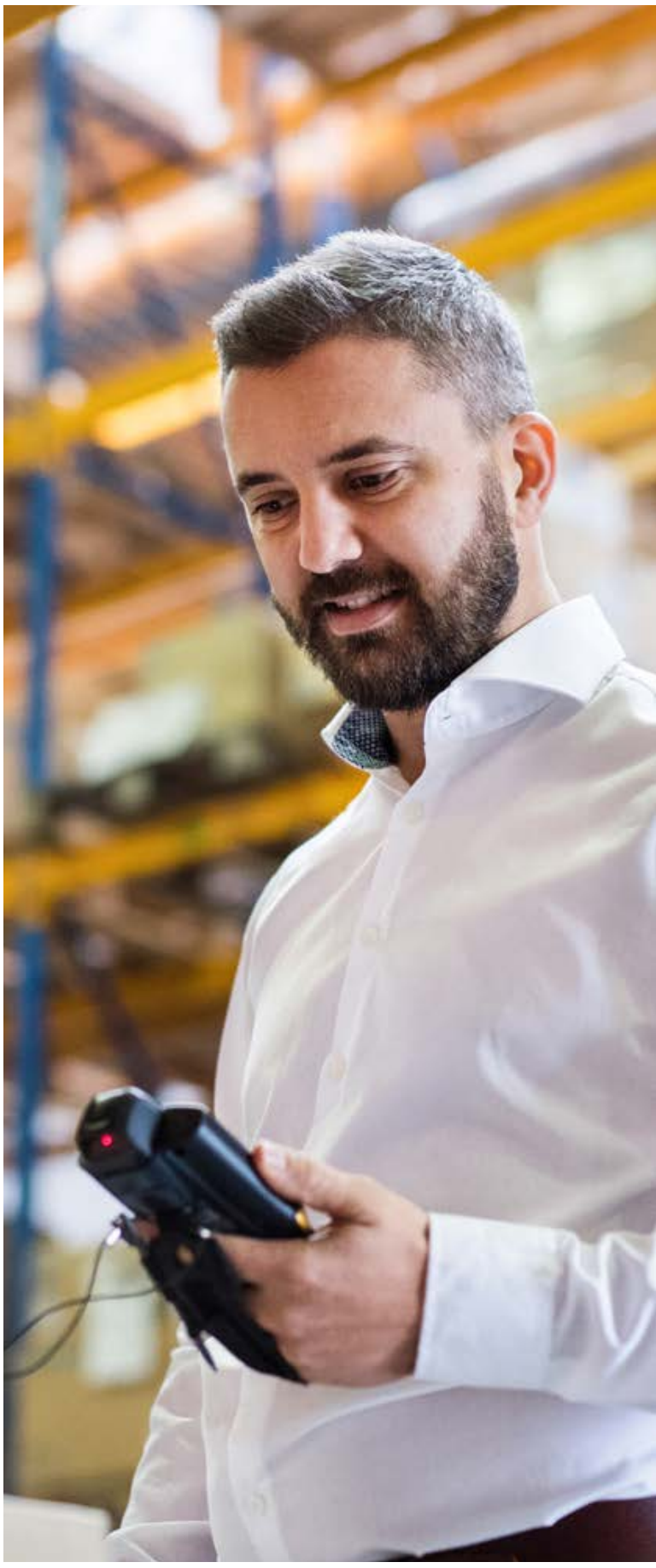
Leitfaden

Ein ganzheitlicher Ansatz zur Stärkung der Cyberresilienz

verizon business

Inhalt



So können Unternehmen resilienter gegen zunehmende Cyberbedrohungen werden

Cyberangriffe werden immer häufiger und immer ausgefeilter. Wie können Unternehmen sich weiterhin zuverlässig schützen? Unserer Meinung nach erfordert das einen ganzheitlichen Ansatz.

Mit dem technischen Fortschritt und der zunehmenden Vernetzung in Unternehmen aller Branchen steigt auch das Risiko von Online-Angriffen. Zudem werden Cyberangriffe immer ausgefeilter. Hinzu kommt, dass durch die steigende Nutzung digitaler Tools und Abläufe immer mehr Daten in der Cloud gespeichert und für andere freigegeben werden – wodurch die Angriffsflächen so gut wie aller Unternehmen wachsen.

Zu ihrem Schutz benötigen Unternehmen ein robustes Cybersicherheitsprogramm, das sowohl ihre individuellen Anforderungen als auch die einschlägigen Vorschriften erfüllt.

Cyberbedrohungen auf dem Vormarsch

Der von Verizon Business in Auftrag gegebene „Data Breach Investigations Report 2024“[1] analysierte

30.458

dokumentierte Sicherheitsvorfälle.

10.626

davon waren bestätigte Datenschutzverletzungen mit Opfern in

94

Ländern.

Steigende Risiken unter Kontrolle bringen

Der Bericht zeigt einen erheblichen Anstieg der Anzahl der Angriffe, bei denen Schwachstellen (zumeist in Web-Anwendungen) ausgenutzt wurden: erschreckende 180 % gegenüber dem Vorjahr.

Bei rund einem Drittel der Angriffe wurde Ransomware eingesetzt. 92 % der Befragten nannten Ransomware als eine ihrer größten Sorgen, da die Kosten eines erfolgreichen Angriffs enorm sein können. 95 % der Angriffe mit einer Erpressungskomponente, die dem Internet Crime Complaint Center (IC3) des FBI gemeldet wurden, verursachten Verluste zwischen 3 US-Dollar und 1.141.467 US-Dollar. Der Mittelwert lag bei 46.000 US-Dollar.[2]

1, 2: Data Breach Investigations Report 2024. (n.d.). Verizon Business. https://www.verizon.com/business/de-de/resources/reports/dbir/

Die Anzahl der Angriffe ist jedoch nicht der einzige Grund zur Sorge. Cyberkriminelle bauen zudem ihre Kapazitäten aus und entwickeln immer komplexere Angriffsmethoden, um auch die neuesten Technologien zur Angriffsabwehr und Verhinderung von Datenverlusten auszuhebeln und Richtlinien zu umgehen, die die Sorgfalt im Unternehmen verbessern sollen. ANSSI, die französische Behörde für die IT-Sicherheit, stellte 2022 in ihrem Bericht über Cyberbedrohungen fest: „Angreifer bauen ihre Kapazitäten kontinuierlich aus, um Ziele wie finanzielle Bereicherung, Spionage und Destabilisierung zu erreichen. Dies zeigt sich vor allem an ihren gezielten Versuchen, sich unbemerkt dauerhaften Zugang zu den Netzwerken ihrer Opfer zu verschaffen.“[3]

Mehr Schwachstellen

Unternehmen sollten sich vor Augen führen, dass technische Neuerungen, umfangreichere Netzwerkfunktionen und moderne Arbeitsweisen auch dazu führen, dass es mehr Schwachstellen gibt, die von Cyberkriminellen ausgenutzt werden können. „Ein wesentlicher Faktor sind die Remote-Arbeit und hybride Arbeitsmodelle in Unternehmen, die eine Neuausrichtung der IT-Sicherheit bedingen“, sagt Steven Gevers, Associate Director, Security Consulting Services bei Verizon Business.

3. ANSSI (2022). PANORAMA DE LA CYBERMENACE 2022. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

Wie im DBIR erläutert, hat sich die Anzahl der Datenschutzverletzungen, bei denen Schwachstellen (oft Teil Zero-Day-Exploits) ausgenutzt wurden, in jüngster Vergangenheit verdreifacht. Eine grundlegende Sicherheitshygiene sollte in Unternehmen daher unbedingt eingehalten werden. Diese Entwicklung zeigt aber auch, wie wichtig Konzepte wie Zero Trust und Defense in Depth weiterhin sind.

> Deshalb sollten Sie sich eine klare Übersicht, darüber verschaffen, in welchen Bereichen Ihrer Infrastruktur die größten Risiken drohen. Dann können Sie Ihr Sicherheitsbudget genau dort einsetzen, wo es am meisten bewirkt.
>
> **Steven Gevers**
> Associate Director, Security Consulting Services bei Verizon Business

Probleme können auch entstehen, wenn Beschäftigte versuchen, Dinge selbst zu regeln. Heutzutage sind wir alle daran gewöhnt, unsere Aufgaben zügig und auf digitalem Weg zu erledigen.
Wenn ein Problem sich nicht schnell genug lösen lässt, ist es oft sehr verlockend, nicht genehmigte oder ungesicherte Software oder Hardware einzusetzen, ohne vorher zu prüfen, ob wir damit vielleicht gegen Sicherheitsvorschriften verstoßen. Bei einer Umfrage des Harvard Business Review gaben 67 % der Befragten zu, Richtlinien zur Cybersicherheit schon mindestens einmal nicht vollständig eingehalten zu haben.[4] Dadurch entsteht die sogenannte Schatten-IT – und mit ihr zusätzliche Schwachstellen und potenzielle Einfallstore für Cyberkriminelle.

4. Verizon (2023). Whitepaper „Mobile Security Index 2023“. https://www.verizon.com/business/resources/T19d/reports/mobile-security-index-report.pdf

Sicherheit, die genau zum Unternehmen passt

Die zunehmende Gefahr von Cyberangriffen war Anlass für viele Unternehmen, Zero-Trust- und SASE-Lösungen einzuführen. Das verbessert zwar die Netzwerksicherheit, wirkt sich aber möglicherweise negativ auf die Interoperabilität der Infrastruktur aus.

„Verschiedene Geschäftsbereiche verwenden unterschiedliche Anwendungen, haben ihre eigenen Abläufe und Anforderungen“, sagt Stephen Young, Director, Cyber Defense Consulting Services bei Verizon Business. „Bei der Sicherheit musss eine ganze Reihe von Aspekten berücksichtigt werden und jeder von ihnen wirkt sich auf die weitere Umgebung und die Fähigkeit, verschiedenen Angriffsarten standzuhalten, aus. Eine Universallösung gibt es leider nicht. Resiliente Sicherheit muss daher über Zero Trust und SASE hinausgehen.“

> Eine Universallösung gibt es nicht. Resiliente Sicherheit muss daher über Zero Trust und SASE hinausgehen.

Stephen Young
Director, Cyber Defense Consulting Services bei Verizon Business

Grundlegende Maßnahmen richtig umsetzen

Mitunter konzentrieren sich Unternehmen so sehr auf einzelne große Sicherheitsrisiken, dass sie die einfachen, grundlegenden Sicherheitsmaßnahmen aus den Augen verlieren. „Je komplexer die Situation und je größer die Bedrohung, desto mehr vernachlässigen Unternehmen die einfachsten Dinge“, sagt Young.

> Wirksame Sicherheit gibt es nur, wenn grundlegende Prinzipien beachtet werden.
>
> **Stephen Young**
> Director, Cyber Defense Consulting Services bei Verizon Business

Natürlich müssen Unternehmen die Sicherheit ihrer Infrastruktur in der Gesamtheit im Blick haben und Lösungen für die großen Probleme finden. Trotzdem dürfen sie die Grundkomponenten der Sicherheit nicht vergessen, etwa Updates für ihre Systeme einzuspielen oder Firewalls korrekt einzurichten. Durch die sorgfältige Erledigung dieser Aufgaben können IT-Teams nicht nur verhindern, dass sich kleine Sicherheitsprobleme einschleichen, sondern möglicherweise auch die Anschaffung unnötiger Sicherheitssysteme vermeiden.

Ein ganzheitlicher Ansatz

Viele Unternehmen versuchen, die Sicherheit durch immer mehr Sicherheitsebenen zu stärken. Tatsächlich kann dies jedoch kontraproduktiv sein, weil es die Komplexität und die Kosten steigert. Besser ist es, die gesamte Situation zu betrachten und genau zu schauen, was wo und warum wirklich gebraucht wird. Deswegen geht Verizon die Sicherheit ganzheitlich an. Ausgangspunkt ist die genaue Analyse des Unternehmens, von der vorhandenen Hard- und Softwareausstattung bis hin zu den Anforderungen einzelner Nutzer.

Hier orientiert sich Verizon am Sicherheitsframework des National Institute of Standards and Technology (NIST), das auf fünf Achsen aufbaut.[5]

Verizon kann die individuellen Anforderungen eines Unternehmens mittels detaillierter Sicherheitsbewertungen ermitteln. Anschließend begleiten wir die Bereitstellung speziell auf diese Anforderungen abgestimmter Sicherheitsmaßnahmen.

- Identifizierung
- Schutz
- Erkennung
- Reaktion
- Wiederherstellung

5. National Institute of Standards and Technology (2024). „The NIST Cybersecurity Framework (CSF) 2.0“. In NIST CSWP 29[Bericht]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

> Jedes Unternehmen hat seine eigene Kultur und Risikobereitschaft – und daher auch einen individuellen Sicherheitsansatz.

Steven Gevers
Associate Director,
Security Consulting bei Verizon Business

„Manche Unternehmen betrachten Technologien wie die generative KI als Risiko für ihr geistiges Eigentum, das eliminiert werden muss. Andere sehen es als Geschäftschance mit etwas Schulungsbedarf. Wir helfen unseren Kunden, den Reifegrad ihrer Sicherheitsinfrastruktur zu verbessern und sich dabei auf die größten Risiken zu konzentrieren, ohne die Geschäftsanforderungen aus den Augen zu verlieren. Das erfordert eine mehrschichtige Sicherheit, d. h. den Einsatz mehrerer Sicherheitsmaßnahmen zum Schutz der Unternehmensressourcen. Dadurch können Organisationen Flexibilität auf einer Ebene nutzen und das Risiko durch Kontrollen auf einer anderen Ebene im akzeptablen Bereich halten. Gibt es einen Sicherheitsvorfall auf einer Ebene, können die anderen Ebenen den Angriff stoppen oder seine Auswirkungen begrenzen.“

Diese Herangehensweise sorgt nicht nur für einen äußerst robusten Schutz Ihrer IT, sondern trägt auch zu einem effektiven Kostenmanagement bei, denn so können Unternehmen in die zu ihren Anforderungen passenden Lösungen investieren und ihre Budgets effektiver einsetzen. „Hat man die Anforderungen eines Unternehmens in ihrer Gesamtheit im Blick, kann man maßgeschneiderte Lösungen liefern und so den Wildwuchs redundanter Sicherheitslösungen vermeiden“, sagt Young. „Diese Art von Rationalisierung ermöglicht eine bessere Kostenkontrolle.“

Dieser ganzheitliche Sicherheitsansatz eröffnet Unternehmen den Weg zu den richtigen Sicherheitslösungen, die zu ihren Anforderungen und ihrem Budget passen. So können sie Cyberangriffe besser abwehren.

Hier erfahren Sie, wie Verizon Sie unterstützen kann, Cyberbedrohungen mit ganzheitlichen Lösungen abzuwehren, die den Anforderungen Ihres Unternehmen gerecht werden: verizon.com/business/de-de. Melden Sie sich hier an, um E-Mails mit Informationen zu unseren Sicherheits- und SASE-Lösungen zu erhalten.