Whitepaper

Cyber Security

Cyberangriffe: Unternehmen aller Größen im Visier der Hacker

Warum der KI-Boom die Anforderungen an **Cyber Security** noch erhöht, und wie Unternehmen ein handhabbares Schutzkonzept etablieren.

vodafone business

Together we can

Die Bedrohungen und Schäden durch Cyberattacken nehmen signifikant zu

21 Tage

war die durchschnittliche Downtime nach einem Angriff.
(Seite 7)

3,9 Mio. €

betrug der durchschnittliche Schaden durch einen Cyberangriff.
(Seite 7)

206 Mrd. €

ist die Summe der Schäden für die deutsche Wirtschaft durch Cybervorfälle im Jahr 2023.
(Seite 4)

59%

der befragten Unternehmen aus 14 Ländern waren 2023 von Erpressungsversuchen durch Ransomware betroffen.
(Seite 4)

5x

so hoch wie noch vor 12 Monaten waren 2023 die Lösegeld-Forderungen nach Ransomware-Attacken.
(Seite 4)

Vorwort

Die Bedrohungslage durch Cyberattacken ist in den letzten Jahren gestiegen – nicht zuletzt durch neue Angriffstechniken mithilfe von KI. Hinzu kommen neue gesetzliche Anforderungen an Cyber-Resilienz.

Die Zahlen, Daten und Fakten zu Cyberattacken machen deutlich: Kein Unternehmen – **egal wie groß oder klein und egal, in welcher Branche** es tätig ist – sollte die Augen vor dieser Bedrohung verschließen.

Ein Grund dafür ist, dass die möglichen **Einfallstore für Cyberbedrohungen zugenommen** haben: Remote Work, digitaler Austausch mit Kund:innen und Geschäftspartner:innen sowie eine Vermischung privat und beruflich genutzter IT-Geräte. **Künstliche Intelligenz** lässt Phishing-Mails realistischer aussehen und liefert sogar überzeugende Fälschungen von Stimmen am Telefon.

Auch die **geopolitische Lage** spielt eine Rolle. So ist die Zahl an Hackerangriffen mit vermutetem staatlichem Hintergrund gestiegen. Gleichzeitig ist eine **Professionalisierung der Angriffe** zu beobachten – so ermöglichen „Ransomware as a Service"-Pakete Cyberangriffe fast ohne Vorwissen.

Dabei sind sich Unternehmen dieser Gefahren zwar bewusst – oft wird aber angenommen, dass man aufgrund seiner Größe oder seines Tätigkeitsfeldes für Cyberkriminelle nicht oder weniger interessant sei. Dabei sind die **potenziellen Schäden gewaltig**.

Hinzu kommt, dass die **gesetzlichen Anforderungen an Unternehmen gestiegen** sind, sich gegen Cyberangriffe zu schützen – etwa durch die Umsetzung der EU-Richtlinie NIS2, die weitreichende technische, organisatorische und operative Maßnahmen vorschreibt.

Deshalb ist ein **starkes, aber gleichzeitig leicht handhabbares Schutzkonzept** unverzichtbar. Wie Unternehmen dies erreichen, zeigen wir Ihnen auf den folgenden Seiten.

Inhaltsverzeichnis

0 Zahlen, Daten und Fakten zu Cyberattacken und den verursachten Schäden 2

1 Wirklich jedes Unternehmen ist durch Cyberangriffe bedroht 4

2 Typische Einfallstore und Angriffsmethoden 5

3 Die Folgen und Kosten von Cyberangriffen sind enorm 7

4 Unternehmenspflichten bezüglich Sicherheitsrisiken verschärfen sich mit NIS2 8

5 Maßnahmen für höhere Cyber-Sicherheit: So gehen Unternehmen am besten vor 9

6 Vodafone Cyber Security Services: Sicherheitslösungen aus einer Hand 13

7 Glossar: Malware, Ransomware & Co – was steckt hinter diesen Begriffen? 14

1 Wirklich jedes Unternehmen ist durch Cyberangriffe bedroht

In ihrem „Risk Barometer 2024“ [1] führt die Allianz-Versicherungsgruppe **Cybervorfälle als höchstes Einzelrisiko** auf. Die Einordnung basiert auf der Befragung von mehr als 3.300 Risikomanagement-Expert:innen aus 92 Ländern. Mit **44 Prozent der benannten Risiken liegt Cyberkriminalität auf Platz 1 der Top-10-Risiken für Unternehmen** – noch vor Naturkatastrophen, Fachkräftemangel oder dem Klimawandel.

Auf einen der Gründe weist das **Bundesministerium des Innern und für Heimat** (BMI) hin: Neben Politik und Behörden unterliegt auch die Wirtschaft in wachsendem Maße zielgerichteten Cyberangriffen. In der zunehmend angespannten geopolitischen Lage sind Angriffe zudem auch Bestandteil von Spionage- oder Sabotage-Aktivitäten. Daher ist die Frage längst nicht mehr, **ob ein Unternehmen Ziel eines Cyberangriffs** wird, sondern **nur noch, wann**. Dieses Risiko betrifft **Unternehmen aller Größen.**

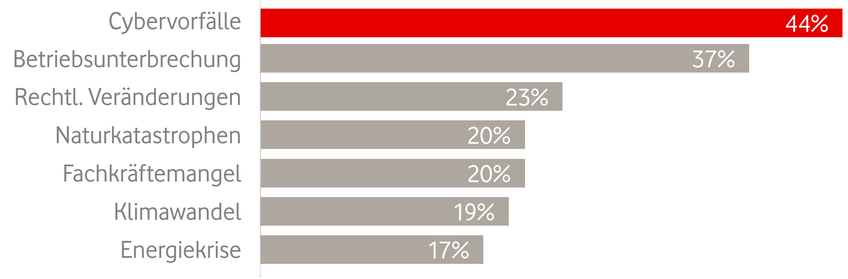
Laut dem **Branchenverband Bitkom** lag der **Gesamtschaden durch Cybervorfälle** für die deutsche Wirtschaft im Jahr 2023 bei **206 Milliarden Euro** (Studie „Wirtschaftsschutz 2023).

Das Bundeskriminalamt verzeichnete in seinem **Bundeslagebild Cybercrime 2023** **134.407 Cyberstraftaten in Deutschland**. Dabei steigt insbesondere die Zahl der sogenannten **Auslandstaten** (Cyberstraftaten, die zu Schäden in Deutschland führen, jedoch aus dem Ausland verübt werden) seit ihrer Erfassung im Jahr 2020 kontinuierlich an – **2023 um 28% gegenüber dem Vorjahr**.

Die Zunahme der Risiken durch Spionage und Sabotage hat andere Bedrohungen jedoch keineswegs schrumpfen lassen. Dies gilt insbesondere für **Ransomware:** Das unterstreicht etwa der im Auftrag des Softwarehauses Sophos vom Marktforschungsunternehmen Vanson Bourne unabhängig erhobene Report **The State of Ransomware 2024** [2]. Er zeigt auf, dass die Zahl betroffener Unternehmen zwar leicht zurückging (2024: 59% der befragten Unternehmen, 2023 und 2022: 66%), dafür die Folgen jedoch gestiegen sind: So **nahmen die Kosten für die Wiederherstellung von Daten um 50% zu**. Wenn ein **Lösegeld** gezahlt wurde, war es **fünfmal so hoch wie noch vor 12 Monaten**.

Allianz: Cybervorfälle liegen auf Platz 1 der Top 10 Geschäftsrisiken weltweit in 2024

Basierend auf den Antworten von mehr als 3.300 Risikomanagement-Expert:innen aus 92 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, weil jeweils bis zu drei Risiken ausgewählt werden konnten.



[1] Quelle: Allianz Global Corporate & Specialty „Risk Barometer 2024“

Die Folgen von Ransomware-Angriffen steigen

Im Januar und Februar 2024 wurden 5.000 IT-Entscheider:innen aus 14 Ländern in EMEA, Nord- und Südamerika und Asien-Pazifik befragt. An der Umfrage nahmen Unternehmen und Organisationen mit 100 bis 5.000 Mitarbeitenden teil.

59%
der Befragten waren im letzten Jahr von Ransomware-Angriffen betroffen

70%
der Angriffe führten zu Datenverschlüsselung

5x
so hohe Lösegeld-Forderungen wie noch vor 12 Monaten

32%
der Angriffe begannen mit einer ungepatchten Schwachstelle

[2] Quelle: Sophos, „The State of Ransomware 2024“

2 Typische Einfallstore und Angriffsmethoden

Der Mensch ist ein wesentlicher Erfolgsfaktor bei der Abwehr von Cyberangriffen, aber gleichzeitig auch eine der zentralen Schwachstellen.

Social Engineering – der Mensch als häufig genutztes Einfallstor

Ein bevorzugtes Werkzeug für Angriffe über das Einfallstor „Mensch" ist **„Social Engineering"**. Gemeint ist das Ausspionieren von Mitarbeitenden und Umgehen von Sicherheitsmaßnahmen mit „sozialen Techniken". Dazu zählen **Phishing-Mails** (siehe Glossar Seite 14) ebenso wie etwa ein Anruf, dessen Urheber:in sich als Mitarbeiter:in der firmeneigenen IT-Abteilung ausgibt. Immer ist das Ziel, das Opfer zur Preisgabe vertraulicher Informationen oder zum Aufweichen von Schutzoptionen zu verleiten.

Ein vergleichsweise neuer Trend ist dabei eine **zunehmende Rolle von Künstlicher Intelligenz** im Kontext von Cyberangriffen. Sie hilft Kriminellen, früher vermeintlich sichere Erkennungszeichen wie etwa sprachliche Fehler zu vermeiden. **Deepfakes bei Bildern, Sprache und Videos** machen es immer schwieriger, legitime von boshaften Inhalten zu unterscheiden.

Dies betrifft Mitarbeitende übrigens gleichermaßen im beruflichen wie auch im privaten Umfeld. Der **Branchenverband Bitkom** berichtet [1], dass **67 Prozent der deutschen Internet-Nutzer:innen im Jahr 2023 in Berührung mit versuchten Cyberangriffen gekommen sind**.

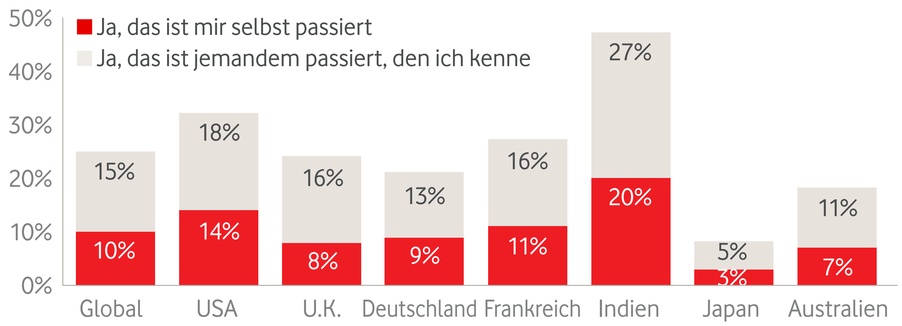
Ausnutzung technischer Schwachstellen

Hinzu kommen technische Angriffsmethoden (in der Fachsprache: **„Angriffsvektoren"**) – etwa bekannte **Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen** oder Unterwanderungsmethoden wie DDoS- oder „Man in the Middle"-Attacken (siehe Glossar Seite 14). Eine **technische Schutzebene** – von Malwareschutz bis zu Sicherheitsüberwachung – ist deshalb ebenfalls **unverzichtbar**.

Häufig kombinieren Angriffe auch beide Varianten. Daher muss das Schutzkonzept ebenfalls auf verschiedenen Ebenen wirken und sich nicht etwa allein auf technische Maßnahmen verlassen, sondern auch den Faktor Mensch mit einbeziehen (siehe Seite 10ff).

Bedrohungen durch Künstliche Intelligenz

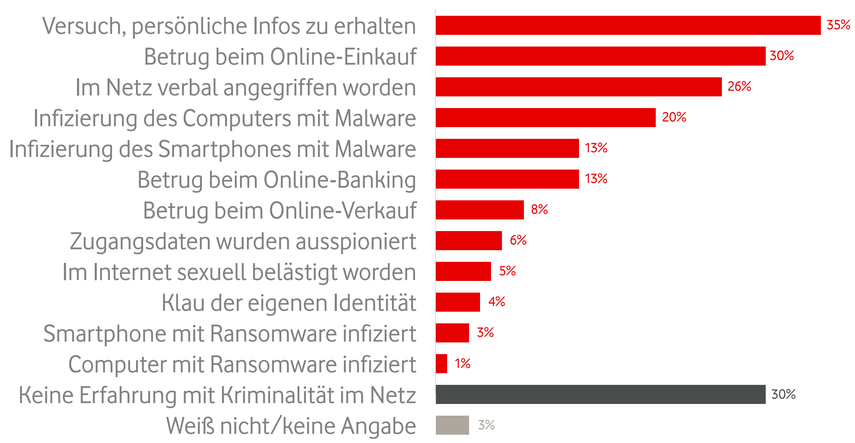
Beispiel KI-generierte Sprach-Fälschungen: Haben Sie oder jemand, den Sie kennen, bereits einen Angriffsversuch mit Fake-Sprache (zum Beispiel gefälschter Anruf oder gefäschte Sprachnachricht) erlebt?



Quelle: McAfee Cybersecurity Artificial Intelligence Report, Mai 2023

Cyber Crime: 7 von 10 Nutzer:innen betroffen

Welche der folgenden Erfahrungen mit kriminellen Vorfällen haben Sie persönlich in den vergangenen 12 Monaten im Internet gemacht?



[1] Quelle: Bitkom Research 2023

2 „Ransomware as a Service“ macht Cyberattacken zum Massen-Phänomen

Ein Grund für die massive Zunahme von Angriffen (und deren Erfolge) ist, dass die dafür erforderliche Expertise massiv gesunken ist. Mittlerweile werden im Darknet **schlüsselfertige „Ransomware-Kits“** angeboten, die Angreifer:innen nur noch für ihre Zwecke anpassen müssen. Die erwirtschafteten „Erlöse“ werden als **Revenue-Share-Modell** zwischen Angreifer:in sowie Anbieter:in des Ransomware-Kits aufgeteilt.

Die Urheber:innen solcher schlüsselfertigen Lösungen haben sich **massiv professionalisiert**: Sie betreiben eigene Entwicklungsabteilungen sowie einen „Kundenservice“ für Cyberkriminelle, der bei der Planung und Durchführung von Angriffen hilft. Affiliates werden trainiert und müssen bei ihrer „Bewerbung“ auch ihre technischen Fähigkeiten unter Beweis stellen

Die „Bemessung“ des erpressten Lösegelds liegt meist **im unteren einstelligen Prozentbereich, bezogen auf den Jahresumsatz** des Unternehmens. Dazu kommt häufig noch die Drohung, **sensible Daten zu veröffentlichen**. Dies führt zu Haftungsrisiken und möglichen Strafzahlungen (siehe Seite 8) sowie noch größeren Imageschäden.

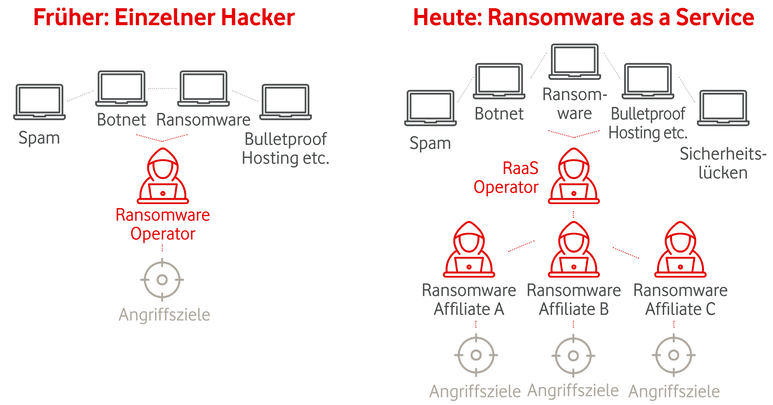
Wie professionell Cyberkriminelle vorgehen, zeigt der typische Ablauf einer Ransomware-Attacke: Zur Vorbereitung oder **Aufklärung** untersuchen Angreifende das Firmennetz auf Schwachstellen. Die Informationssammlung nutzt sogar Geheimdienst-Methoden („OSINT“ – Open Source Intelligence).

Der **erste Zugang** ins Firmennetz nutzt „Social Engineering“ (auf echten oder vorgegebenen sozialen Kontakten basierende Angriffe) ebenso wie technische Schwachstellen. Im nächsten Schritt wird die dauerhafte Kontrolle („**Command & Control**“) über das Firmennetz etabliert – zum Beispiel durch Installation weiterer Malware, die Fernzugriff auf das Netzwerk, die Ausführung weiterer Befehle ermöglicht und versucht, Benutzerrechte auszuweiten („**Privilege Escalation**“) .

Verteidigungsmaßnahmen werden **umgangen**, um die eigene Präsenz dauerhaft zu verankern („**Persistenz**“). In Firmennetzen folgt die **gezielte Verbreitung der Malware auch auf andere Systeme** (Fachbegriff: „**Lateral Movement**“ – Bewegung in die Breite). Am Ende stehen etwa **die Verschlüsselung von Daten** und/oder **Exfiltration und Abfluss sensibler Daten**.

Ransomware as a Service (RaaS)

Cyberangriffe wie Ransomware sind heute ein professionelles und arbeitsteiliges Geschäft. Affiliate-Modelle erhöhen das Potenzial für erfolgreiche Angriffe.



Ablauf einer Ransomware-Attacke

3 Die Folgen und Kosten von Cyberangriffen sind enorm

Cyberattacken führen zu **Betriebsunterbrechungen und Verzögerungen** – die durchschnittliche Downtime beträgt 21 Tage[2]. Dies kann zur Konsequenz haben, dass sich Projekte gar nicht mehr durchführen und Kundenaufträge nicht oder nur noch eingeschränkt beziehungsweise mit deutlichem Zeitverzug realisieren lassen. Von noch größerer Tragweite können negative Einflüsse wie ein nachhaltiger Imageverlust des Unternehmens und damit einhergehendem Vertrauensverlust auf Kund:innenseite sein. Dies geht mit **erheblichen Kosten** und somit **finanziellen Verlusten** einher.

Zu eventuellen **Lösegeldzahlungen kommen immense operative Kosten** für die Wiederherstellung von verlorenen oder verschlüsselten Daten beziehungsweise die Säuberung oder teilweise komplett neue Bereitstellung der IT-Systeme.

Die Kosten durch Cyberattacken sind hoch – und sie steigen kontinuierlich.

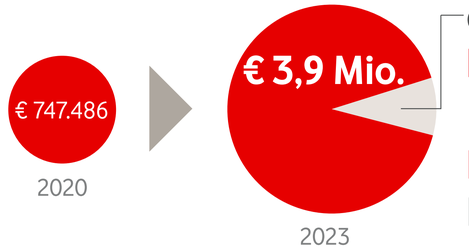
Das Softwarehaus Sophos beziffert in seinem Report „The State of Ransomware 2024“ [2] die **durchschnittlichen Kosten einer Ransomware-Attacke auf 3,9 Millionen Euro**. Dieser Wert hat sich 2024 gegenüber dem Vorjahr **mehr als verfünffacht**. Dabei machen **Lösegeldzahlungen**, die Sophos mit **durchschnittlich 347.732 Euro** angibt, gerade einmal 10 Prozent der entstandenen Gesamtkosten aus. Der Großteil des Schadens entfällt demnach auf die durch den Angriff und seine Folgen verursachten operativen Kosten.

Der Branchenverband Bitkom berechnet die **Schäden durch organisierte sowie Cyber-Kriminalität für die deutsche Wirtschaft im Jahr 2024 auf 267 Milliarden Euro**. Diese Zahl umfasst neben Cyberangriffen auch digitale und analoge Industriespionage, Sabotage sowie den Diebstahl von IT-Ausrüstung und Daten.

Diese und andere Quellen zeigen zudem, dass zu den direkten Kosten wie Betriebsunterbrechung sowie IT-Forensik noch **weitere Kosten** hinzukommen: Etwa durch die **Erfüllung von Datenschutzpflichten, PR- und Krisenkommunikation sowie Marketingmaßnahmen**, um einem entstandenen Imageschaden entgegenzuwirken.

Hohe Folgeschäden durch erfolgreiche Ransomware-Attacken

Die Kosten zur Wiederherstellung des operativen Betriebs sind im Vergleich zur Lösegeldsumme um den Faktor 10 höher. Betriebsunterbrechung und Wiederherstellungskosten sind die Haupt-Kostentreiber nach einer Ransomware-Attacke.



durchschnittliche **Lösegeldsumme: € 347.732** [1]

Downtime: Durchschnittlich **21 Tage** [2]

[1] Quelle: Coveware Quarterly Ransomware Report April 2023
[2] Quelle: Sophos – „The State of Ransomware 2023“

Die direkten Kosten von Ausfallzeiten schmälern das Geschäftsergebnis

Eine Umfrage unter den weltweit 2000 größten Unternehmen zeigt: Umsatzverluste machen den größten Einzelposten aus, aber auch andere direkte Kosten summieren sich.

Quelle: Splunk/Cisco: „Die versteckten Kosten von Ausfallzeiten“, 2023

4 Unternehmenspflichten bezüglich Sicherheitsrisiken verschärfen sich mit NIS2

Die Rechtslage ist sowohl auf deutscher wie auch europäischer Ebene komplex und teils schwer überschaubar. Eine Vielzahl von oft inhaltlich konkurrierenden beziehungsweise sich überschneidenden Gesetzen betrifft etwa die **Haftung von Unternehmen**, **Geschäftsleitung und ihren Mitarbeitenden für durch Cyberangriffe entstandene Schäden.**

Hinzu kommen **Meldepflichten** bei Sicherheitsvorfällen, insbesondere wenn etwa **persönliche Daten von Kund:innen** betroffen sind, sowie **gesetzliche Vorgaben zur Implementation und ständigen Pflege von Sicherheitsmaßnahmen**. Relevant sind in diesem Zusammenhang etwa die europäische Datenschutzgrundverordnung (**DSGVO**), aber auch nationale Gesetze wie das sogenannte **BSI-Gesetz (BSIG)**.

EU-weite Richtlinie NIS2

Die EU-Richtlinie 2022/2555 (NIS2) ersetzt die ältere „**Network and Information Security Directive**" der EU. Alle EU-Mitgliedstaaten müssen eine darauf basierende nationale Gesetzgebung erlassen und anwenden. Die Richtlinie fordert zum Beispiel **weitreichende technische, organisatorische und operative Risikomanagement-Maßnahmen**. Unternehmen sind verpflichtet, **eigenständig Sicherheitsrisiken zu identifizieren** – auch mit Blick auf Zulieferunternehmen.

Die wesentliche Frage für Unternehmen lautet, ob sie **von NIS2 betroffen sind oder nicht**. Dafür gibt es **zwei Kriterien**:

- In welchem **Wirtschaftssektor** ist das Unternehmen tätig? NIS2 benennt Sektoren wie etwa Energie, Verkehr und Transport, Bank- und Finanzwesen, und einige mehr.
- Die **Unternehmensgröße**. Dabei wird zwischen „**besonders wichtigen Einrichtungen**" und „**wichtigen Einrichtungen**" unterschieden – für Letztere sind geringere Geldstrafen vorgesehen und die Behörden haben etwas weniger Durchgriffsmöglichkeiten.

Neben den möglichen **hohen Bußgeldern ist** eine **explizite Haftung der Geschäftsführung** vorgesehen. In gravierenden Fällen ist sogar ein **temporäres Absetzen der Geschäftsleitung** möglich.

Geforderte Cyber-Sicherheits-Maßnahmen (§30 BSIG)

- Risikoanalyse und -management
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Business Continuity (u. a. Backup Management, Wiederherstellung) und Krisenmanagement
- Sicherheit in der Lieferkette
- Sichere Entwicklung, Beschaffung und Wartung von IT
- Wirksamkeitsprüfungen der Risiko- und IT-Sicherheitsmaßnahmen
- Cyber-Hygiene und Schulungen
- Kryptographie und Verschlüsselung
- Sicherheit des Personals und Zugriffskontrolle
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung sowie gesicherte Kommunikationskanäle

Welche Bußgelder drohen im Rahmen von NIS2?

Unternehmen	Mitarbeitende		Umsatz / Bilanzsumme	Bußgelder
Mittelgroß (wichtige)	50 - 249	**oder**	>10 Mio. € / > 10 Mio.	Bis 7 Mio. € oder 1,4% weltweiter Jahresumsatz*
Groß (besonders wichtige)	≥250	**oder**	> 50 Mio. € / >43 Mio.	Bis 10 Mio. € oder 2% weltweiter Jahresumsatz*

*Mögliche Sanktionen für Unternehmen mit einem Jahresumsatz über 500 Mio. €.

Betreiber:innen kritischer Anlagen und Unternehmen, deren Tätigkeit Auswirkungen auf die **öffentliche Ordnung**, **Systemrisiken** oder **grenzüberschreitende Auswirkungen** begründen können, unterliegen ebenfalls **erhöhten Anforderungen**. Weiterführende Informationen hierzu gibt es beim UP KRITIS, einer öffentlich-privaten Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland.

5 Maßnahmen für höhere Cyber-Sicherheit: So gehen Unternehmen am besten vor

Wie können Unternehmen die **Aufgabe Cyber-Sicherheit sinnvoll strukturieren und optimal in ihre Organisation integrieren**? Die Schutzmaßnahmen müssen jeweils auf den Ebenen **Mensch, Technik und Organisation** konzipiert und umgesetzt werden. Die nebenstehende Matrix zeigt die wichtigsten Schritte in den Phasen **Planung, Aufbau und Umsetzung**.

Bei allen erforderlichen Maßnahmen stehen Unternehmen dabei vor der Entscheidung, was sie selbst **intern** (etwa in ihrer IT-Abteilung) **umsetzen** wollen und welche Aufgaben sich für ein **Outsourcing an einen erfahrenen Partner** eignen.

Häufig wird es auch ein Zusammenspiel von beiden Bausteinen sein. So können beispielsweise **regelmäßige Backups und allgemeine Schutzmaßnahmen** von den Mitarbeitenden des Unternehmens geleistet werden. Dazu zählen etwa die Installation und regelmäßige Aktualisierung von **Schutzsoftware**, Installation und Konfiguration einer **Firewall** sowie das regelmäßige Einspielen der **Sicherheits-Patches**, die von den Anbietern der genutzten Betriebssysteme, Applikationen und IT-Infrastrukturlösungen zur Verfügung gestellt werden. Auch ein regelmäßiges **Monitoring des Datenverkehrs** zur frühzeitigen Erkennung des Abflusses ungewöhnlich hoher Datenmengen oder verdächtiger Muster zählt hierzu.

Hinzu kommen regelmäßige **Schulungen**, die auf eine **Sensibilisierung der Belegschaft** zielen, sowie organisatorische Maßnahmen wie die Implementation von **Informationssicherheits- und Compliance-Systemen.** Wichtig ist auch, für den Fall des Falles einen **Notfallplan sowie einen Kommunikationsplan** auszuarbeiten.

Andere Aufgaben wie **Schwachstellenanalysen,** die Erarbeitung eines **Schutzkonzepts, Support bei dessen Umsetzung** oder auch **Netzwerküberwachung** eignen sich hingegen dafür, an einen kompetenten **Dienstleister** ausgelagert zu werden.

Baustein-Konzept für mehr Cyber-Sicherheit

	1. Planung	2. Vorbereitung	3. Umsetzung
Mensch	• **Schulungskonzept** Cyber Security Trainings (Awareness, aber auch Notfalltraining etc., kontinuierliche Updates)	• **Identifikation aktueller Wissensstände** • **Definition neuer Maßnahmen** und Vorbereitung auf deren Einführung	• **Abfrage von Wissensständen** durch theoretische Tests und praktische Übungen
Technik	• **Strategische Planung** von Hard- ware und Software zum optimalen Schutz der IT-Infrastruktur • **Definition von Anforderungen** an die Cyber-Security-Lösung inklusive Backup	• **Gap-Analyse vom Ist- zum Best-Practice-Zustand** als Grundlage für eigene Cyber-Security-Lösung • **Erarbeiten von technischen Anforderungen** Unabhängige Beratung zu passenden Angeboten	• **Konstante Überwachung** der IT-Infrastruktur • **Betrieb der Lösungen** zur Bereitstellung von Security Operations • **Zusammenarbeit** mit IT-Operations und Management
Organisation	• **Implikationen gesetzlicher Anforderungen** wie DSGVO, BSI, NIS2, KRITIS, ISO, BaFin, VDA oder HIPAA für interne Maßnahmen • **Erstellung eines Notfallplans** inkl. Krisenkommunikation	• **Definition der Aufgaben** zur Umsetzung • **Katalogisierung geeigneter Lösungen** für Support bei der Einführung neuer Maßnahmen	• **Training und Dokumentation** zur Implementierung der Maßnahmen • **Ständige Beratung** durch Fachexpert:innen wie Chief Information Security Officer (CISO)

5 Dreiklang für Cyber-Sicherheit: Prävention – Detektion – Reaktion

Auch wenn es keinen hundertprozentigen Schutz gegen Cyberattacken gibt, so stehen doch **viele effiziente Werkzeuge zur Abwehr von Angriffen** zur Verfügung.

Basierend auf den drei Ebenen Organisation, Technik und Mensch, wie sie auf der vorherigen Seite dargestellt wurden, lassen sich Maßnahmen zur Verbesserung der Cyber-Sicherheit in drei Phasen einteilen: Prävention, Detektion und Reaktion. Sie umfassen je nach Unternehmensbedarf die gesamte IT-Infrastruktur vom Netzwerk über die Server und Services bis hin zu den Endgeräten.

Im Rahmen der **Prävention** geht es um Erkennen von Gefahren, bevor Schäden entstehen. Es gilt, Cyberkriminelle von den Systemen des Unternehmens fernzuhalten.

Laufende Angriffe müssen durch geeignete Maßnahmen zur **Detektion** schnell erkannt werden. Das Ziel ist, einen laufenden Überblick darüber zu gewinnen und zu behalten, was aktuell in der IT-Landschaft des Unternehmens vor sich geht. Hacker und Eindringlinge müssen umgehend aufgespürt werden.

Wenn ein Sicherheitsvorfall eintritt, ist eine wirksamne **Reaktion** unabdingbar. Dabei gilt es, schnell und zielgerichtet Gegenmaßnahmen zu ergreifen. Eindringlinge müssen effizient und dauerhaft aus den Systemen des Unternehmens entfernt werden.

Wie diese aufeinander aufbauenden Phasen mit konkreten Maßnahmen umgesetzt werden können, lesen Sie auf den folgenden Seiten.

Die drei Bausteine eines wirksamen Cyber-Sicherheits-Konzepts

Prävention

Schwachstellen erkennen

Detektion

Angriffe entdecken

Reaktion

Gegenmaßnahmen ergreifen

5 Schwachstellen erkennen: Werkzeuge im Bereich Prävention

Prävention: Scans, Tests und Analysen

Um potenzielle Gefahren und Schwachstellen zu identifizieren, bevor sie von Cyberkriminellen ausgenutzt werden, sind die folgenden, aufeinander aufbauenden Scans und Analysen unverzichtbar:

Security Awareness

Die Sensibilität der Mitarbeitenden gegenüber **Phishing**-Versuchen lässt sich mithilfe simulierter Phishing-Mails testen. Reagieren die Adressaten adäquat oder fallen sie auf den **Test-Angriff** herein? Basierend auf den Ergebnissen lassen sich dann Maßnahmenkataloge wie insbesondere **regelmäßige Trainings** zur Erhöhung der Mitarbeitenden-Kompetenz und damit des „menschlichen Schutzwalls" definieren und umsetzen.

Vulnerability Assessment

Discovery Scans suchen nach Schwachstellen in der internen Netzwerkumgebung des Unternehmens sowie auch über externe Schnittstellen. Ein Abschlussbericht nennt alle identifizierten Sicherheitslücken.

Penetration Tests

Weiter gehen die sogenannten Penetration Tests – **gezielte Angriffe auf die IT-Umgebung** der Unternehmen, um deren Schutz zu verbessern. Auch Apps können miteinbezogen werden. Die Rahmenbedingungen werden im Vorfeld definiert. Am Ende steht ein detaillierter Ergebnisbericht.

Cyber Exposure Diagnostic

Umfangreiche Diagnosen geben Aufschluss darüber, ob die IT-Systeme des Unternehmens vor Cyberangriffen geschützt sind. **Aufgedeckte Sicherheitslücken** können dann gezielt geschlossen werden. Diese **Komplettdiagnose** umfasst die drei Bereiche **Netzwerk**, **Endpunkte** sowie **Benutzer(-Authentifizierung)**.

Die Ergebnisse führen zu **Empfehlungen**, die das Schutzkonzept und die Prozesse des untersuchten Unternehmens verbessern und auch einen **Notfallplan** umfassen, wie alle Beteiligten im Fall eines erfolgreichen Angriffs vorzugehen haben.

Menschliche und technische Schwachstellen identifizieren

Vulnerability Assessment:
Der digitale Sicherheitsinspektor

Penetration Test: Der „digitale Einbrecher" im Auftrag

Security Awareness:
Gegen „digitale Enkeltricks" wappnen

Cyber Exposure Diagnostic:
Die digitale Spurensicherung

5 Detektion und Reaktion: Hacker aufspüren und entfernen

Proaktiver Schutz

Zu einem umfassenden Schutzkonzept zählen zudem **proaktive Maßnahmen**. So schützt **E-Mail and Endpoint Security** im Büro und Homeoffice eingesetzte Geräte gegen Bedrohungen wie Ransomware-Attacken. **Mobile Endpoint Security** wiederum schützt die mobile Endgeräte-Flotte eines Unternehmens gegen diese Angriffstypen. Ein **Secure Access Gateway** überwacht Angriffsflächen wie über das Internet erreichbare Zugangspunkte. Eine sogenannte **Zero-Trust-Architektur** stellt auf Basis von Unternehmensrichtlinien sichere Verbindungen zwischen Nutzer:innen und ihrem Ziel her.

Detektion: Angriffe erkennen

Kommt es zu einem Cyberangriff, gilt es, diesen schnell zu erkennen (Detektion) und darauf umgehend und angemessen zu reagieren (Reaktion). Beides erfordert umfangreiche Ressourcen. Deshalb kann es sehr sinnvoll sein, diese Aufgaben als **Managed Service an Dienstleister outzusourcen**.

Sicherheitsüberwachung und -Management

Entsprechende Dienstleister bieten Sicherheitsüberwachung rund um die Uhr (zum Beispiel als **„Managed Extended Detection & Response", kurz MxDR.** Häufig überwacht dann ein „SOC" (Secure Operations Center) permanent die Sicherheit des Unternehmensnetzwerks.

Reaktion: Wiederherstellung und Forensik

Nach erkannten Cyberangriffen sind unbedingt **Maßnahmen** erforderlich, um den **Schaden zu begrenzen** und die **Wiederherstellungszeit zu verkürzen**. Um in solchen Situationen schnell und effektiv auf die Bedrohung reagieren zu können, sollten **schon im Vorfeld Prozesse zur Eindämmung des Schadens und zur Wiederherstellung von Daten und IT-Services** definiert werden. Die in diesem Zusammenhang sinnvolle Daten-Forensik ist von entsprechenden Dienstleistern ebenfalls als **Managed Service** erhältlich.

Proaktiver Schutz von Endpoints und Gateways

E-Mail and Endpoint Security
Der digitale Schutzzaun gegen Bedrohungen wie Ransomware-Attacken.

Secure Access Gateway:
Der digitale Türsteher

Mobile Endpoint Security
Schutz der mobilen Flotte

Detektion von und Reaktion auf Cyberattacken als Managed Services

Managed Extended Detection & Response: Die digitale Sicherheitsleitstelle

Breach Response & Forensics:
Das digitale Einsatzkommando für den Fall der Fälle

6 Sicherheitslösungen aus einer Hand: Vodafone Cyber Security Services

Unabhängig von Größe und Tätigkeitsfeld benötigt jedes Unternehmen ein individuelles Cyber-Security-Konzept. In jedem Fall erfordert umfassende Cyber Security **leistungsfähige, ineinandergreifende Lösungen**.

Das **Vodafone Lösungsportfolio für Cyber Security** bietet alle dazu nötigen Bausteine an – **für alle Unternehmensgrößen und alle Phasen von Prävention über Detektion bis Reaktion**.

Mit seinen **Managed Security Services** entlastet Vodafone die IT-Abteilungen von Unternehmenskund:innen – so können sich diese auf strategische Aufgaben konzentrieren. Zudem entfällt die Notwendigkeit, das eigene Personal permanent zu Cyber-Security-Themen up to date zu halten.

Die Cyber-Security-Lösungen von Vodafone helfen Unternehmen, **Schwachstellen aufzudecken und Cyberattacken früher zu erkennen**. So können Unternehmen **schneller auf Angriffe reagieren und langfristige Auswirkungen reduzieren.**

Für unsere Lösungen arbeiten wir mit **erfahrenen und renommierten Partnern** zusammen, die zu den führenden Expert:innen auf ihrem jeweiligen Gebiet zählen.

Unsere Cyber Security Services für Unternehmen aller Größen im Überblick

Penetration Test
Schützen Sie Ihr Unternehmen, indem Sie Schwachstellen in der wichtigen IT-Infrastruktur erkennen, bevor sie von Cyberkriminellen ausgenutzt werden.

Vulnerability Assessment
Gibt es Schwachstellen in Ihrem Sicherheitssystem? Wir prüfen Ihr Unternehmen auf mögliche Schwachstellen.

Managed Extended Detection & Response
Echtzeit-Security-Monitoring rund um die Uhr sorgt dafür, dass Cyberangriffe schnellstmöglich erkannt und abgewehrt werden.

Breach Response & Forensics
Sichern Sie Ihr Unternehmen gegen Cyberattacken. Wir liefern die Tools, Prozesse und Expert:innen dafür. Ein vorab definierter Maßnahmenplan hilft, im Fall der Fälle schnell reagieren zu können

Security Awareness
Sensibilisieren Sie Ihre Mitarbeitenden für die Gefahren von Cyberangriffen und schützen Sie so Ihr Unternehmen.

Cyber Exposure Diagnostic
Ist Ihr IT-System vor Cyberangriffen geschützt? Cyber Exposure Diagnostic gibt Ihnen Aufschluss darüber.

E-Mail and Endpoint Security
Schützen Sie Ihre Geräte im Büro und Homeoffice. mit Windows oder MacOS sowie Chromebooks gegen Ransomware und fortgeschrittene Bedrohungen

Mobile Endpoint Security
Schützen Sie die mobile Geräteflotte Ihres Unternehmens und Ihrer Mitarbeitenden – und kommen Sie mit weniger Ressourcen für deren Verwaltung und Schutz aus.

Security Access Gateway
Die Zero-Trust-Architektur beseitigt Angriffsflächen im Internet und wirkt so als digitaler Türsteher für Ihr Unternehmens-Netz.

Weiterführende Informationen

Sie haben Fragen zu Cyber Security oder allgemein zur Digitalisierung? **Unser Expert:innen-Team** berät Sie kostenlos und unverbindlich telefonisch unter **0800 505 4513**

Zusätzliche **Infos im Web**: https://www.vodafone.de/business/loesungen/cyber-security-services

V-Hub – unsere Digitalisierungsplattform mit Wissen, News und Tipps zu Technologien, Tools und Trends. Zum Lesen, Hören oder als Live Sessions: https://www.vodafone.de/business/blog/security

7 Glossar: Malware, Ransomware & Co – was steckt hinter diesen Begriffen?

Ransomware
verschlüsselt und/oder stiehlt Daten, um Lösegeld zu erpressen

Spyware
stiehlt sensible Daten

Würmer
verbreiten sich im Rechner und Netzwerk

Trojaner
schmuggeln Malware auf PCs oder ins Netzwerk

Adware
spammt Nutzer mit Werbung voll

Botnets
kapern PCs für Angriffe auf Dritte

In der Diskussion um Cyberkriminalität und sinnvolle Schutz- sowie Gegenmaßnahmen geht es oft um die konkreten Bedrohungsarten. Hier ein nach Relevanz beziehungsweise struktureller Bedeutung sortierter Überblick über Varianten und Fachbegriffe.

Malware Diese englische Bezeichnung für „Schadsoftware" ist der Überbegriff für alle softwarebasierten Bedrohungen. Es handelt sich um Computerprogramme, die gezielt entwickelt wurden, um (aus Sicht des Opfers) unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Die Verbreitung von Malware erfolgt zum Beispiel über E-Mail-Anhänge oder präparierte Links, die zu einer maliziösen Website führen.

Computerviren/Würmer/Trojaner Die Analogie von Computerviren zu biologischen Viren soll verdeutlichen, dass sich diese Art von Schadprogrammen selbstständig in den befallenen Systemen und darüber hinaus verbreitet. Der Begriff „Wurm" deutet an, dass sich solche Schadprogramme durch IT-Netzwerke „hindurchfressen". Die Bezeichnung „Trojaner" spielt auf das trojanische Pferd aus der klassischen Sagenwelt an und drückt damit aus, dass der schädliche Inhalt sich oft in einer vermeintlich interessanten oder nützlichen Hülle tarnt. Diese Begriffe sind mittlerweile in den Alltags-Sprachgebrauch eingegangen, und nicht immer ganz trennscharf definiert.

Ransomware Mittlerweile eine der am weitesten verbreiteten Arten von Malware. Ransomware (aus engl. ransom = Lösegeld und Software) verschlüsselt auf dem befallenen System die Nutzerdaten mit einem geheimen Schlüssel. Die Angreifer verlangen vom Angriffsopfer ein Lösegeld, um wieder auf die nicht mehr zugänglichen Daten zugreifen zu können. Sie versprechen im Gegenzug zur Zahlung, den Verschlüsselungscode auszuhändigen – was aber keineswegs immer stattfindet.

Spyware Verkürzter Begriff für Spionage-Software – und somit für Malware, die sensible beziehungsweise vertrauliche Daten ausspäht. Das können neben Passwörtern beziehungsweise Zugangsdaten und digitalen Identitäten beispielsweise auch Zahlungsdaten wie Konto- und Kreditkartennummern sein – oder auch persönliche, private Informationen, die das Angriffsopfer nicht veröffentlicht wissen will.

Phishing/Smishing/Spoofing Da Passwörter eine wichtige Hürde für Angreifer darstellen, versuchen sie, diese auszuspionieren. „Phishing" ist ein Kunstwort, das für „Password fishing" steht – das „Angeln" nach Passwörtern. Typisch sind etwa gefälschte E-Mails, die den Nutzer verleiten sollen, seine Zugangsdaten auf einer gefälschten Webseite einzugeben. Auch per SMS werden solche Spionageversuche häufig verbreitet – dann spricht man von „Smishing" (SMS Phishing). Fälschungen werden im Englischen auch als „spoof" bezeichnet. „Spoofing" bezeichnet allgemein Täuschungsmethoden, die bei Cyberangriffen zum Einsatz kommen.

Social Engineering Sammelbegriff für Angriffstechniken, die auf den Menschen beziehungsweise soziale Beziehungen abzielen. Ein Beispiel wäre, wenn die Angreifer:in gegenüber dem Opfer vorgibt, ein Vorgesetzter oder eine Vorgesetzte zu sein oder der IT-Abteilung anzugehören, um es so zur Herausgabe sensibler Daten zu bewegen.

DoS/DDoS (Distributed) Denial of Service. Weil die Verfügbarkeit von Ressourcen wie Webseiten, Cloud-Diensten oder E-Mail-Servern für Unternehmen wie Anwender heute sehr wichtig ist, können Angriffe (entweder als Grundlage von Erpressungsversuchen oder auch „nur", um das Angriffsopfer zu schädigen) auf die Überlastung und somit den Ausfall solcher Ressourcen abzielen. In der Variante DDoS (engl. distributed = verteilt) arbeiten mehrere Systeme für solche Angriffe zusammen.

Botnets Cyberangriffe finden häufig (teil-) automatisiert statt. Zum Einsatz kommen dann Software-„Roboter", kurz „Bots". Wenn mehrere davon in einem Netzwerk zusammenarbeiten (etwa für **DDoS**-Attacken), spricht man von einem „Botnet".

Man in the Middle Schutzkonzepte gegen Cyberbedrohungen basieren häufig auf der Ende-zu-Ende-Verschlüsselung von Kommunikationsstrecken (etwa SSL – Secure Socket Layer – bei Webseiten). Gelingt es einer Angreifer:in, in diese Kette einzudringen, kann sie oder er quasi als „Mann (oder Frau) in der Mitte" die Kommunikation abhören oder infiltrieren.