Der MSP-Guide für ein mehrstufiges Sicherheitskonzept

8 Schritte, mit denen Sie sicherstellen können, dass Ihre **Sicherheitspraktiken** den **gesamten Lebenszyklus** des Cybersicherheitsmanagements abdecken.

Über diesen Guide

In diesem Leitfaden wird erörtert, wie wichtig es ist, KMUs bei der Absicherung ihres Unternehmens zu unterstützen. Dazu muss ein mehrstufiges umfassendes Sicherheitskonzept mit umfangreicher Abdeckung des gesamten Cybersicherheitslebenszyklus implementiert werden.

Unter Druck

Warum KMUs ihre Unternehmen absichern müssen

Die Bedrohung ist real. Wie die folgenden erschreckend hohen Zahlen zeigen, stehen Unternehmen enorm unter Druck. Cyberangriffe können jederzeit passieren und haben das Potenzial, irreparable Schäden zu verursachen. Kleine und mittlere Unternehmen (KMUs) sind besonders gefährdet, da es ihnen häufig an Bewusstsein, Wissen und Ressourcen mangelt. Angesichts der sich verschärfenden Bedrohungslandschaft fühlen sie sich schnell überfordert und allein gelassen.

Mehr Cyberkriminalität gegen KMUs

68 %

der KMUs wurden im Jahr 2022 Opfer von schwerwiegenden Cloud-Sicherheitsvorfällen.[1]

61 %

der KMUs befürchten, dass ihr Unternehmen in den nächsten 12 Monaten Opfer eines Ransomware-Angriffs werden könnte.[2]

Steigende Kosten

2,8 Millionen

Malware-Angriffe wurden in der ersten Hälfte des Jahres 2022 weltweit verzeichnet.[3]

Wachsende Unvorbereitetheit

42 %

der KMUs führen ihreSicherheitsprobleme auf mangelnde Schulungen zurück.[2]

Unter Druck

MSPs müssen sich zuerst selbst schützen, bevor sie ihre Kund:innen schützen können

MSPs stellen eine der größten Bedrohungen für die Sicherheit ihrer Kund:innen dar. Durch RMM-Tools (Remote Monitoring and Management) hat ein MSP direkten Zugriff auf die Kunden-Endpoints. Das ist genau der Zugriff, den Cyberkriminelle sich wünschen: Anstatt in jedes Unternehmen einzeln eindringen zu müssen, nutzen sie einfach das RMM-Tool eines MSP als Angriffsziel. So können sie sich Zugriff auf das System verschaffen und Ransomware an alle MSP-Kund:innen auf einmal verbreiten.

MSPs müssen sich selbst schützen, bevor sie ihre Kund:innen schützen können – befolgen Sie also auch selbst die Best Practices, die Sie Ihren Kund:innen empfehlen.

Unter Druck

Bedrohungen von allen Seiten

Was besonders beunruhigend an der modernen Cybersicherheitslage ist: Die Cyberkriminalität nimmt insgesamt zu und es gibt immer mehr Arten von Bedrohungen, über die Unternehmen Bescheid wissen und vor denen sie sich schützen müssen.

Von direkten Brute-Force-Angriffen (z. B. DDoS-Angriffe auf Netzwerke und Algorithmus-gestützte Passwortangriffe) bis hin zu eher unbemerkten Angriffen, die darauf abzielen, die Systemabwehr zu umgehen und Schaden anzurichten oder vertrauliche Informationen zu stehlen: Es gibt immer mehr und vielfältigere Cyberangriffe, die auf die digitale Infrastruktur Ihrer Kund:innen abzielen.

Cyberkriminelle werden immer raffinierter und sind daher immer schwerer zu bekämpfen.

Social-Engineering-Techniken manipulieren das menschliche Verhalten und nutzen es aus, um Nutzer:innen zur Preisgabe wertvoller Informationen zu verleiten. Dies ist besonders effektiv, wenn das Passwort einer Person kompromittiert wurde und die Angreifer das Vertrauen des Opfers in seine Kontakte ausnutzen können.

Phishing-Versuche sind inzwischen immer schwerer zu erkennen: Grammatikalische Fehler, ungeschickte Formulierungen und verdächtige Formatierungen gehören der Vergangenheit an. Phishing-E-Mails und -Websites können echte Personen und seriöse Marken immer besser imitieren und so Endnutzer:innen zur Preisgabe vertraulicher Informationen verleiten.

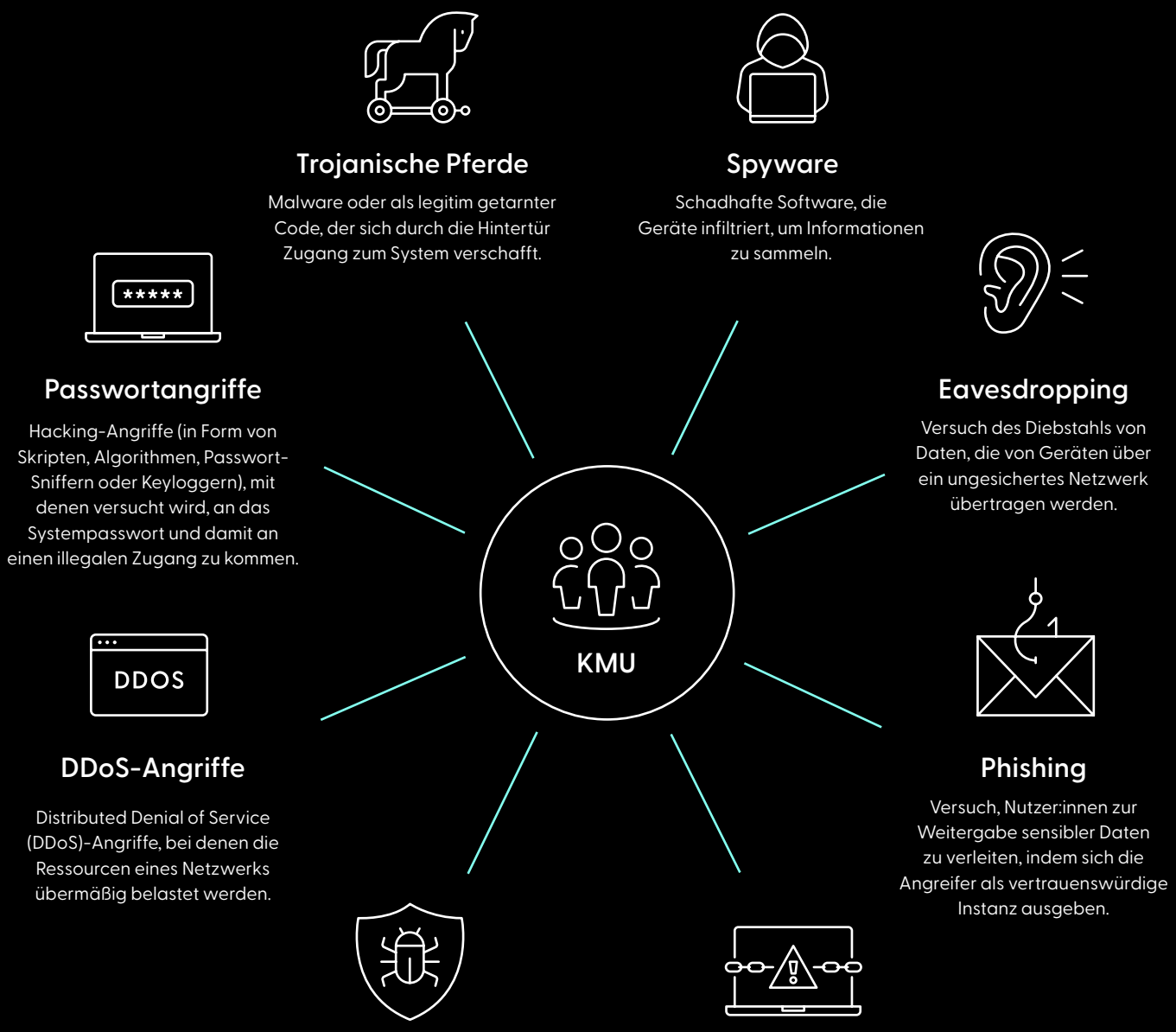
Business Email Compromise (BEC)-Angriffe können selbst versierte Nutzer:innen treffen: Sie denken, sie sehen eine dringende Nachricht von ihrem Chef und möchten möglichst schnell antworten.

Auch **Spoofing-Techniken** sind heute wesentlich ausgereifter. Mithilfe professioneller Grafiken werden vertrauenswürdige Marken imitiert und die Nutzer:innen zum Herunterladen von Malware verleitet.

Zero-Day-Angriffe und dateilose, ausführbare Malware, die sich an Tools zum Scannen von Anhängen vorbeimogelt, werden ebenfalls immer häufiger.

Unter Druck

Bedrohungen von allen Seiten



Trojanische Pferde

Malware oder als legitim getarnter Code, der sich durch die Hintertür Zugang zum System verschafft.

Spyware

Schadhafte Software, die Geräte infiltriert, um Informationen zu sammeln.

Passwortangriffe

Hacking-Angriffe (in Form von Skripten, Algorithmen, Passwort-Sniffern oder Keyloggern), mit denen versucht wird, an das Systempasswort und damit an einen illegalen Zugang zu kommen.

Eavesdropping

Versuch des Diebstahls von Daten, die von Geräten über ein ungesichertes Netzwerk übertragen werden.

DDoS-Angriffe

Distributed Denial of Service (DDoS)-Angriffe, bei denen die Ressourcen eines Netzwerks übermäßig belastet werden.

Phishing

Versuch, Nutzer:innen zur Weitergabe sensibler Daten zu verleiten, indem sich die Angreifer als vertrauenswürdige Instanz ausgeben.

Malware, Würmer und Viren

Schadhafte Software, die darauf abzielt, Daten auf einem Gerät oder Netzwerk zu beschädigen oder zu stehlen.

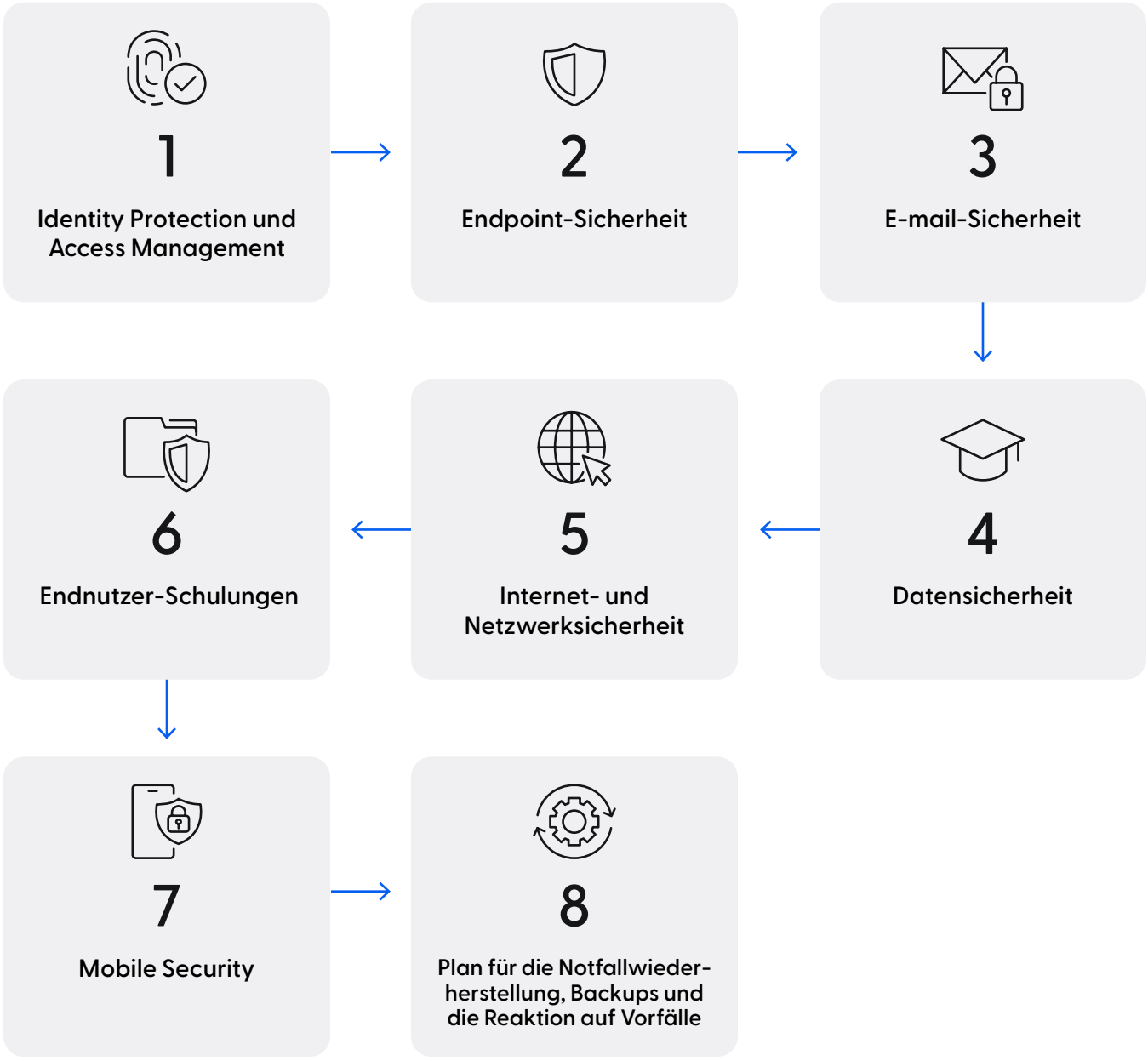
Ransomware

Malware, durch die Nutzer:innen von einem Gerät, System oder von Daten ausgesperrt werden, bis sie eine Gebühr bezahlen.

Verstärken der KMU-Schutzmaßnahmen

Proaktive Sicherheitsmaßnahmen sind unerlässlich

Um sich gegen die zunehmende Zahl und Bandbreite von Angriffen zu schützen, müssen Unternehmen einen vielschichtigen Verteidigungsansatz verfolgen, der Sicherheitsmaßnahmen, Zugangsbeschränkungen, Endnutzer-Schulungen und Schutzmaßnahmen am Netzwerkperimeter miteinander verbindet. Im Grunde genommen müssen moderne Unternehmen zu digitalen Festungen mit mehreren Ebenen proaktiver Schutzmaßnahmen werden, die dazu dienen, die unzähligen Cyberangriffe zu erkennen, zu melden und zu verhindern.



Verstärken der KMU-Schutzmaßnahmen

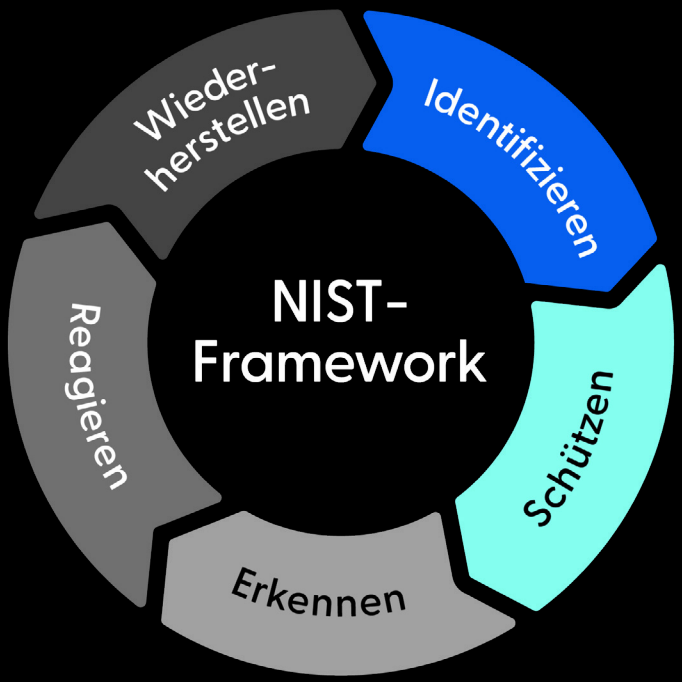
Industriestandards als Richtschnur

Die Center for Internet Security (CIS) Critical Security Controls (auch als CIS Controls bezeichnet) sind eine Reihe von Handlungsempfehlungen für die Cyberabwehr, die spezifische und umsetzbare Möglichkeiten zur Vereitelung von Cyberangriffen bieten. Darunter sind 18 Maßnahmenpakete mit hoher Priorität und 153 Einzelmaßnahmen mit unterschiedlicher Priorität, die eine gute Grundlage für jedes Unternehmen bilden, das seine Sicherheitslage verbessern möchte.

18 Maßnahmen mit hoher Priorität

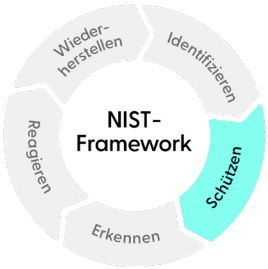
153 Einzelmaßnahmen

Ein Sicherheits-Framework besteht aus Tools, Richtlinien, Personen und Dokumentation. Es definiert Richtlinien und Verfahren für die Einrichtung und Aufrechterhaltung einer Reihe von Sicherheitsmaßnahmen. Die Implementierung der CIS Controls, die von PCI, NIST und Agenturen für Cyberversicherung unterstützt werden, sorgt für Compliance und einen hohen Schutz vor Cyberbedrohungen. Damit sind Sie auch für eine Zukunft gerüstet, in der Compliance-Maßnahmen immer weiter ausgebaut werden. Angesichts von Angriffen auf die Lieferkette, Bedenken hinsichtlich der Compliance sowie Regressforderungen von Versicherern ist es von entscheidender Bedeutung, dass Sie eine Verteidigungsstrategie für Ihr Unternehmen entwickeln.



8 Schritte für den Aufbau umfassender Sicherheitspraktiken

1. Implementieren von Identity Protection-Richtlinien und -Lösungen



Passwörter schützen den Zugriff auf Unternehmensdaten, aber Hacker können sie immer einfacher knacken. Daher sind nicht nur strenge Passwortrichtlinien wichtig, sondern auch zusätzliche Sicherheitsebenen wie die Multi-Faktor-Authentifizierung (MFA). Es ist jedoch genauso wichtig, ein Gleichgewicht zwischen Sicherheit und Produktivität zu finden – andernfalls kann bei Nutzer:innen aufgrund des Aufwands, für jedes Konto eindeutige Passwörter zu erstellen und zu verwalten, eine „Passwortmüdigkeit" auftreten. Oder sie sind frustriert, weil sie bei jeder Anmeldung eine MFA durchführen müssen.

Strenge Passwortrichtlinien durchsetzen

Auch wenn Passwörter nicht die einzige Absicherung für Ihre Daten sein sollten, sollten sie so sicher wie möglich sein. Dafür können bewährte Passwortrichtlinien für das gesamte Unternehmen festgelegt werden.

- Sie sollten ausreichend lang sein und eine Mischung aus Buchstaben, Zahlen, Sonderzeichen und Großbuchstaben enthalten.
- Legen Sie Zeitlimits für Passwörter fest und dass das gleiche Passwort nicht mehrmals verwendet werden kann.

24 %

der KMUs führen Cybersicherheitsprobleme auf schwache Passwörter zurück.[2]

MFA aktivieren

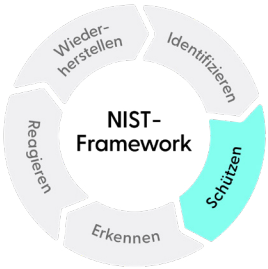
Eine MFA ist die beste zusätzliche Sicherheitsebene für Passwörter und einen höheren Zugriffsschutz. Der Zugriff auf Apps und Daten ist dann nur über eine zweite Form der Authentifizierung (zusätzlich zum Passwort) möglich, z. B. über zeitlich limitierte Codes, die per Textnachricht, E-Mail oder App gesendet werden, Fingerabdrücke oder Antworten auf persönliche Sicherheitsfragen.

99 %

der kompromittierten Konten hatten keine MFA-Absicherung.[4]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

1. Implementieren von Identity Protection-Richtlinien und -Lösungen



Single Sign-on (SSO) nach Möglichkeit mit MFA kombinieren

App-Anmeldungen können mit der MFA bis zu 10–30 Sekunden länger dauern, was sich mit jeder genutzten App summiert. Damit die Nutzer:innen trotz schärferer Sicherheitsmaßnahmen produktiv bleiben, sollten Sie wann immer möglich SSO (einmalige Anmeldung) aktivieren, z. B. für alle Microsoft-Apps. So müssen die Nutzer:innen weniger Anmeldeinformationen verwalten und sich nicht jeden Tag mehrmals bei Apps anmelden. SSO kann auch helfen, die Anzahl der Helpdesk-Tickets für das Zurücksetzen von Passwörtern zu reduzieren.

16 %

der Mitarbeitenden nutzen eine SSO-Lösung.[5]

Regeln für die Zugriffsbeschränkung (Conditional Access, CA) festlegen

Um ein besseres Gleichgewicht zwischen Sicherheit und Nutzerfreundlichkeit zu erreichen, kann die MFA für Nutzer:innen im Büro reduziert werden, aber weiterhin in nicht vertrauenswürdigen Netzwerken (zu Hause, an Flughäfen, in Cafés usw.) angefordert werden. Dann fühlen sich Nutzer:innen durch die zusätzlichen MFA-Schritte weniger gestört und ausgebremst.

24 %

der KMUs meinen, dass das Access Management zu den schwierigsten Sicherheitsherausforderungen zählt.[2]

Tool für Passwortverwaltung anbieten

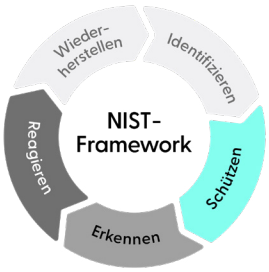
Nicht jede App kann mit SSO kombiniert werden. Um die Anzahl der Passwörter, die die Nutzer:innen verwalten müssen, weiter zu reduzieren (und damit zu verhindern, dass sie die gleichen Passwörter in verschiedenen Apps nutzen), sollten Sie ein Passwortmanagement-Tool anbieten, das sichere Passwörter generiert und Anmeldedaten verschlüsselt und speichert.

11

ist die durchschnittliche Anzahl an Passwörtern, die sich Mitarbeitende von KMUs merken müssen. [5]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

2. Etablieren von Endpoint-Sicherheit



Durch die Zunahme mobiler Geräte hat sich die Zahl der Endgeräte (Endpoints) in Unternehmen drastisch erhöht. Zusätzlich zu Servern und Desktops stellen die Laptops, Tablets und Smartphones der Mitarbeitenden eine weitere mögliche Schwachstelle dar, über die Malware in das Unternehmensnetzwerk eingeschleust werden kann. Einfach nur Antivirensoftware zu installieren, reicht aufgrund der zunehmenden Verbreitung von Angriffsvektoren, einschließlich E-Mail-Anhängen und Hyperlinks, Websites, sozialen Medien und Apps, nicht mehr aus.

Traditionelle Antivirenlösungen können Angriffe nur verhindern, wohingegen moderne EDR-Lösungen (Endpoint Detection and Response) Bedrohungen auf Geräten, Desktops und Servern aktiv erkennen und beheben. Fortschrittliche Lösungen zum Endpoint-Schutz nutzen Automatisierung, maschinelles Lernen und Verhaltensüberwachung, um eine Vielzahl von Bedrohungsvektoren zu erkennen, darauf zu reagieren und sie zu beseitigen, darunter ausführbare oder dateilose Malware, Dokumenten- und Browser-Exploits, bösartige Skripte und das Auslesen von Anmeldeinformationen. Darauf sollten Sie bei EDR-Tools achten:

- Sichtbarkeit von Endpoints, Apps, laufenden Prozessen und verschlüsseltem Datenverkehr
- Bedrohungsforensik
- Möglichkeit, infizierte Endpoints zu isolieren und vom Netzwerk zu trennen
- Dateiwiederherstellung und Geräte-Rollback

68 %

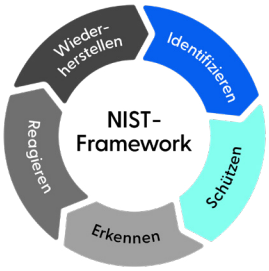
der Unternehmen waren von einem oder mehreren Endpoint-Angriffen betroffen, durch die ihre Daten und IT-Infrastruktur erfolgreich kompromittiert wurde.[6]

70 %

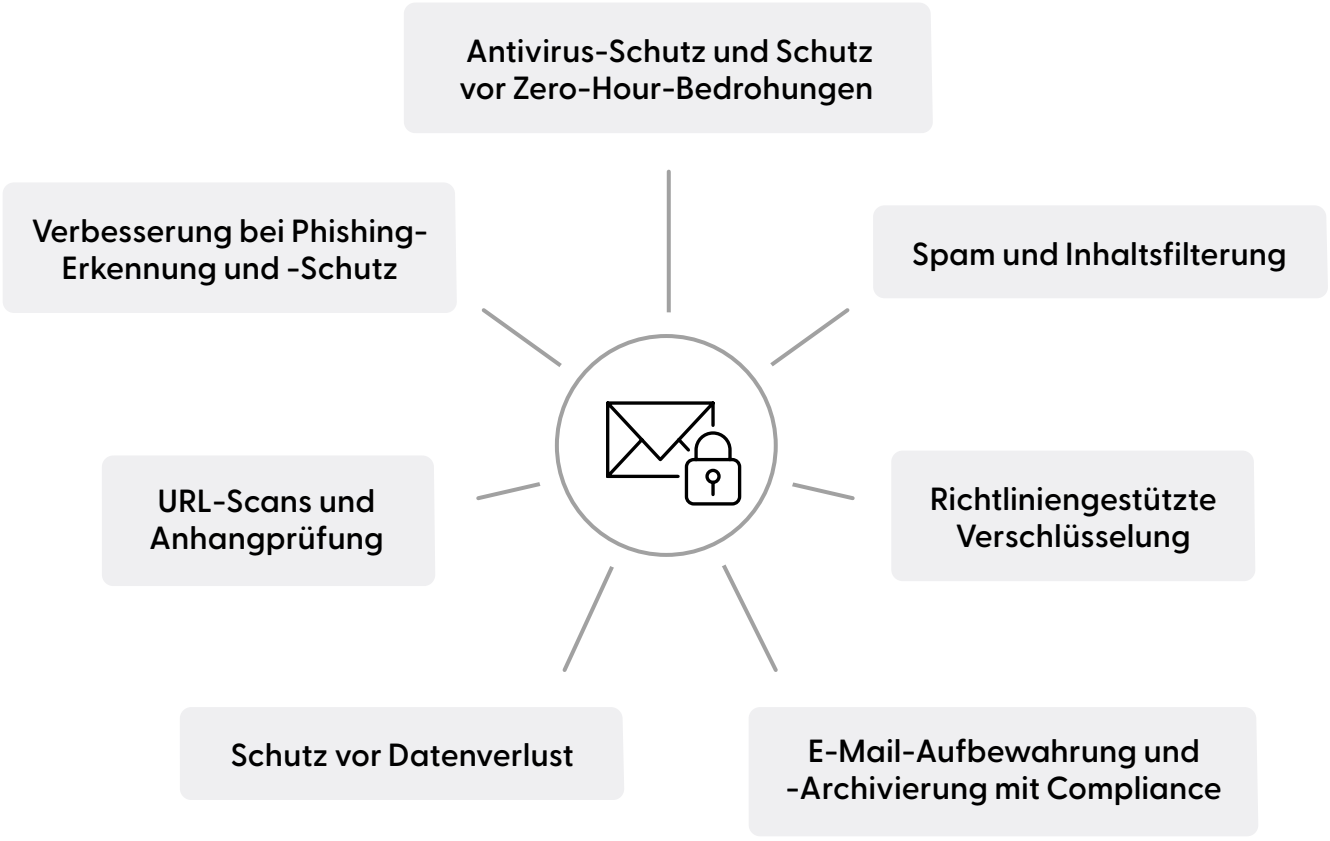
der erfolgreichen Angriffe beginnen auf Endpoints.[6]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

3. Anwenden zusätzlicher E-Mail-Sicherheit

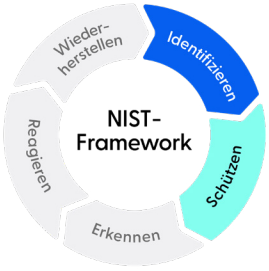


E-Mails sind die größte Schwachstelle für Phishing, Ransomware, Spam und Malware. Es ist von entscheidender Bedeutung, dass sensible Daten nicht das Unternehmen verlassen und dass Bedrohungen gestoppt werden, bevor sie über diesen Weg in Ihr Netzwerk gelangen können. Die nativen Sicherheitsfunktionen der meisten E-Mail-Lösungen, einschließlich Microsoft 365, bieten keinen ausreichenden Schutz vor modernen Bedrohungen. Sie sollten daher zusätzlich die Lösung eines Drittanbieters mit erweiterten Sicherheitsfunktionen nutzen.



8 Schritte für den Aufbau umfassender Sicherheitspraktiken

4. Verstärken der Datensicherheit und Compliance



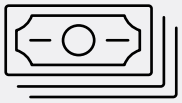
54 % der KMUs wurden 2022 Opfer eines Cyberangriffs, aber nur 30.000 Unternehmen sind nach Cyber Essentials zertifiziert. [9, 10]

Der Schutz von sensiblen Informationen eines Unternehmens durch Datenverlust-Prävention und E-Mail-/Dateiverschlüsselung hilft, Datenschutzverletzungen und die potenziellen Kosten für Rechtsstreitigkeiten, Strafen, Bußgelder und Vergleiche abzuwenden. Dies ist besonders wichtig für Unternehmen, die Vorschriften einhalten müssen, wie z.B. ISO 27001 Zertifizierungen und Payment Card Industry (PCI) Standards.

Jedes Jahr werden Millionen von Unternehmen Opfer von Cyberangriffen und verlieren dadurch wichtige Gewinne und ihren guten Ruf. Die Einhaltung anerkannter Cybersicherheits-Frameworks bedeutet, dass Sie Ihr Unternehmen und die Unternehmen Ihrer Kund:innen vor Cyberkriminalität schützen. Mit einem klaren Fahrplan in puncto Cybersicherheit sind Sie für den schlimmsten Fall gewappnet.

Bösartige Angriffe

sind die häufigste und teuerste Ursache für Datenschutzverletzungen.

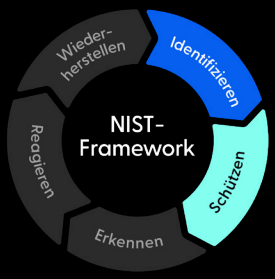


Kleine Unternehmen

sind im Vergleich zu größeren Unternehmen mit unverhältnismäßig höheren Kosten aufgrund von Datenschutzverletzungen konfrontiert.

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

4. Verstärken der Datensicherheit und Compliance



Schutz vor Datenverlust

Sorgen Sie bei vertraulichen und wichtigen Informationen dafür, dass sie nicht versehentlich weitergegeben werden, verloren gehen, preisgegeben oder gestohlen werden, und zwar durch regelbasierte Überwachung und Warnungen (z. B. „in ausgehenden E-Mails dürfen keine Nummern enthalten sein, die auf eine Bankverbindung hinweisen“).

E-Mail-Verschlüsselung

Verschlüsseln Sie ein- und ausgehende E-Mails auf der Grundlage von Richtlinien, um sicherzustellen, dass sensible Informationen innerhalb und außerhalb des Unternehmens sicher weitergegeben werden können.

Verschlüsselung der gesamten Festplatte

Implementieren Sie auf allen Laptops eine Verschlüsselung der gesamten Festplatte, damit Unternehmensdaten bei Verlust oder Diebstahl des Geräts geschützt bleiben.

App-Sperrlisten und Web-Sicherheit

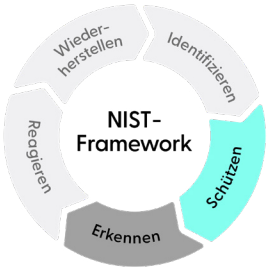
Um sicherzustellen, dass Unternehmensdaten nicht über unüberwachte und ungeschützte Kanäle versendet werden, können Sie den Nutzer:innen die Verwendung ihrer persönlichen E-Mail-Adresse oder Apps wie Dropbox auf Arbeitsgeräten untersagen.

Kontrolle über USB-Geräte

Sperren Sie in Hochsicherheitsumgebungen die USB-Anschlüsse, um zu verhindern, dass sensible, geschützte oder vertrauliche Daten das Unternehmen auf USB-Sticks verlassen.

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

5. Implementieren von Netzwerk- und Websicherheit, die aufeinander abgestimmt sind



Für Unternehmen ist es von entscheidender Bedeutung, Verbindungen abzusichern, um den Zugang zu ihrer Umgebung zu schützen und zu kontrollieren. Für den Schutz des ein- und ausgehenden Netzwerkverkehrs müssen Netzwerk- und Websicherheit aufeinander abgestimmt sein. Die Netzwerksicherheit trägt dazu bei, Netzwerksysteme und Daten vor unbefugtem oder böswilligem Zugriff zu schützen, während die Websicherheit Nutzer:innen vor dem Zugriff auf schadhafte Websites schützt.

Netzwerksicherheit

1. Installieren Sie eine seriöse Firewall der nächsten Generation, die Eindringschutz und -erkennung, URL-Filterung und Schutz vor Datenverlust bietet.

2. Deaktivieren Sie unnötige Ports, um die Angriffsfläche zu verringern und Cyberkriminellen weniger Schwachstellen zu bieten, die sie ausnutzen können. So bietet beispielsweise das Remote-Desktop-Protokoll (RDP) Administratoren leistungsstarke Funktionen, kann aber auch Einfallstor für Angriffe sein. Die Zugangsbeschränkung oder Erzwingung einer ordnungsgemäßen Authentifizierung ist daher von entscheidender Bedeutung.

3. Legen Sie ein Netzwerksegment für Gäste und auch für die privaten Geräte von Mitarbeitenden fest, damit unbefugte Nutzer:innen keinen Zugriff auf nicht für sie bestimmte Ressourcen haben. Außerdem entsteht so eine bessere Trennung zwischen beruflichen und privaten Surfaktivitäten.

47 %

der KMUs planen für das Jahr 2023 umfangreiche Investitionen in die Netzwerksicherheit. [2]

Web-Sicherheit

1. Ob Nutzer:innen einfach nur im Internet surfen oder durch raffinierte Techniken dazu verleitet werden, auf einen schadhaften Link in einer Phishing-E-Mail zu klicken: Schützen Sie die Nutzer:innen, indem Sie verhindern, dass sie schadhafte Websites besuchen.

2. Verhindern Sie, dass Nutzer:innen unangemessene Websites, z. B. pornografische Websites, Websites mit Glücksspielen oder Gaming-Websites aufrufen.

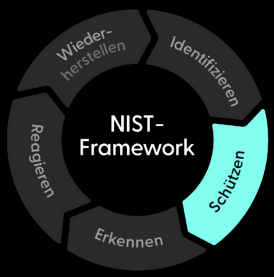
3. Sorgen Sie für einen möglichst geringen Bandbreitenverbrauch, indem Sie die Nutzung von Streaming-Diensten wie Netflix blockieren, die wertvolle Bandbreite verbrauchen.

27 %

der KMUs geben an, dass schadhafte Websites/Webanzeigen der Hauptgrund für Sicherheitsprobleme sind. [2]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

6. Anbieten kontinuierlicher Sicherheitsschulungen für Endnutzer:innen



Die Sicherheitslage eines Unternehmens ist immer abhängig vom/von der unsichersten Mitarbeiter/-in. Und da Phishing-Versuche immer raffinierter werden, kann es selbst versierten Nutzer:innen passieren, dass sie versehentlich auf bösartige Links klicken, riskante Anhänge öffnen oder einer gut gefälschten URL vertrauen und vertrauliche Informationen preisgeben. Bieten Sie daher kontinuierliche Sicherheitsschulungen an, damit Nutzer:innen verschiedene Arten von Bedrohungen erkennen und darauf reagieren können.

Phishing Simulation

Mit Phishing-Simulationstools wird Mitarbeitenden gezeigt, wie sie auf Phishing-Versuche in ihrem Posteingang achten, diese erkennen und melden sollten.

Nur 35 %

Nur 35 % der Unternehmen führen Phishing-Simulationstrainings durch.[7]

Kontinuierliche Mikroschulungen

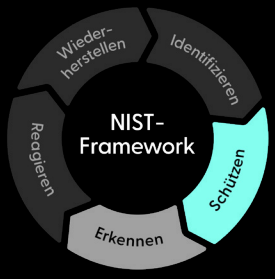
Da Cyberkriminelle immer wieder neue Wege beschreiten, ist es wichtig, dass sich die Nutzer:innen ständig weiterbilden und über die neuesten Bedrohungen auf dem Laufenden bleiben. In geeigneten Schulungen sind Mikroinhalte und Quizfragen enthalten, um den Kenntnisstand abzufragen und zu erheben und den Fortschritt unternehmensweit zu verfolgen.

74 %

74 % der Unternehmen haben formale Sicherheitstrainings.[7]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

7. Berücksichtigen von Mobile Security



Bereits vor der Corona-Pandemie haben viele Unternehmen begonnen, das mobile Arbeiten in Form von Remote-Arbeit und Bring-your-own-device (BYOD)-Richtlinien zu fördern. Die Pandemie hat diesen Wandel beschleunigt, sodass Mitarbeitende heute erwarten, dass sie bequem und flexibel überall dort arbeiten können, wo sie es wollen. Dies bedeutet jedoch, dass die Sicherheitsmaßnahmen innerhalb des Netzwerks nicht mehr ausreichen, um Unternehmensressourcen zu schützen. Mobile Geräte sind heute beliebte Einfallstore für Malware, und zwar durch unsichere WLANs, Anwendungsschwachstellen oder auch verlorene und gestohlene Geräte.

Mobile-Security-Lösungen unterstützen Unternehmen bei der Verwaltung und dem Schutz von mobilen Smartphones, Tablets, Laptops und IoT-Geräten im Unternehmensnetzwerk und bieten eine zusätzliche Sicherheitsebene für mobile Endpoints. Zu den häufigsten Funktionen gehören:

- Das Gerätemanagement umfasst die Geräteadministration einschließlich Registrierung, Konfiguration, Richtlinienverwaltung, Verwaltung von BYOD-Datenschutzeinstellungen und Fernlöschung (Remote Wipe).
- Die Verwaltung mobiler Anwendungen bietet die Möglichkeit, Apps auf Geräte zu verteilen, Push-Benachrichtigungen für benötigte Updates zu versenden und zu verhindern, dass Nutzer:innen unsichere Apps herunterladen.
- Im Rahmen des Content-Managements können Nutzer:innen über Verschlüsselung und Autorisierung sicher auf Unternehmensdokumente auf mobilen Geräten zugreifen und diese gemeinsam nutzen.
- Die Netzwerkzugriffskontrolle ermöglicht autorisierten Geräten einen sicheren Zugriff auf das Unternehmensnetzwerk und interne Ressourcen.
- Durch Isolierung werden die arbeitsbezogenen Apps von Nutzer:innen von den privaten Apps getrennt, sodass geschäftliche Daten bei Bedarf gelöscht werden können, ohne dass die persönlichen Informationen der Nutzer:innen gefährdet sind.

45 %

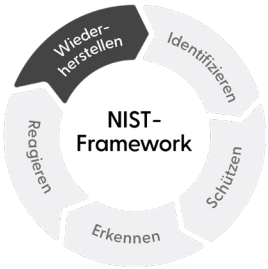
45 % der Unternehmen wurden im Jahr 2022 durch ein mobiles Gerät kompromittiert.[8]

53 %

53 % der mobilen Geräte haben Zugang zu mehr sensiblen Daten als im Jahr 2021. [8]

8 Schritte für den Aufbau umfassender Sicherheitspraktiken

8. Erstellen eines Plans zur Notfallwiederherstellung und -reaktion



Nur 29 % der KMUs meinen, dass sie über eine solide Strategie zur Notfallwiederherstellung verfügen. [2]

Von böswilligen Bedrohungen und Benutzerfehlern bis hin zu physischen Katastrophen und Hardwareausfällen: Es gibt unzählige Möglichkeiten, wie ein Unternehmen wertvolle Daten verlieren oder Ausfallzeiten erleiden kann. Dies kann sich stark auf die Produktivität auswirken, zu steigenden IT-Kosten führen und die Marke des Unternehmens schädigen.

Unternehmen jeder Größe müssen im Voraus planen, wie sie im Falle einer Datenschutzverletzung, eines Ausfalls oder eines Cyberangriffs am besten so reagieren, dass Daten geschützt werden und der Betrieb aufrechterhalten wird. Dies ist vor allem für Unternehmen in Branchen wichtig, die der Einhaltung von Vorschriften unterliegen, wie z. B. das Gesundheits- und Finanzwesen.

Ein effektiver Plan zur Sicherung und Wiederherstellung im Notfall sollte Folgendes umfassen:

- Identifizieren der wichtigsten Bedrohungen für Daten und den Betrieb sowie deren Wahrscheinlichkeitsgrad
- Definition der Toleranz des Unternehmens gegenüber Ausfallzeiten und Datenverlusten
- Inventarisierung aller Hardware, Software, Apps und Daten – dann Priorisierung der kritischen Elemente
- Konzipieren einer Strategie für die Datenwiederherstellung, einschließlich Dienst/Lösung, Speicherort und Prozesse, und Festlegen der Prioritäten für die Wiederherstellung
- Etablieren von Prozessen zur Wiederherstellung des Zugangs zu wichtigen IT-Ressourcen, Apps und Daten
- Festlegung von Rollen und Verantwortlichkeiten im Rahmen des Aktionsplans
- Erstellung eines Kommunikationsplans für die interne und externe Kommunikation bei Ausfällen
- Einführung eines Programms zur Schulung und Sensibilisierung der Mitarbeitenden

Microsoft + Backup von Drittanbietern

Microsoft-Kund:innen sind unter Umständen erstaunt, wenn sie erfahren, dass Microsoft selbst Backup-Lösungen von Drittanbietern empfiehlt.

Der Abschnitt „Dienstverfügbarkeit“ im Microsoft-Servicevertrag besagt Folgendes:

Wir bemühen uns, die Dienste am Laufen zu halten. Alle Online-Dienste leiden gelegentlich unter Störungen und Ausfällen. Microsoft ist nicht für eine Unterbrechung des Diensts oder für Datenverluste verantwortlich. Im Fall eines Ausfalls oder einer Unterbrechung des Diensts sind Sie möglicherweise nicht in der Lage, Ihre Inhalte oder Daten abzurufen. Es wird empfohlen, die Inhalte und Daten regelmäßig zu sichern, die Sie in den Diensten oder während der Verwendung von Drittanbieter-Apps und -Diensten speichern.

Ihre Sicherheitsexperten

Resümee

Das in diesem Guide beschriebene mehrstufige Sicherheitskonzept kann für KMUs mit begrenzten IT-Ressourcen kompliziert und herausfordernd wirken – vor allem, wenn aufgrund der potenziellen Schadenskosten bei einem Verstoß so viel auf dem Spiel steht. Tatsächlich geben drei von vier KMUs an, dass sie nicht genügend Personal für die IT-Sicherheit haben.

Da sich kleine und mittelständische Unternehmen überfordert fühlen und nicht ausreichend auf die zunehmende Zahl und Vielfalt von Cyberangriffen vorbereitet sind, sind MSPs wie Sie von entscheidender Bedeutung, um ihre Kund:innen zu modernen, proaktiven Verteidigungsmaßnahmen anzuleiten.

Und Sie sind damit nicht allein – Pax8 hilft Ihnen, Lücken in den Technologiestrukturen Ihrer Kund:innen zu erkennen und die Cloud-Sicherheitslösungen zu implementieren, die sie zur Bekämpfung der modernen Cyberbedrohungen benötigen.

Weitere Ressourcen

Infografik: **NIST Framework (Englisch)**

Infografik: **Kostenkalkulator für Ausfallzeiten (Englisch)**

Möchten Sie mit uns über Sicherheitslösungen sprechen, die Sie als zusätzliche Schutzebenen anbieten können?

Jetzt Termin vereinbaren

Quellen

1. Snyk, The State of Cloud Security Report 2022, 2022
2. Datto, 2022 SMB Cybersecurity Report for MSPs, 2023
3. Annual Number of Malware Attacks Worldwide from 2015–2022, Statista, 2023
4. Microsoft, 2023 Identity Security Trends and Solutions from Microsoft, 2023
5. Specops Software, The 2022 Weak Password Report, 2022
6. PurpleSec, Cyber Security Stats for 2023, 2023
7. Proofpoint, 2023 State of the Phish Report, 2023
8. Verizon, 2022 Mobile Security Index, 2022
9. Vodafone, Half of SMEs experience surge in cyber-attacks, 2023
10. 30,000 organisations have certified to Cyber Essentials, 2019

