Whitepaper

Cyber Security

Edition 2026

Cyberangriffe im KI-Zeitalter

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

vodafone business

Together we can

Cyberangriffe im Wandel: Warum Unternehmen jetzt handeln müssen

289 Mrd. €

ist die Summe der Schäden für die deutsche Wirtschaft durch Cybervorfälle im Jahr 2025.
(Seite 7)

356.000 €

betrug die durchschnittlich bezahlte Lösegeldsumme nach einem erfolgreichen Ransomware-Angriff.
(Seite 7)

84 %

der 2025 erfolgreichen Cyberangriffe auf deutsche Unternehmen waren Phishing-Angriffe
(Seite 5)

80 %

der 2025 angezeigten Cyberangriffe zielten auf kleine und mittlere Unternehmen.
(Seite 4)

52 %

der befragten Unternehmen nennen Cybervorfälle als größtes Geschäftsrisiko – damit liegt diese Bedrohung auf Platz 1.
(Seite 4)

Vorwort

Die Bedrohungslage durch Cyberattacken steigt kontinuierlich – nicht zuletzt durch neue Angriffstechniken mithilfe von KI.

Cyberangriffe haben sich zu einem der **zentralen Geschäftsrisiken für Unternehmen** entwickelt. Gleichzeitig verändert sich die Bedrohungslage spürbar: **Angriffe werden gezielter, schneller und professioneller** – nicht zuletzt durch KI-gestützte Technologien und eine zunehmende Arbeitsteilung innerhalb cyberkrimineller Strukturen.

Die Entwicklungen betreffen **Unternehmen jeder Größe und Branche**. Dabei sind Cyberangriffe und ihre Abwehr längst kein rein technisches Thema mehr. **Entscheidend ist vielmehr das Zusammenspiel aus Technologie, Organisation und Menschen.** Wer den Risiken wirksam begegnen will, muss verstehen, wie Angriffe heute entstehen und wo typische Schwachstellen liegen.

Dieses Whitepaper gibt einen Überblick über die aktuelle Bedrohungslage, zeigt **typische Einfallstore und Angriffsmethoden** und beleuchtet die **wirtschaftlichen, operativen und regulatorischen Auswirkungen** von Cyberangriffen. Wir stellen **konkrete Handlungsfelder** vor, **mit denen Unternehmen ihre Cybersicherheit stärken können**.

*In das vorliegende Whitepaper sind die Erfahrungen aus dem Alltag des **Security-Experten Marc Atkins** eingeflossen. Marc ist Leiter des Security Operations Center (SOC) von Vodafone Deutschland. Mit seinem Team sorgt er dafür, dass Unternehmen in Deutschland cybersicher aufgestellt sind. Er und sein Team kennen die Methoden der Angreifer sowie die richtigen Strategien und Lösungen, mit denen sich Unternehmen dagegen wappnen können.*

Marc Atkins
Leiter der Cyber-Sicherheitszentrale von Vodafone

Inhaltsverzeichnis

1 Unternehmen jeder Größe im Visier der Hacker

In ihrem „Risk Barometer 2026“ [1] führt die Allianz-Versicherungsgruppe **Cybervorfälle als höchstes Einzelrisiko** auf. Mit **52 Prozent der benannten Risiken liegt Cyberkriminalität auf Platz 1 der Top-10-Risiken für Unternehmen** – noch vor Betriebsunterbrechungen, Änderungen in Gesetzgebung und Regulierung, den Auswirkungen Künstlicher Intelligenz oder geopolitischer Risiken.

Auf einen der Gründe weist das **Bundesministerium des Innern** (BMI) hin: Neben Politik und Behörden unterliegt auch die Wirtschaft in wachsendem Maße zielgerichteten Cyberangriffen. In der zunehmend angespannten geopolitischen Lage sind Angriffe zudem 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 2025 bei **289 Milliarden Euro** (Studie „Wirtschaftsschutz 2025).

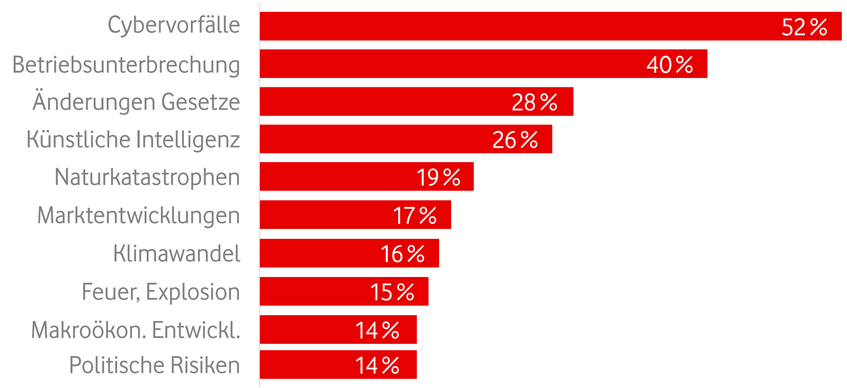
Das **Bundesamt für Informationssicherheit** (BSI) gibt in seinem **Lagebericht 2025** [2] an, dass rund **80 Prozent der 2025 angezeigten Angriffe kleine und mittlere Unternehmen** ins Visier nahmen.

Diese Entwicklung zeigt sich nicht nur in den Zahlen, sondern auch in der Praxis: Marc Atkins und sein Team erleben im Rahmen ihrer täglichen Arbeit im **Security Operations Center** von Vodafone Deutschland eine **deutliche Zunahme von Cyberangriffen auf kleine und mittlere Unternehmen**.

Eine weitere Erkenntnis des BSI: **25 Prozent** der weltweit erfassten **Cyberangriffe durch** hochspezialisierte, **oft staatlich gesteuerte Akteure** richteten sich **2025 gegen Deutschland**. Solche Angreifer werden in der Fachsprache als „APT-Gruppen“ bezeichnet („Advanced Persistent Threats“).

Allianz: Cybervorfälle liegen auf Platz 1 der Top-10-Geschäftsrisiken weltweit in 2026

Basierend auf den Antworten von mehr als 3.300 Risikomanagement-Expert:innen aus 97 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 2026“

KMU stehen klar im Fokus

80 % der 2025 angezeigten Angriffe zielten auf kleine und mittlere Unternehmen

[2] Quelle: Lagebericht des Bundesamts für Informationssicherheit 2025

> *„Wir sehen im Markt, dass immer mehr Cyberangriffe auf kleine und mittlere Unternehmen zielen.“*
>
> **Marc Atkins,** Leiter Security Operations Center von Vodafone Deutschland

2 Typische Einfallstore und Angriffsmethoden

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

Social Engineering – der Mensch als häufig genutztes Einfallstor

Ein bevorzugtes Werkzeug für Angriffe über das Einfallstor „Mensch" ist **„Social Engineering"**: Mit „sozialen Techniken" werden Mitarbeitende ausspioniert und Sicherheitsmaßnahmen umgangen.

Dazu zählen vor allem **Phishing-Mails.** Gemäß einer Befragung, die der TÜV 2025 unter 89 Unternehmen durchführte, waren Phishing-Angriffe an 84 % der erkannten Sicherheitsvorfälle beteiligt. Auch **„CEO Fraud"** zählt hierzu: Anrufe oder E-Mails, deren Urheber:in sich als Führungskraft oder Mitarbeiter:in der IT-Abteilung ausgibt – mit dem Ziel, das Opfer zur Preisgabe vertraulicher Informationen oder zum Aufweichen von Schutzoptionen zu verleiten.

Dabei machen Cyberangriffe zunehmend auch vom Boom **Künstlicher Intelligenz** (KI) Gebrauch. Darauf weist unter anderem das britische National Cyber Security Center (NCSC) hin. KI hilft Kriminellen, früher vermeintlich sichere Erkennungszeichen wie sprachliche Fehler zu vermeiden. **Deepfakes bei Bildern, Sprache und Videos** machen es immer schwieriger, legitime von gefälschten Inhalten zu unterscheiden.

Hinzu kommen technische Angriffsmethoden („**Angriffsvektoren**") wie ausgenutzte **Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen** sowie Unterwanderungsmethoden wie DDoS- (Distributed Denial of Service) oder „Man in the Middle"-Attacken (beide siehe Glossar, S. 15). Dass technische Schwachstellen eine zentrale Rolle spielen, zeigt auch der unabhängig erhobene Sophos-Report **The State of Ransomware 2025**[1]: In 42 % der Fälle waren technische Schwachstellen die Ursache erfolgreicher Angriffe, während in 20 % der Fälle kompromittierte Zugangsdaten den initialen Zugriff ermöglichten. Mehr als die Hälfte der Angriffe (51 %) führte letztlich zu einer erfolgreichen Kompromittierung.

Ein Blick auf die im Vodafone Security Operations Center ausgewerteten Vorfälle zeigt: **Angreifer nutzen gezielt Situationen aus, in denen Unternehmen nur eingeschränkt reagieren können** – etwa außerhalb regulärer Betriebszeiten.

Einfallstore und Schwachstellen

Von Januar bis März 2025 wurden 3.400 IT-/Cyber-Security-Entscheider:innen aus 17 Unternehmen befragt, darunter 300 aus Deutschland. An der Umfrage nahmen Unternehmen und Organisationen mit 100 bis 5.000 Mitarbeitenden teil.

51 %
der Angriffsversuche waren insgesamt erfolgreich.

42 %
der Angriffe gelangen wegen technischer Schwachstellen.

20 %
erfolgreicher Angriffe hatten kompromittierte Zugangsdaten als Ursache.

[1] Quelle: Sophos, „The State of Ransomware in Germany 2025"

> *„Viele Angriffe finden außerhalb der Geschäftszeiten statt. Hacker warten ja nicht darauf, dass die Ladentür um 8 Uhr aufgeht."*
>
> **Marc Atkins,** Leiter Security Operations Center von Vodafone Deutschland

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 Kriminelle 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 nachweisen.

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

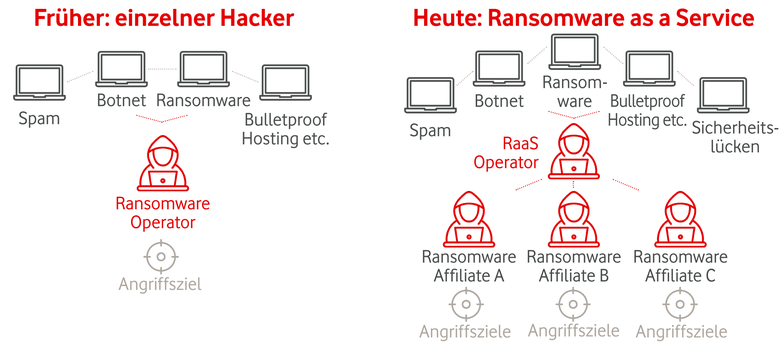
Wie professionell Cyberkriminelle vorgehen, zeigt der typische Ablauf einer Ransomware-Attacke: Zur Vorbereitung oder **Aufklärung** untersuchen Angreifende das Firmennetz auf Schwachstellen. Der **erste Zugang** ins Firmennetz nutzt „Social Engineering“ (auf echten oder vorgegebenen sozialen Kontakten 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 Cyberangriffe verursachen weitreichende Schäden

Cyberattacken führen zu **Betriebsunterbrechungen und Verzögerungen** – die durchschnittliche Downtime beträgt eine Woche[1], kann aber auch erheblich länger ausfallen – gerade bei kleineren Unternehmen, die unzureichend auf Angriffsabwehr und Datenwiederherstellung vorbereitet sind. Oft lassen sich dann Projekte gar nicht mehr durchführen und Kundenaufträge nicht, nur noch eingeschränkt oder mit erheblichem Zeitverzug realisieren. Von noch größerer Tragweite können negative Einflüsse wie ein dauerhafter Imageverlust des Unternehmens und damit einhergehender Vertrauensverlust auf Kundenseite sein. Dies verursacht **erhebliche Kosten** und somit **finanzielle Verluste**. Zu eventuellen **Lösegeldzahlungen kommen hohe operative Kosten** für die Wiederherstellung von verlorenen oder verschlüsselten Daten bzw. die Säuberung oder teilweise ganz neue Bereitstellung der IT-Systeme.

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

In seinem Report „The State of Ransomware 2025“[1] beziffert das Softwarehaus Sophos die **durchschnittlichen Kosten einer Ransomware-Attacke** für Deutschland **auf 1,56 Millionen US-Dollar (ca. 1,35 Millionen Euro)**. Dabei machen **Lösegeldzahlungen**, die Sophos mit **durchschnittlich 412.000 US-Dollar bzw. rund 356.000 Euro** angibt, gerade einmal 26 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 Cyberkriminalität für die deutsche Wirtschaft im Jahr 2025 auf 289 Milliarden Euro**.[2] 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 fast dreimal so hoch wie die Lösegeldsumme. Betriebsunterbrechung und Wiederherstellungskosten sind die Haupt-Kostentreiber nach einer Ransomware-Attacke.

[1] Quelle: Sophos, „The State of Ransomware in Germany 2025“

Zu den direkten Schadenssummen kommen weitere Kosten hinzu

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden? Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland 2025; in Milliarden Euro (Mehrfachnennungen möglich, Zahlen gerundet)

	Schadensummen in Mrd. €		
Schaden durch…	**2025**	**2024**	**2023**
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	**73,5**	54,5	35,0
Kosten für Rechtsstreitigkeiten	**53,0**	53,1	29,8
Kosten für Ermittlungen und Ersatzmaßnahmen	**37,0**	32,2	25,2
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	**30,6**	39,2	15,3
Datenschutzrechtliche Maßnahmen, z. B. durch Behörden	**23,8**	27,2	12,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	**23,1**	11,2	21,5
Patentrechtsverletzungen, auch vor Anmeldung	**16,0**	14,8	10,4
Imageschaden bei Kunden/Lieferanten, negative Berichterstattung	**15,9**	20,2	35,3
Erpressung mit gestohlenen Daten	**15,6**	13,4	16,1
Geldabfluss durch Betrugsversuche	**15,6**	13,4	16,1
Sonstige Schäden	**0,9**	0,8	3,9
Gesamtschaden pro Jahr	**289,2**	**266,6**	**205,9**

[2] Quelle: Bitkom Research 2025

4 NIS-2: Verschärfte Pflichten für Unternehmen

Die Rechtslage ist sowohl auf deutscher als 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 NIS-2 in Deutschland seit Ende 2025 gesetzlich verpflichtend

Im Dezember 2025 ist in Deutschland das **NIS-2-Umsetzungsgesetz** in Kraft getreten. Es regelt die Umsetzungspflicht der EU-Richtlinie 2022/2555 (Network and Information Security Directive 2, kurz NIS-2).

In Deutschland sind **rund 29.500 Unternehmen betroffen**. Sie müssen sich registrieren, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) **erhebliche Sicherheitsvorfälle melden**, **Risikomanagement-Maßnahmen implementieren und dokumentieren** – auch mit Blick auf Zulieferunternehmen.

Die wesentliche Frage für Unternehmen lautet, ob sie **von NIS-2 betroffen sind oder nicht**. Dafür gibt es **zwei Kriterien**:

- In welchem **Wirtschaftssektor** ist das Unternehmen tätig? NIS-2 benennt Sektoren wie 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 eine **temporäre Absetzung der Geschäftsleitung** möglich.

Geforderte Cybersicherheits-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 NIS-2?

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

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

Betreiber 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 So stärken Unternehmen ihre Cybersicherheit

Wie können Unternehmen die **Aufgabe Cybersicherheit 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 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 Cybersicherheit

	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 Hardware 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	**24/7-Überwachung** der IT-Infrastruktur **Umsetzung der Maßnahmen,** die in der Gap-Analyse identifiziert wurden **Betrieb der Lösungen** für Security Operations **Zusammenarbeit** mit IT-Operations und Management
Organisation	**Implikationen gesetzlicher Anforderungen** wie DSGVO, BSI, NIS-2, KRITIS, ISO, BaFin, VDA oder HIPAA für interne Maßnahmen **Erstellung eines Notfallplans** inklusive 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 Cybersicherheit: Prävention – Detektion – Reaktion

Auch wenn es keinen hundertprozentigen Schutz gegen Cyberattacken gibt, 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 Cybersicherheit 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. Ein sicheres Setup soll Gefahren vermeiden bzw. minimieren. 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 wirksame **Reaktion** unabdingbar. Dabei gilt es, schnell und zielgerichtet Gegenmaßnahmen zu ergreifen. Eindringlinge müssen effizient und dauerhaft aus den Systemen des Unternehmens entfernt werden.

Ein **SIEM** (Security Information and Event Management) führt kontinuierlich Datenanalysen durch. Es identifiziert Bedrohungen durch die Auswertung von Protokolldaten. Dieses nutzt **SOAR** (Security Orchestration, Automation and Response), um automatisiert auf erkannte Bedrohungen zu reagieren. Ein Beispiel für dieses Zusammenwirken: Erkennt SIEM innerhalb eines kurzen Zeitraums mehrere Anmeldeversuche einer Person aus verschiedenen Ländern, unterbindet SOAR sie. Auch das Security and Operations Center von Vodafone arbeitet mit SIEM und SOAR.

Wie die aufeinander aufbauenden Bausteine Prävention, Detektion und Reaktion mit konkreten Maßnahmen umgesetzt werden können, lesen Sie auf den folgenden Seiten.

Die drei Bausteine eines wirksamen Cybersicherheits-Konzepts

Prävention

Schwachstellen erkennen

Detektion

Angriffe entdecken

Reaktion

Gegenmaßnahmen ergreifen

> *„SOAR (Security, Orchestration, Automation and Response) leitet Schutzmaßnahmen aus vorher gesammelten und analysierten Datenpunkten ab und setzt diese um.“*
>
> **Marc Atkins,** Leiter Security Operations Center von Vodafone Deutschland

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:

Phishing Awareness

Die Sensibilität der Mitarbeitenden gegenüber **Phishing**-Versuchen lässt sich mithilfe simulierter Phishing-Mails testen. Fallen die Adressat:innen auf den **Test-Angriff** herein? Basierend auf den Ergebnissen lassen sich dann Maßnahmenkataloge wie insbesondere **regelmäßige Trainings** umsetzen.

Vulnerability Assessment

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

Penetration Tests

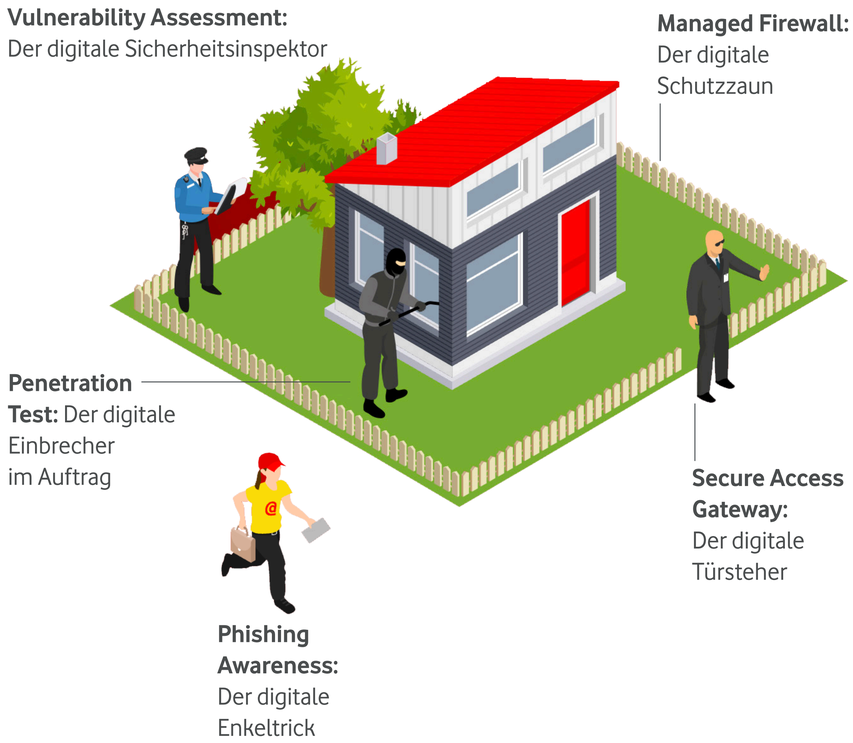
Weiter gehen Penetration Tests – **gezielte Angriffe auf die IT-Umgebung** der Unternehmen, um deren Schutz zu verbessern. Auch Apps können einbezogen werden. Die Rahmenbedingungen werden im Vorfeld definiert. Am Ende steht ein detaillierter Ergebnisbericht.

Managed Firewall

Der digitale Schutzzaun wird laufend aktualisiert und an die Bedürfnisse des Kunden-Unternehmens angepasst. Dabei übernimmt ein kompetenter Dienstleister **Verwaltung und Aktualisierung**. Individuelle Sicherheitsanforderungen der Netzwerkstruktur können berücksichtigt werden.

Eine entscheidende Rolle bei der Prävention spielt die 24/7-Überwachung der Kundensysteme durch ein Security Operations Center. Ein genauerer Blick darauf folgt auf der nächsten Seite.

Menschliche und technische Schwachstellen identifizieren



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 **Zero-Trust-Architektur** stellt auf Basis von Unternehmensrichtlinien sichere Verbindungen zwischen Nutzer:innen und ihrem Ziel her. Außerdem schützt es vor Massenangriffen, in der Fachsprache: **DDoS-Angriffen**. Dabei handelt es sich um Cyberangriffe, bei denen extrem viele Anfragen an einen Internet-Anschluss gesendet werden, um seine Leistung zu beeinträchtigen.

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** (siehe auch Glossar, S. 15) an einen kompetenten Dienstleister **outzusourcen**. Dieser übernimmt dann dauerhaft die Umsetzung für seinen Kunden – zum Beispiel eine Sicherheitsüberwachung rund um die Uhr, 365 Tage im Jahr (**„Managed Extended Detection & Response", kurz MxDR**). Häufig überwacht dann ein SOC permanent die Sicherheit des Unternehmensnetzes.

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 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 nötigen Bausteine an – **für alle Unternehmensgrößen und alle Phasen von Prävention über Detektion bis Reaktion**.

Mit seinen **Security Services** entlastet Vodafone die IT-Abteilungen von Unternehmen – so können sich diese auf strategische und operative Aufgaben konzentrieren.

Unsere Security-Expert:innen unterstützen Kund:innen von der Ersteinrichtung bis zum Betrieb und der Wartung. Wir überwachen Ihre Sicherheit 24/7.

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 Partner:innen** zusammen, die zu den führenden Expert:innen auf ihrem jeweiligen Gebiet zählen.

Vodafone Cyber Security Services für Unternehmen aller Größen

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

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

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

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

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.

E-Mail and Endpoint Security
Schützen Sie Ihre Geräte in 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 ihre 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. Zudem schützt sie vor DDoS-Attacken.

V-Hub: Cyber-Security-Know-how für Ihr Business

mit Wissen, News und Tipps zu Technologien, Tools und Trends. Zum Lesen, Hören oder als Live Sessions:

vodafone.de/blog-security

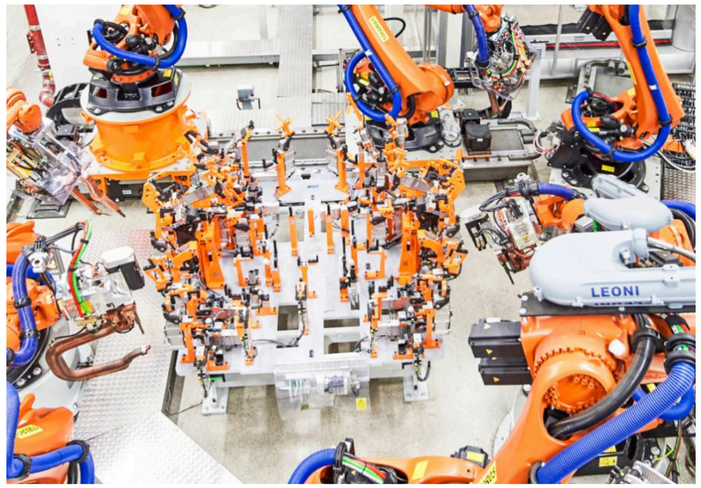
Cyber-Security-Beratung

Sprechen Sie unverbindlich mit unseren erfahrenen Cyber-Security-Spezialist:innen und entwickeln Sie ein maßgeschneidertes Schutzkonzept:

Jetzt beraten lassen

7 Erfolgsgeschichten rund um Cybersicherheit

Wie Unternehmen ihre Cybersicherheit konkret stärken: Die folgenden Praxisbeispiele zeigen, welche Vodafone-Lösungen Unternehmen einsetzen, welche Maßnahmen sich bewährt haben – und welche konkreten Mehrwerte sich daraus ergeben.



Strama Group: Managed Security Services für das Firmennetzwerk

Die Strama Group betreibt international vernetzte Standorte und arbeitet gleichzeitig auf digitalen Plattformen, die kontinuierlich verfügbar sein müssen. Das Ziel: globale Zusammenarbeit, Flexibilität und Sicherheit gleichzeitig zu gewährleisten.

Mit den Managed Security Services von Vodafone Business wurde eine Lösung implementiert, die das Unternehmensnetzwerk umfassend schützt, ohne die Geschwindigkeit und Agilität der internationalen Arbeitsprozesse einzuschränken.

- Managed Security Services entlasten interne IT-Teams
- Zentrale Verwaltung, Aktivierung und Einrichtung
- Sicherheitsberichte für alle einbezogenen Geräte, Netzwerke und Daten

Lesen Sie hier die komplette Erfolgsgeschichte.

Krannich Solar: Sicherer Zugriff auf IT-Ressourcen für international verteilte Teams

Als international tätiges Unternehmen mit über 30 Standorten benötigt Krannich Solar einen sicheren und gleichzeitig flexiblen Zugriff auf zentrale IT-Systeme.

Mit der implementierten Zero-Trust-Lösung von Vodafone Business auf Basis von Zscaler Cloud Security wird der Zugriff auf IT-Ressourcen bedarfsgerecht gesteuert und unabhängig vom Standort abgesichert.

- Zero-Trust ermöglicht sicheren Zugriff unabhängig vom Standort
- Flexible Absicherung für international verteilte Teams
- Zugriffsrechte lassen sich granular und bedarfsgerecht steuern

Lesen Sie hier die komplette Erfolgsgeschichte.

HELDELE: Zero-Trust-Modell für moderne IT-Sicherheit

Die HELDELE Gruppe benötigt sicheren Zugriff auf IT-Systeme und Anwendungen – sowohl intern als auch in Kundenprojekten und von unterschiedlichen Standorten aus. Klassische Sicherheitsansätze wie VPN und Firewalls stießen dabei an ihre Grenzen. Deshalb setzte HELDELE auf eine moderne Zero-Trust-Architektur von Vodafone Business auf Basis von Zscaler Cloud Security.

- Höhere Sicherheit im Firmennetzwerk von Mutter-, Tochter- und Schwesterfirmen
- Geringerer Administrationsaufwand als mit VPN und Firewalls
- Granulare Verwaltung von Zugriffsrechten auf Dienste und Daten

Lesen Sie hier die komplette Erfolgsgeschichte.

8 Glossar

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 Die englische Bezeichnung für „Schadsoftware" ist Überbegriff für alle softwarebasierten Bedrohungen. Es handelt sich um Computerprogramme, die entwickelt wurden, um (aus Sicht des Opfers) unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Die Verbreitung von Malware erfolgt z. B. 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 werden dort nicht immer ganz trennscharf verwendet.

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. Damit das Angriffsopfer wieder auf seine nicht mehr zugänglichen Daten zugreifen kann, soll es ein Lösegeld an die Kriminellen bezahlen. Diese versprechen, den Verschlüsselungscode nach Erhalt der Summe auszuhändigen – was aber keinesfalls immer passiert.

Spyware Verkürzter Begriff für Spionage-Software – und somit für Malware, die sensible bzw. vertrauliche Daten ausspäht. Das können neben Passwörtern beziehungsweise Zugangsdaten und digitale Identitäten beispielsweise 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 Nutzer verleiten sollen, ihre 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 bzw. soziale Beziehungen abzielen. Zum Beispiel durch eine Kontaktaufnahme mit der Behauptung, eine Führungskraft zu sein oder der IT-Abteilung anzugehören, um die Herausgabe sensibler Daten zu erreichen.

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 als Netzwerk zusammenarbeiten (etwa für **DDoS**-Attacken, siehe oben), 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 „Mensch in der Mitte" die Kommunikation abhören oder infiltrieren.

Managed Services sind ausgelagerte IT-Dienstleistungen, bei denen ein externer Anbieter (oft „Managed Service Provider" oder kurz MSP genannt) die Verwaltung, Wartung und das Sicherheits-Monitoring von IT-Infrastruktur, Netzwerken oder Anwendungen für ein Unternehmen übernimmt. Managed Services basieren auf Service Level Agreements (SLAs), sind präventiv statt reaktiv und dienen der Kostenkontrolle, Entlastung interner Teams sowie Sicherstellung der IT-Sicherheit und -Verfügbarkeit.