber Cyber-Bedrohungen.
2. **Schnelles Handeln im Ernstfall minimiert Schäden:** Ein gut definierter Incident Response Plan (IRP) stellt sicher, dass alle Beteiligten wissen, was im Falle eines Cyberangriffs zu tun ist. Die frühzeitige Erkennung und Eindämmung eines Vorfalls reduziert die Auswirkungen auf den Geschäftsbetrieb erheblich.

3. **Lernen aus Vorfällen führt zu kontinuierlicher Verbesserung:** Unternehmen sollten nach jedem Cyber-Vorfall eine detaillierte Analyse durchführen, um aus Fehlern zu lernen und ihre Sicherheitsmaßnahmen zu optimieren. Eine regelmäßige Überprüfung und Anpassung des Notfallkonzepts trägt dazu bei, neue Bedrohungen frühzeitig zu erkennen und abzuwehren.

4.4.2 Ausblick und zukünftige Maßnahmen

Die IT-Sicherheitslandschaft entwickelt sich ständig weiter, weshalb KMU ihre Cyber-Resilienz fortlaufend verbessern müssen. Es wird empfohlen, dass Unternehmen regelmäßig:

- **Neue Bedrohungen analysieren und Sicherheitsstrategien anpassen:** Cyberkriminelle entwickeln ständig neue Angriffsvektoren. Die Integration aktueller Sicherheitsempfehlungen von Organisationen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), NIST oder ENISA hilft, stets auf dem neuesten Stand zu bleiben.
- **Technologische Fortschritte nutzen:** Der Einsatz von künstlicher Intelligenz (KI) für Bedrohungserkennung, automatisierten Incident-Response-Systemen und modernen Authentifizierungsmethoden kann Unternehmen helfen, sich besser zu schützen.
- **Zusammenarbeit mit externen Sicherheitsdienstleistern suchen:** Gerade für KMU ohne eigene IT-Abteilung kann es sinnvoll sein, auf externe Dienstleister für Penetrationstests, IT-Forensik oder Managed Security Services zurückzugreifen.
- **Das Bewusstsein für Cybersicherheit in der Belegschaft stärken:** Sicherheitsschulungen sollten nicht als einmalige Maßnahme betrachtet werden, sondern regelmäßig durchgeführt werden, um Mitarbeitende über aktuelle Bedrohungen und Schutzmaßnahmen aufzuklären.

4.4.3 Abschließende Empfehlung

Cybersicherheit ist keine einmalige Maßnahme, sondern ein fortlaufender Prozess. Unternehmen, die sich mit präventiven Sicherheitsmaßnahmen, strukturierten Notfallplänen und kontinuierlichen Verbesserungen auf mögliche Cyber-Bedrohungen vorbereiten, minimieren nicht nur ihre Risiken, sondern sichern auch langfristig ihre Geschäftsfähigkeit. Dieses Handbuch bietet eine Grundlage für den Aufbau eines effektiven Cyber-Notfallmanagements und sollte regelmäßig überprüft und weiterentwickelt werden.

4.5 Ressourcen & weiterführende Informationen

Dieses Kapitel stellt wichtige Anlaufstellen, nützliche Tools und bewährte Frameworks vor, die KMU bei der Implementierung und Weiterentwicklung ihres Cyber-Notfallkonzepts unterstützen können. Diese Ressourcen bieten praxisnahe Informationen und aktuelle Sicherheitsrichtlinien für den Schutz vor Cyber-Bedrohungen.

4.5.1 Wichtige Anlaufstellen und Behörden

Für Unternehmen, die von einem Cyber-Vorfall betroffen sind oder präventive Maßnahmen ergreifen möchten, stehen verschiedene Organisationen und Behörden als Ansprechpartner zur Verfügung:

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)** – Bietet Leitlinien und Handlungsempfehlungen für Unternehmen zum Schutz vor Cyber-Bedrohungen. https://www.bsi.bund.de
- **Allianz für Cybersicherheit (BSI ACS)** – Netzwerk zur Förderung des Informationsaustauschs und der Zusammenarbeit zwischen Unternehmen zur Verbesserung der Cybersicherheit. https://www.allianzfuer-Cybersicherheit.de

- **Zentrale Ansprechstelle Cybercrime (ZAC)** – Anlaufstelle für Unternehmen zur Meldung von Cyberangriffen und zur Unterstützung durch Strafverfolgungsbehörden. https://www.bka.de
- **Europäische Agentur für Cybersicherheit (ENISA)** – Entwickelt Strategien und Best Practices für Cybersicherheit in der EU. https://www.enisa.europa.eu
- **Industrie- und Handelskammern (IHKs)** – Viele IHKs bieten Beratung und Weiterbildungen zum Thema IT-Sicherheit für KMU an. https://www.dihk.de
- **Deutsches Institut für Normung (DIN)** – Veröffentlicht Sicherheitsstandards wie ISO 27001, die für Unternehmen relevant sind. https://www.din.de

4.5.2 Kostenlose Tools für Incident Management

Neben offiziellen Anlaufstellen gibt es eine Vielzahl von kostenlosen Tools, die Unternehmen dabei unterstützen, Cyber-Risiken zu erkennen, Vorfälle zu analysieren und darauf zu reagieren:

- **AlienVault OTX** – Open-Source-Bedrohungsdatenbank zur Identifikation aktueller Cyber-Bedrohungen. https://otx.alienvault.com
- **Wireshark** – Netzwerk-Analyse-Tool zur Untersuchung verdächtiger Aktivitäten in Unternehmensnetzwerken. https://www.wireshark.org
- **Snort** – Open-Source Intrusion Detection System (IDS) zur Erkennung von Cyberangriffen. https://www.snort.org
- **VirusTotal** – Online-Dienst zur Analyse von Dateien und URLs auf Malware-Befall. https://www.virustotal.com
- **CyberChef** – Webbasierte Anwendung zur schnellen Analyse und Verarbeitung von Daten (Verschlüsselung, Kodierung, Log-Analyse). https://gchq.github.io/CyberChef
- **TheHive & Cortex** – Open-Source-Plattformen für Incident Response Management und forensische Analysen. https://thehive-project.org

Diese Tools können Unternehmen helfen, Sicherheitsvorfälle schneller zu erkennen und ihre IT-Resilienz zu erhöhen. Vor der Implementierung sollte jedoch geprüft werden, ob die jeweilige Software mit den Sicherheitsrichtlinien des Unternehmens konform geht.

4.5.3 Standards und Frameworks für Cyber-Resilienz

Es gibt eine Reihe etablierter Frameworks und Normen, die Unternehmen als Grundlage für ihr Cyber-Notfallkonzept nutzen können:

- **ISO/IEC 27001** – Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS). https://www.iso.org
- **NIST Cyber-Security Framework** – US-amerikanischer Leitfaden für Cybersicherheitsstrategien, der sich auch in Europa bewährt hat. https://www.nist.gov/cyberframework
- **IT-Grundschutz-Kompendium (BSI)** – Sammlung bewährter Verfahren für IT-Sicherheitsmanagement. https://www.bsi.bund.de/DE/Themen/ITGrundschutz
- **CIS Controls (Center for Internet Security)** – Praktische Maßnahmen zur Stärkung der IT-Sicherheit in Unternehmen. https://www.cisecurity.org/controls
- **EU NIS 2-Richtlinie** – Anforderungen für Netzwerk- und Informationssicherheit in der EU. https://digital-strategy.ec.europa.eu/en/policies/nis-directive

4.5.4 Fazit

Die hier aufgeführten Ressourcen, Tools und Standards bieten eine wertvolle Unterstützung für KMU bei der Entwicklung, Implementierung und Weiterentwicklung eines Cyber-Notfallkonzepts. Unternehmen sollten regelmäßig prüfen, welche neuen Technologien, Methoden und Empfehlungen verfügbar sind, um ihre IT-Sicherheit kontinuierlich zu verbessern. Die Kombination aus präventiven Maßnahmen, strukturierten Notfallplänen und fortlaufender Weiterbildung hilft KMU, ihre Resilienz gegen Cyber-Bedrohungen nachhaltig zu erhöhen.

4.6 Anlage: Cyber-Notfallplan

HOLZBAU SCHNEIDER GMBH
Erstellt am: [Datum]
Letzte Aktualisierung: [Datum]
Verantwortlich: Geschäftsführung & IT-Support Meier GmbH
Version: 1.0

1. UNTERNEHMENSPROFIL & IT-LANDSCHAFT

Unternehmensdaten

- **Name:** Holzbau Schneider GmbH
- **Branche:** Zimmerei & Holzbau
- **Standort:** Ländlicher Raum, Niederbayern
- **Mitarbeitende:** 25 Personen
- **Geschäftsführer:** Hans Schneider
- **IT-Partner:** IT-Support Meier GmbH

KRITISCHE IT-SYSTEME (PRIORITÄTSLISTE)

System	Beschreibung	Kritikalität	Max. Ausfallzeit
ERP-System (Lexware)	Auftragsabwicklung, Buchhaltung	**KRITISCH**	4 Stunden
Kundendatenbank	Digitale Kundenakten, Projektdaten	**HOCH**	8 Stunden
CNC-Maschinensteuerung	Produktionssteuerung Werkstatt	**HOCH**	6 Stunden
E-Mail-System	Kommunikation m. Kunden/Lieferanten	**MITTEL**	12 Stunden
Bauleiter-Laptops	Mobile Projektdokumentation	**MITTEL**	24 Stunden
Fileserver	Zentrale Datenspeicherung	**HOCH**	8 Stunden

Tabelle 3: Kritische IT-Systeme

2. CYBER-NOTFALLTEAM & VERANTWORTLICHKEITEN

NOTFALLTEAM-STRUKTUR

Rolle	Name	Telefon	E-Mail	Verantwortung
Incident Commander	**Hans Schneider (GF)**	0171-1234567	h.schneider@holzbauschneider.de	Strategische Entscheidungen
IT-Koordinator	**Thomas Meier (extern)**	0172-9876543	t.meier@it-supportmeier.de	Technische Maßnahmen
Kommunikations-verantwortlicher	**Mia Schneider (Büro)**	0173-5555555	m.schneider@holzbauschneider.de	Interne/externe Kommunikation
Produktionsleiter	**Josef Huber**	0174-7777777	j.huber@holzbauschneider.de	Werkstatt & Baustellen

Tabelle 4: Notfallteam-Struktur

EXTERNE NOTFALLKONTAKTE

Organisation	Kontakt	Telefon	E-Mail	Zuständigkeit
IT-Support Meier GmbH	**Thomas Meier**	0172-9876543	notfall@it-support-meier.de	24/7 IT-Support
Polizei Bayern (Cybercrime)	**ZAC Bayern**	089-12345678	cybercrime@polizei.bayern.de	Strafverfolgung
Datenschutzbehörde Bayern	**BayLDA**	0981-180093-0	poststelle@lda.bayern.de	DSGVO-Meldungen
Cyber-Forensik Spezialist	**SecurIT GmbH München**	089-98765432	notfall@securit-muenchen.de	Forensische Analyse
Rechtsanwalt	**Kanzlei Weber**	0871-444444	info@kanzlei-weber.de	Rechtliche Beratung

Tabelle 5: Externe Notfallkontakte

3. INCIDENT RESPONSE PROZESS

PHASE 1: ERKENNUNG & BEWERTUNG (0-30 MIN)

Erkennungszeichen für Cyber-Vorfälle:

- Ungewöhnlich langsame Systeme (ERP, CNC-Steuerung)
- Verschlüsselte Dateien mit Lösegeldforderung
- Verdächtige E-Mails an Mitarbeitende
- Unbekannte Software-Installationen
- CNC-Maschinen reagieren nicht auf Befehle
- Bauleiter können nicht auf Projektdaten zugreifen

Sofortige Maßnahmen:

1. **Vorfall melden** → Sofort Hans Schneider (GF) informieren
2. **Betroffene Systeme isolieren** → Netzwerkkabel ziehen, WLAN trennen
3. **IT-Support Meier kontaktieren** → 24/7 Hotline: 0172-9876543
4. **Keine Lösegeldzahlung** → Niemals ohne Rücksprache zahlen
5. **Dokumentation beginnen** → Zeitpunkt, betroffene Systeme notieren

INCIDENT-KLASSIFIZIERUNG:

Stufe	Beschreibung	Beispiel	Reaktionszeit
NIEDRIG	Verdächtige E-Mail, einzelner PC betroffen	Phishing-Mail an einen Mitarbeiter	2 Stunden
MITTEL	Mehrere Systeme betroffen, Betrieb eingeschränkt	Malware auf 3-4 Arbeitsplätzen	1 Stunde
HOCH	Produktionsausfall, Kundendaten gefährdet	CNC-Steuerung gehackt, ERP-System down	30 Minuten
KRITISCH	Kompletter IT-Ausfall, Ransomware	Alle Systeme verschlüsselt, Lösegeld gefordert	15 Minuten

Tabelle 6: Incident-Klassifizierung

PHASE 2: EINDÄMMUNG & SCHADENSBEGRENZUNG (30 MIN - 2 STD)

Sofortmaßnahmen je nach Szenario:

Bei Ransomware-Angriff:

1. Alle betroffenen Geräte sofort vom Netzwerk trennen
2. CNC-Maschinen in sicheren Modus versetzen
3. Backup-Status prüfen (letzte Sicherung vor Verschlüsselung?)
4. Externe IT-Forensik beauftragen (SecurIT GmbH)
5. KEINE Lösegeldzahlung ohne Expertenberatung

Bei Phishing/E-Mail-Kompromittierung:

1. Betroffenes E-Mail-Konto sofort sperren
2. Passwort-Reset für alle Mitarbeiter-Accounts
3. Verdächtige E-Mails aus allen Postfächern entfernen
4. Prüfung: Wurden Kundendaten übertragen?

Bei CNC-Maschinensteuerung-Hack:

1. Maschinen sofort stoppen und vom Netzwerk trennen
2. Manuelle Bedienung aktivieren (falls möglich)
3. Prüfung der Produktionsdaten auf Manipulation
4. Backup der Steuerungssoftware einspielen

PHASE 3: BEWEISSICHERUNG (PARALLEL ZU PHASE 2)

Wichtige Spuren sichern:

- Screenshots von Fehlermeldungen/Lösegeldforderungen
- Logfiles der Firewall (durch IT-Support Meier)
- Zeitpunkt der ersten Auffälligkeiten dokumentieren
- Betroffene Systeme NICHT ausschalten (RAM-Daten gehen verloren)
- Externe Festplatten/USB-Sticks sicherstellen
- E-Mail-Header verdächtiger Nachrichten speichern

PHASE 4: KOMMUNIKATION (1-4 STD NACH VORFALL)

Interne Kommunikation:

1. **Mitarbeiter-Information** (durch Maria Schneider):
   - WhatsApp-Gruppe: „Wichtige IT-Störung - Details folgen"
   - Anweisung: Keine Passwörter weitergeben, verdächtige E-Mails melden

2. **Bauleiter informieren:**
   - Alternative Kommunikation: Private Handys nutzen
   - Projektdokumentation vorübergehend auf Papier

Externe Kommunikation:

1. **Kunden** (bei Projektdaten-Betroffenheit):

> „Sehr geehrte Damen und Herren,
> aufgrund technischer Probleme kann es zu Verzögerungen bei der Projektabwicklung kommen. Wir arbeiten an einer schnellen Lösung und informieren Sie über weitere Entwicklungen. Bei Rückfragen: Tel. 08531-12345"

2. **Behörden-Meldung** (bei DSGVO-Relevanz):
   - Datenschutzbehörde Bayern: Binnen 72 St
   - Polizei: Bei Erpressung/Betrug sofort
   - Vorlage für Meldung verwenden (siehe Anlage A)

PHASE 5: WIEDERHERSTELLUNG (4-48 STD)

Backup-Wiederherstellung:

1. **ERP-System:** Tagesaktuelle Sicherung von IT-Support Meier
2. **Kundendaten:** Wöchentliche Sicherung auf externe Festplatte
3. **CNC-Programme:** Backup auf separatem Server in der Werkstatt
4. **E-Mails:** Cloud-Backup beim Provider

Schritt-für-Schritt Wiederherstellung:

1. Forensische Freigabe der bereinigten Systeme
2. ERP-System zuerst wiederherstellen (höchste Priorität)
3. Kundendatenbank und Fileserver
4. CNC-Steuerung nach Sicherheitsprüfung
5. Arbeitsplatz-Computer sukzessive
6. Bauleiter-Laptops zuletzt

System-Härtung vor Wiederinbetriebnahme:

- Alle Passwörter ändern
- Windows-Updates installieren
- Antivirus-Definitionen aktualisieren
- Firewall-Regeln verschärfen
- Zusätzliche Überwachung aktivieren

4. PRÄVENTIVE MASSNAHMEN

Technische Schutzmaßnahmen

- **Firewall:** Business-Firewall (verwaltet durch IT-Support Meier)
- **Antivirus:** Business-Antivirus-Lösung auf allen Geräten
- **Backups:**
  - ERP täglich automatisch (Cloud + lokale NAS)
  - Kundendaten wöchentlich auf externe Festplatte
  - CNC-Programme monatlich auf separaten Server
- **Updates:** Automatische Windows-Updates aktiviert
- **E-Mail-Security:** Spam-Filter beim E-Mail-Provider

Organisatorische Maßnahmen

- **Mitarbeiter-Schulungen:** Jährlich durch IT-Support Meier
- **Passwort-Richtlinie:** Mindestens 8 Zeichen, alle 6 Monate ändern
- **USB-Policy:** Keine privaten USB-Sticks an Firmen-PCs
- **BYOD-Regelung:** Private Geräte nur mit Mobile Device Management
- **Zugriffskontrolle:** VPN für Remote-Zugriff auf Firmennetzwerk

5. BUSINESS CONTINUITY PLAN NOTFALL-BETRIEBSMODUS BEI IT-AUSFALL

Auftragsabwicklung ohne ERP:

- **Papier-Formulare** für neue Aufträge (Vorrat im Büro)
- **Handschriftliche Rechnungen** mit Durchschlag
- **Telefonische Koordination** mit Lieferanten
- **Manuelle Zeiterfassung** auf Baustellen

Produktionssteuerung ohne CNC:

- **Manuelle Maschinenbedienung** (erfahrene Mitarbeiter)
- **Papier-Zeichnungen** aus Archiv verwenden
- **Reduzierte Produktionskapazität** einkalkulieren

Alternative Arbeitsplätze:

- **Büro-Arbeitsplätze:** Tablets mit Cloud-Zugang (Office-Suite)
- **Bauleiter:** Private Smartphones für Dokumentation
- **Buchhaltung:** Externe Steuerberatung als Backup

Lieferanten & Partner informieren:

- **Holzlieferant Bayern-Holz GmbH:** Lieferungen evtl. verzögert
- **Dachdecker-Partner Müller:** Koordination per Telefon
- **Steuerberater Kanzlei Fischer:** Bei Buchhaltungs-Problemen einspringen

6. INCIDENT-SZENARIEN & REAKTIONSPLÄNE

Szenario A: Ransomware-Angriff auf ERP-System

Erkennungszeichen:

- ERP-System (Lexware) startet nicht
- Dateien haben Endung „.encrypted“
- Lösegeldforderung auf Desktop

Sofortmaßnahmen:

1. ERP-Server sofort isolieren (Netzwerkkabel ziehen)
2. Backup-Status prüfen: Letzte Sicherung gestern 22:00 Uhr
3. IT-Support Meier informieren: „Code Rot - Ransomware ERP“
4. Geschäftsführer entscheidet über Polizei-Meldung
5. KEINE Lösegeldzahlung ohne Expertenrat

Wiederherstellung:

- Geschätzte Ausfallzeit: 6-12 Stunden
- Datenverlust: Max. 1 Arbeitstag
- Kosten: Ca. 2.000€ für IT-Forensik + Arbeitszeit

Szenario B: Phishing-Angriff auf Buchhalterin

Erkennungszeichen:

- „Rechnung" per E-Mail von vermeintlichem Lieferanten
- Buchhalterin gibt Zugangsdaten auf gefälschter Website ein
- Ungewöhnliche Überweisungen entdeckt

Sofortmaßnahmen:

1. Online-Banking sofort sperren lassen
2. E-Mail-Account der Buchhalterin deaktivieren
3. Alle Firmen-Passwörter ändern (ERP, Banking, Cloud)
4. Bank über Betrugsversuch informieren
5. Polizei-Anzeige erstatten

Schadensbegrenzung:

- Überweisungen rückgängig machen (falls möglich)
- Kunden über mögliche Datenabflüsse informieren
- Zwei-Faktor-Authentifizierung für alle kritischen Systeme

Szenario C: CNC-Maschinensteuerung gehackt

Erkennungszeichen:

- CNC-Maschine führt falsche Programme aus
- Produktionsqualität plötzlich schlecht
- Unbekannte Netzwerkverbindungen an Maschinensteuerung

Sofortmaßnahmen:

1. Maschinen sofort stoppen (Notaus-Schalter)
2. Netzwerkverbindung zur Steuerung kappen
3. Manuelle Bedienung aktivieren
4. Werkstücke auf Beschädigung prüfen
5. IT-Support für Steuerungs-Analyse beauftragen

Wiederherstellung:

- Steuerungssoftware komplett neu installieren
- Alle CNC-Programme aus Backup wiederherstellen
- Netzwerk-Segmentierung für Maschinensteuerung

7. NACHBEREITUNG & LESSONS LEARNED INCIDENT-DOKUMENTATION (NACH JEDEM VORFALL)

Bericht-Vorlage:

- **Datum/Uhrzeit:** Wann wurde der Vorfall entdeckt?
- **Art des Angriffs:** Ransomware, Phishing, Malware, etc.
- **Betroffene Systeme:** ERP, CNC, E-Mail, etc.
- **Schadenssumme:** Ausfallzeiten, Reparaturkosten, Datenverlust
- **Reaktionszeit:** Wie schnell wurde reagiert?
- **Was lief gut:** Positive Aspekte der Incident Response
- **Verbesserungen:** Was muss beim nächsten Mal besser laufen?

Regelmäßige Plan-Updates

- **Quartalsweise:** Kontaktlisten aktualisieren
- **Halbjährlich:** Backup-Tests durchführen
- **Jährlich:** Notfall-Übung mit allen Beteiligten
- **Nach jedem Vorfall:** Plan basierend auf Erfahrungen anpassen

Schulungsplan

- **Alle Mitarbeiter:** Jährliche Cyber-Security-Schulung
- **Führungskräfte:** Incident Response Training
- **IT-Verantwortliche:** Forensik-Grundlagen
- **Bauleiter:** Sicherer Umgang mit mobilen Geräten

8. ANHANG & VORLAGEN

A) DSGVO-Meldung Vorlage

Meldung einer Verletzung des Schutzes personenbezogener Daten

Unternehmen: Holzbau Schneider GmbH
Datum des Vorfalls: [TT.MM.JJJJ]
Art der Verletzung: [Ransomware/Datenleck/etc.]
Betroffene Personen: [Anzahl Kunden/Mitarbeiter]
Datenarten: [Kundenadressen/Projektdaten/etc.]
Bereits ergriffene Maßnahmen: [Systeme isoliert, IT-Forensik beauftragt]
Geplante Maßnahmen: [Kunden informieren, Sicherheit verstärken]

B) Kunden-Information Vorlage

Betreff: Wichtige Information zu Ihren Daten

Sehr geehrte Damen und Herren, wir informieren Sie über einen
IT-Sicherheitsvorfall in unserem Unternehmen vom [Datum].
Möglicherweise sind dabei auch Ihre personenbezogenen Daten betroffen gewesen.
Was ist passiert: [Kurze Beschreibung]
Betroffene Daten: [Art der Daten]
Unsere Maßnahmen: [Sofortmaßnahmen, Behörden-Meldung]
Empfehlung für Sie: [z.B. Passwörter ändern]

Bei Fragen erreichen Sie uns unter: Tel. 08531-12345

Mit freundlichen Grüßen
Holzbau Schneider GmbH

C) Notfall-Checkliste (Schnellübersicht)

Bei Cyber-Vorfall sofort:

- ☑ Betroffene Systeme isolieren
- ☑ Geschäftsführer informieren (0171-1234567)
- ☑ IT-Support Meier kontaktieren (0172-9876543)
- ☑ Erste Dokumentation (Zeit, betroffene Systeme)
- ☑ KEINE vorschnellen Aktionen (Lösegeldzahlung)

Externe Hilfe bei:

- Ransomware → SecurIT GmbH München (089-9876-5432)
- Rechtsfragen → Kanzlei Weber (0871-444444)
- DSGVO-Meldung → BayLDA (0981-180093-0)
- Strafanzeige → Polizei Bayern Cybercrime (089-1234-5678)

Plan-Status: ☑ Genehmigt durch Geschäftsführung
Nächste Überprüfung: [Datum + 6 Monate]
Notfall-Hotline: 0172-9876543 (IT-Support Meier, 24/7)

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union

5

HANDBUCH OT-SECURITY FÜR KMU

Leitfaden zur Verbesserung Ihrer OT-Sicherheit

FH Oberösterreich

Logistikum

FH Salzburg

Technische Hochschule Deggendorf THD

universität innsbruck

Universität Passau

Einleitung

Was ist Operative Technologie (OT)?
Um einen möglichst guten Einstieg in diesen Use-Case zu gewährleisten, ist es erforderlich, zunächst eine gemeinsame Basis an Begrifflichkeiten aufzubauen. Abbildung 13 zeigt den grundlegenden Aufbau Ihres Unternehmens. Man kann es möglichst grob in drei Teile gliedern.

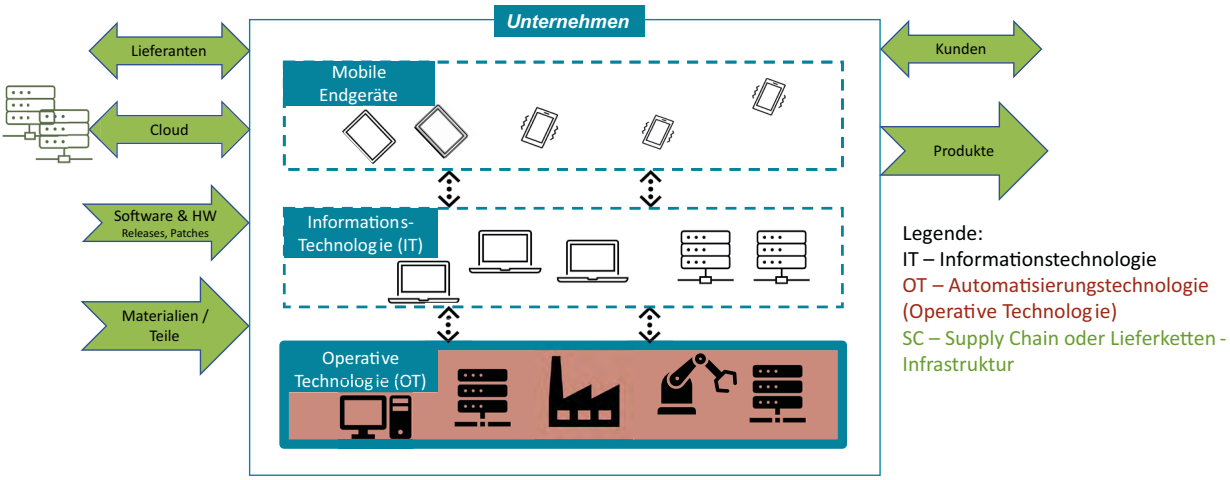


Abbildung 13: Grundlegender Aufbau der digitalen Infrastruktur Ihres Unternehmens.

Außerhalb des Unternehmens zeigen Pfeile in das Unternehmen hinein und hinaus, welche die Supply Chain oder Lieferketteninfrastruktur darstellen. Hier fließen Güter, Informationen und Geld zwischen dem Unternehmen, Lieferanten, Kunden und weiteren Stakeholdern hin bzw. her. Die ersten beiden inneren Ebenen des Unternehmens bilden die mobilen Endgeräte und Informationstechnologie (IT), welche miteinander kommunizieren und aus Geräten wie Computern, Tablets, Smartphones und Servern bestehen. Hauptsächlich ermöglichen sie den Mitarbeitern Kommunikation, Kollaboration, Datensicherung, Finanzbuchhaltung etc.
Unter der IT und abgeschirmt von den mobilen Endgeräten befindet sich die Operative Technologie (OT), oder auch Automatisierungstechnologie. Diese besteht aus Geräten wie Sensoren, speicherprogrammierbare Steuerungen, Industrierobotern oder Fertigungsmaschinen. Die Hauptidee hinter der OT ist, Aufgaben zu automatisieren, Effizienz zu steigern und Sicherheit in der Produktion und anderen Bereichen herzustellen. Daher können auch andere Geräte wie ICS, SCADA, DCS, RTU, PLC, CNC, Energieüberwachung, Verkehrssysteme etc. zur OT gezählt werden. Ein Teil dieser Abkürzungen wird im Glossar erklärt.

5.1.1 Warum ist OT-Sicherheit für kleine und mittlere Unternehmen wichtig?

In den Jahren 2014–2024 wurden fünf große Schadprogramme entwickelt, welche gezielt OT-Systeme angreifen. Hierbei handelt es sich um den Wurm Stuxnet, die Trojaner Havex und Triton/Trisis und die Frameworks Industroyer/Crashoverride und BlackEnergy/Cr4sh. Die meisten dieser Schadprogramme zielen auf größere und vor allem kritische Anlagen ab, da sie häufig der digitalen Kriegsführung dienen. Jedoch wurde in der Vergangenheit Havex auch bei Angriffen auf kleinere Unternehmen nachgewiesen.

Vor allem aufgrund fehlender Ressourcen werden KMU nach und nach immer mehr zu beliebten Zielen von Cyberkriminellen. Einige Schadprogramme besitzen Schnittstellen, sodass sie mit „Plug-ins“ bei Bedarf erweitert werden können. So kann die Malware beispielsweise nach einer vollständigen und verdeckten Infektion der gewünschten Systeme eine Ransomware-Attacke starten und das Unternehmen erpressen.

OT-Systeme können aber auch durch „herkömmliche“ Angriffe und Schadsoftware infiziert werden. Dies ist in der Praxis am häufigsten der Fall und hat dieselben Auswirkungen: die Maschinen stehen, es kann nichts mehr produziert werden und jede kostbare Minute zählt. Sollte der Fall der Fälle eingetreten sein, so hilft nur noch ein ausreichend dokumentiertes Notfallkonzept. Hierfür haben wir jedoch einen extra Use-Case, weswegen dies nicht in diesem Handbuch beschrieben wird. Dieser Use-Case zielt stattdessen darauf ab, durch proaktive Prävention die Wahrscheinlichkeit und den potenziellen Schaden von Cyberangriffen deutlich zu minimieren (siehe Kapitel 4).

5.1.2 Was sind die größten Pitfalls?

Viele Unternehmen behandeln die OT genauso wie die IT – bei manchen ist die IT-OT-Konvergenz sogar schon so weit fortgeschritten, dass diese gar nicht mehr unterschieden oder voneinander getrennt werden können. Während die IT-OT-Konvergenz zwar einige Vorteile mit sich bringt, so birgt sie doch eine große Gefahr: OT-Geräte verfügen in der Regel über wenig Schutz gegen Schadsoftware. Die Infektion ist für einen Angreifer dementsprechend wesentlich unkomplizierter.

Des Weiteren sind beide Bereiche von Grund auf verschieden aufgestellt: Im Sinne der CIA-Triade steht in der OT die Verfügbarkeit an höchster Stelle, da Ausfälle zu einem gesamten Produktionsstopp führen würden, während in der IT kleinere Ausfälle nicht besonders tragisch sind. Während in der IT-Updates fast schon an der Tagesordnung stehen, sind diese in der OT nur schwer möglich und meistens mit Produktionspausen verbunden, weswegen sie meistens so lange wie möglich hinausgezögert werden. Daher sind diese Geräte auch weniger gut gegen Angriffe geschützt. Ein sehr bekannter Unterschied ist auch der Lebenszyklus der Geräte, welcher in der IT eher kurz ist und in der OT sehr lange.

Sicherheitskonzepte, welche in der IT-Anwendung finden, sind daher in der OT zwar auch anwendbar, bringen aber aus all diesen Gründen nur wenig adäquaten Schutz.

5.2 Schritte vor der Erhöhung der OT-Security-Posture

Die erfolgreiche Umsetzung eines jeden Projektes erfordert eine klare Zielsetzung vor Beginn eines solchen Projektes. Da die Anforderungen je nach Unternehmen, Branche und regulatorischen Vorgaben variieren, sollten die Projektinhalte flexibel an die individuellen Bedürfnisse angepasst werden. Die folgenden Überlegungen helfen, diese Aspekte zielgerichtet zu strukturieren und eine fundierte Basis für ein OT-Security-Projekt zu schaffen.

5.2.1 Zielsetzung festlegen

Zunächst sollten klare Ziele für die Umsetzung von OT-Security definiert werden, da die Projektinhalte variabel an die eigenen Bedürfnisse angepasst werden können. Folgende Überlegungen können dabei hilfreich sein:

- Ziele definieren: Was soll erreicht werden? Ein detaillierter Überblick über einzelne Ziele wird dann in Abschnitt 5.3.1.4 erarbeitet.
- Erforderliche Standards prüfen: Strebt das Unternehmen eine Zertifizierung oder die Einhaltung einer Norm an (bspw. TISAX)? Müssen gesetzliche Vorschriften eingehalten werden? Einen Überblick über geeignete Regularien findet sich in Abschnitt 5.3.1.3.

- Ressourcen planen: Wie viele personelle und finanzielle Ressourcen stehen für das Projekt zur Verfügung? Welche Daten liegen bereits über die OT-Umgebung vor?
- Zeitrahmen festlegen: Liegt der Schwerpunkt auf kurz- oder langfristigen Projektinhalten? Wie schnell sollen Resultate sichtbar sein, bzw. können sie sichtbar werden (aufgrund von Terminknappheit des externen OT-Wartungspersonals)?

5.2.2 Verantwortlichkeiten festlegen

Ein oder zwei zentrale Ansprechpartner im Unternehmen sollten für die Umsetzung der Cybersicherheitsmaßnahmen verantwortlich sein. Bei der Auswahl dieser Personen sollte darauf geachtet werden, dass sie mindestens ein grundlegendes Verständnis von Cybersicherheit und den OT-Prozessen haben (siehe 2.3.2).

5.2.3 Priorisierung der Projektinhalte und Festlegung eines Projektplanes

Bevor mit der Umsetzung der im Handbuch beschriebenen Inhalte begonnen werden kann, ist eine Priorisierung und strukturierte Planung auf Basis der Projektziele erforderlich.
Als Hilfestellung steht Ihnen ein anpassbares Gantt-Diagramm (siehe beiliegende Excel-Datei) zur Verfügung, dass die in Kapitel 5.3 beschriebene Vorgehensweise sowie eine grobe Aufwandsschätzung bereits enthält. Es soll Ihnen helfen, die Projektinhalte vor Projektbeginn individuell auf Ihr Unternehmen abzustimmen und zu priorisieren. Es sollte während der Projektlaufzeit regelmäßig aktualisiert werden, um den Projektfortschritt nachvollziehbar zu dokumentieren.

5.3 Vorgehensweise zur Umsetzung eines OT-Security- Projektes

Dieses Handbuch bietet vier Phasen zur Umsetzung von Maßnahmen im Bereich OT-Security. Diese sind an den PDCA-Zyklus angelehnt und daher nicht in der Reihenfolge veränderbar. Die Reihenfolge, in der die Maßnahmen oder Best Practices implementiert werden sollen, kann jedoch frei gewählt werden.

5.3.1 Plan: Bestehende OT-Security bewerten und Verbesserungspotenzial identifizieren

Zunächst ist es wichtig, seine OT-Umgebung zu bewerten, um sie anschließend verbessern zu können. Für eine Bewertung wiederum ist es ausschlaggebend, einen Überblick über die gesamte OT-Umgebung zu erhalten. Bei ISO 27001-zertifizierten Unternehmen ist eine regelmäßig aktualisierte Inventarliste vorgeschrieben, welche sich nach einer Aktualisierung perfekt hierfür eignet. Nichtzertifizierten Unternehmen wird ans Herz gelegt, eine solche Inventarliste anzulegen. Diese hilft auch beispielsweise zur Identifikation von unbekannten Geräten im eigenen Netzwerk. In der Praxis kann eine solche Liste entweder physisch oder digital gepflegt werden. Bei digitaler Führung ist jedoch zu beachten, dass diese sicher aufbewahrt wird, damit sie im Notfall abrufbar ist. Das CySeReS-KMU-Team hat solche Inventarlisten bereits sowohl in Papierform als auch in Form einer Excel-Tabelle oder eines „Wikis“ vorgefunden. Nach Belieben sind selbstverständlich auch andere Lösungen denkbar.

Zum Beispiel könnte eine solche Liste folgendermaßen aussehen (die folgende Vorlage kann – je nach Anwendungsfall – unzureichend oder auch zu komplex sein. Aufgrund sensitiver Daten sollte die Liste nur verschlüsselt gespeichert werden und nur bestimmten Personen Zugriff erteilt werden):

- Interne_ID_des_Geräts (Gerätename):
  - Hersteller mit Kontaktdaten: XX
  - Instandhalter mit Kontaktdaten: XX
  - Notfallkontaktdaten: XX
  - SLAs:
    - XX
    - YY
  - Modellnummer: XX
  - Seriennummer: XX
  - Installationsdatum: XX.XX.XXXX
  - EOL-Datum: XX.XX.XXXX
  - Standort: XX
  - Funktion: XX
  - Hardware-Version: XX
  - Firmware-Version: XX
  - Software-Version: XX
  - Schnittstellen: XX
  - Netzwerkkonfiguration: Produktionsnetz/Halle XX
  - Letzte Wartung: XX
  - Wartungsintervall: XX
  - Wartungsprotokolle und Berichte:
    - XX
    - YY
  - Zustand: XX
  - Verantwortlicher: XX
  - Passworthinweis: XX
  - Bekannte Schwachstellen: XX
  - Compliance-Anforderungen: XX
  - Handbücher und weitere Dokumentation:
    - XX
    - YY
  - Letzte Aktualisierung dieses Eintrags: XX.XX.XXXX
  - Weitere Bemerkungen: XX
- Interne_ID_des_Geräts_2 (Gerätename 2): [...]

Mithilfe dieser Inventarliste kann nun die OT identifiziert werden. So identifizierte Geräte, Software, Daten und Datenkörper sollten in der Inventarliste speziell gekennzeichnet werden. Danach kann die OT-Security bewertet werden. Hierfür gibt es mehrere Möglichkeiten: wir haben die „wichtigsten" Best Practices in Abschnitt 5.3.1.1 aufgelistet und kurz beschrieben, um einen Überblick über größere Verbesserungspotenziale zu schaffen. Zum anderen existieren auch kostenlose Tools zur Selbsteinschätzung, welche in Abschnitt 5.3.1.2 beschrieben sind. Zu guter Letzt können auch gängige Standards konsultiert werden, um mögliche Maßnahmen festzustellen (siehe Abschnitt 5.3.1.3). Jedoch sind die meisten Standards zu komplex für KMU und daher nicht wirklich realisierbar. Unsere Best Practices wurden daher so ausgewählt, dass sie bereits einen großen Teil dieser Standards abdecken, ohne zu sehr ins Detail zu gehen.

Hier ist allerdings auch besonders wichtig, nicht nur seine eigene OT-Sicherheit zu bedenken: liefert man selbst Geräte aus, welcher der OT zuzuschreiben sind, so sollten auch diese bei der Bewertung seiner eigenen OT-Security mitbedacht werden. Des Weiteren ist die eigene digitale Infrastruktur nur so sicher wie die des schwächsten Glieds in der eigenen Lieferkette. Wird ein anderes Unternehmen aus meiner Lieferkette kompromittiert, so kann dies sofortige Auswirkungen auf mein eigenes Unternehmen haben. Beispielsweise kann Schadsoftware über die Lieferkette in mein Unternehmen gelangen. Der Stillstand eines Lieferanten kann für mich allerdings auch ein Importstopp oder der eines Kunden kann ein Exportstopp für mein eigenes Unternehmen bedeuten. Für Lieferkettensicherheit in KMU haben wir jedoch einen eigenen Use-Case (siehe Kapitel 2).

5.3.1.1 Die „wichtigsten" Best Practices

Dieser Abschnitt listet die „wichtigsten" Best Practices, welche wir sowohl der wissenschaftlichen als auch nicht-wissenschaftlichen Literatur entnommen haben. Diese sind nach „Wichtigkeit" sortiert, wobei der erste Best Practice der „wichtigste" ist. Feedback hierzu erhielten wir unter anderem von Teilnehmern bei unserem OT-Security-Workshop auf der IKT-Sicherheitskonferenz 2024 sowie durch Experteninterviews. Die meisten dieser Best Practices wurden in vielen KMU vor allem wegen einem Mangel an Ressourcen (Geld, Wissen etc.) nicht angewandt. Allerdings spielten sicher oft auch eine falsche Einschätzung der Wichtigkeit von OT-Security sowie „Bequemlichkeit" eine große Rolle.

5.3.1.1.1 Backups

Risikominimierung: hoch
Kosten: mittel (Backup-Anbieter oder eigene Medien sowie Duplikat aller Geräte erforderlich)
Zeitaufwand: mittel (lediglich Initialkonfiguration und regelmäßige Wartung erforderlich)

Backups sollten in zweierlei Hinsicht bedacht werden: zum einen sollten Datensicherungen angelegt werden – zum anderen werden „Backup-Geräte" benötigt.

Datensicherungen für den Notfall sollten möglichst nach der 3-2-1-Methode angefertigt werden. Diese besagt, dass drei Kopien der Daten angefertigt werden sollten, wovon zwei auf verschiedenen Speichermedien sind und eine „off-site" gelagert wird. Das Backup sollte möglichst allumfassend sein und kann inkrementell geschehen. Jedoch sollte auch von Zeit zu Zeit wieder ein vollständiges Backup durchgeführt werden, um sicher zu stellen, dass die inkrementellen Backups korrekt sind.

Die Backup-Geräte sollten in der Lage sein, zum einen über einen kürzeren Zeitraum, wie beispielsweise während Updates, aber auch über mehrere Tage hinweg im Falle eines größeren Cyberangriffs, die Produktion bis zu einem bestimmten Level aufrecht zu erhalten. Die Inventarliste eignet sich auch hier zur Identifikation des individuellen Bedarfs.

5.3.1.1.2 Netzwerksegmentierung

Risikominimierung: hoch
Kosten: mittel (Firewall-Hardware erforderlich)
Zeitaufwand: hoch (Konfiguration durch Experten nötig)

Es ist unbestritten, dass der wichtigste Punkt in Sachen OT-Security die Netzwerksegmentierung ist. Bei der Netzwerksegmentierung geht es im Allgemeinen darum, der IT-OT-Konvergenz entgegenzuwirken. Hierfür wird mindestens eine Firewall eingerichtet, welche die OT von der IT abschirmt. Zusätzlich wird darauf geachtet, dass es auch sonst keine Möglichkeit gibt, sich von außen direkt zur OT verbinden zu können. Im Idealfall werden sogar mehrere Firewalls eingerichtet, um zwischen diesen eine DMZ einrichten zu können. Das BSI hat für OT-Netze einen eigenen Leitfaden erstellt.[3]

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/BS_ICS-OT-Netze.html

Hier ist es vor allem wichtig, die Struktur an das Unternehmen anzupassen. Manche Unternehmen erlauben einen Zugriff auf die OT durch VPNs. Dies kann beispielsweise sinnvoll sein, wenn auf die OT häufig zugegriffen werden muss. Allerdings muss hier bedacht werden, dass dies eine mögliche Tür darstellt, welche Angreifer ausnutzen könnten. Die nötigen Zugangsdaten für den VPN-Zugriff könnten beispielsweise durch Phishing, aber auch durch sämtliche Schadsoftware ohne Nutzerinteraktion erlangt werden.
In jedem Fall ist die Firewall entsprechend zu konfigurieren, dass alle nicht benötigten Ports und Zugriffe vollständig blockiert werden. Ausnahmen müssen hier sehr gut durchdacht und für die Zukunft dokumentiert werden. Auch eine Kommunikation der Geräte in der OT untereinander sollte nur mit Bedacht ermöglicht werden, da sonst ein Domino-Effekt nicht ausgeschlossen werden kann. Wird ein Gerät kompromittiert, so kann bei unzureichendem Schutz ein weiteres Gerät bereits nach kurzer Zeit auch betroffen sein.
In manchen Unternehmen kann sogar ganz auf einen „externen" Zugriff auf die OT komplett verzichtet werden. In diesen Fällen ist es sinnvoll, alle physischen Verbindungen zwischen IT und OT zu trennen, da dann offensichtlich keine Firewall und ähnliche Hard- und Software benötigt wird.

5.3.1.1.3 Zugriffskontrolle

Risikominimierung: mittel
Kosten: mittel (bei physischer Zugriffskontrolle extra Hardware benötigt)
Zeitaufwand: mittel (Einrichtung könnte aufwendiger werden)

Der Oberbegriff der Zugriffskontrolle umfasst hier nicht nur die digitale, sondern auch die physische Zugriffskontrolle. Bei der ersteren eignet sich vor allem das Least-Privilege-Prinzip besonders, um Daten vor ungewollten Zugriffen zu schützen. Ziel des Prinzips ist es, jedem Benutzer eine Rolle zuzuweisen, welche es ihm erlaubt, nur auf bestimmte Funktionen zugreifen zu können. Diese Funktionen sollten so eingeschränkt wie nur möglich und so offen wie nur nötig sein. Meistens wird das Prinzip aus „Bequemlichkeit" missachtet – beispielsweise braucht ein Programmierer keinen Administratorzugang zu einer Datenbank, wenn er nur Daten auslesen will. Genau so wenig braucht die Sekretärin keinen Zugang zum zentralen Server. Für die physische Zugriffskontrolle werden beispielsweise verschiedene Schlüssel angelegt, damit nur bestimmte Personen Zugang zum Serverraum besitzen. Genau so können auch Maschinen gleichzeitig digital und physisch gesichert werden – mit Benutzeraccounts und einer Abschirmung, welche einen bestimmten Schlüssel benötigt. Es ist besonders wichtig zu erwähnen, dass physische Zugriffskontrolle von vielen Standards explizit gefordert wird, wie bspw. im TISAX-Standard.

5.3.1.1.4 Updates

Risikominimierung: mittel
Kosten: gering bis mittel (ggf. SLAs und Rücksprache mit Instandhalter erforderlich)
Zeitaufwand: gering (Instandhalter führt normalerweise Updates durch)
Besonders wichtig sind auch „regelmäßige" Updates der OT-Systeme. Die Frequenz der Updates spielt hierbei eine nebensächliche Rolle. Es ist vor allem wichtig, dass dieser Prozess dokumentiert stattfindet (benötigte Zeit, Arbeitskräfte, falls vorhanden Patchnotizen etc.). Somit kann bereits nach zwei erfolgreichen Durchläufen ein weiteres Update gut geplant werden, da bereits bekannt ist, welche Auswirkungen dies haben wird und was alles genau hierfür vorbereitet werden muss. Besonders wichtig zu bedenken sind hierbei folgende Punkte: Manchmal brauchen Updates Zugriff auf das Internet und sollten daher nur in einem definierten Zeitslot möglich sein, in welchem dieser Zugriff gestattet wird. Automatische Updates sind daher „tabu"! Außerdem sollte mit einer Downtime gerechnet werden, welche mit Backup-Geräten gefüllt werden kann, bzw. muss. Updates sollten außerdem nicht nur für spezifische Programme durchgeführt werden, sondern das gesamte Betriebssystem sowie sämtliche Programme, welche sicher aktualisiert werden können, sollten in einem Lauf erledigt werden. Werden in der Zukunft neue Sicherheitslücken bekannt, welche geschlossen werden müssen, kann dies entweder einen Update-Zyklus einsparen, da die installierte Version bereits neu genug ist oder die Zeit für das Update zumindest verkürzt werden, da die Versionen bereits nicht mehr so veraltet sind.

5.3.1.1.5 Dokumentierter Prozess

Risikominimierung: gering
Kosten: gering (Dokumentations-Software nötig)
Zeitaufwand: hoch (Einrichtung eher aufwendig; muss danach regelmäßig aktualisiert und eingehalten werden)
In den meisten KMU fehlt ein dokumentierter Prozess bezüglich Updates, Backups etc. Für eine ISO 27001-Zertifizierung ist dies jedoch sogar erforderlich. Hierbei ist es ausreichend, ein Intervall festzulegen, in welchem bestimmte Prozesse ausgeführt werden sollten. Des Weiteren muss festgehalten werden, was genau für diese Prozesse zu tun ist: Vorbereitung, Durchführung und Nachbereitung. Es ist selbstverständlich möglich, hier bestimmte Standards anzuwenden, jedoch ist es für die meisten KMU nicht unbedingt erforderlich. Ein Leitfaden sowie Zeitplan (also ein konkreter Plan darüber, wie die Updates, Backups etc. ablaufen sollen) sind bereits genug, damit Ihr Unternehmen schon viel besser als die meisten KMU aufgestellt wäre. Beispielsweise sollte im Detail hier definiert werden, welche Arbeitskraft welche Arbeit erledigen sollte, welche Systeme betroffen sind, welche Systeme aktualisiert werden, was in dieser Zeit nicht funktioniert, wann und wie oft Updates passieren sollten etc.

5.3.1.1.6 Awareness

Risikominimierung: mittel
Kosten: mittel (Cybersicherheits-Training-Programm erforderlich)
Zeitaufwand: mittel (Arbeitskräfte müssen oft „trainieren")
In den meisten KMU gibt es keine dedizierte Person, welche sich um die OT kümmert. Oftmals übernimmt einfach ein Mitarbeiter der IT auch die OT, ohne überhaupt auf die eigenen Herausforderungen in diesem Bereich gefasst zu sein. Wie bereits erwähnt, ist die OT-Umgebung äußerst unsicher und kann daher auch bei kleineren Fehlern schnell zum Angriffsziel werden. Daher ist es überaus wichtig, Awareness speziell für die OT-Umgebung zu schaffen. Zur Schaffung von Awareness im Allgemeinen haben wir noch einen eigenen Use-Case (siehe Kapitel 3).

5.3.1.1.7 Grundschutz

Risikominimierung: mittel
Kosten: hoch (zusätzliche Hardware normalerweise erforderlich)
Zeitaufwand: hoch (Einrichtung kann aufwendig sein)
In Anlehnung an den vom BSI geprägten Begriff, existieren auch Grundschutz-Konzepte, welche spezifisch in der OT-Umgebung anwendbar sind. Da wir allerdings auch hierfür einen dedizierten Use-Case (siehe Kapitel 1) haben, geht dieses Dokument hier nicht ins Detail. Allerdings deckt der in Abschnitt 5.3.1.3.4 beschriebene CIS Controls Implementation Guide for Industrial Control Systems Version 7 bereits einen sehr großen Teil der „typischen" Grundschutz-Kriterien für OT ab (geht allerdings möglicherweise ein wenig zu sehr ins Detail).

5.3.1.1.8 Monitoring

Risikominimierung: gering
Kosten: mittel (zusätzliche Soft- und Hardware könnte erforderlich sein)
Zeitaufwand: mittel (Einrichtung eher leicht; Pflege aufwendig)
Monitoring, oder auch Überwachung, versucht, die OT-Systeme kontinuierlich zu überwachen, um Cyber-Bedrohungen, Fehlkonfigurationen etc. so schnell wie möglich aufzudecken. Primär wird in der OT passives Monitoring empfohlen, wobei Netzwerkverkehr an verschiedenen Schnittstellen analysiert wird. Meldungen müssen daher immer manuell überprüft und dementsprechend dann gegebenenfalls Aktionen veranlasst werden.
Einige KMU besitzen bereits ein SIEM für ihre IT-Infrastruktur. Dieses kann theoretisch auch in der OT Anwendung finden – jedoch gibt es auch dedizierte SIEMs für OT. Hier ist es besonders wichtig, darauf zu achten, dass das SIEM mit den OT-spezifischen Herausforderungen gut umgehen kann. Vor allem der fehlende Zugriff auf das Internet aus dem OT-Intranet heraus kann hierbei besonders Probleme bereiten. Die für das SIEM benötigten Daten können oftmals auch heruntergeladen werden, um sie dann „offline" dorthin zu übertragen – beispielsweise über einen USB-Stick. Alternativ kann hier, wie bei den Updates in Abschnitt 5.3.1.1.3, ein bestimmtes Zeitfenster festgelegt werden, in dem das SIEM kurzzeitig auf das Internet zugreifen darf.

5.3.1.2 Frei verfügbare Self-Assessment-Tools

Online existieren haufenweise Self-Assessment-Tools, welche versuchen, die OT so gut wie möglich abzudecken. Besonders ins Auge gesprungen sind uns LARS ICS und CSET.

5.3.1.2.1 LARS ICS

Light and Right Security ICS (LARS ICS) ist kostenfrei auf der Seite des BSI verfügbar[4] und basiert auf dem IT-Grundschutz, ISO 27001, IEC 62443 und dem BSI ICS Security-Kompendium und ist besonders gut für KMU jeder Größe geeignet. Entwickelt wurde es 2014 im Auftrag des BSI von der Sirrix AG security technologies zusammen mit der TÜV SÜD Rail GmbH. Sämtlicher Code des Tools ist open-source und liegt dem Installationspaket bei.

Um das Tool verwenden zu können, muss allerdings eine Java-Laufzeitumgebung (JRE) installiert sein. Beim ersten Programmstart muss zunächst ein Benutzer und dann ein Projekt angelegt werden. Somit kann eine Programm-Installation sogleich für mehrere Unternehmen oder Bereiche verwendet werden. Das Tool listet auf der linken Seite verschiedene Bereiche mit weiteren Unterbereichen auf. Ein Bereich hat ein gelbes Dreieck, wenn eine Antwort in diesem Bereich noch ausstehend ist, einen roten Kreis, wenn der Bereich noch nicht vollständig abgedeckt ist und einen grünen Kreis, wenn alle Controls umgesetzt sind. Jedem Bereich können Assets hinzugefügt werden, welche wiederum über die Assetverwaltung verwaltet werden können. So kann man seine Inventarliste sogar mit den einzelnen Controls verknüpfen. Die Controls selbst beantwortet man mit „umgesetzt“, „teilweise umgesetzt“, „nicht umgesetzt“ oder „nicht relevant“. Man kann zu jedem Control Notizen hinzufügen und Verweise auf gängige Standards einsehen.

Insgesamt bietet das Tool eine gute Möglichkeit, die eigene OT-Sicherheit dokumentiert zu verbessern. Allerdings enthält das Tool sehr viele Fragen, was KMU abschrecken könnte. Des Weiteren wird technisches Wissen benötigt, um die Fragen adäquat beantworten zu können.

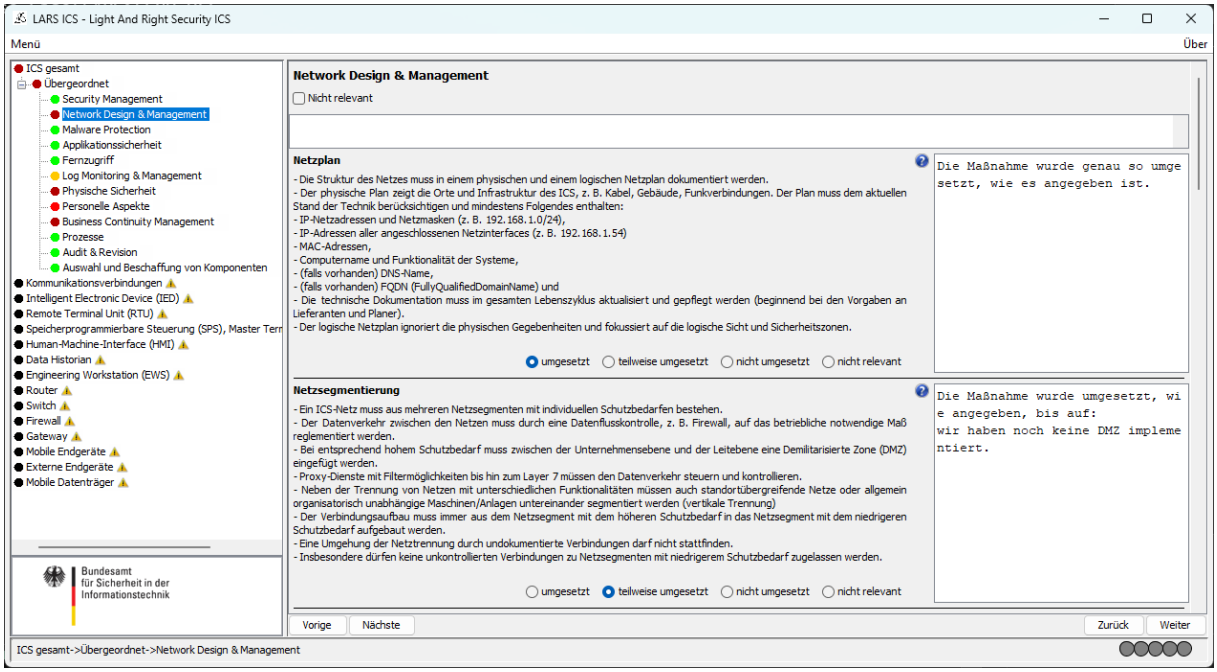


Abbildung 14: Grafische Oberfläche von LARS ICS.

[4] https://www.bsi.bund.de/dok/7029486

5.3.1.2.2 CSET

CSET[5] ist ebenfalls ein open-source Tool zum Self-Assessment der eigenen Cybersicherheit. Allerdings ist es nicht auf OT fokussiert, sondern kann IT und OT gleichermaßen abfragen. Aus diesem Grund ist es in gewisser Weise zwar ähnlich zu LARS ICS, ist jedoch wesentlich detaillierter und daher vermutlich zu umfangreich für KMU. Entwickelt wurde das Tool von der CISA und es läuft hauptsächlich über eine lokale Datenbank. CSET hat Vorlagen für viele, verschiedene Standards, welche es abfragen kann. Aufgrund der Komplexität des Tools ist es eher für mittlere Unternehmen geeignet und wir verweisen für weitere Details auf deren Dokumentation.

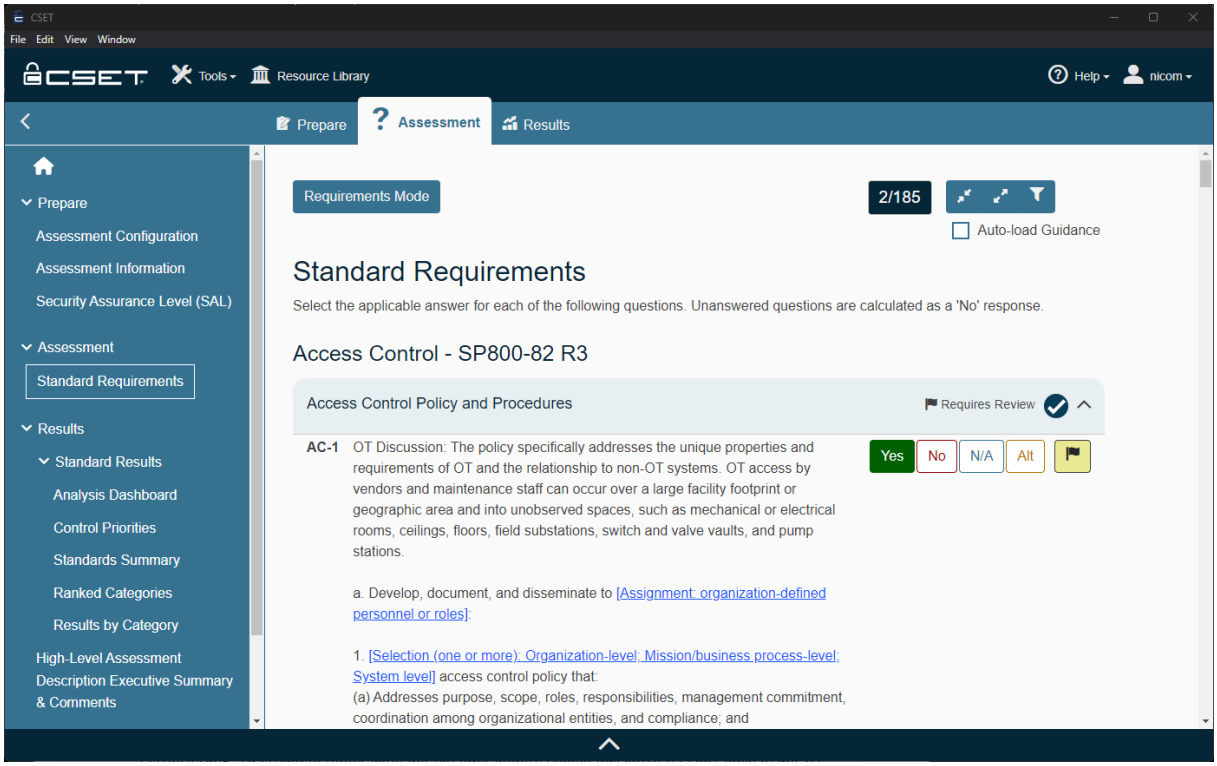


Abbildung 15: Grafische Oberfläche von CSET am Beispiel des NIST SP 800-82r3-Standards

5.3.1.3 OT-Security-Standards und -Guides

In der Literatur wurden vor allem vier Standards für OT-Security in KMU immer wieder genannt: ISA/IEC 62443, NIST SP 800-82 Rev. 3 und VDI/VDE 2182. Aus unserer Erfahrung heraus ist jedoch auch der CIS Controls Implementation Guide for Industrial Control Systems Version 7 sehr empfehlenswert. Links zu allen diesen Dokumenten finden sich bei den Quellen.

5.3.1.3.1 ISA/IEC 62443

Die einzelnen Bände der ISA/IEC 62443-Reihe können grundsätzlich in sechs Bereiche aufgeteilt werden (Stand Februar 2025): Allgemeine Grundlagen, Sicherheitsanforderungen für Betreiber & Dienstleister, Automatisierungssysteme, Automatisierungskomponenten, Profile der IEC 62443 (noch in Planung) sowie Evaluationsmethodik. Da für die OT-Security in KMU im Allgemeinen alle Bereiche anwendbar wären, ist nach unserer Analyse der Standard zu komplex.

[5] https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

5.3.1.3.2 NIST SP 800-82 Rev. 3

Bei diesem Standard handelt es sich um eine Publikation der NIST. Daher ist er nur auf Englisch verfügbar, jedoch kostenlos. Des Weiteren ist auch dieser Standard zu umfangreich für KMU. Im Großen und Ganzen bietet der Standard über 100 Controls, welche von der OT-Umgebung erfüllt werden sollten. Diese sind aufgeteilt in acht Kategorien, welche an einen anderen Standard, dem NIST SP 800-53 Rev. 5, angelehnt sind. Des Weiteren werden noch über 100 Control Enhancements vorgeschlagen, welche die OT-Security noch weiter stärken sollen.

5.3.1.3.3 VDI/VDE 2182

Laut unseren Recherchen ist der VDI/VDE 2182 Standard sehr gut in KMU anwendbar. Ähnlich zum Demingkreis werden hier acht Schritte angewandt: Schutzobjekt identifizieren, Bedrohungen analysieren, Relevante Schutzziele ermitteln, Risiken analysieren und bewerten, Schutzmaßnahmen aufzeigen & Wirksamkeit bewerten, Schutzmaßnahmen auswählen, Schutzmaßnahmen umsetzen und Prozessaudit durchführen, woraufhin wieder am Anfang angefangen wird. Parallel dazu findet eine Prozessdokumentation statt. Der Standard besteht wieder aus mehreren „Blättern", wobei das erste Blatt ein allgemeines Vorgehensmodell erläutert, die zweiten und dritten Blätter sowie das fünfte Blatt verschiedene Anwendungsbeispiele darlegen und das vierte Blatt allgemeine Empfehlungen enthält. Hierbei ist allerdings wichtig zu erwähnen, dass dieser Standard keine „Best Practices" enthält, sondern den Prozess der OT-Security standardisiert.

5.3.1.3.4 CIS Controls Implementation Guide for Industrial Control Systems Version 7

Der CIS Controls Implementation Guide erweitert die CIS Controls, indem er für jedes CIS-Control erläutert, wie es in einer OT-Umgebung umgesetzt werden könnte. In der detaillierten Bestands- und Bedarfsanalyse von CySeReS-KMU haben wir zur Einschätzung der OT-Security eben diesen Guide verwendet und können daher aus erster Hand bestätigen, dass sich dieser zur Einschätzung besonders gut eignet. Eine Angleichung der einzelnen Controls an die CIS Critical Security Controls Version 8 ist ebenso möglich und wurde von uns auch bereits in der Vergangenheit durchgeführt, um sogar einen Vergleich der Sicherheit der IT-Umgebung und der OT-Umgebung zu ermöglichen. Die 20 Controls sind unterteilt in drei Stufen: Basic, Foundational und Organizational. Hierbei ist mindestens eine Umsetzung der ersten beiden Stufen für KMU empfohlen.

5.3.1.4 Identifikation der Verbesserungsmöglichkeiten

Nachdem mögliche Lücken und Risiken in der OT-Umgebung anhand der Best Practices und/oder Referenzen aus den vorherigen Abschnitten identifiziert wurden, sollten diese bewertet werden. Da dies je nach Unternehmen und Fokus unterschiedlich passiert, werden hier nur Kriterien aufgelistet, nach welchen diese Bewertung stattfinden kann.

Vor allem wichtig bei KMU ist der Kostenfaktor. Best Practices wie ein dokumentierter Prozess können kostenlos umgesetzt werden (nur der Zeitaufwand muss hier eingerechnet werden). Heutzutage gibt es sogar open-source SIEMs, welche möglicherweise den gewünschten Funktionsumfang liefern können. Andere Maßnahmen wie Netzwerksegmentierung könnten kostspieliger werden, da sie möglicherweise die Anschaffung neuer Router oder Infrastruktur benötigen, welche zusätzlich wieder auf ihre Funktionalität hin geprüft werden müssen.

Wie bereits erwähnt, ist auch der Zeitfaktor besonders wichtig zu bedenken: Schulungen zu OT-Security und Awareness können die jeweiligen Teilnehmer eine Zeit lang beschäftigen und sie auch nicht sofort zu 100% sensibilisieren. Hier spielt auch die praktische Erfahrung nach einem solchen Training eine große Rolle. Der Prozess der Umsetzung eines Best Practices kann daher mehrere Wochen dauern, um möglichst reibungslos abzulaufen. Vor allem bei der ersten Umsetzung einer Maßnahme kann es durch den Mangel an vorherigen Erfahrungen einen zuvor gesetzten Zeitrahmen sprengen. Nach den ersten zwei bis drei Durchläufen sollte jedoch anhand der Protokolle der letzten Durchläufe besser ersichtlicher sein, wie viel Zeit und sonstige Ressourcen für die jeweiligen Maßnahmen in Zukunft eingeplant werden sollten.

Zu guter Letzt sollte ein Unternehmen überlegen, welche Maßnahme den größten Vorteil in der eigenen Infrastruktur bringen würde. Beispielsweise könnte unzureichende Netzwerksegmentierung einen wesentlich größeren Schaden anrichten als ein fehlendes SIEM. Hier ist eine individuelle Bewertung der einzelnen Maßnahmen erforderlich.

Diese Kriterien führen zusammen zu einer Art „Preis-Zeit-Leistungs-Bewertung" der einzelnen Maßnahmen, die Aufschluss über die besten „Quick Wins" für die eigene OT-Security gibt.

5.3.1.5 Erfassung von Test-Kriterien

Wie auch bei Tests in der Software-Entwicklung sollten Test-Kriterien erfasst werden, welche die jeweiligen Geräte erfüllen müssen. Diese Kriterien sind wichtig, um nach der Verbesserung der OT-Security feststellen zu können, ob die Geräte noch mindestens genauso gut funktionieren wie davor. Beispiele für solche Kriterien sind funktionale Leistung (Reaktionszeit, Genauigkeit etc.), Effizienz (Energieverbrauch, Geschwindigkeit etc.), Kompatibilität (Schnittstellen etc.), Dokumentation (ist diese vollständig, aktuell und tatsächlich für das Gerät anwendbar? etc.), Umweltbedingungen (Temperaturbedingungen, Feuchtigkeit etc.), Compliance (welchen Normen entspricht das Gerät? etc.), bereits vorhandene Sicherheit (Zugriffskontrolle, Sicherheitslücken, Stand der Updates etc.) und Zuverlässigkeit (Ausfälle, Störungen, Reparaturdauer, MTBF etc.). Diese Kriterien können auch in der Inventarliste aus Abschnitt 5.3.1 den jeweiligen Geräten zugeschrieben werden (beispielsweise unter „Funktion"), um schnellstmöglichen Zugriff auf die Daten zu ermöglichen.

5.3.1.6 Planung der Verbesserung

Bei der Planung sollten nun passende Maßnahmen ausgewählt werden, welche implementiert werden sollten. Hierfür ist es besonders wichtig, mögliche SLAs zu konsultieren und mit dem jeweiligen Hersteller oder Instandhalter Kontakt aufzunehmen. Da die jeweiligen Geräte für eine gewisse Zeit während der Implementierung der Maßnahmen „offline" sein werden, sollte hier vor allem ausreichend Backup eingeplant werden. Dieses sollte, wie bereits in Abschnitt 5.3.1.1.1 erwähnt, nicht nur Backup-Maschinen, sondern auch ein vollständiges Backup der jeweiligen Daten auf den Geräten beinhalten. Nach Absprache mit dem Instandhalter und der Durchführung und Planung sämtlicher Backups sollte hier ein Zeitplan erarbeitet werden, damit der Zeitpunkt des Umstiegs von den Backup-Geräten auf die normalen Geräte wieder klar ist.

Die Entscheidung, ob alle, nur einige oder nur eine relevante Verbesserung umgesetzt werden soll, liegt allein beim KMU. Werden mehrere Verbesserungen auf einmal umgesetzt, besteht natürlich die Gefahr, dass es zu mehreren Komplikationen kommen könnte, deren Behebungen mehr Zeit in Anspruch nehmen könnten. Umgekehrt kostet es selbstverständlich mehr Geld, wenn der Instandhalter mehrmals kommen muss, um jeweils nur eine Verbesserung durchzuführen. Hier ist abzuwägen und ggf. mit dem Hersteller oder dem Instandhalter abzustimmen, was sinnvoller ist.

5.3.2 Do: Testweise Verbesserung der OT-Security an einem Gerät

Nachdem klar ist, welche Verbesserung durchgeführt werden soll und diese komplett durchdacht und geplant wurde, ist es Zeit, sie testweise an einem OT-Gerät anzuwenden. Dazu ist es „nur" erforderlich, den Plan aus Abschnitt 5.3.1 durchzuführen. Wie bereits erwähnt, sind in den meisten Fällen Maßnahmen des Herstellers oder Instandhalters erforderlich. In allen Fällen sollte hier bereits die Inventarliste aktualisiert werden, damit die Verbesserung oder Aktualisierung sowie der hierfür nötige Prozess und Arbeitsaufwand dokumentiert sind.

5.3.3 Check: Überprüfung der Funktionalität

In der dritten Phase muss nun geprüft werden, ob das Gerät (mindestens) gleichermaßen gut funktioniert wie zuvor. Hierzu können die Test-Kriterien aus Abschnitt 5.3.1.5 konsultiert werden, um einen systematischen Vergleich zu dem vorherigen Stand zu ermöglichen. Diese Phase kann durchaus mehrere Wochen dauern, da so viele Daten wie möglich gesammelt werden sollten (siehe Abschnitt 5.3.1.5; vor allem in Richtung Zuverlässigkeit). Bei Problemen sollte der Hersteller oder Instandhalter kontaktiert werden und immer ein Backup-Gerät vorhanden sein.

5.3.4 Act: Anwendung des Best Practices in allen relevanten Bereichen

Sollten die Tests erfolgreich gewesen sein, so kann der Best Practice auch auf den anderen relevanten Geräten umgesetzt werden. Hierzu ist höchstwahrscheinlich wieder eine Rücksprache mit dem jeweiligen Hersteller oder Instandhalter notwendig. Es kann mit Abschnitt 5.4 fortgefahren werden.

Sollte ein Test fehlgeschlagen sein, so gibt es zwei Möglichkeiten: ein Rollback oder weitere Verbesserung. Diese werden in den nächsten beiden Absätzen jeweils beschrieben.

Bei einem Rollback wird der Hersteller oder Instandhalter angewiesen, das Update oder die „Verbesserung" rückgängig zu machen, um den ursprünglichen Zustand des Geräts wiederherzustellen. Dies ist allerdings oftmals mit Problemen verbunden, da zum einen somit der Best Practice nicht umgesetzt wird und zum anderen Downgrades oftmals nicht ohne weiteres möglich sind. Sollte man sich für diesen Pfad entscheiden, so sollte eine weitere Planungsphase nach Abschnitt 5.3.1 durchgeführt werden (und der PDCA-Zyklus dementsprechend neu angefangen werden).

Die weitere Verbesserung würde hierbei bedeuten, dass das Gerät vom Wartungspersonal entweder repariert oder weiter aktualisiert wird. Hierzu sollte eine weitere Planungsphase nach Abschnitt 5.3.1 erfolgen (und der PDCA-Zyklus dementsprechend neu angefangen werden).

5.4 Kontinuierliche Verbesserung

Nachdem eine Verbesserung der OT-Security durchgeführt wurde, sollte ein Prozess eingerichtet werden. Besonders wichtig ist dieser bei Updates, Backups und ähnlichen periodischen Aktivitäten. Auch Penetrationstests sind hier durchaus denkbar, jedoch für die OT-Sicherheit in KMU vermutlich zu weit gedacht. Auch sollte der nächste Durchlauf des PDCA-Zyklus fest eingeplant werden. Festgehalten werden die jeweiligen Aufgaben sowie die Ausführungsfrequenz am besten in einer Art Wartungsplan.

Des Weiteren sollte über regelmäßige Qualitätsmanagement-Audits (QM-Audits) nachgedacht werden, um das erreichte Sicherheitsniveau zu halten. Ein vollständiger QM-Audit pro Jahr ist hierbei eine gute Frequenz, welche sich auch gut einplanen und einhalten lässt.

Ist all das passiert, so kann wieder bei Abschnitt 5.3.1 angefangen und der PDCA-Zyklus erneut gestartet werden.

5.5 Anlage: Projektzeitplan Vorschlag

Firmenname	Max Mustermann	**Projektanfang:**	26.2.2026
Projektleiter	Max Mustermann	**Projektende (Prognose) :**	8.7.2026

Arbeitspaket		Tasks	Verant-wortl.	Beteiligt	Status	Dauer (Wochen)	Start	Ende
AP0	**Vorprojekt**	0.1 Zielsetzung festlegen	Name	Namen	Abgeschlossen	0,5	26.2.26	1.3.26
		0.2 Verantwortlichkeiten festlegen	Name	Namen	Abgeschlossen	0,5	1.3.26	5.3.26
		0.3 Festlegung Projektplan	Name	Namen	im Review	0,5	5.3.26	8.3.26
AP1	**Plan: Ist- und Soll-Stand dokumentieren**	1.1 Anlegen/Aktualisieren einer Inventarliste	Name	Namen	im Review	1	8.3.26	15.3.26
		1.2 Identifikation der Verbesserungsmöglichkeiten	Name	Namen	in Arbeit	1	15.3.26	22.3.26
		1.3 Erfassung von Test-Kriterien für die Geräte	Name	Namen	in Arbeit	1	22.3.26	29.3.26
		1.4 Planung der Verbesserung	Name	Namen	noch nicht begonnen	2	29.3.26	12.4.26
AP2	**Do: Testweise Anwendung an einem Gerät**	2.1 Verbesserung eines ausgwählten OT-Geräts	Name	Namen		0,2	12.4.26	13.4.26
		2.2 Aktualisierung Inventarliste	Name	Namen		0,2	13.4.26	15.4.26
AP3	**Check: Überprüfung der Funktionalität**	3.1 Testphase mit normalem Betrieb des Geräts	Name	Namen		10	15.4.26	24.6.26
		3.2 Kontiuierliche Überwachung des Geräts	Name	Namen		10	15.4.26	24.6.26
AP4	**Act: Allgem. Anwendung**	4.1 Generelle Umsetzung oder Rollback	Name	Namen		2	24.6.26	8.7.26

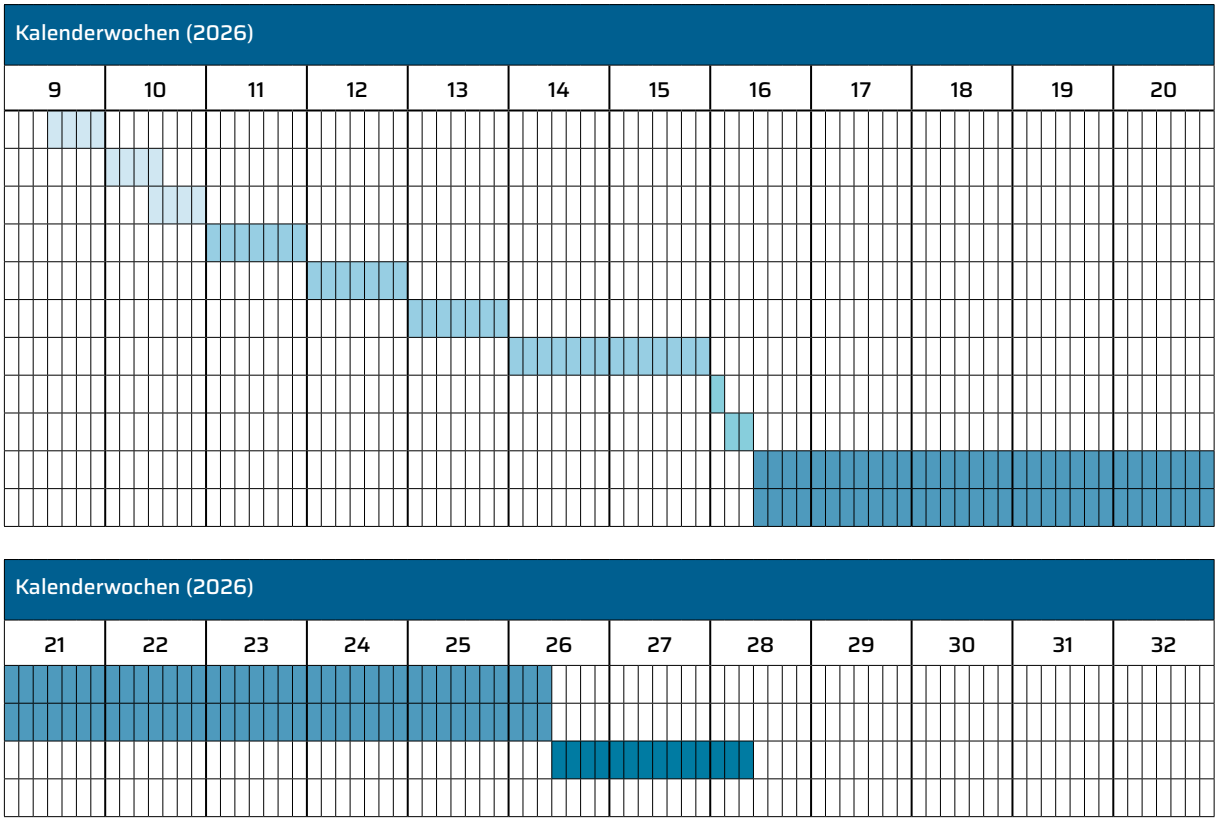


Abbildung 16: Excel Gantt-Chart Projektzeitplan Handbuch 5

GLOSSAR

Begriffe in 1 Cyber-Security Grundschutz für KMU

C

Cyber Resilience Act (Kapitel 1.1.1) Ein EU-Gesetz, das Unternehmen und Organisationen dazu verpflichtet, ihre digitalen Systeme und Dienste widerstandsfähiger gegen Cyberangriffe zu machen und somit ihre Resilienz und Reaktion zu Cyberangriffen zu stärken.

Cyberangriffe (Kapitel 1.1) Angriffe auf Computersysteme oder Netzwerke, bei denen Hacker versuchen, Daten zu stehlen, Systeme zu stören oder Schaden anzurichten.

Cybersicherheit (Kapitel 1.1.1) Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cybersicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

D

DNS-Firewall-Lösung (Kapitel 1.4.2.1) Eine Sicherheitslösung, die den DNS-Datenverkehr überwacht und vor Bedrohungen schützt, indem sie z. B. den Zugriff auf schadhafte Websites verhindert.

F

Filter (Kapitel 1.4.2.1) Software oder Hardware, die bestimmte Daten blockiert oder herausfiltert, z. B. Spam-E-Mails, schadhafte Websites oder unerwünschte Inhalte.

Firewalls (Kapitel 1.4.2.1) Ein Sicherheitsmechanismus, der den Datenverkehr zwischen einem Netzwerk und der Außenwelt überwacht und unbefugte Zugriffe blockiert.

K

Kodierungsschlüssel (Kapitel 1.4.1.4) Ein Schlüssel, der verwendet wird, um Daten zu verschlüsseln (oder zu entschlüsseln). Er sorgt dafür, dass nur berechtigte Personen Zugriff auf sensible Informationen haben.

M

Malware (Kapitel 1.4.3.1) Schadhafte Software, die entwickelt wurde, um ein System zu beschädigen oder Daten zu stehlen, z. B. Viren, Trojaner oder Ransomware.

N

NFC-Protokolle (Kapitel 1.4.8.3) Near Field Communication (NFC) ist eine Technologie, die es ermöglicht, Daten über kurze Entfernungen hinweg zwischen Geräten auszutauschen, z. B. beim kontaktlosen Bezahlen oder Datentransfer.

P

Passphrase (Kapitel 1.4.4.1) Ein längeres Passwort, das aus einer Kombination von Wörtern oder Phrasen besteht und als sicherer gilt als ein einfaches Passwort.

Patches (Kapitel 1.2.1.2) Software-Updates, die Sicherheitslücken schließen oder Fehler beheben. Sie sind wichtig, um Systeme vor Angriffen zu schützen.

Phishing E-Mails (Kapitel 1.4.3.1) Betrügerische E-Mails, die so aussehen, als kämen sie von vertrauenswürdigen Quellen, aber darauf abzielen, sensible Daten wie Passwörter oder Kreditkarteninformationen zu stehlen.

Proxys (Kapitel 1.4.2.1) Ein Server, der als Zwischenstation zwischen einem Nutzer und dem Internet fungiert, um Daten zu filtern, die Verbindung zu sichern oder die IP-Adresse zu verbergen.

T

Tethering (Kapitel 1.4.8.3) Die Verbindung eines mobilen Geräts (z. B. eines Smartphones) mit einem anderen Gerät, um eine Internetverbindung bereitzustellen, z. B. durch USB, Bluetooth oder WLAN.

V

VPN (Virtual Private Network) (Kapitel 1.4.2.1) Ein Tool, das eine sichere Verbindung über das Internet ermöglicht, indem es den Datenverkehr verschlüsselt und die IP-Adresse des Nutzers verbirgt.

W

White- und Blacklisting (Kapitel 1.4.2.1) Whitelist: Eine Liste von vertrauenswürdigen Quellen oder Programmen, die erlaubt sind. Blacklist: Eine Liste von unerwünschten Quellen oder Programmen, die blockiert werden.

Begriffe in 2 Supply Chain Cyber-Security

B

BACS (Kapitel 2.7.5) Bundesamt für Cybersicherheit in der Schweiz

Blacklists (Kapitel 2.7.3) Sperrlisten mit bekannten schädlichen oder unerwünschten Einträgen (z. B.: IP-Adressen, Domains, E-Mail-Absendern), die von Systemen automatisch blockiert oder markiert werden.

C

Chipsätze (Kapitel 2.7.5) Verbund elektronischer Bausteine (Chips) auf einem Mainboard, die den Datenverkehr zwischen Prozessor, Arbeitsspeicher und anderen Komponenten steuern und Leistungsfähigkeit und Funktionen des Systems mitbestimmen.

Cloud Access Security Broker (CASB) (Kapitel 2.7.3) Sicherheitslösung zwischen Nutzern und Cloud-Diensten, die Zugriffe überwacht, Sicherheitsregeln durchsetzt, Datenbewegungen kontrolliert und riskante Aktivitäten in der Cloud blockieren kann.

D

Defacements (Kapitel 2.7.3) Verunstaltung oder Manipulation einer Website durch Angreifer, z. B.: durch Austausch der Startseite oder Einfügen fremder Botschaften.

Domains (Kapitel 2.7.3) Eindeutige, für Menschen lesbare Namen im Internet, die auf Websites oder Server zeigen, z. B.: firma.at, anstelle von schwer merkbarer IP-Adressen.

L

Log Files (Kapitel 2.7.3) Protokolldateien, in denen IT-Systeme automatisch Ereignisse (z. B.: Anmeldungen, Fehlermeldungen, Änderungen) speichern, um Probleme und Sicherheitsvorfällt analysieren zu können.

M

Management by Objectives Systeme (Kapitel 2.7.4) Führungssysteme, bei denen Führungskräfte mit Mitarbeitenden oder Abteilungen konkrete, messbare Ziele vereinbaren und Leistung danach beurteilen, wie gut diese Ziele erreicht werden.

Middleware (Kapitel 2.7.5) Software-Schicht, die zwischen Betriebssystem und Anwendungen oder zwischen verschiedenen Anwendungen vermittelt, damit unterschiedliche Systeme miteinander kommunizieren können.

P

Penetration Tests (Kapitel 2.7.3) Geplante und autorisierte „Probeangriffe“ auf IT-Systeme, bei denen Sicherheitsexperten oder spezialisierte Tools wie echte Angreifer vorgehen, um Schwachstellen zu finden, bevor Kriminelle sie ausnutzen können.

Q

Quickfix (Kapitel 2.7.5) Schnelle, meist provisorische Problemlösung, um den Betrieb kurzfristig wiederherzustellen; ersetzt nicht die langfristig saubere Lösung.

S

Schadcode (Kapitel 2.7.5) Oberbegriff für schädliche Software (z. B.: Viren, Trojaner, Ransomware), die Systeme stört, Daten stiehlt, verändert oder zerstört.

Service Level Agreement (SLA) (Kapitel 2.7.5) Vertragliche Vereinbarung zwischen Dienstleister und Kunde in der Leistungsumfang, Verfügbarkeiten, Reaktionszeiten und Konsequenzen bei Nichteinhaltung genau festgelegt sind.

SSL-Verschlüsselung (Kapitel 2.7.3) Verfahren zur verschlüsselten Datenübertragung im Internet (heute meist TLS), erkennbar an https:// und Schloss-Symbol im Browser; schützt Daten vor Mitlesen und Manipulation.

Begriffe in 4 Cyber-Notfallkonzept für KMU

A

Angriffsvektor (Kapitel 4.2.3.4) Die Methode oder der Weg, über den ein Angreifer in ein Computersystem eindringt. Beispiele sind E-Mail-Anhänge, unsichere Webseiten oder USB-Sticks.
Beispiel: Ein infizierter E-Mail-Anhang ist ein häufiger Angriffsvektor für Ransomware.
→ Siehe auch: **Phishing, Malware**

Authentifizierung (Kapitel 4.2.1.3) Der Prozess der Überprüfung der Identität eines Benutzers, bevor ihm Zugang zu einem System gewährt wird (z.B. durch Passwort, Fingerabdruck).
Beispiel: Die Eingabe von Benutzername und Passwort beim Login. → Siehe auch: **MFA**

Automatisierte Incident-Response-Systeme (Kapitel 4.4.2) Software, die automatisch auf Sicherheitsvorfälle reagiert, ohne dass menschliches Eingreifen erforderlich ist.
Beispiel: Ein System, das automatisch verdächtige IP-Adressen blockiert.

B

Backup (Kapitel 4.2.1.4, 4.2.3.2, 4.3.2, 4.6) Eine Sicherheitskopie von Daten oder Systemen, die zur Wiederherstellung nach einem Datenverlust verwendet werden kann.

BCP (Business Continuity Planning) (Kapitel 4.2.1.5, 4.6) Ein Plan zur Aufrechterhaltung kritischer Geschäftsfunktionen während und nach einer Krise oder einem Notfall.

Beweissicherung (Kapitel 4.2.3.4, 4.3.2) Das systematische Sammeln und Sichern von digitalen Spuren nach einem Cyberangriff für spätere Analysen oder rechtliche Zwecke.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (Kapitel 4.4.2, 4.5.1, 4.5.3) Die deutsche Bundesbehörde, die für IT-Sicherheit zuständig ist und Unternehmen bei Cybersicherheitsfragen unterstützt.

C

Cloud-Dienste (Kapitel 4.2.1.3, 4.6) Internetbasierte Dienste, bei denen Daten und Programme nicht auf dem eigenen Computer, sondern auf externen Servern gespeichert und verarbeitet werden.

Cyber-Notfall (Kapitel 4.1.1, 4.2) Ein schwerwiegender Sicherheitsvorfall, der die IT-Systeme eines Unternehmens erheblich beeinträchtigt und sofortige Gegenmaßnahmen erfordert.

Cyber-Resilienz (Kapitel 4.4.1, 4.5.3) Die Fähigkeit eines Unternehmens, Cyberangriffe zu überstehen und sich schnell davon zu erholen.

Cybercrime (Kapitel 4.3.1, 4.5.1) Straftaten, die mithilfe von Computern oder über das Internet begangen werden.

Cyberangriff (Kapitel 4 Einleitung, 4.1.1, 4.2) Ein gezielter Versuch, in Computersysteme einzudringen, um Daten zu stehlen, zu manipulieren oder Systeme zu beschädigen.

D

Datenleck (Kapitel 4.1.2, 4.2.3.1, 4.3.2) Ein Sicherheitsvorfall, bei dem vertrauliche Daten unbeabsichtigt oder durch einen Angriff nach außen gelangen.

Datenschutzbeauftragter (Kapitel 4.2.2.1, 4.2.2.2, 4.3.1, 4.6) Eine Person im Unternehmen, die für die Einhaltung der Datenschutzgesetze verantwortlich ist.

Denial-of-Service (DoS) (Kapitel 4.1.2) Ein Angriff, bei dem ein System durch Überlastung für legitime Nutzer unzugänglich gemacht wird.

Digitale Forensik (Kapitel 4.2.3.4) Die Untersuchung von Computersystemen nach einem Sicherheitsvorfall, um Beweise zu sammeln und den Angriff zu verstehen.

DSGVO (Datenschutz-Grundverordnung) (Kapitel 4.1.3, 4.2.3.3, 4.6) Europäisches Gesetz zum Schutz personenbezogener Daten, das Unternehmen verpflichtet, Datenschutzverletzungen zu melden.

E

Eindämmung (Kapitel 4.2.3.2, 4.3.3) Maßnahmen zur Begrenzung der Ausbreitung eines Cyberangriffs auf weitere Systeme.

Endpoint Protection (Kapitel 4.2.3.1) Sicherheitssoftware, die einzelne Geräte (Computer, Smartphones) vor Bedrohungen schützt.

ENISA (Europäische Agentur für Cyber-Sicherheit) (Kapitel 4.4.2, 4.5.1) EU-Agentur, die bei der Verbesserung der Netzwerk- und Informationssicherheit in Europa unterstützt.

ERP-System (Enterprise Resource Planning) (Kapitel 4.2.1.1, 4.6) Eine Software zur Verwaltung und Steuerung aller Geschäftsprozesse eines Unternehmens.

Eskalationsstufen (Kapitel 4.2.1.2, 4.2.3.1) Vordefinierte Ebenen, die festlegen, wann und an wen ein Sicherheitsvorfall weitergeleitet werden muss.

F

Firewall (Kapitel 4.2.3.1, 4.2.3.4, 4.3.2) Ein Sicherheitssystem, das den Datenverkehr zwischen Netzwerken kontrolliert und unerwünschte Zugriffe blockiert.

Forensische Analyse (Kapitel 4.2.3.4) Detaillierte technische Untersuchung eines Sicherheitsvorfalls zur Aufklärung des Angriffs.

G

Georedundante Cloud (Kapitel 4.6) Datenspeicherung in der Cloud an mehreren geografisch getrennten Standorten zur erhöhten Ausfallsicherheit.

H

Hacker (Kapitel 4.1.2, 4.2.3.4) Person, die versucht, unerlaubt in Computersysteme einzudringen (kann böswillig oder ethisch motiviert sein).

I

IDS (Intrusion Detection System) (Kapitel 4.2.3.1, 4.2.4.3, 4.3.2) System zur automatischen Erkennung von Angriffsversuchen auf ein Netzwerk oder einen Computer.

Incident Response Plan (IRP) (Kapitel 4.2.3, 4.3.3, 4.4.1) Detaillierter Plan mit konkreten Handlungsanweisungen für den Fall eines Sicherheitsvorfalls.

Insider-Bedrohungen (Kapitel 4.1.2) Sicherheitsrisiken, die von Mitarbeitern oder anderen internen Personen ausgehen.

ISO/IEC 27001 (Kapitel 4.5.3) Internationaler Standard für Informationssicherheits-Managementsysteme.

ISMS (Informationssicherheits-Managementsystem) (Kapitel 4.5.3) Systematischer Ansatz zur Verwaltung der Informationssicherheit in einem Unternehmen.

IT-Forensik (Kapitel 4.2.3.4, 4.3.1, 4.4.2) Spezialisierter Bereich der digitalen Forensik, der sich mit der Untersuchung von IT-Sicherheitsvorfällen befasst.

IT-Grundschutz (Kapitel 4.5.3) Vom BSI entwickelte Methodik zur Absicherung von IT-Systemen.

IT-Penetrationstests (Kapitel 4.2.2.5) Autorisierte simulierte Angriffe auf IT-Systeme, um Schwachstellen zu identifizieren.

K

Kompromittiert (Kapitel 4.2.3.2, 4.2.3.4) Ein System oder Konto, das von einem Angreifer übernommen oder infiltriert wurde.

Kritische Systeme (Kapitel 4.2.1.1, 4.2.1.5) IT-Systeme, die für den Geschäftsbetrieb unverzichtbar sind.

L

Lessons Learned (Kapitel 4.2.4.1, 4.3.2, 4.3.3) Systematische Auswertung eines Vorfalls, um daraus für die Zukunft zu lernen.

Log-Dateien (Logfiles) (Kapitel 4.2.3.4, 4.2.4.3, 4.3.3) Automatisch erstellte Protokolldateien, die Aktivitäten in IT-Systemen aufzeichnen.

Lösegeld (Ransom) (Kapitel 4.1.2, 4.1.3, 4.2.3.2) Geldforderung von Cyberkriminellen für die Freigabe verschlüsselter Daten.

M

Malware (Kapitel 4.2.3.1, 4.5.2) Oberbegriff für schädliche Software wie Viren, Trojaner oder Würmer.

Managed Security Services (Kapitel 4.4.2) Externe Dienstleister, die die IT-Sicherheit eines Unternehmens überwachen und verwalten.

MFA (Multi-Faktor-Authentifizierung) (Kapitel 4.2.1.3, 4.2.4.3, 4.3.2) Sicherheitsverfahren, bei dem mehrere unabhängige Nachweise zur Identitätsbestätigung erforderlich sind.

Monitoring (Kapitel 4.2.4.3) Kontinuierliche Überwachung von IT-Systemen zur frühzeitigen Erkennung von Problemen.

N

Netzwerksegmentierung (Implizit in Kapitel 4.2.1.1) Aufteilung eines Netzwerks in kleinere, isolierte Bereiche zur Erhöhung der Sicherheit.

NIS 2-Richtlinie (Kapitel 4.5.3) EU-Richtlinie zur Netzwerk- und Informationssicherheit mit verbindlichen Sicherheitsanforderungen.

NIST Cyber-Security Framework (Kapitel 4.4.2, 4.5.3) US-amerikanisches Rahmenwerk mit Best Practices für Cyber-Sicherheit.

O

Open-Source (Kapitel 4.5.2) Software, deren Quellcode öffentlich zugänglich und frei nutzbar ist.

P

Patch (Kapitel 4.2.3.4) Software-Update zur Behebung von Sicherheitslücken oder Fehlern.

Penetrationstest (Kapitel 4.2.2.5, 4.2.4.3, 4.4.2) Siehe IT-Penetrationstests.

Phishing (Kapitel 4.1.2, 4.2.1.3, 4.2.2.4, 4.2.3.1, 4.2.3.4, 4.2.4.3) Betrugsversuch, bei dem gefälschte E-Mails oder Webseiten verwendet werden, um an vertrauliche Daten zu gelangen.

R

RAM-Speicher (Kapitel 4.2.3.4) Arbeitsspeicher eines Computers, der flüchtige Daten während des Betriebs enthält.

Ransomware (Kapitel 4.1.2, 4.1.3, 4.2.2.4, 4.2.3.2, 4.2.4.4, 4.3.2) Schadsoftware, die Daten verschlüsselt und Lösegeld für deren Freigabe fordert.

Recovery Time Objective (RTO) (Kapitel 4.6) Die maximal akzeptable Zeit, bis ein System nach einem Ausfall wiederhergestellt sein muss.

Redundanter Server (Kapitel 4.6) Zusätzlicher Backup-Server, der bei Ausfall des Hauptservers einspringt.

S

SaaS (Software as a Service) (Kapitel 4.6) Software, die über das Internet bereitgestellt und genutzt wird, ohne lokale Installation.

Schwachstelle (Kapitel 4.1.2, 4.2.1.1, 4.2.1.4, 4.2.2.4, 4.2.3.4, 4.2.3.5, 4.2.4.3) Sicherheitslücke in Software oder Systemen, die von Angreifern ausgenutzt werden kann.

Sicherheitsaudit (Kapitel 4.2.2.5, 4.2.4.3, 4.4.1) Systematische Überprüfung der IT-Sicherheitsmaßnahmen eines Unternehmens.

SIEM (Security Information and Event Management) (Kapitel 4.2.3.1) System zur zentralen Sammlung und Analyse von Sicherheitsereignissen.

Social Engineering (Kapitel 4.1.2, 4.2.1.3) Manipulationstechniken, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben.

Systemlogs (Kapitel 4.2.4.3) Siehe Log-Dateien.

T

Trojaner (Implizit in Malware-Definition) Schadsoftware, die sich als nützliches Programm tarnt.

V

Verschlüsselung (Kapitel 4.2.2.3, 4.6) Verfahren zur Umwandlung von Daten in eine unleserliche Form zum Schutz vor unbefugtem Zugriff.

Virenscanner (Kapitel 4.3.2) Software zur Erkennung und Entfernung von Computerviren und anderer Malware.

Vulnerabilität (Implizit in Schwachstellen-Diskussion) Siehe Schwachstelle.

W

Wiederherstellung (Kapitel 4.2.3.5, 4.3.3, 4.6) Prozess zur Rückführung von IT-Systemen in den normalen Betriebszustand nach einem Vorfall.

Z

ZAC (Zentrale Ansprechstelle Cybercrime) (Kapitel 4.3.1, 4.5.1) Polizeiliche Anlaufstelle für Unternehmen bei Cyberkriminalität.

Zero-Day-Schwachstelle [S] (Implizit in Schwachstellen-Diskussion) Sicherheitslücke, die dem Hersteller noch nicht bekannt ist und für die es noch keinen Patch gibt. → siehe auch: **Schwachstelle, Patch**

Begriffe in 5 OT-Security für KMU

C

CIA-Triade (Kapitel 5.1.2) Die drei Grundbausteine der Informationssicherheit: Confidentiality (Vertraulichkeit: Schutz von Daten vor unbefugtem Zugriff), Integrity (Integrität: Gewährleistung, dass Daten unverändert sind) und Availability (Verfügbarkeit: Sicherstellung, dass Daten und Systeme immer verfügbar sind)

D

DCS (Distributed Control System/Verteiltes Steuerungssystem) (Kapitel 5) System zur automatisierten Steuerung und Überwachung industrieller Prozesse.

Demilitarisierte Zone (DMZ) (Kapitel 5.3.1.1.1) Pufferzone zwischen einem internen (z. B. OT) und einem externen Netzwerk (z. B. IT oder Internet), um den Zugriff auf bestimmte Dienste zu ermöglichen, ohne das interne Netzwerk direkten Gefahren auszusetzen.

Digitale Kriegsführung (Kapitel 5.1.1) Gezielte, koordinierte Cyberangriffe auf eine Menge an Geräten zur Sabotage oder Spionage. Oftmals sind bestimmte Länder oder Regionen im Fokus.

I

Industrial Control System (ICS) (Kapitel 5.3.1.3.4, 5.3.1.1.6) Oberbegriff für Systeme bestehend aus Hard- und Software, die zur Steuerung, Überwachung und zum Betrieb von Anlagen, Maschinen und Prozessen in industriellen Umgebungen zum Einsatz kommen.

Industrial Internet of Things (IIoT)/Industrielles Internet der Dinge (IIdD) untereinander verbundene Sensoren, Instrumente und andere Geräte, die mit industriellen Anwendungen von Computern vernetzt sind, einschließlich Fertigung und Energiemanagement.

Information Security Management System (ISMS) Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

IT-OT-Konvergenz durch den Anstieg von Edge Computing bedingt. Beim Edge Computing werden Rechenressourcen näher zum physischen Standort des Nutzers oder der Datenquelle verschoben. Auch die zunehmende Vernetzung von Industriellen Steuerungssystemen sorgt für eine Verschmelzung von IT und OT.

M

Mean Time Between Failures (MTBF) durchschnittliche Betriebszeit zwischen Ausfällen von Komponenten oder Systemen, um die Zuverlässigkeit zu bewerten und vorbeugende Wartungsstrategien zu optimieren.

O

Operative Technologie (OT) (Kapitel 5) auch Automatisierungstechnologie genannt. Erkennt oder bewirkt eine Veränderung durch die direkte Überwachung und/oder Steuerung von Industrieanlagen, Anlagen, Prozessen und Ereignissen. Beispiele für OT-Bestandteile: Maschinen (+ Steuerungs-PCs, daran angeschlossene Netzwerktechnologien etc.), Kameras, Zutrittskontrolle, Lüftungsanlagen etc.

P

PDCA-Zyklus (Kapitel 5.3) auch Demingkreis oder Shewhart-Zyklus. Zugrundeliegender Prozess bei gängigen Standards wie ISO 27K. Steht für Plan-Do-Check-Act: einen Prozess zu planen, ihn probeweise einzuführen, zu überprüfen, allgemein einzuführen und dieses Verfahren kontinuierlich auszuführen.

PLC (Programmable Logic Controller/Speicherprogrammierbare Steuerung/SPS) (Kapitel 5) Instrument zur automatischen Steuerung anderer Geräte.

Plug-ins (Kapitel 5.1.1) Optionale Software-Komponenten, welche ein Programm erweitern, um so neue Funktionalitäten hinzuzufügen.

R

Ransomware-Attacke (Kapitel 5.1.1) Angriff mit dem Ziel, ein Opfer zu erpressen (oft durch Datenverschlüsselung), um so an Geld, Informationen oder ähnliches zu gelangen

RTU (Remote Terminal Unit/Fernbedienungsterminal) (Kapitel 5) Instrument zur Fernsteuerung anderer Geräte

S

Security Information and Event Management (SIEM) (Kapitel 5.3.1.1.8) integriertes Sicherheitssystem, das Sicherheitsdaten aus verschiedenen Quellen sammelt, analysiert und verwaltet. Die meisten SIEMs bieten ein Dashboard mit einem schnellen Überblick über die Infrastruktur sowie allgemein sicherheitsrelevante Daten.

Self-Assessment-Tools (Kapitel 5.3.1.2) Werkzeuge (bspw. Fragebögen oder Checklisten) zur einfachen Einschätzung der eigenen Cyber-Sicherheit

Supervisory Control and Data Acquisition (SCADA) (Kapitel 5) Netzwerk aus Hardware und Software für die Echtzeitüberwachung, Kontrolle und Steuerung von Industriemaschinen und -anlagen. Das Computersystem/die Software eines ICS.

Service Level Agreement (SLA) (Kapitel 5.3.1, 5.3.1.6) definiert messbare Leistungsstandards und Verantwortlichkeiten zwischen einem Dienstleister und einem Kunden, um die Verfügbarkeit, Zuverlässigkeit und Reaktionszeiten von kritischen Systemen und Diensten zu gewährleisten.

V

Virtual Private Network (VPN) (Kapitel 5.3.1.1.1) ermöglicht eine sichere, verschlüsselte Verbindung für den Fernzugriff und die Kommunikation zwischen Geräten, um die Integrität und Vertraulichkeit der Daten zu gewährleisten.

QUELLEN UND WEITERFÜHRENDE LITERATUR

Informationsseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI)	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html
IT-Grundschutz-Kompendium des BSI zur Cybersecurity	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
Übersicht zu KMU Cybersecurity vom National Institute of Standards and Technology (NIST) (US)	https://www.nist.gov/itl/smallbusinesscyber
Cybersecurity Tipps von der Federal Communications Commission (US)	https://www.fcc.gov/communications-business-opportuni-ties/cybersecurity-small-businesses
Überblick über Cybersicherheitsmaßnahmen (Federal Trade Commission) (US)	https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
Cybersicherheitsframework für KMU der australischen Regierung (AU)	https://www.cyber.gov.au/sites/default/files/2025-03/Small%20business%20cybersecurity%20guide%20%28January%202025%29.pdf
Cybersicherheitsinformationsseite der australischen Regierung (AU)	https://www.cyber.gov.au/business-government/small-business-cyber-security/small-business-hub/small-business-cyber-security-guide
Cybersicherheitsinformationsseite des National Cybesecurity Centre (UK)	https://www.ncsc.gov.uk/cyberessentials/overview
Cybersecurity für KMU – Herausforderungen und Empfehlungen (ENISA)	https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf
Cybersicherheitsframework für KMU der kanadischen Regierung (CA)	https://www.cyber.gc.ca/sites/default/files/cyber/publications/Baseline.Controls.SMO1_.2-e%20.pdf

NIST-Richtlinien für das Management von Cybersecurity-Risiken in der Lieferkette	https://csrc.nist.gov/pubs/sp/800/161/r1/final
Aktualisierte NIST-Richtlinien zur Verbesserung der Sicherheit in Lieferketten	https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final
Cybertrustaustria-Datenschutzrating	https://cyberrisk-rating.at/cyberrisk-2025-schema-de.pdf
Überblick über Datenschutzmaßnahmen und Bewertungsschema des KSV1870-Ratings	https://cyberrisk-rating.at/datenschutz-folder-de.pdf
KSV1870 Datenschutzrating - Homepage	https://cyberrisk-rating.at/datenschutzrating.html
Mustervertrag für Service Level Agreements (SLA) im Bereich Cybersecurity.	https://itrechtler.de/Mustervertrage/Cybersecurity_SLA/cybersecurity_sla.html
Beispielhafte Informationssicherheitsrichtlinie für Lieferanten von Schmalz	https://media.schmalz.com/MAM_Library/Dokumente/Company%20and%20Press/Company/8139a148380f_Document_Schmalz_Purchasing_DE_Informationssicherheitsrichtlinie.pdf
NIST-Richtlinien zur Supply Chain Cybersecurity Risk Management (aktualisierte Version)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf
IT-Grundschutz-Kompendium des BSI zur Cybersecurity	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
Anforderungen an Lieferanten im Bereich Kritische Infrastrukturen (KRITIS)	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-anforderungen-lieferanten.html
Beispielhafte Informationssicherheitsrichtlinien und -verfahren der Firma Corning	https://www.corning.com/IS_supplier_training/en/IS_policy_and_procedures_summary_EN.pdf
Strategien zur Cybersecurity und Risikomanagement in Lieferketten	https://www.dataguard.de/blog/cybersicherheit-und-lieferketten-risikomanagement/
ENISA-Empfehlungen für sichere Lieferketten	https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

ENISA-Überblick über regulatorische Rahmenbedingungen für Cybersecurity	https://www.enisa.europa.eu/about-enisa/regulatory-framework/legislation
Beispielhafte Versicherungsbedingungen für Cyberrisiko-Versicherungen	https://www.gdv.de/re-source/blob/6100/d4c013232e-8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf
Praxisbeispiel zur Implementierung eines Risikomanagementsystems	https://media.haufe-group.com/media/attachmentlibraries/rp/profirma/Gratis-Fachbeitrag_Risikomanagementsystemrichtigeinfuehren.pdf
Methoden zur Bewertung von Cybersecurity-Risiken	https://www.ibm.com/de-de/think/topics/cybersecurity-risk-assessment
Wie KMU durch Supply Chain Angriffe bedroht werden – Blog	https://www.industry-of-things.de/wie-supplychain-attacken-kleine-und-mittlere-unternehmen-bedrohen-a-6fd361ec31c16a19e7bedd6782f81ebb
Weshalb die Sicherheit in der gesamten Lieferantenkette so wichtig ist – Blog	https://www.infoguard.ch/de/blog/cyber-supply-chain-risk-management-sicherheit-in-der-lieferantenkette
Studie zu Sicherheitslücken in globalen Lieferketten	https://www.isaca.org/resources/reports/supply-chain-security-gaps-a-2022-global-research-report
Beispielhafte Vertragsklauseln zur Informationssicherheit und Cybersecurity	https://www.lawinsider.com/de/clause/informationssicherheit-cyber-security
Schadensregulierung und Bedingungen bei Cyberversicherungen – Blog	https://www.mittelstandswiki.de/wissen/Schadensregulierung_bei_Cyberversicherungen/
Beispielhafte Datenschutzklauseln und Datenregelungen in Verträgen und AGB	https://www.mme.ch/de-ch/magazin/artikel/datenschutzklauseln-und-datenregelungen-in-vertraegen-und-agb
Leitfaden zur Cybersicherheit in Lieferketten vom Schweizer NCSC	https://www.ncsc.admin.ch/supply-chain-de
Überblick zur Bewertung der Cybersicherheit in Lieferketten (UK NCSC)	https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
Sammlung von Maßnahmen zur Absicherung von Lieferketten (UK NCSC)	https://www.ncsc.gov.uk/collection/supply-chain-security

Überblick über Supply Chain Security-Maßnahmen	https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Supply-Chain-Security/Uebersicht-zu-Supply-Chain-Security.html
Zehn Schritte zum langfristigen Schutz der OT-Lieferkette	https://www.radiflow.com/blog/ten-steps-for-protecting-the-ot-supply-chain-long-term/
Chancen und Bedrohungen der Lieferketten durch IT-Sicherheit und KMU	https://www.researchgate.net/publication/357243406_IT_security_in_SMEs_-_Threats_and_Chances_for_Supply_Chains
Anforderungen an Lieferketten gemäß der NIS2-Richtlinie	https://www.stueckmann.de/leistungen/digital-compliance/news-digital-compliance/anforderungen-an-lieferketten-im-rahmen-der-nis-2-richtlinie/
Artikel: Back to basics. Cybersecurity is everyone´s job	https://www.forbes.com/councils/forbesbusinesscouncil/2022/02/08/back-to-basics-cybersecurity-is-everyones-job/
Artikel: Es kommt auf die menschliche Firewall an	https://www.itsicherheit-online.com/security-manage-ment/es-kommt-auf-die-menschliche-firewall-an-2/
Studie Deloitte: Cyber Security Report 2024	https://www.deloitte.com/content/dam/assets-zone2/at/de/docs/services/risk-advisory/2024/at-cyber-security-report-24.pdf
Whitepaper Deloitte: Die Zukunft sichern: Cyber Security für das Jahr 2030	https://www.deloitte.com/de/de/services/consulting-risk/perspectives/cyber-security-szenarien-2030.html
Willie, M.: The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture	https://ritha.eu/journals/JORIT/issues/4/articles/5
Studie HSD: Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)	https://doi.org/10.20385/2625-3690/2018.1
Aufsatz Neumann, S. et al.: Effektiver Schutz vor betrügerischen Nachrichten. Ein Schulungsprogramm zur Erkennung betrügerischer Nachrichten für KMU	https://link.springer.com/article/10.1007/s11623-018-0945-x
Weber K., Schütz,A.: Mitarbeiter sensibilisieren statt informieren	https://www.researchgate.net/profile/AndreasSchuetz-3/publication/323640529_ISIS12Hack_Mitarbeiter_sensibili-sieren_statt_informie-ren/links/5aa15ccda6fdcc22e2d1106e/ISIS-12Hack-Mitarbei-ter-sensibilisieren-statt-informieren.pdf

Kurzerklärung von SCADA	https://www.emaint.com/de/blog-what-is-scada/
Kurzerklärung von SIEM	https://enginsight.com/de/glossar/siem/
Zusammenfassung des ISA/IEC 62243 Standards	https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung
Wissenschaftliche Arbeit über einen Vergleich verschiedener Cybersicherheits-Standards	https://doi.org/10.1109/IECON.2019.8927559
Wissenschaftliche Arbeit über Cybersicherheits-Open-Source-Software	https://doi.org/10.1201/9781003426134
Wikipedia-Artikel über das IIoT	https://en.wikipedia.org/wiki/Industrial_internet_of_things
Kurzerklärung von ICS	https://www.security-insider.de/was-ist-einindustrielles-steuerungssystem-ics-a-1064736/
Wikipedia-Artikel über ISMS	https://de.wikipedia.org/wiki/Information_Security_Management_System
Kurzerklärung von OT	https://www.redhat.com/en/topics/edge-computing/what-ot
Wikipedia-Artikel über OT	https://en.wikipedia.org/wiki/Operational_technology
Bericht des BMK über Sicherheit für die digitale Transformation der Produktion	https://www.bmimi.gv.at/themen/innovation/publikationen/produktion/sigi.html
Zusammenfassung des ISO/IEC 27k Standards	https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheit-leitfaden-Informationssicherheitsmanagememt.pdf
Empfehlungen des BSI für Betreiber von ICS	https://www.bsi.bund.de/dok/6603566
Wissenschaftliche Arbeit über Cybersicherheit von tschechischen und slowakischen KMU	https://ieeexplore.ieee.org/document/9261506
Wissenschaftliche Arbeit über Anwendbarkeit von OT-Cybersicherheits-Standards in KMU	https://doi.org/10.1109/EMCTECH49634.2020.9261506

Artikel über NIS 2 und OT-Cybersicherheit im Allgemeinen	https://www.diva-portal.org/smash/get/diva2:1784461/FULLTEXT01.pdf
Ein Orientierungsleitfaden für Hersteller zur IEC 62443	https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/
Artikel über NIS 2 und OT-Cybersicherheit im Allgemeinen	https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/nis2-and-its-impact-on-operational-technology-cybersecurity/
Der europäische (ENISA) Rechtsakt zu zertifizierbarer Cybersicherheit	https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
Überarbeitung der europäischen Maschinenrichtlinie	https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733576/EPRS_BRI(2022)733576_EN.pdf
Die ursprüngliche europäische Maschinenrichtlinie	https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0042
Weitere Überarbeitung der europäischen Maschinenrichtlinie	https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02023R1230-20230629
Die ISA/IEC 62443-Standard-Reihe	https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
Die ISO/IEC 27k-Standard-Familie	https://www.iso.org/standard/iso-iec-27000-family
Der NIST SP 800-82r3 Standard	https://doi.org/10.6028/NIST.SP.800-82r3
Die VDI/VDE 2182-Standard-Reihe	https://www.vdi.de/2182
Der CIS Controls Implementation Guide for Industrial Control Systems	https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1-industrial-control-systems-ics-guide

Tabelle 8: Quellen und weiterführende Literatur

RÜCKBLICK UND DANK

Nach 3,5 Jahren geht das Forschungsprojekt „Cyber Security und Resilienz in Supply Chains mit Fokus auf KMU“ (CySeReS-KMU) zu Ende. Das Projekt wurde im Rahmen des Programms INTERREG VI-A Bayern-Österreich 2021–2027 durchgeführt, das von der Europäischen Union kofinanziert wird (Projektnummer BA0100016). Die Projektlaufzeit war geprägt von intensivem Austausch, vertrauensvoller Zusammenarbeit und zahlreichen wertvollen Impulsen für die gemeinsame Arbeit.

Unser besonderer Dank gilt allen beteiligten Unternehmen, Projektpartnern und Mitwirkenden, die dieses Vorhaben mit großem Engagement, fachlicher Expertise und Offenheit begleitet und mitgestaltet haben.

CySeReS KMU

Interreg Bayern-Österreich

Kofinanziert von der Europäischen Union