Bundesministerium Finanzen

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

CyberGuide

Anforderungen von KMU zur Cybersicherheit

finanziert im Sicherheitsforschungs-Förderprogramm KIRAS des Bundesministeriums für Finanzen

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Finanzen, Radetzkystraße 2, 1030 Wien
Autorinnen und Autoren:
BRIMATECH Services GmbH und Silicon Austria Labs GmbH
Autorinnen 1: Theresa Hirsch MSc. und Mag. Johanna Berndorfer
Autoren 2: Dr. Willibald Krenn und Dr. Florian Lorber
Wien, Oktober 2024.

Inhalt

1 Kurzfassung 4

2 Abstract 7

3 Einleitung 10

3.1 Ausgangssituation und Zielsetzung 10

3.2 Studieninhalt und Methodik 11

3.3 Abgrenzung 14

4 Cybersicherheit in Österreich 15

4.1 Bedeutung Cybersicherheit 15

4.2 Aktuelle Bedrohungslage und Angriffsvektoren 20

4.3 Ökosystem 23

4.4 Status Cybersicherheit in österreichischen KMU 30

4.5 Bedürfnisse KMU zu Cybersicherheit 35

5 Rahmenbedingungen 40

5.1 Rechtliche Anforderungen 40

5.2 Technische Anforderungen 45

5.3 Organisatorische Anforderungen 46

5.4 Gesellschaftliche Anforderungen 47

5.5 Barrieren und Herausforderungen 48

5.6 Trends 51

6 Handlungsfelder und Empfehlungen 54

6.1 Cybersicherheit verankern 54

6.2 Risikomanagement aufbauen 57

6.3 Technologische Schutzmauern festigen 59

6.4 Compliance sichern 63

7 Verzeichnisse 66

Abbildungsverzeichnis 67

Literaturverzeichnis 69

Abkürzungen 71

8 Anhang: Leitfaden 73

1 Kurzfassung

Cybersicherheit zielt darauf ab, Netz- und Informationssysteme, die Nutzerinnen und Nutzer solcher Systeme und andere von Cyberbedrohungen betroffenen Personen zu schützen. Diese umfassende Perspektive reicht von der Absicherung einzelner Geräte und Netzwerke bis zur Etablierung einer gefestigten Sicherheitskultur durch Mitarbeiterschulungen und Awareness-Trainings. Ein gut strukturiertes Risikomanagement stärkt die Abwehr gegen potenzielle Cyberangriffe und -vorfälle.

Die gegenständliche Studie CyberGuide wurde im Rahmen des österreichischen Förderprogramms für Sicherheitsforschung, KIRAS, als F&E Dienstleistung „Anforderungen von KMU zur Cybersicherheit“ ausgeschrieben. Ziel ist es, die gegenwärtige Situation in österreichischen KMU zu analysieren, einen Leitfaden zu entwickeln, Handlungsfelder darzustellen und Handlungsempfehlungen für eine erhöhte Cybersicherheit abzuleiten.

Dabei werden Fragen beantwortet wie: Welche Fähigkeiten zur Cybersicherheit sind bei österreichischen KMU vorhanden? Welche Standards bestehen, sind für KMU relevant und den KMU bekannt? Mit welchen Herausforderungen sind KMU konfrontiert? Welche Bedürfnisse hinsichtlich Cybersicherheit haben KMU?

Die **Fähigkeiten österreichischer KMU** variieren deutlich nach Unternehmensgröße. Sei es in Bezug auf die Häufigkeit von Risikobewertungen, der unterschiedlich implementierten Sicherheitsmaßnahmen oder der Investitionen in Cybersicherheit. Während mittlere Unternehmen tendenziell häufiger Risikobewertungen durchführen, sind Kleinst- und kleine Unternehmen hier zurückhaltender. Die am weitesten verbreitete Cybersicherheitsmaßnahme sind regelmäßige Sicherheitsupdates, gefolgt von der Sicherung des Netzwerks vor unberechtigtem Zugriff von außen und der Verwendung sicherer Passwörter. Vorreiter sind mittlere Unternehmen im Bereich der klaren Zuständigkeiten und des Zugriffsmanagements nach Berechtigungskonzepten. Weniger verbreitet in KMU sind hingegen Maßnahmen wie regelmäßige Mitarbeiterschulungen und das Erstellen von Notfallplänen. Zusätzlich ergreifen die meisten KMU entweder keine oder nur wenige Maßnahmen zur Risiko-minimierung bei Drittanbietern. Bezüglich der Investitionen in die Cybersicherheit, gibt ein Fünftel der KMU an, dass sie keine gezielten Investitionen tätigen. Bei Unternehmen mit gezielten Investitionen werden großteils 6-10 % des IT-Budgets für Cybersicherheit verwendet.

Es bestehen zahlreiche **Cybersecurity-Standards**, die für KMU in Österreich relevant sein könnten, abhängig von ihrer Branche und den gesetzlichen Vorgaben. Internationale und nationale Organisationen wie ISO, IEC, NIST und BSI bieten verschiedene Normen an, die eine Orientierung in der IT-Sicherheit geben, beispielsweise die ISO/IEC 27001 für Informationssicherheitsmanagement. Dennoch zeigt sich, dass viele KMU nur eine begrenzte Kenntnis über diese Standards und Richtlinien haben. Bekannte Verordnungen wie die Datenschutzgrundverordnung sind den meisten KMU geläufig, während neuere oder spezialisierte Regelungen wie der Digital Operational Resilience Act kaum bekannt sind. Für KMU sind weniger aufwändige Grundschutz-Varianten (wie die des BSI oder der WKO) oft praktikabler und sollten als Mindeststandard etabliert sein

Die **Herausforderungen** für KMU sind vielfältig und reichen von begrenzten finanziellen Ressourcen über fehlendes Bewusstsein für die Bedeutung von Cybersicherheit bis hin zu einem Mangel an Fachkräften. Zusätzlich steigen Compliance-Anforderungen und Cyberkriminelle entwickeln zunehmend raffiniertere Angriffsstrategien. Viele Angriffe, wie Phishing oder Social Engineering, nutzen gezielt menschliche Schwächen aus. Hinzu kommt, dass die Komplexität des Themas und das Fehlen maßgeschneiderter, kostengünstiger Lösungen, die den Bedürfnissen KMU gerecht werden, den Einstieg zusätzlich erschweren.

Der Wunsch nach praxisnaher Unterstützung und passgenauen Cybersicherheitslösungen prägt die **Bedürfnisse österreichischer KMU.** Viele Unternehmen möchten ihre Sicherheitsrichtlinien und -technologien modernisieren sowie gezielt IT-Expertise aufbauen, stoßen jedoch auf finanzielle und technische Hürden. Daher wünschen sie sich vor allem finanzielle Förderungen, kostengünstige Beratung und Schulungen, die speziell auf die Bedürfnisse kleinerer Betriebe zugeschnitten sind. Zusätzlich streben sie nach einfacheren und erschwinglichen Cybersecurity-Lösungen, die weniger komplex und schneller implementierbar sind. Der Wunsch nach einem niederschwelligen Zugang zu europäischer IT-Sicherheit und einer Notfall-Hotline für akute Probleme verdeutlicht, dass KMU einen flexiblen, bedarfsgerechten Ansatz zur Verbesserung ihrer Cybersicherheit bevorzugen.

Zur Stärkung der Cybersicherheit in österreichischen KMU wurden **vier zentrale Handlungsfelder** identifiziert. Zunächst ist es entscheidend, Cybersicherheit fest im Unternehmen zu verankern. Dies geschieht aufgrund von klaren Verantwortlichkeiten, regelmäßigen Trainings und einer offenen Fehler- und Kommunikationskultur. Darauf aufbauend hilft ein strukturiertes Risikomanagement, Bedrohungen frühzeitig zu erkennen und gezielt Maßnahmen zu priorisieren. Ergänzend hierzu sind technologische Schutzmaßnahmen wie Netzwerksicherheit und Endgeräteschutz unerlässlich, um gegen

Cyberangriffe gewappnet zu sein. Schließlich spielt die Einhaltung gesetzlicher Vorgaben eine wesentliche Rolle, um rechtliche Risiken zu minimieren und Sicherheitsstandards nachhaltig zu sichern. Daraus resultieren **Handlungsempfehlungen** für die öffentliche Hand: Bewusstsein bilden, Mitarbeiterschulungen subventionieren, Cybersecurity Tool und Services Datenbank aufbauen, Open Source Paket und KMU-Ratgeber bereitstellen.

Der **CyberGuide für KMU - Praxisleitfaden für Cybersicherheit** ist ein Leitfaden, der speziell auf die Bedürfnisse von KMU zugeschnitten ist. Die enthaltenen 19 Maßnahmen sind leicht-verständlich formuliert, schrittweise aufgebaut und erfordern keine umfassenden IT-Vorkenntnisse. Der Leitfaden bietet grundlegende Sicherheitsmaßnahmen, die jedes KMU umsetzen sollte. Die Maßnahmen sind in fünf Abschnitte unterteilt, die auf unterschiedliche Aspekte der Cybersicherheit abzielen: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

Die Politik steht in der Verantwortung, in den kommenden Jahren klare Leitlinien, verbindliche Vorgaben und wirkungsvolle Anreizsysteme zur Förderung der Cybersicherheit in KMU zu formulieren. Die Studie CyberGuide kann eine Basis für weitere strategiepolitische Maßnahmen seitens der öffentlichen Hand sein.

2 Abstract

Cybersecurity aims to protect network and information systems, their users, and other individuals affected by cyber threats. This comprehensive perspective ranges from securing individual devices and networks to establishing a robust security culture through employee training and awareness programs. A well-structured risk management approach strengthens defense against potential cyberattacks and incidents.

The current CyberGuide study was commissioned as part of the Austrian KIRAS security research funding program as an R&D service titled "Cybersecurity Requirements for SMEs." The goal is to analyze the current cybersecurity landscape in Austrian SMEs, develop a guideline, identify key action areas, and derive recommendations to enhance cybersecurity. The study addresses questions such as: What cybersecurity skills are present in Austrian SMEs? Which standards exist, are relevant for SMEs and are SMEs aware of them? What challenges do SMEs face? What are their specific cybersecurity needs?

The **cybersecurity capabilities of Austrian SMEs** vary significantly by company size, including differences in the frequency of risk assessments, implemented security measures, and cybersecurity investments. Medium-sized companies tend to conduct risk assessments more frequently, while smaller enterprises are often more cautious. The most common cybersecurity measure is regular security updates, followed by network protection against unauthorized access and the use of strong passwords. Medium-sized businesses lead in assigning clear responsibilities and implementing access management based on authorization schemes, while measures such as regular employee training and emergency plans are less common. Additionally, most SMEs take few or no measures to mitigate risks from third-party vendors. Regarding investments in cyber security, a fifth of SMEs state that they do not make any targeted investments. In companies with dedicated investments, 6-10% of the IT budget is used for cyber security.

There are various cybersecurity **standards** that may be relevant to SMEs in Austria, depending on their industry and regulatory requirements. International and national organizations such as ISO, IEC, NIST, and BSI offer various standards to guide IT security practices, such as ISO/IEC 27001 for information security management. However, many SMEs have limited awareness of these standards and guidelines. Well-known regulations like the General Data Protection Regulation (GDPR) are widely recognized, while newer or

specialized regulations, such as the Digital Operational Resilience Act, are less familiar. For SMEs, simpler, baseline security models (such as those from BSI or WKO) are often more practical and should be established as a minimum standard.

The **challenges** facing SMEs are diverse, ranging from limited financial resources and a lack of awareness about cybersecurity importance to a shortage of skilled labor. In addition, compliance requirements are increasing, and cybercriminals are developing more sophisticated attack strategies. Many attacks, such as phishing or social engineering, exploit human weaknesses. Furthermore, the complexity of the issue and the lack of customized, cost-effective solutions that meet the needs of SMEs make it even more difficult to deal with.

A strong need for practical support and tailored cybersecurity solutions shapes the **needs of Austrian SMEs**. Many companies want to modernize their security policies and technologies and build specific IT expertise but encounter financial and technical barriers. Therefore, they primarily seek financial support, affordable consulting, and training specifically geared towards the needs of smaller enterprises. Additionally, they desire simpler and more affordable cybersecurity solutions that are less complex and quicker to implement. The need for accessible European IT security and an emergency hotline for urgent issues indicates that SMEs prefer a flexible, needs-based approach to improving their cybersecurity.

To strengthen cybersecurity in Austrian SMEs, **four central action areas** have been identified. Firstly, establishing cybersecurity within the company is essential, achieved through clear responsibilities, regular training, and an open culture for handling errors and communication. Building on this, a structured risk management system helps to identify threats early and prioritize targeted measures. In addition, technological safeguards such as network security and endpoint protection are essential to be well-prepared against cyberattacks. Lastly, compliance with regulatory requirements plays a crucial role in minimizing legal risks and sustainably maintaining security standards. From these areas, **recommendations** for public authorities emerge: promoting awareness, subsidizing employee training, creating a cybersecurity tools and services database, offering an open-source package, and a guide for SMEs.

The **CyberGuide for SMEs - Practical Guide for Cybersecurity** is a guide specifically tailored to the needs of SMEs. It contains 19 straightforward and step-by-step measures that do not require extensive IT expertise. The guide provides fundamental security measures that

every SME should implement. These measures are divided into five sections targeting different aspects of cybersecurity: Identify, Protect, Detect, Respond, and Recover.

The government is responsible for developing clear guidelines, binding requirements, and effective incentive systems in the coming years to promote cybersecurity in SMEs. The CyberGuide study can serve as a foundation for further strategic measures from public authorities.

3 Einleitung

3.1 Ausgangssituation und Zielsetzung

Kleine und mittlere Unternehmen (KMU) sind zunehmend Cyberangriffen, die erhebliche Schäden verursachen können, ausgesetzt. Diese Angriffe führen nicht nur zu direkten finanziellen Schäden, wie Reparatur- oder Wiederherstellungskosten, sondern auch indirekten Schäden, wie zum Beispiel Umsatzeinbußen. Laut einem Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) gaben bei einer Umfrage zu Cybersicherheit in KMU über 80 % der KMU an, dass Cybersicherheitsprobleme innerhalb einer Woche ernsthafte negative Auswirkungen auf ihre Geschäftstätigkeit hätten. Besonders alarmierend ist, dass 57 % der befragten KMU angaben, dass ein schwerwiegender Cyberangriff sie in den Konkurs oder zur Einstellung ihrer Geschäftstätigkeit zwingen könnte. (European Union Agency for Cybersecurity, CYBERSECURITY FOR SMES, 2021)

Zusätzlich sind KMU in ein Netzwerk von Geschäftspartnern, Lieferant:innen und Kund:innen eingebettet, wodurch sie eine Rolle in der Wertschöpfungskette spielen. Aufgrund ihrer begrenzten Ressourcen und oft mangelnden Cybersicherheitsmaßnahmen gelten sie in Bezug auf Informationssicherheit als das „schwächste Glied“ in der Wertschöpfungskette. Cyberkriminelle nutzen gezielt diese Schwachstellen, um über KMU in größere Unternehmen einzudringen. Ein Angriff auf ein einzelnes KMU kann daher schwerwiegende Auswirkungen auf die gesamte Lieferkette haben, indem die Produktion unterbrochen, Daten von Partnern kompromittiert oder der Betrieb verzögert wird. Solche Angriffe verbreiten sich oft wie ein Dominoeffekt und schaden nicht nur dem angegriffenen Unternehmen, sondern auch anderen, die auf dessen Dienstleistungen und Daten angewiesen sind.

Um die Cybersicherheit in österreichischen KMU zu verbessern und dabei ihre speziellen Herausforderungen, Bedürfnisse, Fähigkeiten und Anforderungen zu berücksichtigen, wurde die gegenständliche Studie im Rahmen des Sicherheitsforschungsprogramms KIRAS als F&E Dienstleistung „Anforderungen von KMU zur Cybersicherheit“ ausgeschrieben.

Im Rahmen der Studie, „Anforderungen von KMU zur Cybersicherheit“, kurz CyberGuide, werden folgende Zielsetzungen definiert:

- Ziel 1: Entwicklung eines Leitfadens für KMU als Hilfestellung für die Implementierung der wirkungsvollsten Maßnahmen

- Ziel 2: Entwicklung von Handlungsfeldern und Handlungsempfehlungen für die öffentliche Hand zur Stärkung der Cyber-Resilienz von KMU

- Ziel 3: Sensibilisierung der KMU

Das Ergebnis umfasst einen Leitfaden mit empfohlenen Cybersicherheitsmaßnahmen für KMU, sowie einen Endbericht und eine Endpräsentation mit Handlungsfeldern und Handlungsempfehlungen.

3.2 Studieninhalt und Methodik

Als Ausgangsbasis werden im Rahmen von CyberGuide folgende im Ausschreibungsleitfaden definierten Themenbereiche untersucht.

Erhebung der Bedürfnisse von KMU zu Cybersicherheit, Cyber-Resilienz und Cyber-Hygiene

Hierbei lautet die zu beantwortende Frage wie folgt: Wie ist die Wahrnehmung österreichischer KMU zu Cybersicherheit und welche Bedürfnisse haben sie? Dabei werden die spezifischen Bedürfnisse von KMU in den Bereichen Cybersicherheit, Cyber-Resilienz und Cyber-Hygiene erhoben. Die Analyse konzentriert sich insbesondere darauf zu verstehen, wie österreichische KMU Cybersicherheit wahrnehmen und welche Schutzmaßnahmen und Strategien sie als besonders wichtig erachten. Zu möglichen Bedürfnissen gehören der Schutz vor Cyberangriffen, der Aufbau sicherer Netzwerke, der Datenschutz sowie die effektive Verwaltung von Sicherheitsrisiken. Ebenso werden der Kompetenzaufbau der Mitarbeiter und der Einsatz von Cyberversicherungen miterhoben.

Erhebung der vorhandenen Fähigkeiten von KMU

In diesem Themenbereich werden folgende essenzielle Fragen beantwortet: Welche Fähigkeiten zur Cybersicherheit sind bei österreichischen KMU vorhanden und wie branchenspezifisch sind diese? Welche Maßnahmen zur Cybersicherheit wurden bereits getroffen? Welche Maßnahmen sind für die Zukunft geplant? Wie begegnet man Cybersicherheitsrisiken in der Lieferkette? Die Erhebung fokussiert sich insbesondere auf vorhandene Fähigkeiten, im Bereich der technischen Expertise, dem

Sicherheitsbewusstsein, Risikomanagement, Aus- und Weiterbildung, finanzielle Ressourcen, sowie dem Umgang mit Risiken in der Wertschöpfungskette.

Identifikation aktueller und zukünftiger Anforderungen an KMU

Die zu beantworteten Fragen lauten wie folgt: Wie wirken sich Richtlinien, wie etwa die NIS2-Richtlinie, auf KMU aus? Sind sich KMU ihren Verpflichtungen, die aus den erweiterten Anforderungen resultieren, bewusst? Dabei werden die spezifischen Anforderungen an KMU, wie die Sicherstellung von Netz- und Informationssystemen, die Einführung von Sicherheitsrichtlinien auf Unternehmensebene und die Durchführung von Risikobewertungen, identifiziert und analysiert.

Erhebung nationaler und internationaler Standards und Industrie-Best Practices und deren Eignung für KMU

In diesem Kontext sind die folgenden Fragen zu beantworten: Welche Standards bestehen und sind für KMU relevant? Kennen KMU diese Standards? Inwiefern können für Großunternehmen entwickelte Lösungen für KMU adaptiert werden? Gibt es bereits zielgerichtete Best-Practice Beispiele, die auf KMU übertragbar sind? In der Erhebung wird speziell auf geltende Richtlinien, wie die ISO 27001, Richtlinien des BSI, COBIT, NIST SP 800-53, NIST Cybersecurity Framework eingegangen.

Erstellung einer Best Practice Leitfadens für KMU zu Cybersicherheit und Supply Chain Security unter Berücksichtigung der NIS2-Richtlinie

Unter Einbeziehung der erhobenen Bedürfnisse und Fähigkeiten österreichischer KMU und den aktuellen und zukünftigen Anforderungen durch verschiedene Richtlinien, Standards und Best-Practice Beispielen der Industrie wird ein auf KMU zugeschnittener Leitfaden entwickelt. Zusätzlich werden bei Bedarf branchenspezifische Maßnahmen aufgezeigt. Als Zielgruppe des Leitfadens wurden CEOs österreichischer KMU festgelegt.

Handlungsempfehlungen, wie aus staatlicher Sicht die KMU unterstützt werden können

Basierend auf den gewonnenen Erkenntnissen werden Rahmenbedingungen nach ausgewählten PESTEL-Kategorien (wirtschaftlich, organisatorisch, technisch, und rechtlich) herausgearbeitet, Handlungsfelder entwickelt und Handlungsempfehlungen für die öffentliche Hand abgeleitet.

Die methodische Herangehensweise von CyberGuide, wie in Abbildung 1 dargestellt, bestand aus fünf Schritten. Im ersten Schritt erfolgte die Sekundärforschung, wobei bestehende Erkenntnisse aus Fachliteratur, Studien und Statistiken zusammengetragen und

analysiert wurden. Dies beinhaltet die Analyse bestehender Strategien, Leitfäden, Richtlinien, Anforderungen und Barrieren im Bereich der Cybersicherheit von KMU. Zusätzlich wurden für KMU relevante Standards und Zertifizierungen identifiziert. Zahlreiche Publikationen befassen sich umfassend mit dem Thema Cybersicherheit und den umzusetzenden Maßnahmen. Einige wenige Publikationen fokussieren sich auf KMU.

Zu den wichtigsten Hintergrunddokumenten für die vorliegende Studie zählen:

- Cybersecurity for SMEs (European Union Agency for Cybersecurity, CYBERSECURITY FOR SMES: Challenges for SMEs, 2021)
- Österreichische Strategie für Cybersicherheit 2021 (BKA, 2021)
- Österreichisches Informationssicherheitshandbuch (Bundeskanzleramt & Zentrum für sichere Informationstechnologie - Austria, 2023)
- Cyber Risk Rating & Cyber Trust Label (Kompetenzzentrum Sicheres Österreich, 2024)
- Cybersicherheitsstrategie für Deutschland 2021 (Bundesministerium des Innern für Bau und Heimat, 2021)
- Die Lage der IT-Sicherheit in Deutschland 2023 (Bundesamts für Sicherheit in der Informationstechnik, 2023)
- Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-22 (ISB, 2018)

Abbildung 1: Methodik CyberGuide (eigene Darstellung)

Die Online-Umfrage diente der Erhebung der IST-Situation, der Bedürfnisse und dessen Erfüllungsgrad, sowie den aktuellen Fähigkeiten von österreichischen KMU. Es nahmen 51 Personen an der Erhebung teil, von denen sich 32 % zu Kleinst-, 31 % zu Klein- und 37 % zu mittleren Unternehmen zuordneten.

Interviews mit Expert:innen gaben Aufschluss zu Anforderungen, Rahmenbedingungen, Trends und zeigten Herausforderungen auf. Die Auswahl der Gesprächspartner:innen beruhte auf einer möglichst breiten Abdeckung aus Forschung, Privatsektor und Interessenvertretungen. Sieben Gespräche mit Fachleuten aus der Cybersicherheit wurden geführt: Verena Becker (WKO), Louise Beltzung (ACR), Michael Herburger (FH Oberösterreich), Aleksandar Lacarak (Certitude), Otmar Lendl (CERT.at), Christoph Moser

(A1) und Martin Zandonella (Net4You). Um die Unternehmensperspektive miteinzubeziehen, wurden zusätzlich fünf Gespräche mit österreichischen KMU geführt: Christian Berger (Lieber.Group), Hannes Fohringer (Alpex Technologies), Constantin Gessner (DIGIDO), Moritz Novak (GATE Space) und Roland Zeilinger (PRIME Aerostructures).

Die erhobenen Einschätzungen, Erfahrungen und Statements wurden zusammengefasst und in Handlungsfelder abgeleitet, die zur Erhöhung der Cybersicherheit in österreichischen KMU dienen sollen.

3.3 Abgrenzung

Der Fokus von CyberGuide liegt auf österreichischen KMU. Als Grundlage für KMU wird die EU-Definition herangezogen, die KMU unter anderem nach Zahl der Beschäftigten kategorisiert. Demnach werden Unternehmen innerhalb dieser F&E Dienstleistung als KMU gewertet, wenn sie folgenden Kategorien entsprechen. Mittlere Unternehmen haben zwischen 50 und 250 Beschäftigte, kleine Unternehmen haben zwischen 10 und 50 Beschäftigte und Kleinstunternehmen haben weniger als 10 Beschäftigte. (European Commission, 2003)

In Abstimmung mit dem Auftraggeber konzentrieren sich die Untersuchungen nicht auf eine dezidierte Branche, sondern es werden branchenübergreifende Informationen mit Relevanz für KMU erhoben.

Der regionale Fokus der Studie liegt auf Österreich. Dies betrifft vor allem die Online-Umfrage und die Interviews mit Expert:innen und Unternehmer:innen. Hinsichtlich Publikationen, Berichte, Strategiepapiere und Best-Practice-Beispiele wird keine regionale Einschränkung vorgenommen.

Die in diesem Bericht zusammengefassten Ergebnisse basieren auf bestehender Literatur (siehe Literaturverzeichnis Kapitel7) und den durch Umfrage, Interviews mit Expert:innen und Unternehmer:innen generierten Erkenntnissen für Österreich. Es wird kein Anspruch auf Vollständigkeit erhoben.

4 Cybersicherheit in Österreich

Dieses Kapitel beleuchtet die Cybersicherheit in Österreich und hebt zunächst die wachsende Bedeutung dieses Themas hervor. Anschließend wird das Cybersecurity-Ökosystem in Österreich näher beleuchtet, wobei sowohl der Forschungssektor als auch Unternehmenssektor betrachtet werden. Abschließend wird der aktuelle Status von Cybersicherheit in KMU eingehend analysiert, einschließlich der Bedrohungslandschaft, der gängigen Angriffsvektoren sowie der Fähigkeiten und Bedürfnisse österreichischer Unternehmen.

4.1 Bedeutung Cybersicherheit

In der heutigen digitalen Wirtschaft ist Cybersicherheit eine Grundlage für die Geschäftskontinuität und den langfristigen Erfolg von Unternehmen. Der Global Risk Report 2024 des World Economic Forum (WEF) identifiziert Cyberkriminalität als eine der größten Bedrohungen für die globale Wirtschaft und Gesellschaft. Cyberangriffe rangieren mittlerweile unter den zehn bedeutendsten globalen Risiken und werden als zunehmende Gefahr für die Unternehmenslandschaft, insbesondere in Industrieländern, wahrgenommen. Die Auswirkungen betreffen nicht nur große Konzerne, sondern auch kleine und mittlere Unternehmen, die oft über weniger Ressourcen zur Abwehr solcher Bedrohungen verfügen und daher besonders gefährdet sind. Darüber hinaus schaffen die weltweite digitale Vernetzung und der technologische Fortschritt neue Angriffsflächen für Cyberkriminelle. Durch die immer engere Verflechtung von Technologien und die zunehmende Abhängigkeit von Daten sind auch KMU anfällig für Cyberbedrohungen. Diese Risiken werden in einer komplexen Risikolandschaft verstärkt, die auch politische und wirtschaftliche Instabilitäten sowie soziale Verwundbarkeiten umfasst. Cyberkriminalität wird immer häufiger in die Geschäftstätigkeit von organisierten kriminellen Netzwerken integriert, die dabei auf digital vernetzte Geschäftsmodelle setzen und sowohl digitale als auch physische Märkte ausnutzen. (World Economic Forum, 2024).

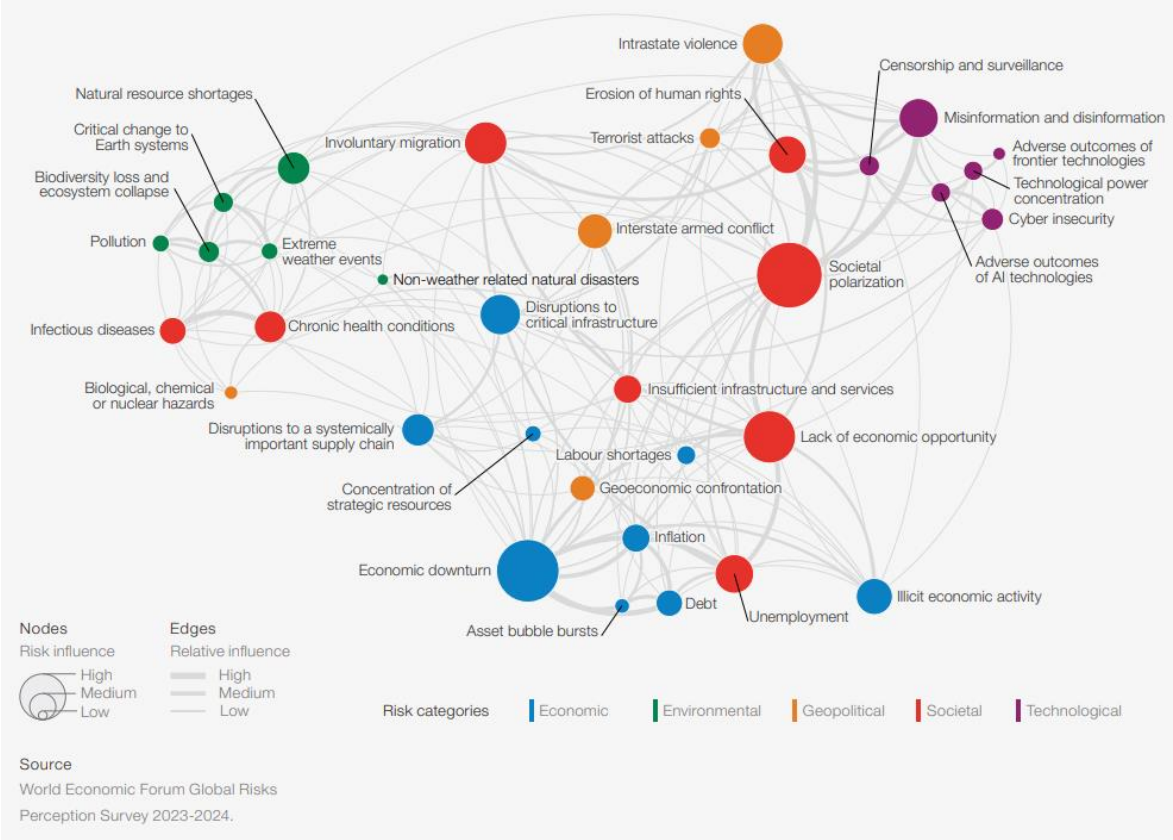

Abbildung 2: Globale Risikolandschaft (World Economic Forum, 2024)

Laut einer repräsentativen Unternehmensbefragung aus Deutschland (Dreißigacker, Skarczinski, & Wollinger, 2020) zielen die schwerwiegendsten Cyberangriffe vor allem auf unternehmenskritische Systeme, die essenziell für die Geschäftsprozesse sind, ab. Besonders E-Mail- und Kommunikationssysteme, die in 54,5 % der Fälle betroffen sind, geraten ins Visier der Angreifer, was zeitweise die gesamte interne und externe Kommunikation lahmlegt. Diese Ausfälle beeinträchtigten nicht nur die Effizienz und Koordination innerhalb der Unternehmen, sondern haben auch erhebliche Auswirkungen auf die Beziehungen zu Kund:innen und Partner:innen, da die Reaktionsfähigkeit und Servicequalität stark eingeschränkt werden. Ebenso häufig werden Kundenverwaltungs- und Rechnungswesen-Software angegriffen, was dazu führt, dass das Management von Kundendaten und die Finanzprozesse zum Teil massiv beeinträchtigt und teilweise sogar komplett zum Erliegen gebracht wird.

Die durch Cyberkriminalität verursachten Kosten steigen weltweit an, wie Abbildung 3 deutlich veranschaulicht. Prognosen zufolge werden die globalen Kosten für Cyberkriminalität von 0,73 Milliarden Euro im Jahr 2018 auf 12,78 Milliarden Euro im Jahr

2028 anwachsen, was einer Steigerung von 1.650 % entspricht (Erk, Koch, Lau, & Scheytt, 2024).

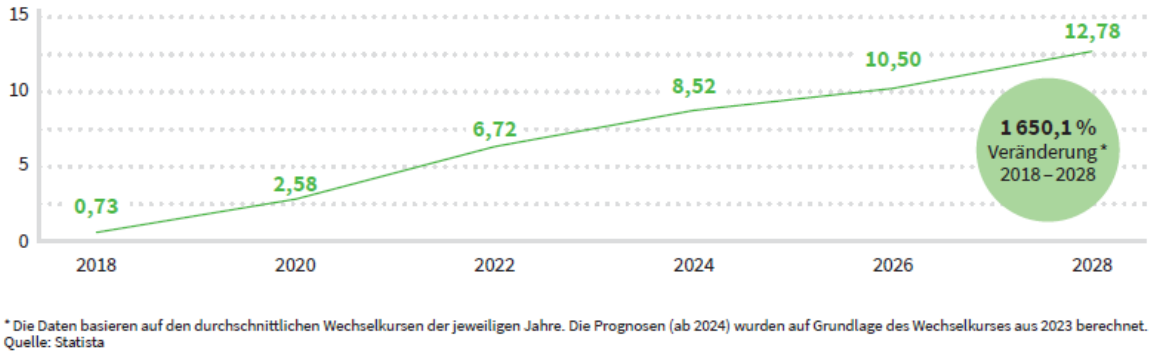

Abbildung 3: Zukünftige Entwicklung der durch Cyberkriminalität verursachten weltweiten Kosten; in Milliarden Euro (Erk, Koch, Lau, & Scheytt, 2024)

Die finanziellen und betrieblichen Auswirkungen von Cyberangriffen stellen eine erhebliche Belastung für Unternehmen dar, insbesondere für kleine und mittlere Unternehmen. Neben den direkten finanziellen Schäden, wie Einnahmeverlusten, und dem Verlust sensibler Kundendaten, fürchten Unternehmen auch um ihre Reputation, da Schäden an der Unternehmensmarke, sowie der Verlust geistigen Eigentums und Betriebsunterbrechungen ernsthafte Bedrohungen darstellen. Darüber hinaus werden Unternehmen bei Ransomware-Angriffen, bei denen Daten verschlüsselt und Lösegeld gefordert wird, besonders hart getroffen. Denn KMU sehen sich häufig gezwungen, spezialisierte IT-Teams oder externe Dienstleister zu beauftragen, um ihre Daten wiederherzustellen. Dies ist ein kostspieliger Prozessmit teilweise begrenztem Erfolg, da mitunter Daten unwiederbringlich verloren gehen. In manchen Fällen sehen die Unternehmen aus Gründen der Reputation und Datensicherung keinen anderen Weg, als das geforderte Lösegeld zu zahlen. Der Schutz des Unternehmensrufs ist mit 38 % der wichtigste Beweggrund für diese KMU Lösegeld zu bezahlen, da ein Vertrauensverlust gravierende Auswirkungen auf ihre Marktstellung haben könnte. Ebenso relevant ist der Schutz sensibler Daten. 35 % der KMU zahlten Lösegeld, um Personaldaten zu sichern, und 36 % zur Sicherung von Kundendaten. Für 42 % der KMU spielte der Schutz vertraulicher interner Dokumente eine zentrale Rolle bei der Entscheidung zur Zahlung. Auch die schnelle Wiederherstellung der Handlungsfähigkeit nach einem Angriff und die Wiederherstellung von Daten aufgrund eines fehlenden oder gelöschten Back-ups gelten als entscheidende Faktoren (Erk, Koch, Lau, & Scheytt, 2024).

Diese Beweggründe zeigen das Dilemma, in dem sich KMU häufig befinden. Sie müssen abwägen, ob sie die finanziellen Kosten einer Lösegeldzahlung in Kauf nehmen, um

möglicherweise ihre sensiblen Daten zu schützen und den Betrieb aufrechtzuerhalten oder ob sie das Risiko eingehen, durch den Verlust dieser Daten erheblichen Reputations- und Betriebsschaden zu erleiden. Jedoch bringt die Zahlung eines Lösegelds bei Ransomware-Angriffen häufig nicht den gewünschten Erfolg. 2023 wurden weltweit 20 % der Unternehmen nach der Zahlung eines Lösegelds erneut Opfer eines Angriffs. In 22 % der Fälle forderten die Angreifer nach der ersten Zahlung mehr Geld, was die finanzielle Belastung der betroffenen Unternehmen weiter erhöhte. Eine erfolgreiche Wiederherstellung der Daten gelang nur in 46 % der Fälle. 33 % der Unternehmen mussten trotz Erhalt des Wiederherstellungsschlüssels ihre Systeme komplett neu aufzubauen. Bei 25 % der Unternehmen wurden die Daten trotz Lösegeldzahlung geleakt, also veröffentlicht oder weiterverbreitet (Erk, Koch, Lau, & Scheytt, 2024). Diese Zahlen verdeutlichen, dass die Zahlung eines Lösegelds bei Ransomware-Angriffen oft keine Lösung ist und in vielen Fällen zusätzliche Sicherheits- und Erpressungsrisiken mit sich bringt.

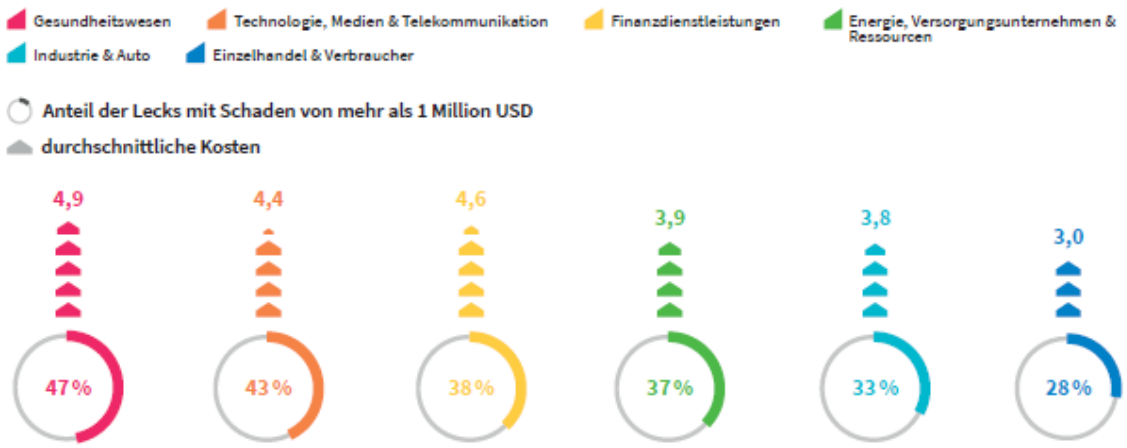

Abbildung 4: Durchschnittlicher Schaden durch ein Datenleck; weltweit; 2023; in Millionen Euro / in Prozent (Erk, Koch, Lau, & Scheytt, 2024)

Abbildung 4 zeigt die durchschnittlichen Kosten durch Datenlecks in verschiedenen Branchen weltweit auf (Erk, Koch, Lau, & Scheytt, 2024). Zusätzlich ist der Anteil der Lecks ersichtlich, dessen Schäden mehr als 1 Million US-Dollar betragen. Die höchsten durchschnittlichen Kosten pro Datenleck entstehen im Gesundheitswesen mit 4,9 Millionen Euro, wobei 47 % der Vorfälle mehr als 1 Million US-Dollar an Schaden verursachen. In den Branchen Technologie, Medien und Telekommunikation betragen die durchschnittlichen Kosten 4,4 Millionen Euro, mit einem Anteil von 43 % für Schäden über 1 Million US-Dollar. Finanzdienstleistungen und Energie, Versorgungsunternehmen und Ressourcen liegen bei durchschnittlich 4,6 Millionen und 3,9 Millionen Euro, mit 38 % bzw. 37 % solcher großen Schäden. Die Sektoren Industrie und Auto und Einzelhandel und Verbraucher weisen

geringere durchschnittliche Kosten pro Datenleck auf, mit 3,8 Millionen Euro und 3 Millionen Euro, wobei der Anteil der Vorfälle mit Schäden über 1 Million US-Dollar bei 33 % bzw. 28 % liegt. Diese Zahlen zeigen, dass Datenlecks in datenintensiven und personenbezogenen Branchen besonders kostspielig sind und dass Unternehmen in diesen Sektoren besonders hohen Sicherheitsanforderungen gerecht werden müssen, um die Risiken zu minimieren.

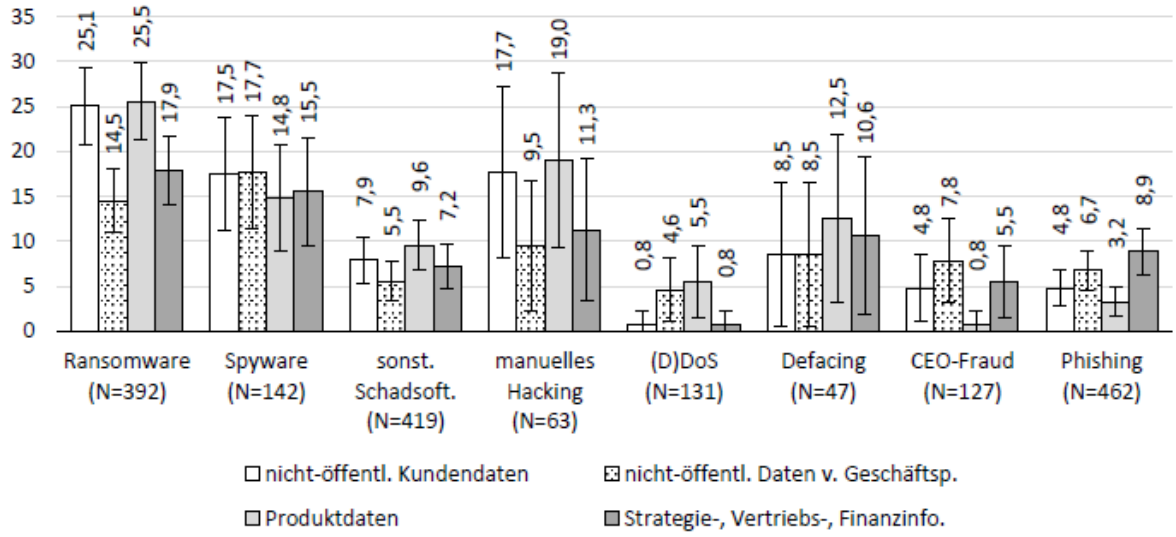

Abbildung 5: Anteil der Unternehmen mit betroffenen Daten nach Daten- und Angriffsart (Dreißigacker, Skarczinski, & Wollinger, 2020)

Abbildung 5 verdeutlicht, dass verschiedene Datentypen bei Cyberangriffen in unterschiedlichen Maßen gefährdet sind. Besonders stark betroffen sind nicht-öffentliche Kundendaten und strategische Informationen wie Vertriebs- und Finanzdaten, die insbesondere durch Ransomware-Angriffe gefährdet sind. Hierbei werden jeweils etwa 25 % dieser Daten kompromittiert. Ein ähnliches Risiko besteht durch manuelles Hacking, das vor allem auf Produktdaten (19 %) und nicht-öffentliche Kundendaten (17,7 %) abzielt. Auch Spyware stellt eine erhebliche Bedrohung dar, indem sie hauptsächlich nicht-öffentliche Kundendaten und nicht-öffentliche Daten von Geschäftspartnern angreift, mit 17,7 % und 18%. Insgesamt zeigt sich, dass besonders nicht-öffentliche Kundendaten und Produktdaten durch Cyberangriffe gefährdet sind, während andere Datentypen je nach Angriffstyp unterschiedlich stark betroffen sind. (Dreißigacker, Skarczinski, & Wollinger, 2020).

Cybersicherheit ist bedeutend, da Cyberangriffe Unternehmen erheblich schaden können. Sei es in finanzieller, operativer oder reputationsbezogener Hinsicht. Angriffe können zum Verlust sensibler Daten wie Kundendaten, Geschäftsgeheimnisse oder strategischer

Informationen führen, was nicht nur rechtliche Konsequenzen, sondern auch einen Vertrauensverlust bei Kund:innen und Partner:innen nach sich ziehen kann. Die Wiederherstellung betroffener Systeme verursacht hohe Kosten und kann den Geschäftsbetrieb über längere Zeit erheblich stören (BSI, 2022). Angesichts der zunehmenden Bedrohung und der immer raffinierteren Angriffsmethoden ist Cybersicherheit unverzichtbar, um Unternehmen vor Datenverlust, Erpressung und den langfristigen Folgen von Cybervorfällen zu schützen und ihre Stabilität und Wettbewerbsfähigkeit in einer digitalisierten Welt zu sichern.

4.2 Aktuelle Bedrohungslage und Angriffsvektoren

Kleine und mittlere Unternehmen sind mit einer breiten und sich ständig weiterentwickelnden Landschaft von Cyberbedrohungen konfrontiert. Zu den gängigsten Angriffsvektoren gehören Ransomware, Phishing, Distributed Denial-of-Service (DDoS)-Angriffe, Advanced Persistent Threats (APT), Insider-Bedrohungen, staatlich gesponserte Angriffe, Angriffe auf die Lieferkette und Social Engineering. Phishing ist dabei oft der erste Schritt für viele dieser Angriffe. Besonders gefährlich sind staatlich gesponserte Cyberangriffe, die sich zunehmend auch gegen KMU richten, insbesondere in Bereichen mit wertvollem geistigem Eigentum, wie Forschung und Entwicklung und die Zulieferindustrie in Bereichen wie Militär, Luft- und Raumfahrt sowie Hightech.

Ransomware ist für KMU eine der gravierendsten Bedrohungen. Während sich solche Angriffe früher vor allem auf große Unternehmen konzentrierten, verlagert sich der Fokus zunehmend auf KMU. Diese Angriffe sind lukrativ für Cyberkriminelle, da sie aufgrund der großen Anzahl von KMU mit geringeren Schutzmaßnahmen dennoch hohe Erträge erzielen können. Besonders gefährlich für KMU sind direkte Schäden durch Ransomware-Angriffe, die zu einem sofortigen Verlust von Daten und Systemzugriff führen. Da viele KMU keine umfangreichen Backups oder Alternativpläne haben, bleibt ihnen oft nur die Möglichkeit, das geforderte Lösegeld zu zahlen oder aufwendig ihre Systeme wiederherzustellen. Diese zusätzlichen Kosten und Anstrengungen können existenzbedrohend sein. Abbildung 6 zeigt die in Österreich angezeigten Ransomware-Fälle. Insgesamt wurden im Jahr 2023 148 Fälle im gesamten Bundesgebiet zur Anzeige gebracht, wobei über ein Drittel der Angriffe auf Unternehmen stattfanden (Bundeskriminalamt, 2024).

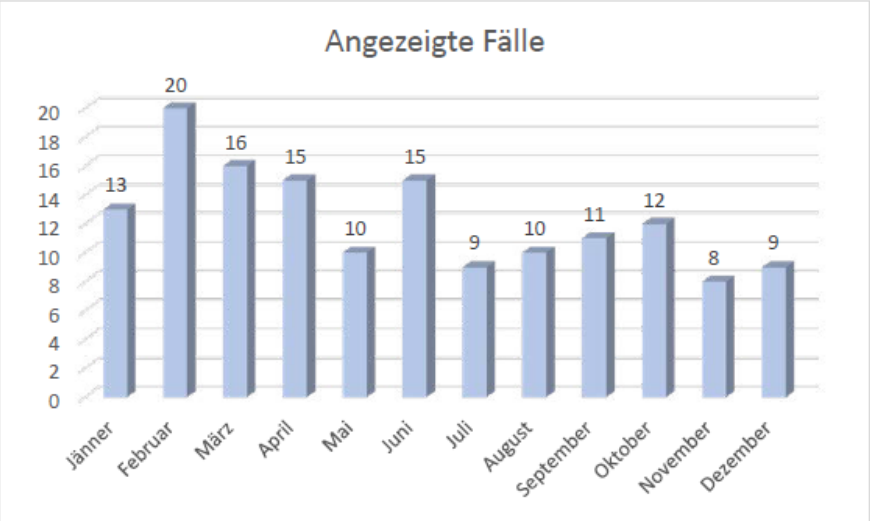

Abbildung 6: Monatliche Verteilung der Ransomware-Fälle 2023 (Bundeskriminalamt, 2024)

Gleichzeitig gewinnen APT-Angriffe an Bedeutung. Diese Angriffe zielen darauf ab, unbemerkt in den Systemen zu bleiben und über längere Zeiträume Informationen abzuziehen oder die Infrastruktur des betroffenen Unternehmens für weitere Angriffe zu nutzen. Eine häufige Folge davon sind Angriffe auf die Lieferkette. Solche Angriffe auf die Lieferkette sind ein weiterer Angriffsvektor. KMU bedenken nur selten, dass sie in der Regel in ein wirtschaftliches Umfeld eingebettet sind, in dem Partner primäre Ziele sein können. Die Bedrohung kann auch indirekt sein, indem sich Angreifer über einen Angriff auf KMU Zugang zu den Netzen der Betreiber verschaffen. So wird ein KMU plötzlich äußerst attraktiv, da der Angreifer das zunächst „uninteressante“ KMU nutzt, um das primäre Ziel zu erreichen. Für KMU sind die Auswirkungen von Cyberangriffen oft gravierender, da sie im Vergleich zu großen Unternehmen über weniger finanzielle Reserven verfügen, um Verluste auszugleichen. Ein erfolgreicher Angriff kann für ein KMU Insolvenz bedeuten, während größere Unternehmen die finanziellen Schäden oft besser abfedern können.

Ein häufig unterschätzter Angriffsvektor ist der Mensch. Social Engineering hat in den letzten Jahren stark zugenommen und ist für viele erfolgreiche Angriffe verantwortlich. Dabei werden Mitarbeiter:innen gezielt manipuliert, um vertrauliche Informationen preiszugeben oder schädliche Aktionen auszuführen. Auch Insider-Bedrohungen stellen ein ernsthaftes Risiko dar, da unzufriedene oder direkt rekrutierte Mitarbeitende Unternehmensdaten abziehen oder Schadsoftware in Systeme einschleusen können. Neben den klassischen Cyberangriffen gibt es auch Bedrohungen durch Extremist:innen oder Aktivist:innen, die im Rahmen von Cyber-Aktivismus oder ideologisch motivierten

Aktionen Schäden verursachen wollen. Diese „Hacktivisten“ verbreiten auf diesem Weg ihre Botschaft oder bestrafen ein Unternehmen für dessen Geschäftspraktiken.

In der Online-Umfrage mit 51 Teilnehmer:innen wurde erhoben, welche Sicherheitsvorfälle in den befragten KMU während der letzten 12 Monaten vorgefallen sind. Die Ergebnisse, aufgeschlüsselt nach Unternehmensgröße, sind in Abbildung 7 grafisch aufbereitet. Phishing-Angriffe stellten mit 63 % die häufigste Bedrohung dar, wobei kleine Unternehmen (14) besonders stark betroffen waren. Malware/Schadsoftware-Angriffe wurden von 23 % der KMU angegeben, während Social Engineering von 13 % als relevante Bedrohung wahrgenommen wurde. Ransomware-Vorfälle machten 10 % der Angriffe aus. Geringere Bedrohungen, wie das Abhören der Kommunikation, Deep Fakes, Identitätsdiebstahl, und Passwortdiebstahl wurden jeweils von 4 % bis 6 % der Unternehmen erfasst. Weitere Vorfälle wie Denial-of-Service-Angriffe, Insider Threats, staatlich unterstützte Angriffe und Datenlecks betrafen nur 2 % der KMU. Besonders auffällig ist, dass 29 % der Unternehmen angaben, keine Sicherheitsvorfälle identifiziert zu haben. Besonders bei kleinen (5) und mittleren Unternehmen (7) ist diese Beantwortung stark vertreten. Dies könnte darauf hindeuten, dass einige KMU entweder keine Sicherheitsvorfälle wahrgenommen haben oder dass sie möglicherweise nicht in der Lage waren, solche Vorfälle zu erkennen.

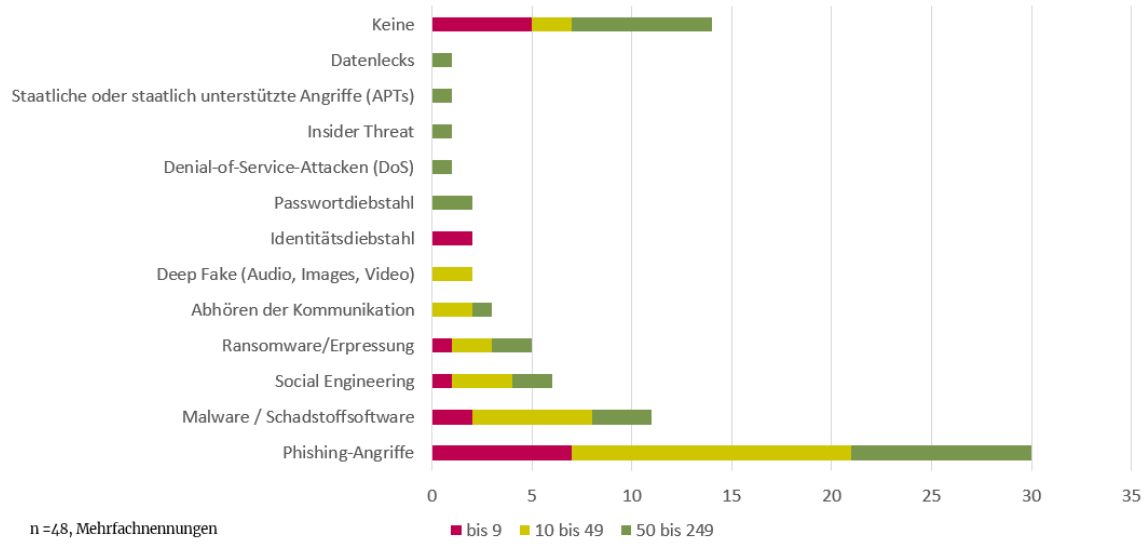

Abbildung 7: Erkannte Sicherheitsvorfälle in österreichischen KMU (eigene Darstellung)

Ein weniger offensichtlicher, aber genauso schwerwiegender Aspekt ist der permanente Datenverlust durch installierte Spyware oder unsichere Programme. Viele KMU sind sich nicht bewusst, wie viele Rechte sie verschiedenen Anwendungen gewähren, die täglich genutzt werden. Diese unbemerkten Datenlecks können langfristig die Privatsphäre

gefährden und wichtige Geschäftsinformationen offenlegen. Insgesamt stellt diese versteckte Bedrohung eine weitere Dimension des Risikos dar, die oft übersehen wird, aber ebenso schwerwiegende Folgen haben kann wie offensichtliche Angriffe wie Ransomware.

Die Identifizierung der Angreifer hinter einem Cybervorfall ist meist eine Herausforderung, da die Motive und Hintergründe variieren. Neben finanziellen Motiven gibt es zunehmend auch politisch oder ideologisch motivierte Angriffe. Auch die Verwendung von Spionagesoftware erschwert die klare Zuweisung der Verantwortlichen, da es schwierig ist, herauszufinden, ob staatliche, politische oder wirtschaftliche Interessen hinter einem Angriff stehen. Dies erfordert eine individuelle Risikobewertung und Bedrohungsanalyse für jedes Unternehmen, abhängig von der Branche und dem Geschäftsumfeld.

Die Bedrohungslage durch Cyberkriminalität ist hochdynamisch und komplex. Der Cyberkriminalitätsmarkt operiert weitgehend unreguliert und ist stark kapitalistisch ausgerichtet, mit einem klaren Fokus auf Profit. Im Darknet handeln Kriminelle Werkzeuge und Dienstleistungen, wobei die Arbeitsteilung innerhalb dieser Szene hochgradig spezialisiert ist. Hier werden nicht nur Informationen, sondern auch vollständige Angriffspläne oder ganze Gruppen von Cyberkriminellen angeboten. Neben rein finanziellen Motivationen wirken auch politische und militärische Konflikte als Katalysator für die steigende Bedrohungslage. Unternehmen, die zuvor nicht im Fokus von Cyberkriminellen standen, geraten aufgrund dieser dynamischen Entwicklungen vermehrt ins Visier von Angriffen. Dieses stetige Wechselspiel zwischen Angreifern und Verteidigern führt zu einem permanenten Wettlauf: Jede Sicherheitsmaßnahme eines Unternehmens wird von den Angreifern durch Anpassung ihrer Taktiken beantwortet, um weiterhin erfolgreich zu sein.

4.3 Ökosystem

Österreich verfügt über ein diverses Cybersicherheits-Ökosystem (vgl. Abbildung 8 – ohne Anspruch auf Vollständigkeit). Kernbereich des Ökosystems sind Unternehmen, die an Cybersicherheitslösungen arbeiten und diese erfolgreich am Markt positionieren. Es lassen sich in Österreich Akteure mit Fokus auf Hardware- als auch auf Software finden. Dies beinhaltet beispielsweise Appliances zur transparenten Verschlüsselung oder zur Überwachung als Hardwarelösungen sowie Scan-Engines und Threat Detectors als Softwareprodukte. Teilweise ist der Übergang fließend, da Softwarelösungen auch in Appliances zum Einsatz kommen. Daneben gibt es ein reichhaltiges Angebot an Consultants, von White-Hat-Hackern bis zu Beratern für den Aufbau von Prozessen und Zertifizierung.

Auf Standards und Vorschriften wird in Kapitel 5.1 näher eingegangen. Schließlich gibt es eine Reihe von Forschungseinrichtungen, Universitäten, Interessensvertretungen, Förderorganisationen und öffentliche Stellen, die wichtige Beträge zur Cybersicherheit leisten.

Die genannten Akteure sind nötig, um den Anforderungen eines ganzheitlichen Unternehmensschutzes gerecht zu werden und üblicherweise müssen mehrere Produkte/Lösungen zu einem wirksamen Gesamtkonzept kombiniert werden.

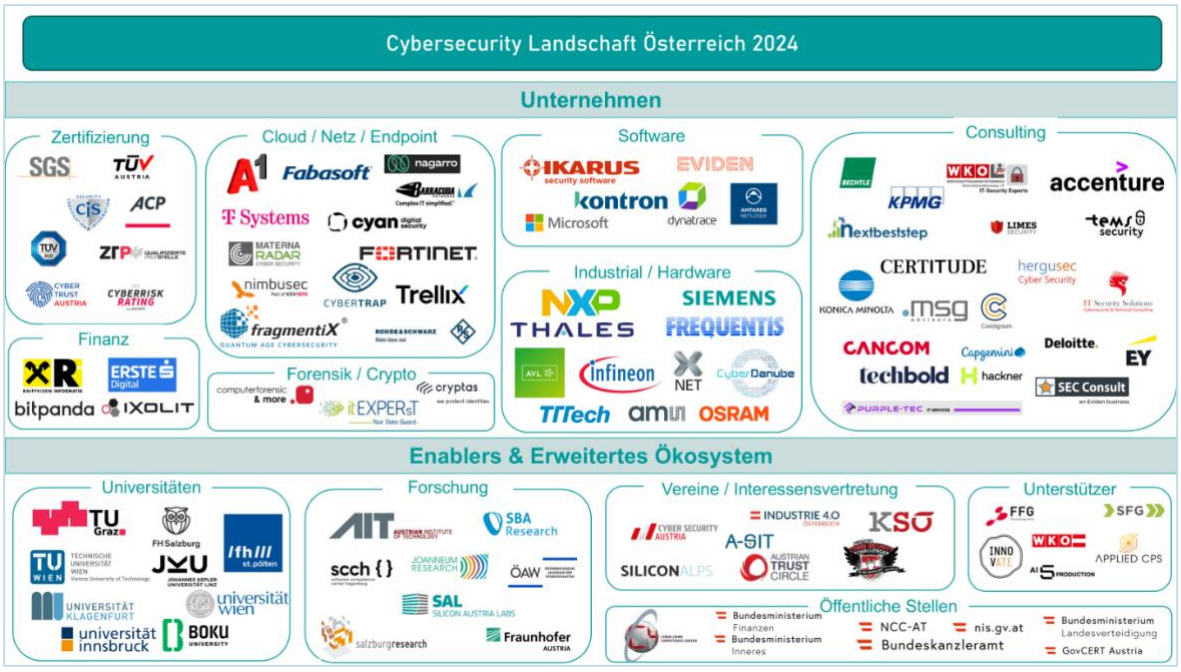

Abbildung 8: Beispielhafte Gliederung der Cybersecurity Landschaft Österreichs inkl. wichtiger Akteure (eigene Darstellung)

Der Überblick über das Ökosystem verdeutlicht die größte Herausforderung für KMUs, die ihre Cybersicherheit verbessern möchten. Ohne bereits vorhandenes Domänenwissen ist es schwierig sich im Dickicht der angebotenen Lösungen (und Anforderungen) zurecht zu finden und eine einmal gewählte Lösung über die Jahre auch aktuell zu halten und den sich ändernden Bedrohungen anzupassen. Da jede zeitliche bzw. monetäre Investition in das komplexe Thema sich nicht unmittelbar umsatzsteigernd auswirkt, besteht die reale Gefahr hier zu wenig zu tun. Geförderte, niederschwellige Beratungsangebote sind genau aus diesem Grund ein wichtiger Teil des Ökosystems, das im Rest des Kapitels genauer beleuchtet wird, beginnend mit der Forschung.

Sicherheitsforschung in Österreich

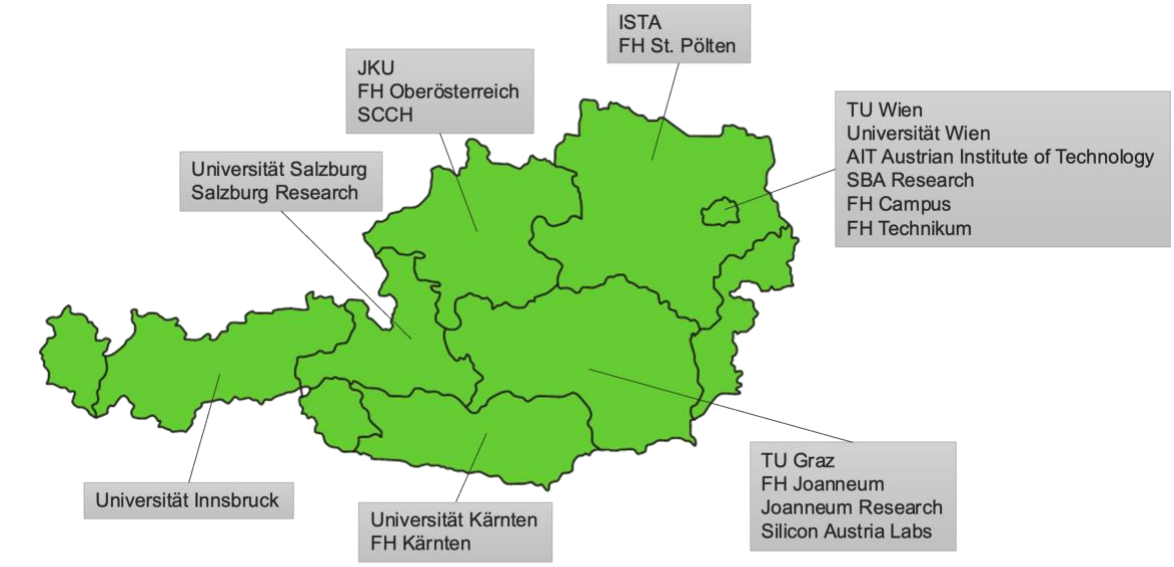

Abbildung 9: Forschungseinrichtungen mit Cyber-Security Bezug in Österreich

Sicherheitsforschung ist in Österreich vor allem auf Forschungseinrichtungen in Graz, Wien, Linz, St. Pölten, Klagenfurt und Salzburg konzentriert. Abbildung 9 gibt einen Überblick über Forschungsinstitute, die im Bereich Sicherheitsforschung tätig sind. Seit Jahrzehnten trägt die Technische Universität Graz (TU Graz), insbesondere das Institut für Angewandte Informationsverarbeitung und Kommunikation (IAIK), wesentlich zur Sicherheitsforschung bei. Durch Prof. Reinhard Posch war das Institut auch bei der Umsetzung der Handysignatur in Österreich beteiligt. In den vergangenen Jahren haben Forschende des Institutes international sehr bedeutende Schwachstellen (mit)aufgedeckt, z.B. Rowhammer, Meltdown, Spectre, und von ihnen entworfene Algorithmen wurden zu internationalen Standards (z.B. ASCON). Dies spiegelt sich auch in der Anzahl an Publikationen in den Top-10 Journalen und Konferenzen im Bereich Cybersicherheit[1] wider (siehe Abbildung 10). Innerhalb Österreichs führt die TU Graz das Ranking mit 6 Forscher:innen an, weiters stechen die Universität Wien, das Austrian Institute of Technology (AIT), die Technische

[1] Quelle: Google, https://scholar.google.com/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography 09 2024

Universität Wien (TU Wien), und SBA Research hervor. Neben Forschung spielen Universitäten und Fachhochschulen auch im Bereich Ausbildung eine wichtige Rolle und sind somit essenzieller Baustein im Ökosystem.

Forschungsorganisation	#Publikationen	# Forscher
Graz University of Technology, Austria	**85**	**6**
Daniel Gruss	41	1
Stefan Mangard	26	1
Maria Eichlseder	8	1
Gaëtan Cassiers	4	1
Hannes Groß	3	1
Roderick Bloem	3	1
University of Vienna, Austria	**34**	**1**
Edgar R. Weippl	34	1
AIT Austrian Institute of Technology, Vienna, Austria	**22**	**3**
Florian Skopik	14	1
Christoph Striecks	5	1
Sebastian Ramacher	3	1
TU Wien, Austria	**21**	**3**
Martina Lindorfer	12	1
Helmut Veith	5	1
Elena Andreeva	4	1
SBA Research, Austria	**11**	**2**
Markus Huber	7	1
Peter Kieseberg	4	1
University of Klagenfurt, Austria	**11**	**2**
Elisabeth Oswald	7	1
Winfried B. Müller	4	1
University of Salzburg, Austria	**4**	**1**
Andreas Uhl	4	1
Universität Klagenfurt, Austria	**3**	**1**
Patrick Horster	3	1
University of Innsbruck, Austria	**3**	**1**
Ruth Breu	3	1
Grand Total	**194**	**20**

Abbildung 10: Publikationen (Autor oder Ko-Autor) österreichischer Forscher in den Top-10 Security Journals/Konferenzen: IEEE Symp. on Security and Privacy, USENIX Security Symposium, Trans. on Information Forensics and Security, Computers & Security, ACM Symp. On Computer and Communications Security, Network and Distributed System Security Symposium, IEEE Trans. on Dependable and Secure Computing, Journal of Information Security and Applications, EuroCrypt, International Cryptology Conference. Quelle: DBLP SPARQL, 09 2024

Bei der Förderung angewandter Sicherheitsforschungsprojekte spielt die österreichische Forschungsförderungsgesellschaft FFG eine Schlüsselrolle und hat seit 2014 mehr als 400 Projekte [2], mit Stichwort „Security“, gefördert. Dies beinhaltet die Förderung von Forschungszentren (COMET, z.B. SBA), von Projekten in nationalen Sicherheitsprogrammen (FORTE, KIRAS), als auch Einzelprojekte im Kontext der Digitalisierung, Energieforschung, und verwandten Themen. Mehr als 260 Unternehmen, 13 Universitäten, und 29 Forschungseinrichtungen haben dadurch bisher Forschungsprojekte zum Thema Security umsetzen können. Abbildung 11 zeigt die teilnehmenden Organisationen aufgeschlüsselt nach Typ: 75 % aller teilnehmenden Organisationen sind Unternehmen, die in Projekten zusammen mit Forscher:innen (Universitäten, Fachhochschulen), gemeinnützigen

[2] Quelle: FFG Projektdatenbank, Stichwort „Security“, 09 2024

Organisationen, Interessensvertretungen, und öffentlichen Stellen (Bund, Länder, Gemeinden) das Thema Cybersicherheit ganzheitlich bearbeiten.

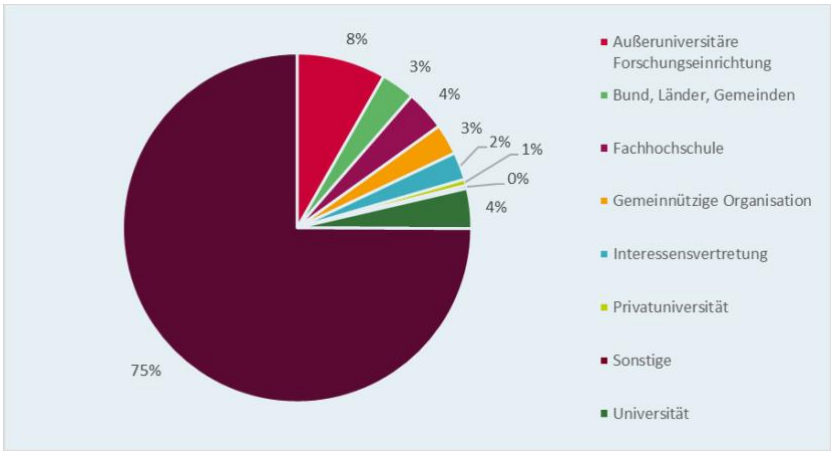

Abbildung 11: FFG geförderte Sicherheitsforschung in Österreich ist gut verankert: Analyse der Teilnehmer nach Organisationstyp. Quelle: FFG Projektdatenbank, Stichwort „Security“, 09 2024

Thematisch ist die österreichische Sicherheitsforschung breit aufgestellt, klassische Schwerpunkte sind unter anderem

- Anomalie-Detektion und Threat-Intelligence
- Attacken & Gegenmaßnahmen (Side Effects/Channels, Software/HW)
- Biometrics
- Distributed Ledger Technology
- Kryptographie (PQC, QKD, Homomorphe Verschlüsselung)
- Malware Analysis
- Network Security, Social Engineering
- Secure AI
- Security-By-Design (Threat Modelling, Verifikation)

Unternehmen im Bereich Cybersicherheit

Auf Anbieterseite sind in Österreich zum einen alle namhaften internationalen Konzerne tätig, zum anderen gibt es viele innovative österreichische Unternehmen und Start-Ups. Die folgende Taxonomie ist ein Versuch die Unternehmen nach Schwerpunkten und Fokusthemen zu gliedern. Dabei ist den Autor:innen bewusst, dass eine eindeutige Zuordnung vieler Unternehmen zu einer der folgenden Kategorien nur schwer möglich ist und viele Unternehmen in mehreren Kategorien aktiv sind.

- Software (Generisch)

Es gibt einige österreichische Unternehmen, die Softwarelösungen im Bereich Cybersicherheit anbieten. Hierzu gehören Antivirenprogramme, Software zur Überwachung technischer Systeme, und auf Kundenwunsch erstellte, maßgeschneiderte Software. Neben den Softwarelösungen bieten viele Unternehmen auch Beratungsdienstleistungen an. Viele der folgenden Schwerpunkte können auch als (teilweise) Untermenge des recht allgemeinen „Software“ Schwerpunkts aufgefasst werden.

- Cloud / Netz / Endpoint

Da Cybersicherheit besonders in vernetzten Systemen und im Cloud-Umfeld eine große Rolle spielt, gibt es viele Unternehmen und Start-Ups, die sich auf diesen Bereich spezialisiert haben und Lösungen für zum Beispiel Monitoring und Intrusion Detection, Verschlüsselung, und sichere Cloud anbieten. Oft sind die angebotenen Lösungen Kombinationen aus Hardware und Software und vor allem auf den IT Bereich ausgerichtet.

- Industrial / Hardware

Im Bereich der Industrie, z.B. Automotive, Aerospace, Produktion, finden sich weitere Unternehmen, die domänenspezifische Cybersicherheitsprodukte anbieten. Hier geht es vor allem um die Absicherung Cyber-Physischer Systeme (IT & OT), jedoch auch immer öfter um Cloud-Themen, wo sich Überschneidungen mit klassischen Anbietern von IT-Sicherheit ergeben. Zusätzlich verfügt Österreich über einige Unternehmen, die Security-Hardware designen und zu den Weltmarkführern in ihrem Bereich zählen.

- Forensik/Crypto

Als spezialisierte Dienstleister gibt es in Österreich Firmen, die aktiv werden, wenn es speziell um Computerforensik oder Angewandte Kryptographie geht. Verglichen mit anderen Bereichen sind hier weniger aktive Unternehmen zu finden.

- Finanz

Sowohl neue Finanzsysteme als auch der Trend zum Online-Banking bei herkömmlichen Banken haben in diesem Bereich Spezialisten entstehen lassen, die sich vor allem um Cybersicherheit für Finanzprodukte bemühen.

- Consulting

Die wahrscheinlich größte Gruppe an Unternehmen findet sich im Bereich Cybersicherheitsberatung. Dabei ist das Leistungsportfolio breit gefächert und reicht von technischem Consulting bis hin zu Prozessberatung. Domänenspezifische Weiterbildungs- und Schulungsangebote sind hier auch zu finden.

- Zertifizierung

Sehr wichtig im Zusammenhang mit Sicherheitsstandards und -normen sind Zertifizierungsstellen, die Unternehmen bzgl. der Umsetzung von Sicherheitsnormen beurteilen und zertifizieren können. Auch hier gibt es in Österreich viele Player.

Vereine, Interessensvertretungen, Konferenzen

In Österreich gibt es eine lebendige Cybersicherheits-Community, die u.a. jährliche Wettbewerbe (ACSC), regelmäßige Meetings (Security Arbeitsgruppen z.B. unter dem Dach der Industrie 4.0 Initiative), und Konferenzen (z.B. rund um KIRAS/FORTE, IKT-Sicherheitskonferenz des BMLV, SCCS Konferenz, IT-S Now, IT SECX, …) organisiert. Querverbindungen zu Themen wie Künstliche Intelligenz (KI) oder Datenräumen (z.B. GAIA-X) existieren und werden aktiv bespielt. Die nationalen Initiativen sind dabei eingebettet in eine europäische Landschaft, mit großen Konferenzen, wie IT-SA.

Unterstützer, Inkubatoren, Beschleuniger

Das österreichische Netzwerk an Unterstützern beinhaltet bekannte Namen, wie z.B. die die Wirtschaftskammer Österreich (WKO), es gibt aber auch weniger bekannte Initiativen, wie die (European) Digital Innovation Hubs (z.B. AI5Production, Applied CPS, Innovate), die Beratungsleistungen kostenlos anbieten.

Öffentliche Institutionen

Öffentliche Institutionen sind im Bereich Cybersicherheit sowohl in der Forschung als auch in der Gestaltung der österreichischen Community aktiv. Die Bedeutung der Cybersicherheit ist den Regierungen bewusst, und so ist teilweise das Bundeskanzleramt selbst mit Agenden in diesem Bereich betraut.

Medien

Als Querschnittsthema über viele Domänen wird Cybersicherheit regelmäßig sowohl in Fachzeitschriften als auch in den allgemeinen Medien thematisiert. Die bedeutendsten Publikationen in dem Bereich (inkl. Bedrohungsdatenbanken etc.) sind allerdings im internationalen Bereich zu finden.

4.4 Status Cybersicherheit in österreichischen KMU

In diesem Kapitel wird näher auf die gegenwärtige Situation der Cybersicherheit in österreichischen KMU eingegangen. Es werden die Zuständigkeiten in den KMU, die Häufigkeit von Cyber-Risikobewertungen, sowie die bereits implementierten Cybersicherheitsmaßnahmen analysiert, ebenso die Höhe der Investitionen in Cybersicherheit. Abschließend wird die Bedeutung des Risikomanagements bei Drittanbietern beleuchtet und untersucht, inwieweit KMU Maßnahmen ergreifen, um potenzielle Risiken zu minimieren.

In KMU sind die Zuständigkeiten für IT-Sicherheit mitunter breit verteilt, wie Abbildung 12 verdeutlicht. In 63 % der KMU liegt diese Verantwortung bei der Geschäftsführung oder dem Vorstand, insbesondere bei Kleinstunternehmen (15 Beantwortungen). 43 % der

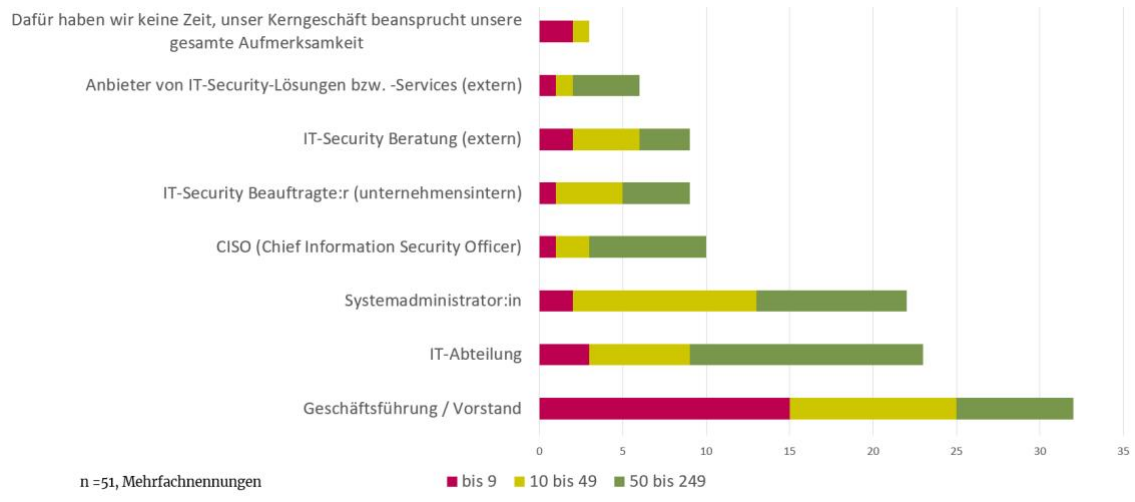

Abbildung 12: Zuständigkeiten nach Unternehmensgröße (eigene Darstellung)

Unternehmen verlassen sich auf deren IT-Abteilung oder einen Systemadministrator, wobei hier vor allem mittlere Unternehmen zu finden sind. Der Einsatz eines Chief Information Security Officers ist mit 20 % deutlich seltener und wird im Wesentlichen von mittleren Unternehmen (7) eingesetzt. Darüber hinaus setzen 18 % der KMU auf interne IT-Security Beauftragte, während weitere 18 % externe IT-Security Berater konsultieren. 12 % der KMU verlassen sich auf externe Anbieter von IT-Sicherheitslösungen und -Services. Bemerkenswert ist, dass 6 % der Unternehmen angaben, keine Kapazitäten für IT-Sicherheit zu haben, da das Kerngeschäft ihre gesamte Aufmerksamkeit erfordert.

Abbildung 13 gibt Aufschluss über die Häufigkeit von Cyber-Risikobewertungen in Kleinstunternehmen, kleinen Unternehmen und mittleren Unternehmen. Demnach weiß jedes fünfte Kleinst- und mittleren Unternehmen nicht, wie oft sie Bewertungen durchführen. 27 % der Kleinstunternehmen und 33 % der kleinen Unternehmen führen nie eine Risikobewertung durch, im Vergleich zu nur 16 % bei den mittleren Unternehmen.

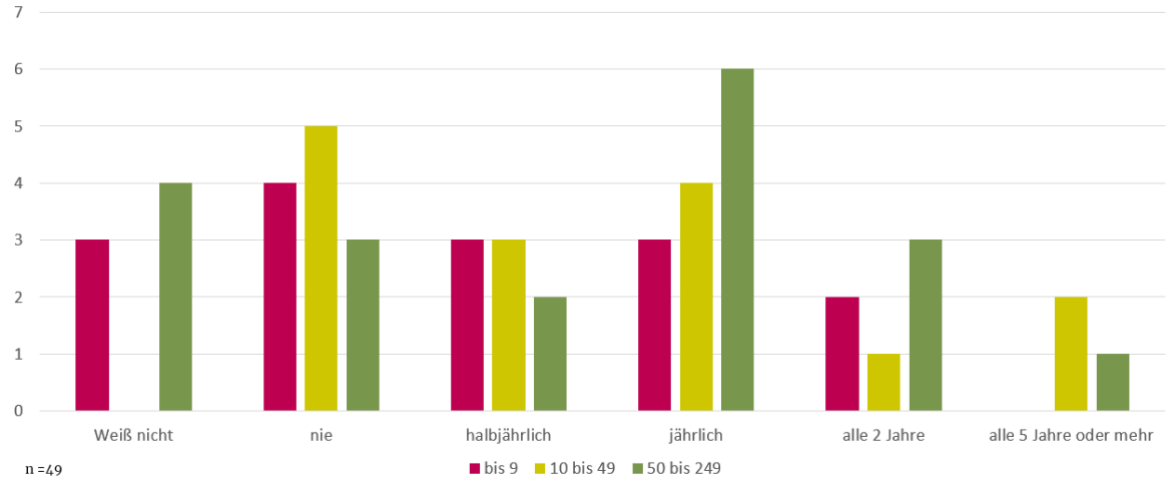

Abbildung 13: Häufigkeit von Cyber-Risikobewertungen (eigene Darstellung)

Jährliche Bewertungen sind bei den mittleren Unternehmen am häufigsten (32 %), gefolgt von 27 % der kleinen und 20 % der Kleinstunternehmen. Halbjährliche Bewertungen werden in 20 % der Kleinst- und kleinen Unternehmen durchgeführt, jedoch nur in 11 % der mittleren Unternehmen. Alle 5 Jahre oder mehr führen nur kleine (13 %) und mittleren Unternehmen (5 %) eine Cyber-Risikobewertungen durch.

Welche Cybersicherheitsmaßnahmen in den befragten KMU bereits implementiert wurden, zeigt Abbildung 14.

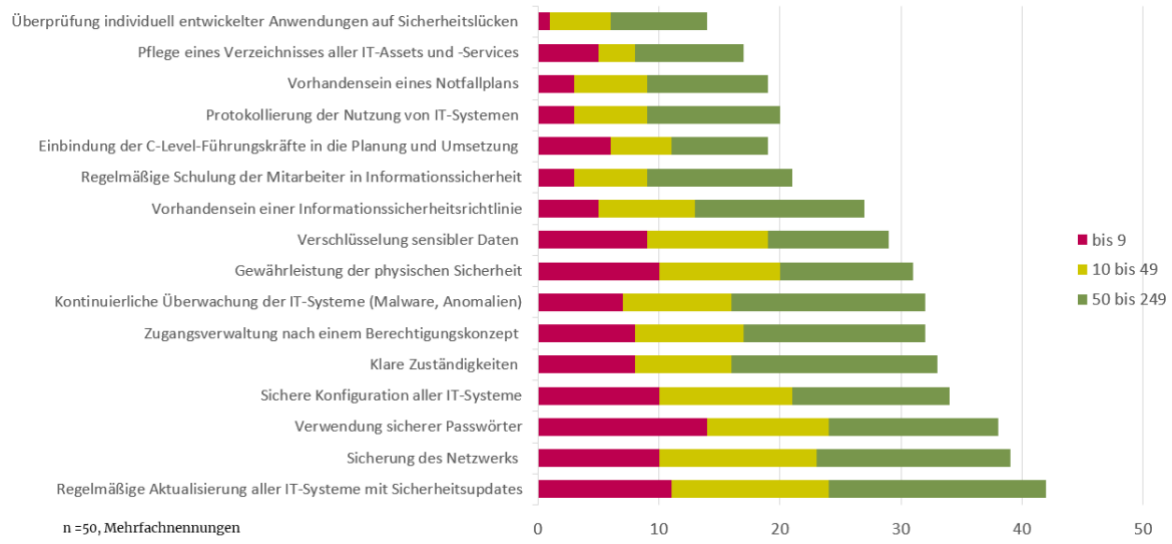

Abbildung 14: Implementierte Cybersicherheitsmaßnahmen in österreichischen KMU (eigene Darstellung)

Die am häufigsten genannte Maßnahme ist die regelmäßige Aktualisierung aller IT-Systeme und Anwendungen mit Sicherheitsupdates, die von 42 Unternehmen umgesetzt wird. In allen Unternehmensgrößen ist diese Maßnahme stark verbreitet, wobei mittlere Unternehmen sie mit 95 % am häufigsten umsetzen, gefolgt von kleinen Unternehmen (87 %) und Kleinstunternehmen (69 %). Die Sicherung des Netzwerks vor unberechtigtem externem Zugriff folgt mit 39 Nennungen, wobei kleine Unternehmen (87 %) diese Maßnahme häufiger umsetzen als mittlere (84 %) und Kleinstunternehmen (63 %). Eine weitere gängige Maßnahme ist die Verwendung sicherer Passwörter (38), die bei Kleinstunternehmen mit 88 % einen höheren Stellenwert hat als bei mittleren (74 %) und kleinen Unternehmen (67 %).

Darüber hinaus zählen die Einhaltung empfohlener Sicherheitseinstellungen (34) und klare Zuständigkeiten für die IT-Sicherheit im Unternehmen (33) zu häufig durchgeführten Maßnahmen. Mittlere Unternehmen implementieren die Zuständigkeiten mit 89 % besonders häufig, während kleine (53 %) und Kleinstunternehmen (50 %) etwas zurückhaltender sind. 32 Unternehmen haben eine Zugangsverwaltung nach einem Berechtigungskonzept sowie eine kontinuierliche Überwachung der IT-Systeme auf Malware implementiert, wobei diese Maßnahmen bei mittleren Unternehmen (79 % bzw. 84 %) tendenziell stärker vertreten sind als bei kleinen (je 60 %) und Kleinstunternehmen (50 % bzw. 44 %).

Die Verschlüsselung sensibler Daten bei der Übertragung (29) und das Vorhandensein einer Informationssicherheitsrichtlinie (27) sind ebenfalls wichtige Sicherheitsmaßnahmen. Diese

werden bei mittleren Unternehmen mit 53 % bzw. 74 % etwas häufiger umgesetzt als bei kleinen (67 % bzw. 53 %) und Kleinstunternehmen (56 % bzw. 31 %). Regelmäßige Schulungen der Mitarbeiter (21) und die aktive Einbindung von Führungskräften in die Cybersecurity-Planung (19) sind weniger verbreitet, wobei mittlere Unternehmen auch hier vorne liegen (63 % bzw. 42 %). Weniger verbreitete Maßnahmen sind die Protokollierung der IT-Nutzung (20) und das Vorhandensein eines Notfallplans (19), welche von mittleren Unternehmen (58 % bzw. 53 %) häufiger umgesetzt werden als von kleinen (je 40 %) und Kleinstunternehmen (je 19 %). Besonders selten wird die regelmäßige Pflege eines Verzeichnisses aller IT-Assets und -Services inklusive Cloud-Dienste umgesetzt. Insgesamt machen das nur 17 Unternehmen, wobei mittlere Unternehmen mit 47 % am häufigsten sind, gefolgt von Kleinstunternehmen mit 31 % und kleinen Unternehmen mit 20 %.

Bei der Frage nach implementierten Maßnahmen zum Risikomanagement von Drittanbietern gaben etwa 47 % der befragten KMU an, derzeit keine Maßnahmen umgesetzt zu haben, siehe Abbildung 15. Die kontinuierliche Überwachung und Zugangsbeschränkungen werden von 18 % der KMU (9) umgesetzt, wobei dies hauptsächlich mittlere Unternehmen (6) betrifft. Die Festlegung klarer Sicherheitsanforderungen in Verträgen wird von 10 % der KMU (5) durchgeführt, relativ gleichmäßig verteilt auf Kleinst-, kleine und mittlere Unternehmen. Ein Reaktionsplan für potenzielle Sicherheitsvorfälle wird von 8 % der Unternehmen (4) genutzt, wobei Kleinstunternehmen diese Maßnahme am häufigsten umsetzen. Eine aktuelle Lieferantenliste führen nur 6 % der Unternehmen (3) und zwar ausschließlich mittlere Unternehmen. Die regelmäßige und gründliche Bewertung der von Anbietern getroffenen Sicherheitsmaßnahmen wird ebenfalls von 6 % der KMU (3) durchgeführt, wobei dies vor allem bei Kleinst- und kleinen Unternehmen der Fall ist.

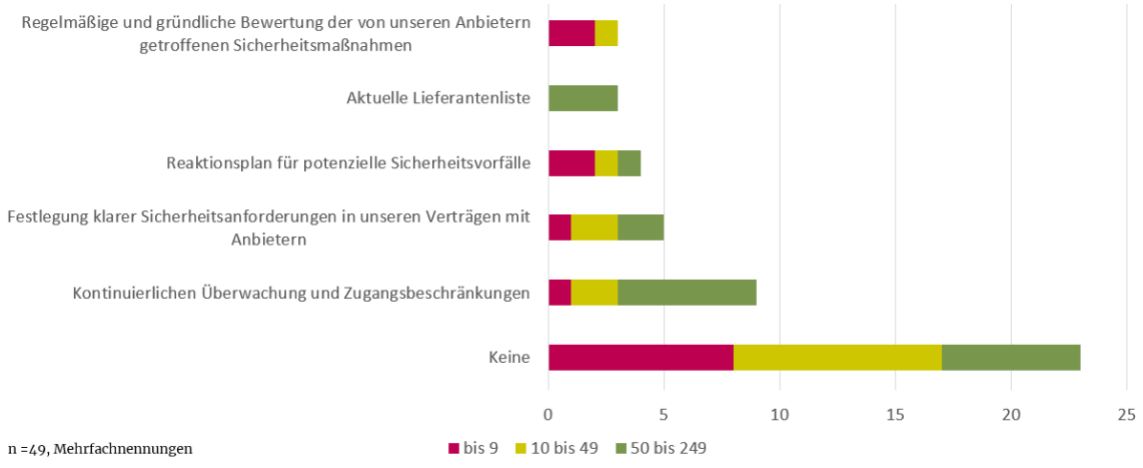

Abbildung 15: Third-Party Risk Management (eigene Darstellung)

Abbildung 16 gibt einen Überblick über den Anteil des IT-Budgets, den KMU in Cybersicherheit investieren. Jede fünfte befragte Person gibt an, nicht zu wissen, wie viel das Unternehmen in Cybersicherheit investiert. Wobei den Großteil davon mittlere Unternehmen betrifft. 4 % der KMU, darunter je ein Kleinst- und ein kleines Unternehmen, wird Cybersicherheit nicht in der Budgetplanung berücksichtigt. 18 % der Unternehmen investieren zwischen 1-5 % ihres IT-Budgets, wobei diese Gruppe vor allem aus Kleinstunternehmen besteht. Die größte Gruppe, 33 % der KMU, setzt 6-10 % ihres Budgets für Cybersicherheit ein; das sind 17 Unternehmen bestehend aus 6 Kleinst-, 7 kleine und 4 mittlere Unternehmen. Investitionen im Bereich von 11-15 % und 16-20 % sind seltener und werden von 8 % bzw. 10 % der Unternehmen getätigt. Bemerkenswert ist, dass 8 % der KMU, vor allem kleinere Unternehmen, sogar mehr als 20 % ihres IT-Budgets in Cybersicherheitsmaßnahmen investieren.

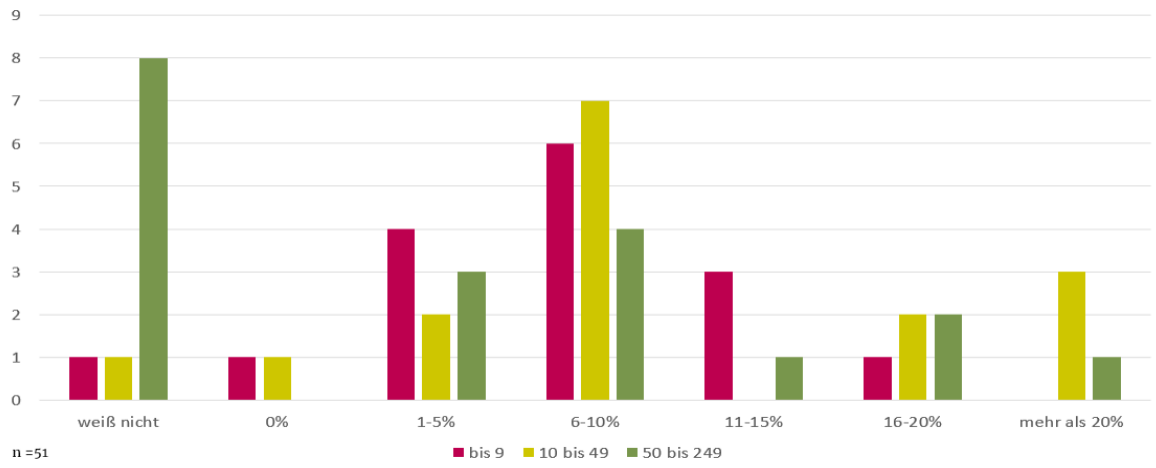

Abbildung 16: Cybersicherheitsinvestitionen als Anteil des IT-Budgets (eigene Darstellung)

Die folgende Abbildung 17 zeigt den Mehrwert, den KMU mit Cybersicherheitsmaßnahmen verbinden. 86 % der befragten Unternehmen sehen den Schutz vor Datenverlust als größten Vorteil von Cybersicherheit an. Darauf folgt der Schutz vor finanziellen Verlusten, der von 76 % der KMU als wichtiger Mehrwert angesehen wird. 68 % der Unternehmen betonen die Betriebssicherheit durch Schutz vor technischen Ausfällen, während 54 % die Reduzierung von Betriebsunterbrechungen als Nutzen betrachten. Die Erfüllung von Compliance-Vorgaben wird von 32 % der KMU als Mehrwert wahrgenommen. Geringer wird der Wettbewerbsvorteil (18 %) und die Stärkung des Unternehmensimages (10 %) eingestuft.

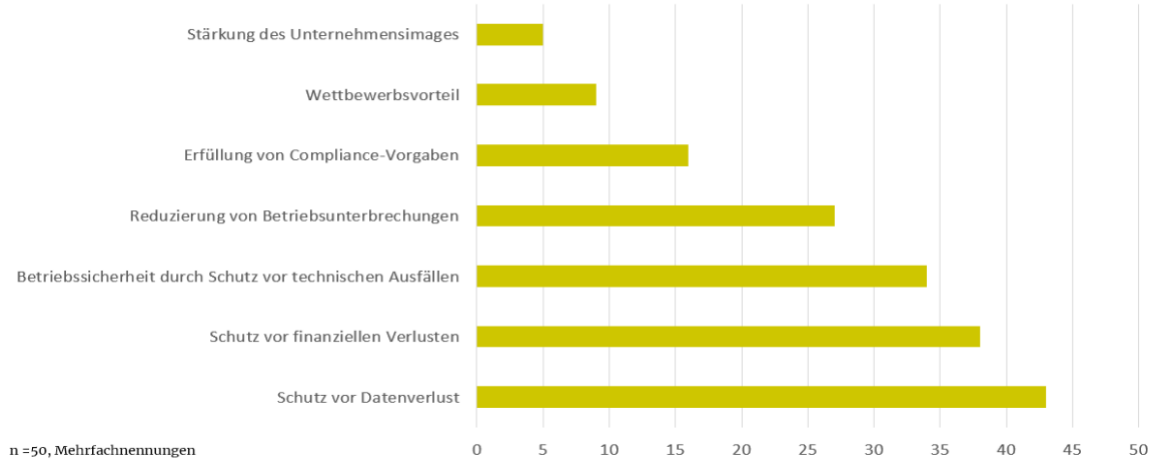

Abbildung 17: Wahrgenommener Mehrwert (eigene Darstellung)

Zusammenfassend zeigt die Analyse der Cybersicherheit in österreichischen KMU eine deutliche Diskrepanz zwischen den Unternehmensgrößen in Bezug auf die Häufigkeit von Risikobewertungen und implementierten Sicherheitsmaßnahmen. Während mittlere Unternehmen tendenziell häufiger Risikobewertungen durchführen, sind Kleinst- und kleine Unternehmen hier zurückhaltender. Regelmäßige Sicherheitsupdates sind die am weitesten verbreitete Maßnahme, insbesondere bei mittleren Unternehmen, gefolgt von der Sicherung des Netzwerks vor unberechtigtem Zugriff von außen und der Verwendung sicherer Passwörter. Vorreiter sind mittlere Unternehmen zudem im Bereich der klaren Zuständigkeiten und des Zugriffsmanagements nach Berechtigungskonzepten. Weniger verbreitet in KMU sind hingegen Maßnahmen wie regelmäßige Mitarbeiterschulungen und Notfallpläne. Die Umfrageergebnisse verdeutlichen, dass die meisten KMU entweder keine oder nur wenige Maßnahmen zur Risikominimierung bei Drittanbietern ergreifen. Zusätzlich kann jeder fünfte der Befragten nicht genau angeben, wie viel das KMU in Cybersicherheit investiert. Ein Großteil der KMU investiert 6-10 % des IT-Budgets in Cybersicherheit.

4.5 Bedürfnisse KMU zu Cybersicherheit

In diesem Kapitel werden die Cybersicherheitsbedürfnisse von KMU detailliert beleuchtet. Es wird analysiert, welche Maßnahmen sie zukünftig umsetzen möchten, wie zufrieden KMU mit aktuellen Cybersecurity-Produkten und Dienstleistungen sind und welche Formen der Unterstützung sie sich wünschen, um ihre IT-Sicherheit zu verbessern.

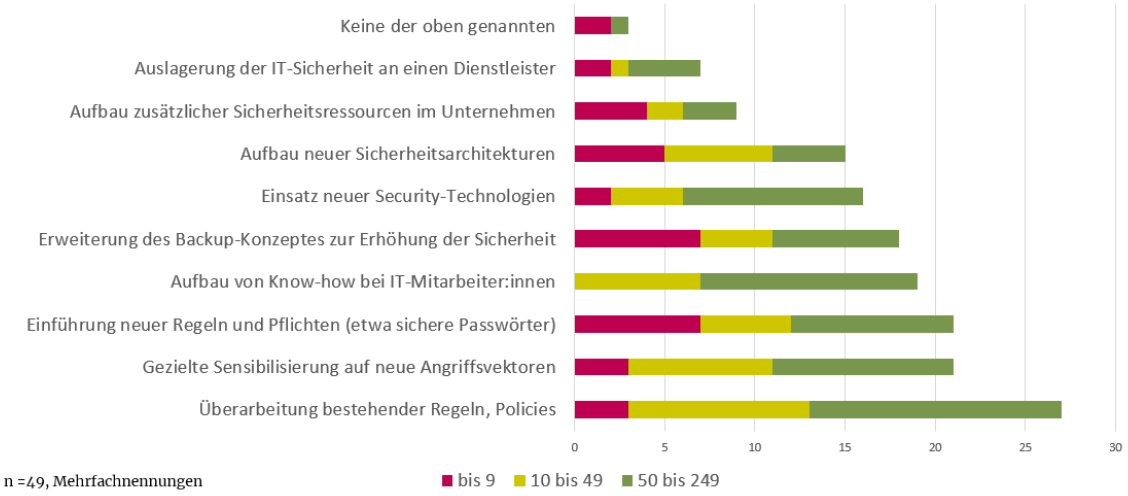

Abbildung 18: Geplante Cybersicherheitsmaßnahmen (eigene Darstellung)

Abbildung 18 zeigt welche Cybersicherheitsmaßnahmen KMU planen zukünftig umzusetzen. Die häufigste Maßnahme ist die Überarbeitung bestehender Regeln und Policies, die von 55 % der Unternehmen angestrebt wird. Dies gilt besonders für mittlere Unternehmen (14). 43 % der KMU planen die Einführung neuer Regeln und Pflichten (beispielsweise sichere Passwörter), sowie die gezielte Sensibilisierung auf neue Angriffsvektoren. Weiter ist der Aufbau von Know-how bei IT-Mitarbeiter:innen für 39 % der Unternehmen ein wichtiger Punkt, insbesondere bei mittleren (12) und kleinen Unternehmen (7). 37 % der KMU möchten ihr Backup-Konzept erweitern, um die Sicherheit zu erhöhen, während 33 % den Einsatz neuer Security-Technologien planen. Der Einsatz neuer Security-Technologien wird von insgesamt 16 Unternehmen geplant, wobei mittlere Unternehmen mit 10 Beantwortungen am stärksten vertreten sind. Der Aufbau neuer Sicherheitsarchitekturen ist bei 31 % der KMU vorgesehen. Darüber hinaus wollen 18 % der Unternehmen zusätzliche Sicherheitsressourcen im Unternehmen schaffen, und 14 % planen, die IT-Sicherheit an einen Dienstleister auszulagern. Nur 6 % der KMU haben keine der genannten Maßnahmen geplant.

Bei der Frage, wie gut die auf dem Markt verfügbaren Cybersicherheitsprodukte und -dienstleistungen den Bedürfnissen von KMU entsprechen, gaben etwa 37 % der befragten Unternehmen an, dass die Angebote ihren Anforderungen überwiegend gerecht werden (siehe Abbildung 19). Dies wurde besonders von mittleren Unternehmen bestätigt. Dennoch wussten 25 % der Unternehmen nicht, ob die Produkte ihren Bedürfnissen entsprechen, vor allem Kleinstunternehmen waren sich unsicher. 20 % der KMU meinten, dass die Produkte teilweise ihren Bedürfnissen entsprechen. Währenddessen 18 % der

befragten Unternehmen, hauptsächlich kleinst- und mittlere Unternehmen, angaben, vollständig zufrieden zu sein.

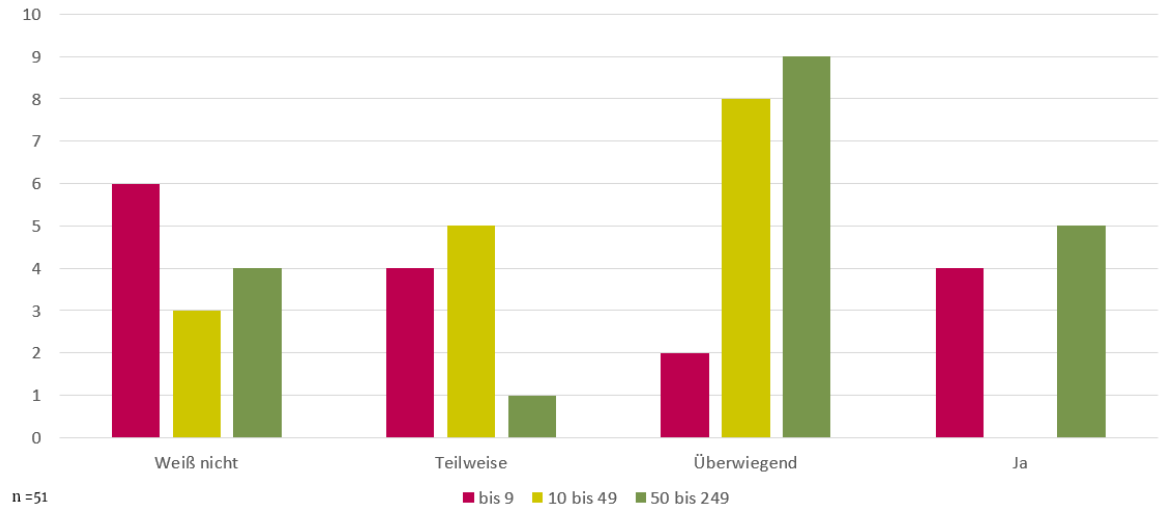

Abbildung 19: Zufriedenheit mit verfügbaren Cybersecurity Produkten und Dienstleistungen (eigene Darstellung)

Weiters gaben KMU einige Gründe an, warum Cybersecurity Produkte und Dienstleistungen nicht ihren Bedürfnissen entsprechen. Unter anderem sind Lösungen für sie zu teuer und auf größere Unternehmen ausgelegt. Darüber hinaus erfordern sie umfangreiche Investitionen und hohe Betreuungskapazitäten. Für kleinere Unternehmen sind diese Produkte häufig überdimensioniert, zu komplex in der Konfiguration oder beeinträchtigen den Datenfluss. Ein weiterer Grund ist, dass manchen Produkten wichtige Updates und Funktionen fehlen, um mit aktuellen Sicherheitsanforderungen Schritt zu halten.

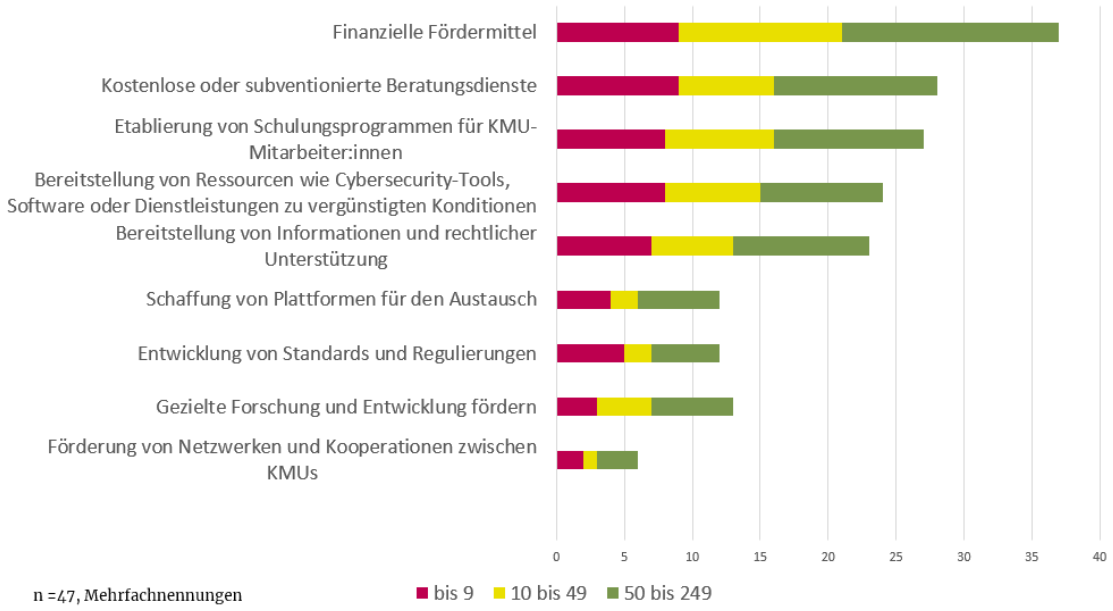

Abbildung 20: Gewünschte Unterstützungsmöglichkeiten seitens KMU (eigene Darstellung)

Die Unterstützungsmaßnahmen, die von KMU gewünscht werden, kann man aus Abbildung 20 entnehmen. 79 % der KMU wünschen sich finanzielle Fördermittel, wobei mittlere Unternehmen mit 16 Beantwortungen am stärksten vertreten sind. Auch kostenlose oder subventionierte Beratungsdienste werden von 60 % der KMU gewünscht, vor allem von kleinsten (9) und mittleren Unternehmen (12). Die Etablierung von Schulungsprogrammen für Mitarbeiter:innen wäre für 57 % der KMU eine wichtige Maßnahme. Diese wird von kleinsten und kleinen Unternehmen gleichermaßen stark nachgefragt (je 8). Währenddessen setzen mittlere Unternehmen mit 11 Beantwortungen noch stärker auf Schulungsprogramme. 51 % der KMU wünschen die Bereitstellung von Ressourcen wie Cybersecurity-Tools oder Dienstleistungen zu vergünstigten Konditionen, insbesondere mittlere Unternehmen (9). Ebenfalls wichtig ist für 49 % der Unternehmen die Bereitstellung von Informationen und rechtlicher Unterstützung, wobei diese Maßnahme vor allem von Kleinstunternehmen (7) und mittleren Unternehmen (10) nachgefragt wird. 26 % der KMU halten die Entwicklung von Standards und Regulierungen sowie die Schaffung von Plattformen für den Austausch für sinnvoll, jeweils besonders für mittlere Unternehmen (5 bzw. 6). Die gezielte Förderung von Forschung und Entwicklung wird von 28 % der KMU unterstützt, und 13 % der Unternehmen wünschen sich die Förderung von Netzwerken und Kooperationen zwischen KMUs, wobei diese Maßnahme hauptsächlich von mittleren Unternehmen nachgefragt wird (3).

Zusätzlich geht aus den Interviews hervor, dass KMU einen niederschwelligen Zugang zu IT-Sicherheitslösungen und externe Beratung wünschen, die ihnen bei der Implementierung

von Cybersicherheitsmaßnahmen helfen, da ihnen oftmals die personellen Ressourcen und das IT-Fachwissen fehlen. Weiters könnten Zwischenstufen, sowie einfache Zertifizierungen den Einstieg erleichtern und helfen, sich schrittweise an umfassendere Sicherheitsanforderungen heranzutasten. Zudem wünschen sich einige KMU eine Notrufnummer, die schnelle Unterstützung bietet, wenn Fragen oder Probleme auftreten, da es oft an interner Fachkompetenz mangelt. Abschließend würden KMU, sofern möglich, verstärkt auf Cybersicherheitsprodukte aus Europa zurückgreifen.

5 Rahmenbedingungen

In der Folge werden Rahmenbedingungen und Anforderungen dargestellt, die den Einsatz von Cybersicherheit in KMU beeinflussen können. Neben technischen, organisatorischen, gesellschaftlichen und rechtlichen Anforderungen werden Treiber und Barrieren untersucht.

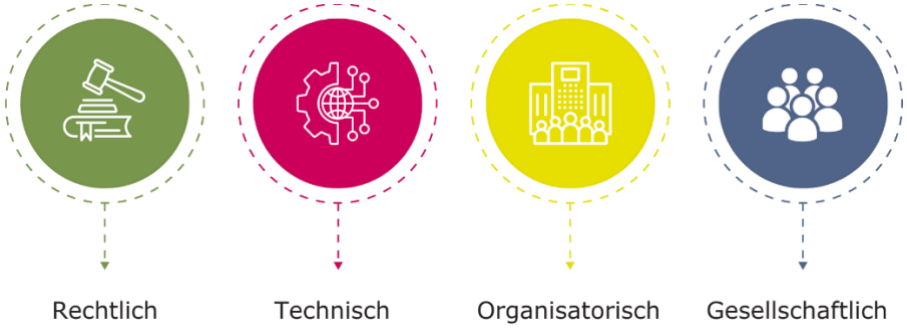

Abbildung 21: Übersicht der Anforderungen (eigene Darstellung)

5.1 Rechtliche Anforderungen

Die rechtlichen Anforderungen lassen sich wie folgt zusammenfassen:

- Standards und Richtlinien
- Gesetze und Verordnungen

Standards und Richtlinien

Cybersecurity Standards werden sowohl von internationalen (ISO, IEC, ETSI, CLC) als auch nationalen (NIST, BSI, ASI) Standardisierungsgremien herausgegeben. Zusätzlich gibt es Handlungsempfehlungen und Frameworks von Berufsverbänden (ISACA, SAE, ISA, OVE) und weiteren Organisationen. Immer öfter ist die Einhaltung bestimmter Security Standards implizit durch den Gesetzgeber vorgegeben. Ein Beispiel dafür ist die ISO/SAE 21434 (Automotive Cybersecurity), deren Einhaltung durch die Bestimmungen der UNECE zur Homologation und der EU-Verordnung zur Typengenehmigung festgeschrieben werden. Ein anderes Beispiel ist die ETSI EN 303 645, die um den EU Cybersecurity Act (CSA) entwickelt wurde. Im Fall der *Network and Information Security Directive* (NIS) gibt der Gesetzgeber

Cybersicherheitsanforderungen sogar vor – ein Indiz für die große Bedeutung, die Cybersicherheit mittlerweile eingenommen hat.

Bekannte Cybersecurity Standards sind die ISO/IEC 2700X[3] ISMS-Normenreihe, die ISO/IEC 15408[4] Common Criteria, die ISA/IEC 62443 Industrial Cybersecurity und die ETSI EN 303 645 Cyber Security for Consumer Internet of Things. Weitere sind oft von diesen abgeleitet bzw. an sie angelehnt, wie z.B. der BSI-Grundschutz, TISAX, CLC TS 50701[5] Railway Applications Cybersecurity. Generell gibt es für verschiedene Anwendungsdomänen eigene Cybersecurity Standards. Speziell für Web-Applikationen sind die Österreichische Norm A7700 (bereits aus 2019) zur Entwicklung sicherer Webapplikationen und das OWASP-Top 10 Projekt, das die Top-10 Sicherheitsrisiken für Webapplikationen erfasst, zu nennen. Bei sicherheitskritischen Systemen müssen im Übrigen Cybersicherheitsstandards (Security) jedenfalls auch immer im Zusammenhang mit den Sicherheitsstandards (Safety) gesehen werden – wie zum Beispiel die ISO/SAE 21434 mit der ISO 26262 im Bereich Automotive.

Gesamt betrachtet decken die Security Standards mittlerweile ein weites Feld an unternehmerischen Tätigkeiten ab, inklusive Business Continuity Management (ISO 22301) und Security Management der Supply Chain (ISO 28000). Weiterhin gibt es viele Frameworks, die das Ziel haben, die Cybersecurity bzw. IT-Risiken von Unternehmen durch Anwendung verschiedener Techniken bzw. Controls zu verringern, wie etwa CIS controls, COBIT oder HITRUST.

Die richtige Auswahl der Frameworks und Standards hängt von der Domäne, der Unternehmensgröße, und nicht zuletzt von den Anforderungen des Gesetzgebers und Geschäftspartner ab. Ein Grundschutz, wie beispielsweise die Baseline Security der WKO kann als Basis dienen.

Gesetze und Verordnungen

Begriffe wie CSA, CRA, DORA, NIS, NIS2, RCE, RED, GDPR und Exportkontrollen sind mittlerweile allgegenwärtig. In den letzten Jahren hat der Gesetzgeber, insbesondere auf EU-Ebene, eine Vielzahl von Verordnungen erlassen, die verbindliche Mindeststandards für

[3] https://www.iso.org/standard/27001
[4] https://www.iso.org/standard/72891.html
[5] https://www.austrian-standards.at/de/shop/ove-clc-ts-50701-2023-10-01~p2673321

Cybersicherheit festlegen und oftmals mit Sanktionen bei Nichteinhaltung verbunden sind. Eine Übersicht über derzeit gültige und kommende Verordnungen findet sich in Abbildung 22.

Regulation		Anwendung Ab	Kommentar
NIS	Network and Information Security Directive	gültig	
NIS2	Network and Information Security Directive 2	ab Okt. 2024	Noch nicht national umgesetzt
CSA	Cybersecurity Act	gültig	Einführung eines einheitlichen europäischen Zertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse.
CRA	Cyber Resilience Act	ab 2027	Cybersicherheit von Produkten, die miteinander oder mit dem Internet verbunden werden können. (Updates...)
DORA	Digital Operational Resilience Act	ab 2025	Gilt für 22.000 Banken, Versicherungsunternehmen und IKT-Dienstleister in der EU (Finanzsektor)
RCE	Resilience of Critical Entities Directive	wie NIS2	reguliert Resilienz kritischer Infrastrukturen (Ausfallssicherheit)
RED	Radio Equipment Directive	gültig	für Funkanlagen (z.B. WIFI)
GDPR	General Data Protection Regulation	gültig	DSGVO
AI Act	Artificial Intelligence Act	ab Aug. 2025	Nicht direkt cybersecurity, aber AI Sicherheit
DGA	Data Governance Act	gültig	Nicht direkt cybersecurity, aber Verordnung zu Daten-Governance
Export Control	Exportkontrolle	gültig	

Abbildung 22: Überblick über aktuelle (Stand 09 2024) und kommende EU-Verordnungen

Aktuell drehen sich viele Aktivitäten um das Update der NIS1, der NIS2. Hier wurden die von der NIS betroffenen Bereiche erweitert und die Anforderungen aktualisiert. Da eine NIS2 Einführung in einem Unternehmen mit viel Aufwand verbunden ist, gibt es eine breite Palette an – teilweise auch kostenlosen – Beratungsdienstleistungen, u.a. von der WKO, die bei einer Ersteinschätzung der Betroffenheit helfen.

Wie schon zuvor erwähnt schafft der Cybersecurity Act Grundlagen für ein Framework zur Zertifizierung von Produkten und Services, worauf z.B. die ETSI 303 645 aufbaut. Der Cyber Resilience Act (CRA) ist eine Ergänzung zur NIS2 und will die Cybersicherheit in Verkehr gebrachter Produkte erhöhen. So schreibt der CRA vor, dass Hersteller digitaler Produkte für maximal 5 Jahre zeitnahe Sicherheitsprobleme des Produkts z.B. durch Updates beheben müssen. Der Digital Operational Resilience Act (DORA) wiederum bringt Cybersecurity-Vorschriften für den Finanzsektor, die Resilience of Critical Entities Directive (RCE früher CER) widmet sich der Resilienz von kritischen Einrichtungen und ist im Zusammenhang mit NIS2 zu sehen, wobei letztere mehr auf Unternehmen abzielt. Die Radio Equipment Directive (RED) wiederum kümmert sich (unter anderem) um die Cybersecurity von Drahtlos-Produkten, die General Data Protection Regulation (GDPR) hat vor allem den Datenschutz im Fokus, gibt damit aber auch Vorgaben zur Cybersecurity. Schließlich ergeben sich Anforderungen an die Cybersecurity in einem Unternehmen durch weitere Gesetze und Vorschriften wie z.B. der Export-Kontrolle.

EU Regulation	Standard/Framework/ Best Practices
NIS 2 Directive, CER Directive, CRA Directive (including sector-specific Radio Equipment regulation)	CIs and Risk Assessment: ISO2700x, ISO/IEC 27033, ISO2800x, ETSI TR 103 866 V1.1., ISO/IEC 15408, ISO/IEC 18045, EN 17640, ISO 31000, IACS Recommendation on Cyber Resilience (2020), ANSI/ISA-62443-3-2-2020, ISA-TR99.00.01-2007, Supply chain cybersecurity: new guidance from the NCSC, ISO 13053, ETSI TS 102 165-1:2017, NIST SP-800-53 Cybersecurity Framework, NIST SP-800-37 Risk Management Framework, NIST SP-800-161, ETSI TS 102 165-1, BSI-Standards 100-2/100-3, OWASP Risk, NISTIR 8276 Key-Practices in Cyber Supply Chain Risk Management, NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management, CVRF, ISA/IEC 62443-3-2, IWA 31:2020, ISO 22301, ISO/IEC 27035 Threat taxonomies: OWASP, CAPEC MITRE, FISMA, STRIDE, ATT&CK MITRE Vulnerabilities disclosure: ISO/IEC 29147:2018, EN-ISO/IEC 29147:2020, ISO/IEC 30111:2019, EN-ISO/IEC 30111:2020, TR 103838, CVE (MITRE), CVSS 3.1 (FIRST), OSV
Cybersecurity Act	ENISA: EUCC, EUCS IT Evaluation: ISO/IEC 15408, ISO/IEC 18045, Conformity Assessment/Audit: ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 17000, ISO/IEC 17007, ISO/IEC 17021series, ISO/IEC 17019, ISO/IEC 17020, ISO/IEC 17024, ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17067, ISO 19011 EU 5G scheme: 3GPP TR 33.894 V0.5.0 (2023-02), ISO/IEC 27404, ETSI EN 303 645, NISTIR 8425 GSMA Network Equipment scheme (Security Assurance-by-design)
GDPR, ePrivacy Regulation, Data Act, eIDAS (including sector-specific EU Health Data Space regulation)	Privacy Assessment/Information Management: EN17529:2022, ISO 3300x series on process assessment, ISO/IEC 2700x information security series, CEN ISO/IEC/TS, 27006-2:2022, ISO/IEC 27701, ISO/IEC TR 27550:2019, BS10012, CEN CWA 16113 Identity Management: ISO/IEC 23220, ISO/IEC 27460, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 27701, ISO/IEC 27018 Encryption: ISO/IEC 18033, ISO/IEC 11770-3, ISO 13491, ISO/IEC 19772:2020, ISO/IEC 18033-6:2019, ISO 13492:2019
AI Act	EU AI cybersecurity certification scheme proposal, ISO/IEC TR 5469, IEC TS 62998-3, Stocktaking National and Regional Cybersecurity Policy (2021), NIST AI 100-2e2023ipd-Adversarial Machine Learning, ISO/IEC 27005, ISO/IEC 27563, ISO/IEC 23894, ISO/IEC 24028, ISO/IEC 5338
Cyber Solidarity Act	Incident Management: ISO/IEC 27035, NIST Incident Response Framework, NIST SP-800-62 Emergency Management: ISO 22322:2015, ISO 22327:2018, ISO 22326:2018 - Security and resilience
Chips Act	CHIPS R&D Metrology Program (NIST), EN 17640, ISO/IEC 15408, CENELEC JTC 13 WG3.
5G, IoT	3GPP TR 33.894 V0.5.0 (2023-02), ETSI EN 303 645 Cybersecurity for Consumer IoT, ISO /IEC 20000, ISO/IEC 27033, IPv6, MANRS, IoT-RFC-9200, RFC-8613, ACE-OAuth framework, EDHOC, ECHC, GSMA/3GPP, GSMA SAS-UP/SAS-SM

Abbildung 23: Übersicht über EU-Verordnungen und zuordenbare Standards/Frameworks. (Kalogeraki & Polemi, 2024)

Abbildung 23 gibt eine Übersicht über die den EU-Verordnungen zuordenbaren Standards bzw. Frameworks. Abgesehen von der schieren Anzahl, sind die Standards teilweise sehr umfangreich und für eine Umsetzung sind externe Berater empfehlenswert. Typische Schritte bei einer Umsetzung sind zumeist (1) Feststellen der auszuwählenden Bereiche (in Standard und Firma), (2) Anpassen der im Standard vorgeschlagenen Maßnahmen, und (3) Ausarbeiten der Argumentation für eventuell Zertifizierung und Umsetzung.

Für Unternehmen, insbesondere KMU, sind nicht alle Standards gleichermaßen relevant und hängen sehr von der Domäne ab, in der sie tätig sind. Jedoch gibt es weniger aufwändige Grundschutz-Varianten (WKO, BSI), die jedes Unternehmen – auch KMU – vollständig umsetzen sollten.

Neben der durch Verordnungen geforderten Standards können auch Markterfordernisse die Umsetzung gewisser Standards im Unternehmen notwendig machen. Beispielsweise

wird TISAX, ein für die Risikobewertung von Lieferanten optimiertes System zum Austausch normierter Prüfergebnisse in der Automobilindustrie, inkl. Prototypenschutz im Automotivbereich von OEMs vielfach vorausgesetzt.

Um festzustellen, ob man als Unternehmen von einer gewissen Verordnung erfasst wird, gibt es teilweise kostenlose Online-Schnelleinschätzungen, z.B. betreffend NIS2 jenes der WKO.

In der Online-Umfrage wurde die Bekanntheit ausgewählter Verordnungen und Richtlinien in KMU erhoben und die Ergebnisse sind in Abbildung 24 dargestellt. Die Datenschutzgrundverordnung ist mit 96 % die bekannteste Verordnung und ist unter den befragten KMU-Größen relativ gleich bekannt. Die NIS2-Richtlinie folgt mit 45 %, und die NIS1 wird von 37 % der KMU als geläufig angegeben. Der Cyber Resilience Act, der AI Act und der Digital Services Act erreichen jeweils eine Bekanntheit von 27 %. Beim AI Act fällt auf, dass Kleinstunternehmen (8) ihn häufiger kennen als kleine oder mittlere Unternehmen.

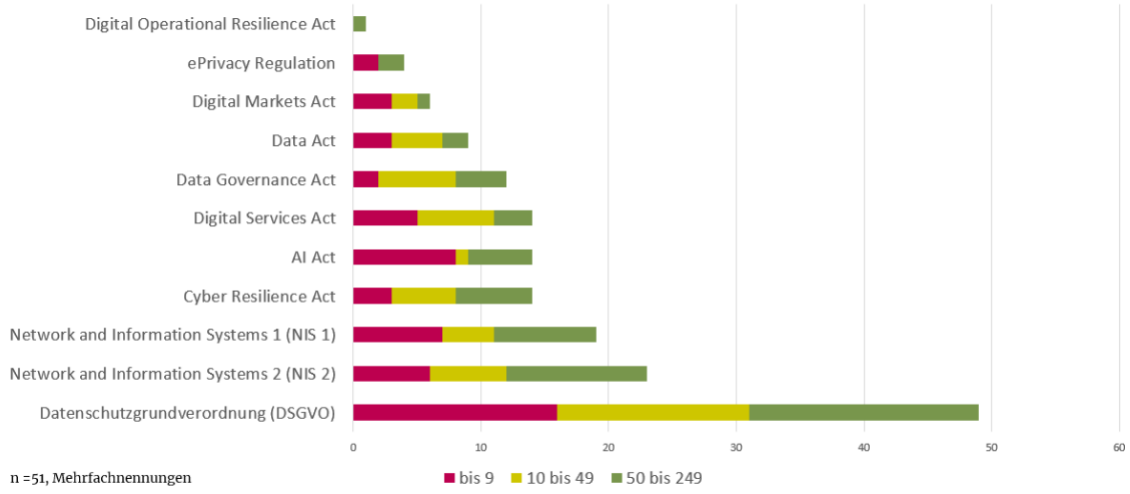

Abbildung 24: Bekanntheit von Richtlinien (eigene Darstellung)

Die Bekanntheit des Data Governance Act liegt bei 24 %, während der Data Act mit 18 % etwas weniger bekannt ist. Weitere Richtlinien, wie der Digital Markets Act und die ePrivacy Regulation sind mit 12 % bzw. 8 % weniger verbreitet. Am wenigsten bekannt ist der Digital Operational Resilience Act, der nur 2 % der KMU geläufig ist.

5.2 Technische Anforderungen

Für die erfolgreiche Umsetzung von Cybersicherheitsmaßnahmen in KMU sollten aus technischer Sicht unter anderem folgende Faktoren berücksichtigt werden:

- Sicherheitsinfrastruktur und Netzwerkarchitektur
- Datenverschlüsselung und Schutz sensibler Informationen
- Automatisierte Updates und Patch-Management
- Sicherer Datenaustausch
- Zugangskontrollen und Identitätsmanagement
- Backup- und Wiederherstellungslösungen
- Vorhandensein von Notfallplänen
- Anwendbare Sicherheit und Benutzerfreundlichkeit
- Herkunft der Technologie

Eine robuste **Sicherheitsinfrastruktur und Netzwerkarchitektur** ist für KMU von zentraler Bedeutung, um interne und externe Bedrohungen effektiv abzuwehren. Mit dem Einsatz von Firewalls und Intrusion-Detection/Prevention-Systemen lassen sich unberechtigte Zugriffe verhindern und das Unternehmensnetzwerk schützen. Ebenso wichtig ist der Schutz sensibler Daten durch **Verschlüsselung**, sowohl während der Übertragung als auch im Ruhezustand. Dies ist besonders relevant in der Kommunikation mit Kunden und Partnern, um sicherzustellen, dass vertrauliche Informationen vor unbefugtem Zugriff sicher sind.

Zusätzlich spielen **automatisierte Updates** und ein effektives **Patch-Management** eine entscheidende Rolle in der Cybersicherheit. Regelmäßige und automatisierte Updates sorgen dafür, dass Sicherheitslücken schnell geschlossen werden, ohne dass manuelle Eingriffe notwendig sind. Um den **sicheren Datenaustausch** zu gewährleisten, sollten KMU Technologien wie VPN und SSL-Verschlüsselungen nutzen, um sensible Daten vor Diebstahl und Manipulation zu schützen. Ergänzend dazu sind **Zugangskontrollen** und ein durchdachtes **Identitätsmanagement** erforderlich, um sicherzustellen, dass nur autorisierte Personen Zugriff auf sensible Systeme und Daten haben. Multi-Faktor-Authentifizierung erhöht hierbei zusätzlich die Sicherheit.

Ein essenzieller technologischer Aspekt ist die Datensicherung und **Wiederherstellung**. Regelmäßige **Backups**, die in externen Rechenzentren oder der Cloud gespeichert werden, sind unerlässlich, um nach Cyberangriffen oder Systemausfällen schnell auf gesicherte

Daten zugreifen zu können. Ergänzend dazu ist ein gut ausgearbeiteter **Notfallplan** entscheidend, damit alle Beteiligten genau wissen, wie sie im Falle eines Cyberangriffs handeln müssen. Um KMU den Zugang zu Sicherheitslösungen zu erleichtern, sollten diese besonders **benutzerfreundlich** und leicht anwendbar sein, da häufig kein spezialisiertes IT-Personal vorhanden ist. Darüber hinaus bevorzugen viele KMU Technologien aus Europa, um sicherzustellen, dass Datenschutzstandards eingehalten werden. Dies könnte ihre Resilienz stärken, da europäische Lösungen oft höhere Transparenz bieten. Dennoch bleibt die Abhängigkeit von globalen Anbietern auch im Sinne der Souveränität eine Herausforderung, da es schwierig ist, die Kontrolle über den Datenfluss und mögliche Sicherheitslücken in nicht-europäischer Hardware und Software vollständig zu gewährleisten.

5.3 Organisatorische Anforderungen

Die organisatorischen Anforderungen lassen sich wie folgt skizzieren:

- Commitment der Geschäftsführung
- Verankerung von Cybersicherheit in der Unternehmenskultur
- Kontinuierliches Engagement
- Humanressourcen und Fachkompetenz
- Festlegung von Zuständigkeiten
- Sensibilisierung und Schulungen
- Aufbau eines vertrauensvollen Netzwerkes

Als organisatorische Grundlage für eine erfolgreiche Umsetzung von Cybersicherheit in KMU ist Engagement und die Unterstützung der **Geschäftsführung** unumgänglich. Ohne die Unterstützung der Geschäftsführung bleibt Cybersicherheit häufig ein Randthema und wird nicht ausreichend priorisiert oder finanziert. Cybersicherheit muss als fester Bestandteil der **Unternehmenskultur** etabliert werden. Dies erfordert ein **kontinuierliches Engagement** auf allen Ebenen, um sicherzustellen, dass Sicherheitsmaßnahmen nicht nur implementiert, sondern auch regelmäßig überprüft und aktualisiert werden. Dabei muss betont werden, dass die Cybersicherheit nicht nur in der Verantwortung des Systemadministrators oder der IT-Abteilung liegt, sondern eine gemeinsame Aufgabe aller Mitarbeiter:innen im Unternehmen ist, die durch klare Richtlinien, regelmäßige Schulungen und ein umfassendes Bewusstsein für Sicherheitsrisiken unterstützt werden muss. **Humanressourcen** spielen dabei eine Schlüsselrolle, da ausreichend qualifiziertes Personal zur Verfügung stehen muss,

um Cybersicherheitsstrategien umzusetzen und zu überwachen. Eine klare Festlegung der **Zuständigkeiten** innerhalb der Organisation stellt sicher, dass alle Mitarbeiter ihre Rollen im Rahmen der Sicherheitsmaßnahmen kennen. Regelmäßige **Schulungen** tragen wesentlich dazu bei, dass die Mitarbeitenden über aktuelle Bedrohungen informiert sind und wissen, wie sie sich in Risikosituationen verhalten sollen. Dadurch wird das allgemeine Sicherheitsbewusstsein gestärkt und das Risiko menschlichen Fehlverhaltens, das zu Sicherheitsvorfällen führen kann, minimiert. Schließlich trägt der Aufbau eines **vertrauensvollen Netzwerks** mit kompetenten Partnern und externen Dienstleistern dazu bei, dass KMU Zugang zu bewährten Lösungen und Fachwissen erhalten, um ihre Cybersicherheitsstrategie erfolgreich umsetzen zu können.

5.4 Gesellschaftliche Anforderungen

Die gesellschaftlichen Anforderungen lassen sich wie folgt zusammenfassen:

- Breitenwirksame Berichterstattung
- Kundendruck
- Transparenz und Kultur der Offenheit
- Gesellschaftliche Verantwortung und kritische Infrastrukturen

Mediale **Berichte** über Cyberangriffe, Datenpannen und Sicherheitslücken haben dazu geführt, dass das Bewusstsein für Cybersicherheit in der breiten Öffentlichkeit wächst. Dieses gesteigerte Bewusstsein wirkt sich auch auf KMU aus, die zunehmend die Dringlichkeit erkennen, ihre IT-Systeme zu schützen, um ähnliche Vorfälle zu vermeiden. Die öffentliche Berichterstattung macht das Thema greifbarer und rückt es stärker in den Fokus der Unternehmen. Gleichzeitig üben **Kunden** erheblichen **Druck** auf KMU aus. Sie erwarten zunehmend, dass ihre Lieferanten zertifiziert sind und internationale Sicherheitsstandards wie ISO 27001 einhalten. Unternehmen, die diese Zertifizierungen nicht nachweisen können, riskieren, Aufträge zu verlieren oder als potenzielles Sicherheitsrisiko angesehen zu werden. Dieser Druck bringt KMU dazu, ihre Sicherheitsvorkehrungen zu verstärken und regelmäßige Überprüfungen durchzuführen, um sowohl wettbewerbsfähig zu bleiben als auch den gestiegenen Anforderungen ihrer Kunden gerecht zu werden.

Offene Diskussionen über Risiken, Sicherheitsvorfälle und verwundbare Bereiche tragen dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen. **Transparenz** in der externen

Kommunikation von Sicherheitsvorfällen schafft nicht nur Vertrauen innerhalb eines Unternehmens, sondern auch gegenüber Kunden und Partnern. Unternehmen, die Vorfälle transparent teilen, fördern eine Kultur der Offenheit, was langfristig zu besseren präventiven Maßnahmen führen kann.

In der Wahrnehmung der Gesprächspartner:innen tragen KMU eine **Verantwortung gegenüber der Gesellschaft**, insbesondere wenn sie mit sensiblen Daten umgehen. Dies umfasst nicht nur den Schutz von Kundendaten, sondern auch die Minimierung/Vermeidung von Sicherheitsvorfällen, die wirtschaftliche Schäden verursachen oder (kritische) Infrastrukturen gefährden können. KMU sollten sicherstellen, dass ihre Cybersicherheitsmaßnahmen ausreichen, um ihre Stakeholder und die Gesellschaft zu schützen.

5.5 Barrieren und Herausforderungen

Im Rahmen der Interviews mit Expert:innen und Unternehmer:innen wurden KMU-spezifische Barrieren und Herausforderungen erhoben, die die Implementierung von Cybersicherheitsmaßnahmen erschweren. Diese Barrieren wurden mitunter durch die Online-Umfrage mit KMU priorisiert und validiert.

Fehlendes Bewusstsein

Ein großes Hindernis für die Cybersicherheit in KMU ist das fehlende Bewusstsein. Viele Unternehmen sind sich nicht der realen Bedrohungen bewusst oder unterschätzen die potenziellen Folgen eines Cyberangriffs. Oft herrscht die Einstellung, dass man selbst nicht betroffen sein könnte, insbesondere wenn das Tätigkeitsfeld eher analog betrieben wird. Ein Desinteresse an Technologie, kombiniert mit der Annahme, die jüngere Generation oder externe Dienstleister könnten solche Probleme ganz alleine lösen, führt dazu, dass notwendige Sicherheitsmaßnahmen nicht ergriffen werden. Zudem fehlt es an einem proaktiven Mindset, Cybersicherheit als fortlaufenden Prozess zu verstehen, der sowohl von der Geschäftsführung als auch den Mitarbeitenden ernst genommen werden muss. Ohne ein grundlegendes Bewusstsein für die Risiken bleiben viele KMU anfällig für Angriffe, die im schlimmsten Fall ihre Existenz gefährden können.

Mangel an Ressourcen und erkennbarem Mehrwert

Eine der größten Barrieren für KMU ist der Mangel an Zeit und finanziellen Ressourcen, um Cybersicherheitsmaßnahmen umzusetzen. Kleinstunternehmen stehen oft unter großem Zeitdruck, sodass ihrFokus zur Gänze auf der Geschäftstätigkeit liegt. Darüber hinaus werden Investitionen in Cybersicherheit als teuer und nicht unmittelbar notwendig wahrgenommen. Investitionen in IT-Sicherheit bringen keinen direkten finanziellen Mehrwert, da das Hauptziel darin besteht, Vorfälle zu verhindern. Mangelndes IT-Budget in KMU erschwert den Zugang zu notwendigen Technologien und Fachkräften.

Komplexität, mangelnde Orientierung und fehlende Unterstützung

Cybersicherheit wird als ein äußerst komplexes Thema wahrgenommen, das für viele KMU schwer greifbar ist. KMU fühlen sich von den Anforderungen der Cybersicherheit überfordert und wissen nicht, wo sie anfangen sollen. Es fehlt an klaren, leicht verständlichen Richtlinien und Unterstützung bei der Umsetzung von Maßnahmen. Ohne ausreichende Beratung und Orientierung fühlen sich viele Unternehmen allein gelassen und unsicher in der Entscheidung, welche Maßnahmen für sie sinnvoll sind. Weiters spielen hierbei sprachliche Barrieren eine Rolle. Besonders wenn es darum geht, die notwendige Beratung oder Expertise für KMU verständlich zu machen. Berater und IT-Fachkräfte müssen die komplexen technischen Anforderungen in eine Form übersetzen, die für Unternehmer:innen nachvollziehbar ist, um somit den Weg zu effektiven Maßnahmen zu ebnen.

Fachkräftemangel und Expertise

Ein weiteres Hindernis ist der Mangel an Fachexpertise. Qualifiziertes Personal ist schwer zu finden und teuer. Kleine Unternehmen können es sich oft nicht leisten, einen spezialisierten IT-Sicherheitsbeauftragten einzustellen oder externe Expertise regelmäßig in Anspruch zu nehmen. Hinzu kommt die Schwierigkeit, IT-Dienstleister zu bewerten und deren Kompetenzen einzuschätzen, da es an Zertifizierungen für IT-Dienstleister mangelt. Weiters erschwert das Fehlen von Schulungs- und Ausbildungsmöglichkeiten, insbesondere in kleineren Unternehmen und ländlichen Regionen, den gezielten Aufbau von Expertise im Unternehmen.

Zielkonflikt Komfort und Sicherheit

Sicherheitsmaßnahmen werden häufig als unbequem und zeitaufwendig empfunden. Es gibt einen Zielkonflikt zwischen dem Wunsch nach Komfort und der Notwendigkeit,

Sicherheitsvorkehrungen umzusetzen. Häufig besteht ein psychologisches Hindernis, sich mit der Thematik auseinanderzusetzen, da es als lästig und nicht essenziell wahrgenommen wird. Diese kulturellen und organisatorischen Barrieren sind tief in der Unternehmenskultur verankert und erfordern einen Wandel in der Einstellung gegenüber Cybersicherheit.

Unzureichende Angebote für KMU

Für KMU fehlen maßgeschneiderte und erschwingliche Cybersicherheitslösungen. Die Beratung und Implementierungen können kostspielig sein und KMU geraten in Abhängigkeit von IT-Dienstleistern. Es fehlen einfache, skalierbare Lösungen, die speziell auf die begrenzten Mittel, Fähigkeiten und Bedürfnisse von KMU abgestimmt sind.

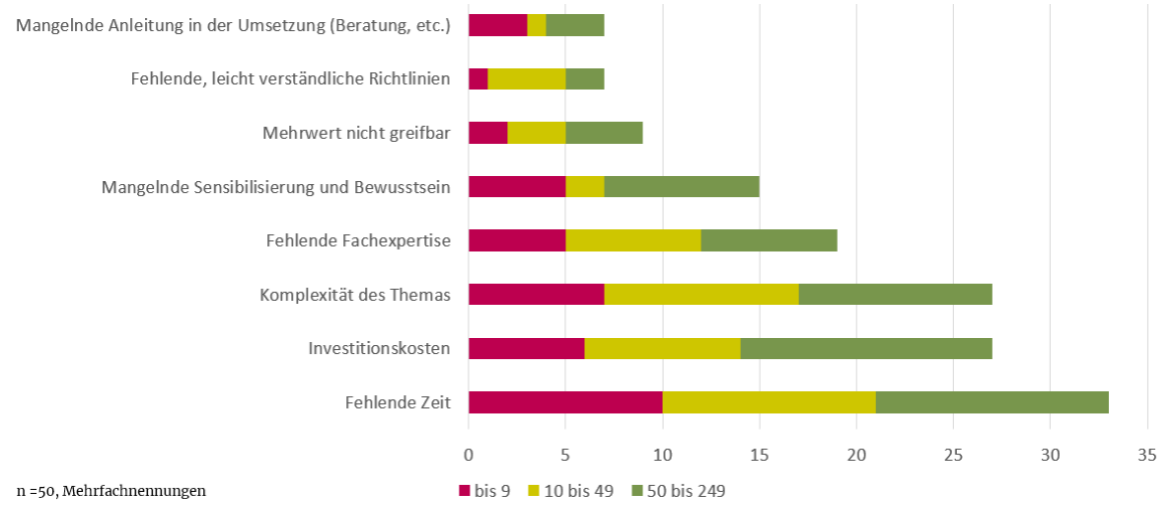

Abbildung 25: Barrieren zur Cybersicherheit (eigene Darstellung)

Wie Abbildung 25 zeigt, bestätigen die Ergebnisse der Online-Umfrage dieses Bild. Dabei werden als die größten Barrieren für KMU bei der Umsetzung von Cybersicherheitsmaßnahmen vor allem fehlende Zeit, hohe Investitionskosten und Komplexität des Themas angeführt. Mittlere Unternehmen haben dabei am stärksten mit Zeitmangel zu kämpfen, was 66 % der KMU betrifft. Die Investitionskosten und die Komplexität des Themas stellen für 54 % der KMU eine bedeutende Herausforderung dar. Während mittlere Unternehmen besonders von den Investitionskosten betroffen sind, stellt die Komplexität der Cybersicherheit gerade bei Kleinst- und kleinen Unternehmen eine hohe Barriere dar. Fehlende Fachexpertise ist ein weiteres Hindernis, das vor allem kleine und mittlere Unternehmen betrifft und insgesamt bei 38 % der KMU auftritt. Zudem nehmen 30 % der KMU mangelnde Sensibilisierung und Bewusstsein für Cybersicherheit als Barriere wahr. Dies gilt insbesondere für Kleinst- und mittleren Unternehmen. Für 18 % der

KMU ist der Mehrwert von Cybersicherheitsmaßnahmen nicht greifbar. Weitere Hürden wie fehlende, leicht verständliche Richtlinien und mangelnde Anleitung bei der Umsetzung betreffen jeweils 14 % der Unternehmen. Akzeptanzprobleme bei Mitarbeitenden treten mit 10 % am seltensten auf, was darauf hindeutet, dass Cybersicherheitsmaßnahmen in der Belegschaft der Umfrageteilnehmer:innen tendenziell gut angenommen werden.

5.6 Trends

Als aktuelle Entwicklungen und Trends im Bereich Cybersicherheit für KMU stehen in der Folge technologie- und infrastrukturbasierte Trends als auch Sicherheitstrends und Schutzstrategien im Fokus.

Technologie- und infrastrukturbasierte Trends

- Künstliche Intelligenz (KI) und Maschinelles Lernen

KI und maschinelles Lernen haben das Potenzial, die Cybersicherheit zu revolutionieren, indem sie Bedrohungen in Echtzeit erkennen und abwehren können. Gleichzeitig nutzen auch Kriminelle diese Technologien, um automatisierte Angriffe durchzuführen, etwa durch das Erstellen raffinierter Phishing-Mails oder das Entdecken von Schwachstellen. Unternehmen müssen sicherstellen, dass ihre KI-gesteuerten Abwehrmechanismen auf dem neuesten Stand sind, um mit den von KI unterstützten Bedrohungen Schritt zu halten.

- Quantencomputing & Post-Quanten-Kryptografie

Quantencomputer haben das Potenzial, herkömmliche Verschlüsselungsverfahren wie RSA und ECC zu brechen, was eine massive Bedrohung für die Sicherheit digitaler Kommunikation darstellt. Unternehmen und Regierungen weltweit arbeiten daher an der Entwicklung von Post-Quanten-Kryptografie, die auch gegen Quantencomputer resistent ist. Während diese Technologien noch nicht weit verbreitet sind, wird ihre Implementierung in den nächsten Jahren immer dringender, um zukünftige Sicherheitsrisiken zu minimieren.

- Cloudsicherheit und SWaaS

Der verstärkte Einsatz von Cloud-Diensten bietet KMU große Vorteile, kann aber auch Sicherheitsrisiken mit sich bringen. Sie ermöglichen eine einfachere Verwaltung und

reduzieren gleichzeitig die Komplexität der Cybersicherheit. Cloud-Dienste können durch automatisierte Updates, zentral eingespielte Patches, sowie durchgehendes Monitoring und proaktiven Maßnahmen Sicherheitslücken minimieren und die frühzeitige Abwehr von Angriffen ermöglichen. Jedoch können KMU durch fehlkonfigurierte Cloud-Umgebungen, mangelnde Zugriffsverwaltung und unsichere Schnittstellen anfällig für Sicherheitsvorfälle, Datenverluste und unbefugte Zugriffe werden. Da immer mehr Daten in die Cloud verlagert werden, ist die Sicherstellung der Cloudsicherheit eine der obersten Prioritäten für IT-Abteilungen. Mit der zunehmenden Nutzung von Cloud-Diensten setzen immer mehr Unternehmen auf Security-as-a-Service.

- Internet of Things

Die zunehmende Vernetzung von Geräten durch das Internet of Things (IoT) erhöht die Angriffsfläche von Unternehmen erheblich. Viele IoT-Geräte sind nicht ausreichend gesichert, was sie zu einem bevorzugten Ziel für Angreifer macht. Diese Geräte können als Einstiegspunkte für Angriffe dienen, die dann auf größere Netzwerke übergreifen. Unternehmen müssen sicherstellen, dass auch ihre IoT-Geräte in die Sicherheitsstrategie integriert sind.

- 5G-Sicherheit

Mit dem Aufkommen von 5G-Netzwerken eröffnen sich neue Möglichkeiten, vor allem durch die schnelle Datenübertragung. Doch vergrößert eine höhere Vernetzung wiederum die potenzielle Angriffsfläche und erhöht dadurch das Sicherheitsrisiko. Unternehmen müssen sicherstellen, dass ihre Sicherheitsinfrastruktur den Anforderungen dieser neuen Technologie gerecht wird, um vor Angriffen auf mobile Netzwerke und verbundene Geräte geschützt zu sein.

Sicherheitstrends und Schutzstrategien

- Zero Trust

Das Zero Trust-Modell revolutioniert die Cybersicherheit, indem es davon ausgeht, dass kein Nutzer oder Gerät von Natur aus vertrauenswürdig ist. Dabei ist es irrelevant, ob man sich innerhalb oder außerhalb des Unternehmensnetzwerks befinden. Dieser Ansatz basiert auf der kontinuierlichen Authentifizierung und Autorisierung, um potenzielle Bedrohungen zu minimieren. Unternehmen, die Zero Trust umsetzen, profitieren von erhöhter Sicherheit,

da sie Zugriffsrechte beschränken und den Datenfluss segmentieren, um das Risiko von Insider-Angriffen oder externen Sicherheitsverletzungen zu verringern.

- Mobile Sicherheit & Bring Your Own Device

Die Nutzung privater Geräte für berufliche Zwecke erhöht das Risiko für Unternehmen, da viele dieser Geräte nicht ausreichend gesichert sind. Das Fehlen von Sicherheitsvorkehrungen wie starken Passwörtern oder Verschlüsselung macht Unternehmen anfälliger für Cyberangriffe. Die Einführung von Mobile Device Management und Unified Endpoint Management wird immer wichtiger, um diese Geräte zu verwalten und zu schützen.

- Cyber-Versicherungen

Mit der wachsenden Bedrohung durch Cyberangriffe steigt auch die Nachfrage nach Cyber-Versicherungen. Diese bieten Unternehmen finanziellen Schutz vor den Folgen von Cyberangriffen, einschließlich der Kosten für Datenwiederherstellung, Forensik und rechtliche Schritte. Angesichts der steigenden Kosten und Risiken durch Cyberkriminalität werden Cyber-Versicherungen zunehmend als unerlässlicher Teil der Risikomanagementstrategie betrachtet.

6 Handlungsfelder und Empfehlungen

Um die Cybersicherheit in österreichischen KMU zu stärken, müssen die spezifischen Rahmenbedingungen und Herausforderungen bei der Anwendung von Sicherheitsmaßnahmen berücksichtigt werden. Die folgenden vier Handlungsfelder wurden von den befragten Expert:innen als entscheidend identifiziert, um effektive Cybersicherheitsstrategien in KMU zu entwickeln und deren Widerstandsfähigkeit gegen Cyberbedrohungen zu erhöhen. Zu den jeweiligen Handlungsfeldern wurden konkrete Handlungsempfehlungen für die öffentliche Hand abgeleitet.

6.1 Cybersicherheit verankern

Für eine verstärkte Cybersicherheit in KMU braucht es ein breites Verständnis in den Unternehmen. Wie die durchgeführte Umfrage und die Interviews zeigen, ist das Bewusstsein und die daraufhin umgesetzten Maßnahmen in österreichischen KMU aktuell sehr heterogen. Während wenige Unternehmen bereits ISO 2700x zertifiziert sind, haben andere KMU keine Ressourcen für Cybersicherheit, da ihr Kerngeschäft ihre gesamte Aufmerksamkeit beansprucht. Wiederum andere KMU setzen verstärkt auf technologische Sicherheitsmaßnahmen, aber vernachlässigen gleichzeitig organisationale Maßnahmen, wie beispielsweise Mitarbeiterschulungen. Um Cybersicherheit in KMU zu verankern, benötigt es Bewusstseinsbildung, definierte Verantwortlichkeiten, Teilnahme an Trainings und Schulungen und eine offene Gespräches- und Fehlerkultur.

- Bewusstseinsbildung

KMU stehen vor der Herausforderung, die Dringlichkeit und den tatsächlichen Mehrwert von Cybersicherheitsmaßnahmen richtig einzuschätzen. Häufig fehlt das Bewusstsein für die reale Bedrohungslage und die möglichen Konsequenzen eines Cyberangriffs, wodurch die Notwendigkeit eines proaktiven Sicherheitsansatzes unterschätzt wird. Sicherheitsmaßnahmen werden dabei oftmals als umständlich und kompliziert empfunden, was zu einer ablehnenden Haltung bei der Implementierung führt. Zudem wird Cybersicherheit als komplex und schwer greifbar wahrgenommen, und viele KMU wissen nicht, wo sie ansetzen sollen. Fehlende klare und leicht verständliche Richtlinien verschärfen das Problem, wodurch notwendige Maßnahmen aus Unsicherheit nicht

ergriffen werden. Unterstützende Maßnahmen zur Bewusstseinsbildung können hier aufklären und Vertrauen schaffen, etwa durch die Kommunikation realer Bedrohungsszenarien, die Vermittlung von Best-Practice-Beispielen sowie die Einbindung von Erfolgsgeschichten, die den Mehrwert von Cybersicherheitsmaßnahmen zeigen. Ein klarer, verständlicher Zugang zur Thematik, unterstützt durch zielgerichtete Beratung und das Aufbrechen technischer Fachsprache, kann zudem dazu beitragen, dass KMU die Relevanz dieser Maßnahmen als weniger abstrakt wahrnehmen und aktiv werden.

- Verantwortlichkeiten definieren

Um die Cybersicherheit in KMU nachhaltig zu stärken, ist die Definition klarer Verantwortlichkeiten essenziell. Die Umfrageergebnisse zeigen, dass in vielen KMU die Zuständigkeit von Cybersicherheit einzig bei der Geschäftsführung liegt, insbesondere in Kleinstunternehmen. Diese enge Verknüpfung mit der Führungsebene in Verbindung mit der Unternehmensgröße birgt jedoch das Risiko, dass IT-Sicherheit im Tagesgeschäft oftmals nur begrenzt Aufmerksamkeit erhält. Häufig fehlt eine dezidierte Ansprechperson oder Fachabteilung, wodurch es an spezialisierter Expertise mangelt. Ein strukturierter Ansatz zur Festlegung von Verantwortlichkeiten, etwa durch die Ernennung eines internen IT-Sicherheitsbeauftragten oder die Einbindung externer Berater, könnte eine wertvolle Unterstützung bieten. Besonders mittlere Unternehmen, die häufiger über eigene IT-Abteilungen verfügen, profitieren von klar definierten Zuständigkeiten, da sie regelmäßige Risikobewertungen durchführen und gezielte Cybersicherheitsmaßnahmen umsetzen. Durch die klare Zuweisung von Rollen und Verantwortlichkeiten kann sichergestellt werden, dass Cyberrisiken frühzeitig erkannt und entsprechende Maßnahmen ergriffen werden.

- Trainings und Weiterbildungen

Regelmäßige Trainings und Weiterbildungen sensibilisieren Mitarbeitende für aktuelle Bedrohungen und klären über Maßnahmen zur Risikominimierung auf. Mitarbeitende sind häufig die erste Verteidigungslinie gegen Cyberangriffe, insbesondere bei Phishing- oder Social-Engineering-Attacken. Trainings helfen, Risiken frühzeitig zu erkennen und gezielt zu reagieren. Dabei ist es wichtig, das Wissen kontinuierlich aufzufrischen und mit neuen Trends und Techniken im Bereich Cybersicherheit zu verknüpfen. Schulungen, die praxisnah gestaltet sind und auf die spezifischen Anforderungen eines KMU abgestimmt werden, erhöhen die Wahrscheinlichkeit, dass Sicherheitsabläufe verstanden und konsequent angewendet werden.

- Offene Gesprächs- und Fehlerkultur

Durch eine offene Gesprächs- und Fehlerkultur wird ein Umfeld geschaffen in dem Mitarbeitende über Sicherheitsvorfälle oder Unsicherheiten offen sprechen können, ohne negative Konsequenzen zu befürchten. Wenn Mitarbeitende Fehler ohne Scheu vor Sanktionen melden können, erhöht das die Transparenz und trägt dazu bei, potenzielle Sicherheitslücken schneller zu erkennen und zu schließen. Offene Kommunikation fördert zudem das Sicherheitsbewusstsein auf allen Ebenen des Unternehmens. Führungskräfte spielen eine Schlüsselrolle, indem sie die Cybersicherheit zu einem festen Bestandteil der Unternehmenskultur machen und die Belegschaft dazu ermutigen, Sicherheitsfragen offen anzusprechen und gemeinsam Lösungen zu finden.

Folgende Handlungsempfehlungen zur Verankerung von Cybersicherheit in KMU lassen sich ableiten:

Bewusstseinsbildung über Fachgruppen und Cluster
Eine gezielte Bewusstseinsbildung über Fachgruppen und Cluster, wie beispielsweise durch die WKO, kann KMU bei Cybersicherheitsmaßnahmen unterstützen. Durch Schulungen, Workshops und Informationsmaterialien sollen KMU branchenspezifisch über aktuelle Bedrohungen und Schutzmaßnahmen aufgeklärt werden. Fachgruppen und Branchennetzwerke bieten dafür eine ideale Plattform, um Expertise gezielt zu vermitteln und den Austausch zwischen KMU und Expert:innen zu fördern.

Subventionen für Mitarbeiterschulungen
Subventionen für Schulungen und Weiterbildungen im Bereich Cybersicherheit helfen KMU, IT-Sicherheitskompetenzen im Unternehmen aufzubauen. Durch praxisnahe Weiterbildung werden die Angestellten in die Lage versetzt, Bedrohungen frühzeitig zu erkennen und abzuwehren.

Kommunikation über Cyberbedrohungen, Verwundbarkeit und Konsequenzen
Öffentliche und private Institutionen sollten Informationen zu Bedrohungen und Schwachstellen intensiver austauschen. Zentral zugängliche Expertise kann die Reaktionszeit und Qualität von Sicherheitsmaßnahmen verbessern. Eine offene Kommunikation zu Cybervorfällen fördert das Sicherheitsbewusstsein und reduziert Ängste, sich zu Sicherheitsvorfällen zu äußern und Angriffe offenzulegen.

KMU-Ratgeber für Cybersicherheitsförderungsanträge
Ein Online-Ratgeber für Cybersicherheitsförderung könnte KMU durch den Prozess der Antragsstellung für Sicherheitsförderungen leiten. Der Ratgeber sollte grundlegende Informationen zur Förderungslandschaft bereitstellen, Teilnahmevoraussetzungen durch eine kurze Umfrage klären und durch eine interaktive Plattform mit Schritt-für-Schritt-Anleitung unterstützen. Der Prozess könnte KMU durch das einfache Durchklicken der Schritte bis zum fertigen Antrag führen, um Einstiegshürden zu senken und die Umsetzung notwendiger Sicherheitsmaßnahmen für KMU zu erleichtern.

6.2 Risikomanagement aufbauen

Der Aufbau eines Risikomanagements in KMU erfordert einen systematischen Ansatz, der alle Schritte von der Risikoidentifikation bis hin zur kontinuierlichen Verbesserung umfasst. Zunächst sollten Bedrohungen und Schwachstellen konsequent erfasst und bewertet werden, um die spezifischen Cybersicherheitsrisiken des Unternehmens zu verstehen. Darauf aufbauend ist es wichtig, Maßnahmen zu priorisieren und umzusetzen, die die identifizierten Risiken adressieren. Ein regelmäßiges Überprüfen und Anpassen der Maßnahmen ist dabei zentral, um auf veränderte Bedrohungslagen und neue Sicherheitsanforderungen zu reagieren. Ein umfassendes Informationssicherheits-Management (IS-Management) unterstützt diesen Prozess, indem es sicherstellt, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewahrt bleibt. Weiters umfasst das Risikomanagement das Notfall- und Business Continuity Management (BCM) als wichtigen Bestandteil, um KMU auf unvorhersehbare Ereignisse vorzubereiten.

- Risikobewertungen

Regelmäßige Risikobewertungen sind entscheidend, um Bedrohungen und Schwachstellen in KMU frühzeitig zu erkennen und angemessen zu handeln. Allerdings fehlt vielen KMU ein systematischer Bewertungsprozess, insbesondere in kleineren Unternehmen, wo Bewertungen unregelmäßig durchgeführt oder nicht klar definiert werden. Die Umsetzung regelmäßiger, strukturierter Bewertungen hilft KMU, ihre Cybersicherheitslage besser zu verstehen und die Dringlichkeit von Schutzmaßnahmen gezielt zu bestimmen.

- Bewertung der Sicherheit innerhalb der Wertschöpfungskette

Cybersicherheitsmaßnahmen sind in KMU entlang der Wertschöpfungskette oft lückenhaft, wodurch Schwachstellen für Angriffe offenbleiben. Während einige KMU, vor allem mittlere Unternehmen, Zugangsbeschränkungen und Überwachungssysteme eingeführt haben, fehlen umfassendere Vorkehrungen wie verbindliche Sicherheitsanforderungen in Verträgen, Reaktionspläne bei potenziellen Vorfällen und regelmäßig aktualisierte Lieferantenlisten. Ein sorgfältiger Blick auf die Risiken, die in der Wertschöpfungskette bestehen, ist für KMU unerlässlich. Um sich als starkes Glied in der Lieferkette zu positionieren, sollten KMU sich gezielt gegen Angriffe auf die Lieferkette absichern. Mit einer proaktiven Absicherung tragen KMU nicht nur zur eigenen, sondern auch zur Cybersicherheit der gesamten Lieferkette bei.

- Informationssicherheits-Management

Ein ganzheitliches IS-Management bildet das Fundament eines nachhaltigen Sicherheitsmanagements in KMU und geht über einfache Schutzmaßnahmen hinaus. Als zentraler Bestandteil des Risikomanagements sichert das IS-Management die Vertraulichkeit, Integrität und Verfügbarkeit sämtlicher Informationen, Prozesse und IT-Systeme. Dieser kontinuierliche Prozess passt Strategien und Maßnahmen regelmäßig an neue Anforderungen an und gewährleistet eine fortlaufende Optimierung der Unternehmenssicherheit in einem dynamischen Umfeld.

- Notfallmanagement und Business Continuity Management

Notfallmanagement und Business Continuity Management (BCM) sind essenzielle Bestandteile eines robusten Sicherheitskonzepts für KMU. Während das Notfallmanagement die Reaktionsfähigkeit bei Störungen sicherstellt, zielt das BCM darauf ab, die Geschäftskontinuität zu gewährleisten und operative Ausfälle zu minimieren. Dennoch verfügen nur wenige KMU über einen Notfallplan, der im Ernstfall entscheidend ist, um schnell und wirksam zu reagieren. Ein durchdachtes BCM umfasst präventive Planung, Risikobewertungen und klare Notfallprozeduren, die regelmäßig getestet und aktualisiert werden. Damit wird KMU ermöglicht, selbst bei unvorhersehbaren Ereignissen betriebsfähig zu bleiben und rasch zu reagieren.

Folgende Handlungsempfehlungen zum Aufbau des Risikomanagements in KMU lassen sich ableiten:

Förderprogramme für die Implementierung von Cybersicherheitsmaßnahmen
Gezielte Subventionen helfen KMU bei der Implementierung von Cybersicherheitsmaßnahmen, fördern strukturiertes Risikomanagement und erleichtern Zugang zu nötigen Ressourcen.

Chatbot als Anlaufstelle für Cybersicherheitsfragen
Ein Chatbot für KMU ist ein nützliches Hilfsmittel für schnelle und einfache Zugänge zu Informationen über Cybersicherheit. Er ermöglicht KMU unkomplizierte und kontinuierliche Unterstützung bei Fragen zu Cybersicherheitsmaßnahmen.

KMU-CERT und Public-Private-Partnerships
Staatlich unterstützte Computer Emergency Response Teams (CERTs) und Partnerschaften zwischen öffentlichen und privaten Akteuren bieten sofortige Hilfe bei Sicherheitsvorfällen und fördern den Wissenstransfer. Diese Responseteams können KMU im Krisenfall schnell unterstützen und stärken die Reaktionsfähigkeit der gesamten Wertschöpfungskette.

6.3 Technologische Schutzmauern festigen

Die Etablierung robuster technischer Schutzmauern ist für KMU essenziell, um ein hohes Maß an Cybersicherheit zu gewährleisten und sich gegen eine wachsende Vielfalt an Bedrohungen zu wappnen. Netzwerksicherheit, Endgeräteschutz und Datensicherheit bilden dabei die grundlegenden Verteidigungslinien, die das gesamte digitale Umfeld eines Unternehmens absichern. Darüber hinaus wird durch den „Security by Design“-Ansatz Cybersicherheit von Beginn an in die Entwicklung von IT-Systemen integriert, während beim Einkauf von Hardware und Software stets hohe Sicherheitsstandards berücksichtigt werden sollten.

- Netzwerksicherheit, Endgeräteschutz und Datensicherheit

Diese drei Bereiche ergänzen sich und stellen die wesentlichen technischen Verteidigungslinien dar, die KMU vor Cyberbedrohungen schützen. Ein ganzheitlicher Ansatz in diesen Bereichen sorgt für eine engmaschige Schutzstruktur, die das gesamte digitale Umfeld eines KMU absichert. Netzwerksicherheit bildet die Grundlage, um den gesamten Datenverkehr zu überwachen und unerlaubte Zugriffe oder Bedrohungen abzuwehren. KMU sollten robuste Firewalls und Intrusion Detection-Systeme einsetzen, um das Unternehmensnetzwerk von außen abzuschirmen und ungewöhnliche Aktivitäten frühzeitig zu identifizieren. Darüber hinaus konzentriert sich Endgeräteschutz darauf, alle Geräte wie Computer, Tablets und Smartphones zu sichern, da diese oft die Einfallstore darstellen. Durch den Einsatz von Antivirensoftware, regelmäßigen Sicherheitspatches und Maßnahmen zur Verschlüsselung von Endgeräten kann das Risiko von Infektionen und Datenverlusten erheblich reduziert werden. Mobile Device Management Lösungen helfen außerdem, den Zugriff auf Unternehmensdaten von mobilen Geräten zu kontrollieren. Datensicherheit schließt diese Schutzmaßnahmen ab, indem sie sich auf den sicheren Umgang mit den Daten selbst konzentriert. Hierzu gehören Verschlüsselungsmaßnahmen, die sowohl die Übertragung als auch die Speicherung (sensibler) Daten schützen. Regelmäßige Backups und Zugangskontrollen gewährleisten, dass Unternehmensdaten im Falle eines Angriffs oder Hardwareausfalls sicher wiederhergestellt werden können und Unbefugte keinen Zugriff erhalten.

- Security by Design

Bei diesem Ansatz wird die Cybersicherheit bereits in der Planungs- und Entwicklungsphase von IT-Systemen und -Anwendungen berücksichtigt. Ziel ist es, Schwachstellen von Beginn an zu minimieren und Sicherheitsmaßnahmen in die gesamte Architektur der Systeme zu integrieren. Für KMU bedeutet dies, dass Sicherheitslücken frühzeitig geschlossen werden und IT-Strukturen resistenter gegenüber Angriffen werden. Security by Design erfordert zwar initiale Investitionen, führt jedoch langfristig zu stabileren und widerstandsfähigeren Systemen.

- Sicherheit bei der Beschaffung mitdenken

Bei der Auswahl und Beschaffung von Hardware, Software und IT-Dienstleistungen sollten KMU stets auf Cybersicherheitsstandards und -anforderungen achten. Die Zusammenarbeit mit Anbietern, die hohe Sicherheitsstandards erfüllen und den Schutz sensibler Daten gewährleisten, minimiert potenzielle Risiken und stärkt die Cybersicherheit auf allen Ebenen. Eine sichere Beschaffung umfasst dabei eine systematische Koordination und

Genehmigung der Auswahl, Installation und Nutzung informationsverarbeitender Komponenten – von Hardware wie externen Laufwerken und Tablets bis hin zu Software und Betriebssystemen. Strategische und operative Beschaffungsprozesse werden durch wiederholbare und risikobasierte Entscheidungen geregelt, um Sicherheitsrisiken zu reduzieren. Ein strukturierter Beschaffungsprozess orientiert sich an klaren Phasen wie Bedarfsermittlung, Marktanalyse, Lieferantenmanagement und abschließender Evaluierung, begleitet durch eine Risikoanalyse. Der Akquisitionsprozess nach ISO/IEC 12207, wie in Abbildung 26 dargestellt, bietet hierfür eine klare Struktur in fünf Phasen: Zunächst erfolgt die Vorbereitung und Planung, bei der Risiken, Schutzbedarf und Lieferantenkriterien festgelegt werden. Anschließend werden die Anforderungen in der Ausschreibung an potenzielle Zulieferer kommuniziert und der passende Anbieter ausgewählt. In der dritten Phase, dem Aufsetzen der Vertragsbeziehung, werden vertragliche Pflichten und Sicherheitsanforderungen definiert. Danach wird die Einhaltung des Vertrags im Monitoring überwacht, bevor das Produkt in der letzten Phase auf Konformität geprüft und offiziell akzeptiert wird. Dieser Prozess stellt sicher, dass alle relevanten Sicherheits- und Qualitätsanforderungen umfassend erfüllt werden.

Abbildung 26: Akquisitionsprozess nach ISO/IEC 12207

Folgende Handlungsempfehlungen zum Festigen technologischer Schutzmauern in KMU lassen sich ableiten:

Cybersecurity Tool und Services Datenbank
Eine Datenbank zu Cybersecurity Produkten und Dienstleistungen dient als strukturierte Übersicht für Sicherheitslösungen und Services, die speziell auf die Bedürfnisse von KMU abgestimmt sind. Durch Filterfunktionen, wie Art der

Bedrohung und Unternehmensgröße, wird KMU ermöglicht, schnell die richtigen Werkzeuge für ihre Anforderungen zu finden und fundierte Entscheidungen bei der Auswahl ihrer Sicherheitsmaßnahmen zu treffen. Diese Datenbank muss auf dem neuesten Stand gehalten werden, um einen Mehrwert zu schaffen.

Anbieterlandkarte

Die Anbieterlandkarte ist eine visuelle Übersicht regionaler und überregionaler Cybersicherheitsdienstleister, die sich auf die Beratung und Umsetzung von Sicherheitsmaßnahmen für KMU spezialisiert haben. Sie kategorisiert Anbieter nach deren Spezialisierung, etwa Netzwerksicherheit oder Endgeräteschutz, und zeigt deren Qualifikationen und Zertifizierungen. Referenzprojekte und Erfolgsgeschichten geben KMU zusätzliche Einblicke in die Kompetenz und Verlässlichkeit der Anbieter. Diese Kompetenzkarte hilft KMU dabei, qualifizierte Partner in ihrer Nähe zu finden und fördert den Zugang zu maßgeschneiderten Sicherheitslösungen.

Zuschüsse für Sicherheitssoftware und Beratungsdienste

Diese Förderungen erleichtern die Anschaffung von essenziellen Sicherheitslösungen, die technische Schutzmauern stärken, wie Firewalls, Intrusion Detection und Prevention Systeme, Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselungstechnologien. Auch regelmäßige Software-Updates und -Patches können durch Förderungen unterstützt werden, um die Effektivität dieser Schutzmauern dauerhaft zu gewährleisten.

Open Source Paket

Ein Open Source-Paket für Cybersicherheit bietet KMU eine kosteneffiziente Möglichkeit, grundlegende Schutzmaßnahmen zu implementieren. Dieses Paket umfasst eine Sammlung bewährter Open Source-Tools, die für technische Schutzmauern notwendig sind, wie Firewalls, Virenschutz, Netzwerkscanner und Verschlüsselungslösungen. Begleitet von umfassenden Dokumentationen und Anleitungen, ermöglicht ein solches Paket KMU, die wichtigsten Sicherheitsmaßnahmen ohne hohe Lizenzkosten zu integrieren und anzupassen.

6.4 Compliance sichern

Um Cybersicherheit in KMU zu gewährleisten, ist die Einhaltung von Sicherheitsrichtlinien und gesetzlichen Verordnungen unerlässlich. Regelmäßige Überprüfungen und die branchenübergreifende Zusammenarbeit stärken nicht nur die Sicherheitsmaßnahmen, sondern fördern auch den Austausch bewährter Praktiken.

- Sicherheitsrichtlinien und Verordnungen

Um Cybersicherheit fest in KMU zu verankern, ist die Einhaltung von Sicherheitsrichtlinien und gesetzlichen Verordnungen essenziell. Diese Richtlinien legen die Mindeststandards fest, die ein Unternehmen erfüllen muss, um seine Daten und Systeme zu schützen. Für KMU ist es wichtig, klare und zugängliche Richtlinien zu entwickeln, die alle relevanten Aspekte der Cybersicherheit abdecken, wie Datenverarbeitung, Zugriffsrechte und Netzwerksicherheit. So können Compliance-Anforderungen im täglichen Betrieb einfach umgesetzt und das Risiko rechtlicher Konsequenzen oder Datenschutzverstöße minimiert werden.

- Regelmäßige Überprüfungen und Audits

Regelmäßige Überprüfungen und Audits tragen dazu bei, dass Cybersicherheitsmaßnahmen kontinuierlich an die sich entwickelnde Bedrohungslage angepasst werden. Durch interne und externe Audits können KMU Schwachstellen identifizieren und Lücken in ihrer Sicherheitsarchitektur rechtzeitig schließen. Diese Audits helfen nicht nur, Compliance zu überprüfen, sondern fördern auch eine Kultur der Cybersicherheitsbewusstheit. KMU profitieren davon, da regelmäßige Audits ihnen nicht nur den aktuellen Sicherheitsstatus aufzeigen, sondern auch konkrete Maßnahmen zur Verbesserung und Einhaltung von Standards bieten.

- (Branchenübergreifende) Zusammenarbeit

Eine branchenübergreifende Zusammenarbeit bei Cybersicherheit ermöglicht es KMU, von den Erfahrungen und Best Practices anderer Unternehmen zu profitieren. Der Austausch mit anderen Branchen, etwa durch Sicherheitsnetzwerke, Fachverbände oder Kooperationen, fördert das kollektive Wissen über Bedrohungen und wirksame Schutzmaßnahmen. Durch solche Partnerschaften können KMU schneller auf neue Bedrohungen reagieren und aktuelle Compliance-Anforderungen effizienter umsetzen.

Diese Zusammenarbeit stärkt nicht nur die Sicherheitslage einzelner Unternehmen, sondern fördert auch den Aufbau einheitlicher Standards, die der gesamten Branche zugutekommen.

Folgende Handlungsempfehlungen zum Sichern von Compliance lassen sich ableiten:

Förderung der Entwicklung von Standards für KMUs
Um KMU bei der Cybersicherheit zu unterstützen, sollte die Entwicklung branchenspezifischer und leicht umsetzbarer Standards gefördert werden. Diese Standards sind auf die besonderen Bedürfnisse und Kapazitäten von KMU zugeschnitten und berücksichtigen Ressourcenbegrenzungen, sodass Sicherheitsanforderungen realistisch und pragmatisch erfüllt werden können.

Bereitstellung klarer Richtlinien und Unterstützung bei der Einhaltung gesetzlicher Anforderungen
Durch die Bereitstellung verständlicher Leitfäden und Hilfestellungen wird KMU eine klare Orientierung bei der Umsetzung von Sicherheitsmaßnahmen gegeben. Diese Anleitungen sollten gezielt auf gesetzliche Anforderungen und Sicherheitsstandards abgestimmt sein, um die Umsetzung im Unternehmensalltag zu erleichtern und die Compliance sicherzustellen.

Regelmäßige (freiwillige) Überprüfungen
Freiwillige Audits und Überprüfungen bieten KMU die Möglichkeit, ihre Cybersicherheitsmaßnahmen regelmäßig auf Schwachstellen zu prüfen und Anpassungen vorzunehmen. Diese Überprüfungen schaffen Transparenz über den Sicherheitsstatus und bieten konkrete Empfehlungen zur Optimierung ohne den Druck einer verpflichtenden Kontrolle.

Stufenweise Zertifizierungen
Ein stufenweises Zertifizierungssystem erlaubt KMU, Compliance in mehreren Etappen zu erreichen. Diese Methode senkt die Einstiegshürden für kleinere Unternehmen, die ihre Cybersicherheit schrittweise verbessern möchten. Von grundlegenden Maßnahmen bis hin zu umfassenden Sicherheitsstandards können Unternehmen so kontinuierlich ihren Schutz steigern.

Hotline für Cyber-Sorgen, (verbindliche) Rechtsauskunftsstelle

Eine eigene Rechtsauskunftsstelle könnte verbindliche Informationen zu gesetzlichen Anforderungen bereitstellen und KMU helfen, sich sicher und rechtskonform im Bereich Cybersicherheit zu bewegen.

7 Verzeichnisse

Abbildungsverzeichnis

Abbildung 1: Methodik CyberGuide (eigene Darstellung) 13
Abbildung 2: Globale Risikolandschaft (World Economic Forum, 2024) 16
Abbildung 3: Zukünftige Entwicklung der durch Cyberkriminalität verursachten weltweiten Kosten; in Milliarden Euro (Erk, Koch, Lau, & Scheytt, 2024) 17
Abbildung 4: Durchschnittlicher Schaden durch ein Datenleck; weltweit; 2023; in Millionen Euro / in Prozent (Erk, Koch, Lau, & Scheytt, 2024) 18
Abbildung 5: Anteil der Unternehmen mit betroffenen Daten nach Daten- und Angriffsart (Dreißigacker, Skarczinski, & Wollinger, 2020) 19
Abbildung 6: Monatliche Verteilung der Ransomware-Fälle 2023 (Bundeskriminalamt, 2024) 21
Abbildung 7: Erkannte Sicherheitsvorfälle in österreichischen KMU (eigene Darstellung). 22
Abbildung 8 Beispielhafte Gliederung der Cybersecurity Landschaft Österreichs inkl. wichtiger Akteure 24
Abbildung 9 Forschungseinrichtungen mit Cyber-Security Bezug in Österreich 25
Abbildung 10 Publikationen (Autor oder Ko-Autor) österreichischer Forscher in den Top-10 Security Journals/Konferenzen: IEEE Symp. on Security and Privacy, USENIX Security Symposium, Trans. on Information Forensics and Security, Computers & Security, ACM Symp. On Computer and Communications Security, Network and Distributed System Security Symposium, IEEE Trans. on Dependable and Secure Computing, Journal of Information Security and Applications, EuroCrypt, International Cryptology Conference. Quelle: DBLP SPARQL, 09 2024 26
Abbildung 11 FFG geförderte Sicherheitsforschung in Österreich ist gut verankert: Analyse der Teilnehmer nach Organisationstyp. Quelle: FFG Projektdatenbank, Stichwort „Security“, 09 2024 27
Abbildung 12: Zuständigkeiten nach Unternehmensgröße 30
Abbildung 13: Häufigkeit von Cyber-Risikobewertungen 31
Abbildung 14: Implementierte Cybersicherheitsmaßnahmen in österreichischen KMU 32
Abbildung 15: Third-Party Risk Management 33
Abbildung 16: Cybersicherheitsinvestitionen als Anteil des IT-Budgets 34
Abbildung 17: Wahrgenommener Mehrwert 35
Abbildung 18: Geplante Cybersicherheitsmaßnahmen 36
Abbildung 19: Zufriedenheit mit verfügbaren Cybersecurity Produkten und Dienstleistungen 37
Abbildung 20: Gewünschte Unterstützungsmöglichkeiten seitens KMU 38
Abbildung 21: Übersicht der Anforderungen (eigene Darstellung) 40

Abbildung 22 Überblick über aktuelle (Stand 09 2024) und kommende EU-Verordnungen 42
Abbildung 23 Übersicht über EU-Verordnungen und zuordenbare Standards/Frameworks. (Kalogeraki & Polemi, 2024) 43
Abbildung 24: Bekanntheit von Richtlinien (eigene Darstellung) 44
Abbildung 25: Barrieren zur Cybersicherheit 50
Abbildung 26: Akquisitionsprozess nach ISO/IEC 12207 61

Literaturverzeichnis

BKA, A. I.–C.-B. (2021). *Österreichische Strategie für Cybersicherheit 2021.* Wien: Bundeskanzleramt.

BSI. (2022). *Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten.* Bonn.

Bundesamts für Sicherheit in der Informationstechnik. (2023). *Die Lage der IT-Sicherheit.* Bonn.

Bundeskanzleramt, & Zentrum für sichere Informationstechnologie - Austria. (2023). *Österreichisches Informationssicherheitshandbuch.* Wien.

Bundeskriminalamt, B. f. (2024). *Cybercrime Report 2023.* Wien: Bundesministerium für Inneres, Bundeskriminalamt.

Bundesministerium des Innern für Bau und Heimat. (2021). *Cybersicherheitsstrategie für Deutschland 2021 .* Berlin.

Dreißigacker, A., Skarczinski, B. v., & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland.* Hannover: Kriminologisches Forschungsinstitut Niedersachsen.

Erk, D., Koch, C., Lau, P., & Scheytt, S. (2024). *Cybersicherheit in Zahlen .* Bochum,: G DATA CyberDefense AG.

European Commission. (2003). *SME definition*. Von https://single-market-economy.ec.europa.eu/smes/sme-definition_en abgerufen

European Union Agency for Cybersecurity. (2021). *CYBERSECURITY FOR SMES.*

European Union Agency for Cybersecurity. (2021). *CYBERSECURITY FOR SMES: Challenges for SMEs.*

ISB, I. d. (2018). *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022.* Bern: Informatiksteuerungsorgan des Bundes ISB.

Kalogeraki, E. M., & Polemi, N. (2024). A taxonomy for cybersecurity standards. *Journal of Surveillance, Security and Safety*, 95-115.

Kompetenzzentrum Sicheres Österreich, C. T. (2024). *Cyber Risk Rating & Cyber Trust Label.*

World Economic Forum. (2024). *The Global Risks Report 2024.* Cologny/Geneva: World Economic Forum.

Abkürzungen

AI	Artificial Intelligence
APT	Advanced Persistent Threats
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT.at	Computer Emergency Response Team Austria
CERTs	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
CRA	Cyber Resilience Act
CSA	EU Cybersecurity Act
DDoS	Distributed Denial-of-Service
DORA	Digital Operational Resilience Act
ENISA	Agentur der Europäischen Union für Cybersicherheit
F&E	Forschung und Entwicklung
FFG	Österreichische Forschungsförderungsgesellschaft
GDPR	General Data Protection Regulation
HW	Hardware
IAM	Identity und Access Management
IoT	Internet of Things
IS-Management	Informationssicherheits-Management
ISMS	Informationssicherheits-Managementsystem
ISO	International Standardization Organisation
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
NIS	Netz- und Informationssystem-sicherheitsgesetz
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OT	Operational Technology
PQC	Post-Quantum Cryptography

QKD	Quantum Key Distribution
R&D	Research and Development
RCE	Resilience of Critical Entities Directive
RED	Radio Equipment Directive
RSA	Rivest–Shamir–Adleman
VPN	Virtual Private Network
WEF	World Economic Forum
WKO	Wirtschaftskammer Österreich

8 Anhang: Leitfaden

CyberGuide für KMU - Praxisleitfaden für Cybersicherheit

AN WEN SICH DER LEITFADEN WENDET

- Geschäftsführung
- IT-Verantwortliche
- Mitarbeitende

WAS DEN LEITFADEN AUSZEICHNET

- Die Maßnahmen sind praxisnah, leicht verständlich und speziell auf die Bedürfnisse von KMU abgestimmt.
- Sie sind schrittweise aufgebaut und erfordern keine umfassenden Vorkenntnisse.
- Die Inhalte umfassen Basismaßnahmen, die jedes KMU umsetzen sollte.
- Der Leitfaden dient als Orientierung und ist keine Zertifizierungs-grundlage.

AUFBAU UND STRUKTUR DES LEITFADENS

Der Leitfaden umfasst 19 Maßnahmen zur Erhöhung der Cybersicherheit und gliedert sich in fünf Abschnitte:

Bundesministerium Finanzen

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

Gefördert durch das Sicherheitsforschungs-Förderprogramm KIRAS des Bundesministeriums für Finanzen

Identifizieren

Physische und softwaretechnische Assets

"Assets" sind wertvolle Objekte oder Systeme, die notwendig sind, um Geschäftsziele zu erreichen, und können sowohl physische IT-Infrastruktur wie Server und Geräte als auch softwaretechnische Ressourcen wie Cloud-Dienste und Geschäftsanwendungen umfassen. Besonders kritische Assets, die als "Kronjuwelen" gelten, könnten bei Verlust oder Diebstahl das Unternehmen existenziell gefährden.

CHECKLIST

- FÜHREN SIE EIN VOLLSTÄNDIGES VERZEICHNIS ALLER IT-ASSETS
- BESTIMMEN SIE IHRE "KRONJUWELEN" (Z.B. GEISTIGES EIGENTUM, KUNDENDATEN).
- ÜBERPRÜFEN UND AKTUALISIEREN SIE DAS VERZEICHNIS REGELMÄSSIG
- PRIORISIEREN SIE DIESE KRONJUWELEN FÜR VERSTÄRKTE SCHUTZMASSNAHMEN

DAS WICHTIGSTE FÜR KMU IST, ZU WISSEN, WELCHE ASSETS BESONDERS SCHÜTZENSWERT SIND UND WELCHE "KRONJUWELEN" DEN GESCHÄFTSBETRIEB SICHERN.

IHR BENEFIT

- Frühe Schwachstellen-Erkennung
- Gezielte Schutzmaßnahmen
- Schutz wichtigster Ressourcen

Identifizieren

Klare Zuständigkeiten

Ein oder eine Informationssicherheitsbeauftragte*r erstellt die Sicherheitsrichtlinie, koordiniert alle Sicherheitsmaßnahmen und wird mit ausreichender Zeit und Ressourcen für diese Aufgabe ausgestattet. Sie sollte über grundlegendes Fachwissen in der Cybersicherheit verfügen und sich regelmäßig über neue Risiken informieren. Die Leitungsebene übernimmt die Gesamtverantwortung, und alle Mitarbeitenden tragen zur Sicherheit an ihrem Arbeitsplatz bei.

CHECKLIST

- BENENNUNG EINER VERANTWORTLICHEN PERSON
- FACHLICHE QUALIFIKATION UND WEITERBILDUNG
- FESTLEGUNG DER AUFGABEN UND BEFUGNISSE
- VERPFLICHTUNG DER MITARBEITENDEN ZUR INFORMATIONSSICHERHEIT

DIE ZUORDNUNG VON ZUSTÄNDIGKEITEN IN DER INFORMATIONSSICHERHEIT SORGT DAFÜR, DASS SICHERHEITSMASSNAHMEN KONSEQUENT UMGESETZT UND ÜBERWACHT WERDEN.

IHR BENEFIT

- Effizientere Umsetzung
- Stärkung der Sicherheitskultur
- Erhöhte Transparenz

Identifizieren

Lieferkettensicherheit

Lieferkettensicherheit bedeutet, Risiken in der gesamten Lieferkette eines Unternehmens zu erkennen und zu minimieren. Da KMU oft auf eine Vielzahl an Dienstleistern und Zulieferern angewiesen sind, ist es wichtig sicherzustellen, dass diese Partner hohe Sicherheitsstandards erfüllen und keine Schwachstellen in die Lieferkette einbringen.

CHECKLIST

- ENTWICKELN SIE KRITERIEN ZUR BEWERTUNG DER LIEFERANTEN-KRITIKALITÄT (Z. B. DATENSENSITIVITÄT, ZUGRIFFSLEVEL, GESCHÄFTLICHE BEDEUTUNG)
- DEFINIEREN SIE SPEZIFISCHE ANFORDERUNGEN FÜR LIEFERANTEN JE NACH KRITIKALITÄT (Z.B.SCHWACHSTELLEN-OFFENLEGUNG, REGELMÄSSIGE UPDATES, VORFALLMELDUNGEN)
- VERANKERN SIE ALLE ANFORDERUNGEN IN VERTRÄGEN UND SERVICE LEVEL AGREEMENTS (SLAS)

EIN SCHWACHPUNKT IN DER LIEFERKETTE KANN DAS GESAMTE UNTERNEHMEN GEFÄHRDEN - ES IST WICHTIG, DIESE RISIKEN ZU ERKENNEN.

IHR BENEFIT

- Schutz vor Betriebsstörungen
- Höhere Transparenz und Kontrolle
- Gezielte Schutzmaßnahmen

Schützen

Notfallplan

Ein Notfallplan legt fest, wie ein Unternehmen auf IT-Sicherheitsvorfälle reagieren soll. Klare Handlungsanweisungen und Verantwortlichkeiten werden definiert, um eine schnelle und wirksame Reaktion sicherzustellen und den Schaden zu minimieren. Durch regelmäßiges Testen wird sichergestellt, dass er in einem Ernstfall effizient funktioniert.

CHECKLIST

- DEFINIEREN SIE DIE ERSTE REAKTION BEI EINEM VORFALL
- BEREITEN SIE VORLAGEN FÜR DIE KOMMUNIKATION MIT WICHTIGEN STAKEHOLDERN VOR
- ERSTELLEN SIE EINE KONTAKTLISTE SAMT VERANTWORTLICHKEITEN
- BEWAHREN SIE DEN PLAN AN EINEM SICHEREN UND ZUGÄNGLICHEN ORT AUF
- LEGEN SIE ERSATZLÖSUNGEN UND ALTERNATIVE ARBEITSMETHODEN FEST
- ÜBEN SIE DEN NOTFALL

EIN NOTFALLPLAN GIBT KMU KLARE ABLÄUFE AN DIE HAND, UM IM KRISENFALL SCHNELL UND EFFEKTIV REAGIEREN ZU KÖNNEN.

IHR BENEFIT

- Schnelle Reaktionsfähigkeit
- Kontinuierliche Geschäftsfähigkeit
- Klare und koordinierte Kommunikation

Schützen

Sensibilisierung und Schulungen

Durch Sensibilisierung und Schulungen wird das Bewusstsein und Wissen der Mitarbeitenden über potenzielle Risiken erhöht. Mitarbeitende lernen wie sie Cyberbedrohungen wie Phishing, Malware oder Social Engineering frühzeitig erkennen und richtig darauf reagieren können. Regelmäßige Trainings und praktische Übungen stellen sicher, dass alle im Unternehmen über aktuelle Bedrohungen informiert sind und angemessen handeln können.

CHECKLIST

- **BIETEN SIE INTERAKTIVE E-LEARNING-MODULE ZU PASSWÖRTERN UND PHISHING AN**
- **FÜHREN SIE REGELMÄSSIGE PHISHING-SIMULATIONEN ZUR ERKENNUNG VON BEDROHUNGEN DURCH**
- **ORGANISIEREN SIE WORKSHOPS UND GRUPPENÜBUNGEN ZUM SICHEREN UMGANG MIT USB-STICKS UND E-MAILS**
- **PLANEN SIE JÄHRLICHE AUFFRISCHUNGEN UND SCHULUNGEN ZU NEUEN BEDROHUNGEN**

SCHULUNGEN SOLLTEN PRAXISNAH UND WIEDERHOLEND SEIN, UM DIE GRUNDFERTIGKEITEN IM UMGANG MIT SICHERHEITSFRAGEN ZU VERMITTELN.

IHR BENEFIT

- Höhere Akzeptanz
- Privater Mehrwert für Mitarbeitende
- Stärkere Sicherheitskultur

Schützen

Passwortmanagement

Sicheres Passwortmanagement verlangt starke, einzigartige Passwörter, die regelmäßig aktualisiert werden. In KMU sollen Richtlinien festgeschrieben sein, die Vorgaben zur Erstellung und Verwaltung von Passwörtern enthalten, einschließlich Anforderungen an Länge und Komplexität, wie auch Regelungen für die Nutzung von Passwort-Managern. Einfache Muster und persönliche Informationen sollten vermieden und besonders sensible Zugänge zusätzlich durch Multi-Faktor-Authentifizierung geschützt werden.

CHECKLIST

- **NUTZEN SIE STARKE, ZUFÄLLIGE PASSWÖRTER MIT GROSS-/KLEINBUCHSTABEN, ZAHLEN, SONDERZEICHEN**
- **VERWENDEN SIE FÜR JEDEN DIENST EIN EINZIGARTIGES PASSWORT; ÄNDERN SIE STANDARD-PASSWÖRTER**
- **HALTEN SIE PASSWÖRTER GEHEIM UND TEILEN SIE SIE NICHT ÜBER UNSICHERE KANÄLE**
- **SETZEN SIE EINEN PASSWORT-MANAGER MIT STARKEM MASTER-PASSWORT EIN**
- **SPEICHERN SIE PASSWÖRTER NICHT IM BROWSER**
- **AKTIVIEREN SIE ZUMINDEST ZWEI-FAKTOR-AUTHENTIFIZIERUNG**

PASSWORTSICHERHEIT IN PRAXISNAHEN SZENARIEN VERANSCHAULICHEN . SCHWACHE PASSWÖRTER SIND AUF ALLEN EBENEN EINE GROSSE HERAUSFORDERUNG.

IHR BENEFIT

- Kosteneffiziente Maßnahme mit umfassender Wirkung
- Sicheres Arbeiten
- Einfache Verwaltung

Schützen

Datensicherung

Eine regelmäßige und getestete Datensicherung schützt vor Datenverlust bei Ausfällen oder Cyberangriffen und ermöglichen eine schnelle Wiederaufnahme des Geschäftsbetriebs. Durch regelmäßige, automatisierte Backups können Daten strukturiert und sicher gespeichert werden. Dabei sollte festgelegt werden, welche Daten zu sichern sind, in welchen Abständen (z. B. täglich oder wöchentlich) dies geschehen soll und wer dafür verantwortlich ist.

CHECKLIST

- LEGEN SIE FEST, WELCHE DATEN REGELMÄSSIG GESICHERT WERDEN MÜSSEN
- FÜHREN SIE REGELMÄSSIGE UND AUTOMATISIERTE BACKUPS DURCH
- BEWAHREN SIE BACKUPS SICHER UND AN EINEM GETRENNTEN ORT AUF
- TESTEN SIE DIE WIEDERHERSTELLUNG IHRER DATEN REGELMÄSSIG, UM SICHERZUSTELLEN, DASS BACKUPS VOLLSTÄNDIG UND NUTZBAR SIND
- STELLEN SIE SICHER, DASS NUR BEFUGTE PERSONEN ZUGRIFF AUF BACKUP-DATENTRÄGER HABEN

“ANGRIFFE ZIELEN OFT DARAUF AB, UNTERNEHMENSDATEN UND BACKUPS ZU VERSCHLÜSSELN – KMU OHNE GETESTETE BACKUP-SZENARIEN STEHEN DANN SCHNELL TAGELANG STILL.”

IHR BENEFIT

- Sicherung der Geschäftskontinuität
- Minimierung von Ausfallzeiten
- Reduzierung finanzieller Verluste

Schützen

Identitäts- und Zugriffsmanagement

Ein effektives Identitäts- und Zugriffsmanagement (IAM) stellt sicher, dass nur berechtigte Personen und Prozesse auf sensible Systeme und Daten zugreifen können. Das Ziel ist, unbefugten Zugriff zu verhindern und sicherzustellen, dass jede*r Mitarbeitende nur auf die Daten und Systeme zugreift, die sie/er tatsächlich benötigt.

CHECKLIST

- DEFINIEREN SIE ZUGRIFFSRECHTE
- DOKUMENTIEREN SIE ALLE BENUTZERROLLEN UND ZUGRIFFSRECHTE
- ÜBERPRÜFEN SIE MINDESTENS JÄHRLICH ALLE BERECHTIGUNGEN UND INAKTIVE BENUTZERKONTEN
- DEAKTIVIEREN ODER LÖSCHEN SIE UMGEHEND DIE KENNUNG UND RECHTE AUSGESCHIEDENER MITARBEITENDER
- ERTEILEN SIE NUR NOTWENDIGE ZUGRIFFS-RECHTE GEMÄSS DEM „NEED-TO-KNOW-PRINZIP“

MIT IAM SORGEN UNTERNEHMEN DAFÜR, DASS NUR BERECHTIGTE PERSONEN AUF WICHTIGE SYSTEME UND DATEN ZUGREIFEN KÖNNEN.

IHR BENEFIT

- Erhöhte Daten-sicherheit
- Klare Verantwortlich-keiten
- Effiziente Verwaltung und Transparenz

Schützen

Informations-sicherheitsrichtlinie

Eine Informationssicherheitsrichtlinie umfasst alle relevanten Aspekte des Umgangs mit IT-Systemen, Netzwerkzugängen und sensiblen Daten. Sie legt spezifische Regeln und Verantwortlichkeiten fest, die von den Mitarbeitenden eingehalten werden müssen, um das Unternehmen und seine IT-Infrastruktur vor Sicherheitsrisiken und rechtlichen Konsequenzen zu schützen.

CHECKLIST

- ERLAUBEN SIE NUR FREIGEGEBENE HARDWARE UND LIZENZIERTE SOFTWARE
- DEFINIEREN SIE DEN UMGANG MIT PERSONENBEZOGENEN UND VERTRAULICHEN DATEN
- ENTWICKELN SIE SICHERE PASSWORTVORGABEN
- ENTWICKELN SIE KLARE REGELN ZUR VERSCHLÜSSELUNG VERTRAULICHER INFORMATIONEN
- ERSTELLEN SIE REGELN FÜR DIE SICHERE NUTZUNG MOBILER GERÄTE
- INFORMIEREN SIE MITARBEITENDE ÜBER FOLGEN BEI SICHERHEITSVERSTÖSSEN

DIE RICHTLINIE MUSS VON DER GESCHÄFTSFÜHRUNG FREIGEGEBEN UND FÜR ALLE MITARBEITER VERFÜGBAR SEIN.

IHR BENEFIT

- Schutz sensibler Daten
- Transparenz
- Klarheit und Verantwortlichkeit

Schützen

Software-Updates und Patches

Software-Updates und Patches sichern IT-Sicherheit und Systemstabilität. Während Updates oft neue Funktionen oder Leistungsverbesserungen einführen, sind Patches speziell darauf ausgelegt, Schwachstellen und Sicherheitslücken zu beheben, die Angreifer ausnutzen könnten. Ein strukturiertes Patch-Management stellt sicher, dass alle Systeme, Anwendungen und Geräte regelmäßig aktualisiert werden, um Schutz vor den neuesten Bedrohungen zu gewährleisten.

CHECKLIST

- **ERMITTELN SIE GERÄTE, DIE MANUELLE UPDATES ERFORDERN, UND PLANEN SIE DIESE EIN**
- **TESTEN SIE UPDATES ZUNÄCHST AUF EINEM EINZELNEN GERÄT, BEVOR SIE SIE UNTERNEHMENSWEIT EINSPIELEN**
- **HALTEN SIE INSBESONDERE BETRIEBSSYSTEME UND WICHTIGE ANWENDUNGEN STETS AKTUELL**
- **GRENZEN SIE NICHT MEHR UNTERSTÜTZTE SOFTWARE VOM NETZWERK AB ODER ERSETZEN SIE DIESE**
- **AKTIVIEREN SIE AUTOMATISCHE UPDATES**

FÜR KMU IST ES WICHTIG, KRITISCHE PATCHES ZEITNAH ZU INSTALLIEREN.

IHR BENEFIT

- Erhöhte Systemstabilität und Performance
- Reduzierte Risiken durch veraltete Software

Schützen

Netzwerksegmentierung

Das Unternehmensnetzwerk wird in kleinere, isolierte Bereiche unterteilt. Dies hilft, den Datenverkehr zu kontrollieren und sensible Informationen besser zu schützen. Durch die Segmentierung können KMU den Zugang zu bestimmten Bereichen einschränken und gewährleisten, dass nur berechtigte Nutzer oder Anwendungen auf bestimmte Netzwerksegmente zugreifen können.

CHECKLIST

- BESTIMMEN SIE SEGMENTE MIT ÄHNLICHEN SICHERHEITS-ANFORDERUNGEN
- LEGEN SIE ZUGRIFFSRICHTLINIEN FÜR JEDES SEGMENT FEST
- RICHTEN SIE FIREWALLS ZWISCHEN DEN SEGMENTEN EIN
- NUTZEN SIE VIRTUAL PRIVATE NETWORKS (VPN) FÜR DIE VERBINDUNG ZWISCHEN GETRENNTEN SEGMENTEN UND FÜR DEN SICHEREN REMOTE-ZUGRIFF
- ÜBERWACHEN SIE DEN DATENFLUSS ZWISCHEN DEN SEGMENTEN

NETZWERKSEGMENTIERUNG VERHINDERT DIE AUSBREITUNG VON BEDROHUNGEN. WIRD EIN SEGMENT ANGEGRIFFEN, BLEIBEN DIE ANDEREN BEREICHE GESCHÜTZT.

IHR BENEFIT

- Begrenzung von Sicherheitsvorfällen
- Erhöhte Netzwerkleistung
- Verbesserte Zugriffssteuerung
- Erleichterte Sicherheitsüberwachung

Erkennen

Virenschutz

Computerviren sind Programme, die sich oft unbemerkt verbreiten und Dateien oder Systeme schädigen können. Viren verbreiten sich heute meist über das Internet und E-Mails. Besonders Anhänge in E-Mails oder Downloads aus unbekannten Quellen stellen eine Gefahr dar.

CHECKLIST

- INSTALLIEREN SIE EINE ZENTRAL VERWALTETE ANTI-VIRUS-LÖSUNG AUF ALLEN UNTERNEHMENSGERÄTEN
- PLANEN SIE AUTOMATISCHE UPDATES UND TÄGLICHE VIRENSCANS FÜR ALLE GERÄTE
- SPERREN SIE RISKANTE DATEIEN UND INHALTE; BLOCKIEREN SIE POTENZIELL SCHÄDLICHE DATEIFORMATE UND AKTIVE INHALTE
- VERWENDEN SIE E-MAIL-GATEWAYS ZUR PRÜFUNG DES MAILSVERKEHRS AUF VIREN UND MALWARE
- VERWENDEN SIE AUSSCHLIESSLICH LIZENSIERTE SOFTWARE

ANTIVIRUS-TOOLS ERKENNEN DAS VERHALTEN VON SCHADPROGRAMMEN UND BLOCKIEREN ENTSPRECHENDE BEDROHUNGEN.

IHR BENEFIT

- Schutz vor Datenverlust
- Kontinuierliche Geschäftsfähigkeit
- Sicherung der Systemintegrität

Erkennen

Protokollierung und Monitoring

Die Protokollierung und das Monitoring von IT-Systemen ermöglichen Sicherheitsvorfälle zu erkennen und nachvollziehen zu können. Eine klare Zuweisung der Verantwortlichkeiten für die Auswertung der Protokolle, idealerweise im Vier-Augen-Prinzip, trägt zur Erhöhung der IT-Sicherheit bei.

CHECKLIST

- FÜHREN SIE SYSTEMATISCHE PROTOKOLLIERUNG FÜR SICHERHEITSRELEVANTE AKTIVITÄTEN EIN
- DEFINIEREN UND DOKUMENTIEREN SIE ZUGRIFFSRECHTE
- SPEICHERN SIE PROTOKOLLE MANIPULATIONSSICHER
- ÜBERPRÜFEN SIE PROTOKOLLE AUF UNREGELMÄSSIGE AKTIVITÄTEN, WIE VERDÄCHTIGE ANMELDUNGEN
- LEGEN SIE KLARE VERANTWORTLICHKEITEN FÜR DIE AUSWERTUNG UND DAS MONITORING FEST

SICHERHEITSRELEVANTE AKTIVITÄTEN UMFASSEN Z.B. BENUTZERANMELDUNGEN, ÄNDERUNGEN AN ZUGRIFFSRECHTEN UND SICHERHEITSKRITISCHE SYSTEMEINGRIFFE.

IHR BENEFIT

- Frühzeitige Bedrohungserkennung
- Verbesserte Notfallbereitschaft
- Erhöhte Nachvollziehbarkeit

Erkennen

Penetrationstests

Penetrationstests sind gezielte Sicherheitsüberprüfungen, bei denen IT-Infrastrukturen auf mögliche Schwachstellen hin untersucht werden, indem reale Angriffe simuliert werden. Ziel ist es, Lücken in Netzwerken, Anwendungen und Systemen frühzeitig zu identifizieren und zu schließen, bevor sie von Angreifern ausgenutzt werden können. Dabei reichen die Methoden von technischen Angriffen über das Netzwerk bis hin zu Social Engineering, um die menschliche Seite der IT-Sicherheit zu testen.

CHECKLIST

- FÜHREN SIE MINDESTENS JÄHRLICH PENETRATIONS-TESTS DURCH
- DEFINIEREN SIE TESTUMFANG UND ZIELE
- LEGEN SIE DIE AGGRESSIVITÄTSSTUFE UND TESTMETHODIK FEST
- VARIIEREN SIE DEN ANBIETER, UM VIELFÄLTIGERE SICHERHEITSANALYSEN ZU ERHALTEN
- BEHEBEN SIE ERKANNTE SCHWACHSTELLEN ZÜGIG
- INFORMIEREN SIE DIE MITARBEITENDEN ÜBER DIE TESTERGEBNISSE

EIN ÜBERBLICK ÜBER DIE GENERELLEN SCHWACHSTELLEN DER INFRASTRUKTUR BRINGT OFT MEHR ALS DIE DETAILLIERTE PRÜFUNG EINZELNER SYSTEME.

IHR BENEFIT

- Früherkennung von Schwachstellen
- Verbesserte Notfallbereitschaft
- Objektive Schwachstellenanalyse

Reagieren

Isolierung und Dokumentation

Die sofortige Trennung infizierter Geräte vom Netzwerk verhindert, dass sich der Angriff weiter ausbreitet. Parallel zur Isolierung ist eine detaillierte Dokumentation des Vorfalls erforderlich. Diese bildet die Grundlage für forensische Analysen und mögliche strafrechtliche Untersuchungen und hilft dem Unternehmen, den Ursprung und das Ausmaß des Angriffs besser zu verstehen und zu beheben.

CHECKLIST

- IDENTIFIZIEREN SIE ALLE BETROFFENEN SYSTEME
- TRENNEN SIE BETROFFENE SYSTEME VOM INTERNEN NETZWERK UND VOM INTERNET
- VERMEIDEN SIE DIE ANMELDUNG MIT ADMIN-RECHTEN AUF POTENZIELL INFIZIERTEN SYSTEMEN
- BEFRAGEN SIE BETROFFENE NUTZER ZU BEOBACHTUNGEN
- SICHERN SIE PROTOKOLLE, LOG-DATEIEN, NOTIZEN UND BILDSCHIRMFOTOS, BEVOR SIE MIT DER ANALYSE BEGINNEN
- PRÜFEN SIE, OB SIE ÜBER AKTUELLE, SAUBERE, INTEGRE BACKUPS VERFÜGEN

NUR EINE VOLLSTÄNDIGE ERFASSUNG UND BESEITIGUNG DER KOMPROMITTIERUNG ERMÖGLICHT EINEN SICHEREN WIEDERANLAUF DER GESCHÄFTSPROZESSE.

IHR BENEFIT

- Begrenzung von Sicherheitsvorfällen
- Verbesserte Ursachenanalyse
- Erhöhte Nachvollziehbarkeit

Reagieren

Interne und externe Kommunikation

Bei einem Cyberangriff bestehen in Österreich wichtige Meldepflichten. Die Datenschutzbehörde muss bei Datenschutzverletzungen mit Risiko für betroffene Personen innerhalb von 72 Stunden informiert werden. Das nationale Computer Emergency Response Team dient als zentrale Meldestelle für Cybervorfälle und nimmt auch freiwillige Meldungen entgegen. Zudem sind Cyberdelikte der Polizei oder Staatsanwaltschaft zu melden, was oft eine Voraussetzung für Versicherungsleistungen bei Erpressung darstellt.

CHECKLIST

- LEGEN SIE EINE ZUSTÄNDIGE PERSON FÜR KOMMUNIKATION FEST
- INFORMIEREN SIE ALLE RELEVANTEN INTERNEN ANSPRECHPARTNER
- PRÜFEN SIE MELDEPFLICHTEN AN DATENSCHUTZBEHÖRDEN
- STELLEN SIE SICHER, DASS ALLE VERTRAGLICHEN INFORMATIONSPFLICHTEN GEGENÜBER PARTNERN EINGEHALTEN WERDEN
- ERWÄGEN SIE EINE STRAFANZEIGE BEI DER POLIZEI UND EINE MELDUNG BEI CERT.AT

FREIWILLIGE MELDUNGEN HELFEN, ANDERE KMU ÜBER AKTUELLE BEDROHUNGEN ZU INFORMIEREN UND ERHÖHEN SO DIE KOLLEKTIVE CYBERSICHERHEIT.

IHR BENEFIT

- Sicherstellung der Compliance
- Erhöhte Transparenz und Vertrauen
- Unterstützung durch externe Stellen

Wieder-herstellen

Systembereinigung

Nach einem Cyberangriff müssen KMU sicherstellen, dass alle Schadsoftware vollständig entfernt wird, um eine gefahrlose Nutzung wiederherzustellen. Dies kann durch gezieltes Entfernen von Schadprogrammen oder durch eine Neuinstallation des Betriebssystems erfolgen, abhängig von der Genauigkeit der Vorfallanalyse. Die Entscheidung, welche Methode anzuwenden ist, sollte gemeinsam mit einem Notfall-Team und der Geschäftsführung getroffen werden.

CHECKLIST

- **ENTFERNEN SIE ALLE KOMPROMITTIERTEN DATEIEN UND BLOCKIEREN SIE ZUGANGSPUNKTE**
- **ÜBERPRÜFEN SIE BACKUPS GRÜNDLICH AUF MANIPULATIONEN, BEVOR SIE DIESE WIEDERHERSTELLEN**
- **INSTALLIEREN SIE ALLE VERFÜGBAREN SICHERHEITS-UPDATES UND PATCHES**
- **HÄRTEN SIE DIE SYSTEME UND RICHTEN SIE EINE KONTINUIERLICHE ÜBERWACHUNG ZUR PRÄVENTION EIN**

DIE BEREINIGUNG DES SCHADPROGRAMMS IST NUR DANN SINNVOLL, WENN DER ANGRIFFSWEG VOLLSTÄNDIG NACHVOLLZOGEN WURDE; ANDERNFALLS IST EINE NEUINSTALLATION DES SYSTEMS EMPFEHLENSWERT.

IHR BENEFIT

- Sicherstellung der Datenintegrität
- Verhindern der Wiederinfektion
- Verbesserte Prävention

Wieder-
herstellen

Wiederherstellen und optimieren

Nach einem Cyberangriff ist es erforderlich, die betroffenen IT-Systeme sicher und in geordneter Reihenfolge in den Produktivbetrieb zu überführen. Falls während des Vorfalls ein Notbetrieb eingerichtet wurde, sollte dieser schrittweise zurückgeführt werden. Ein Abschlussgespräch mit allen Beteiligten ermöglicht eine finale Auswertung des Vorfalls, sodass Abläufe optimiert und Maßnahmen für zukünftige IT-Sicherheitsvorfälle ergriffen werden können.

CHECKLIST

- **BESTIMMEN SIE EINE REIHENFOLGE FÜR DIE WIEDERINBETRIEBNAHME**
- **STELLEN SIE SICHER, DASS SYSTEME MIT ABHÄNGIGKEITEN IN DER KORREKTEN REIHENFOLGE HOCHGEFAHREN WERDEN**
- **HALTEN SIE EIN ABSCHLUSSGESPRÄCH**
- **IDENTIFIZIEREN SIE SCHWACHSTELLEN IN DEN REAKTIONSPROZESSEN**
- **PLANEN SIE GEZIELTE SCHULUNGS- UND SENSIBILISIERUNGSMASSNAHMEN**

“WIEDERHERGESTELLTE SYSTEME SOLLTEN INTENSIV ÜBERWACHT WERDEN, UM STABILITÄT SICHERZUSTELLEN UND WEITERE BEDROHUNGEN AUSZUSCHLIESSEN.”

IHR BENEFIT

- Optimierung der Abläufe
- Behebung von Schwachstellen
- Reduzierung des Ausfallrisikos

ExpertInnen-Tipps und weitere Informationen

TIPPS

DER EXPERTINNEN

- Starten Sie mit kleinen Schritten in die Cybersecurity und lassen Sie sich nicht von der Komplexität abschrecken!
- Entwickeln Sie einen realistischen Plan, um Ihre Sicherheitsmaßnahmen systematisch aufzubauen!
- Greifen Sie auf Unterstützung und bestehende und kostenlose Angebote zurück!

MEHR INFORMATIONEN FINDEN SIE HIER

- WKO it-safe.at
- KSÖ Cyber Risk Rating
- ASIT Cybersecurity Awareness Playbook
- BSI leichter Einstieg
- ENISA Cybersecurity Guide for SMEs

Fördermöglichkeiten

Förderprogramm	Kurzbeschreibung	Einreichfrist
Cyber Security Schecks 2024	Unterstützung österreichischer KMU, die Sicherheit und Cyberabwehrfähigkeit ihrer Netz- und Informationssysteme zu stärken. Gefördert werden Kosten für Technologien sowie für Beratungsleistungen.	Laufende Einreichung (bis längstens 29.11.2024)
Skills Schecks 2024	Mit den Skills Schecks soll Unternehmen mit einer Niederlassung in Österreich ein niederschwelliger Zugang zu einem Zuschuss für Qualifizierungsmaßnahmen ermöglicht werden. Die Weiterbildung muss inhaltlich dem Aufbau digitaler und/oder ökologisch nachhaltiger Kompetenzen dienen.	Laufende Einreichung (bis längstens 28.02.2025)
aws - KMU.DIGITAL	KMU.DIGITAL fördert die individuelle Beratung österreichischer Klein- und Mittelbetriebe (KMU) durch zertifizierte Expert:innen zu den Themen Geschäftsmodelle und Prozesse (inkl. Ressourcenoptimierung), E-Commerce und Online-Marketing, IT-und Cybersecurity sowie Digitale Verwaltung. Gefördert wird anschließend auch die Umsetzung Ihrer Digitalisierungsprojekte mit Hilfe von Neuinvestitionen.	Laufende Erinreichung
Steirische Wirtschaftsförderung	Gefördert werden Maßnahmen, die die IT-Sicherheit erhöhen, etwa zum Schutz von Daten, Netzwerken, Computersystemen, IoT-Komponenten sowie Hard- und Software. Mögliche Projekte können Risikoanalysen, Beratungen, Weiterbildungen und Trainings, die Einführung von Sicherheitsmanagement-Systemen oder Investitionen in neue Hard- oder Software sein.	Laufende Erinreichung
SCHIG mbH – Kompetenzzentrum für Eisenbahnwesen	Mit der Logistikförderung sollen Maßnahmen zur Förderung der Nachhaltigkeit in der Logistik gesetzt werden. Unter anderem werden Schwerpunkte wie Supply Chain Cyber Risk Management, Lieferkettenoptimierung, Nachhaltigkeitsberichterstattung von Unternehmen oder die Optimierung des Produktionsfaktors Energie gefördert. Gefördert werden Durchführbarkeitsstudien sowie Umsetzungspiloten und -begleitung.	Laufende Erinreichung

Stand 2024

Bundesministerium für Finanzen
Radetzkystraße 2, 1030 Wien
+43 (0)1 51433-0