ATTACKS ARE ON THE RISE AGAIN – WHAT YOU NEED TO KNOW

ÜBER HORNETSECURITY

Hornetsecurity ermöglicht es Unternehmen und Organisationen jeder Größe, sich auf ihr Kerngeschäft zu konzentrieren, indem es M365-Workloads und die E-Mail-Kommunikation schützt, Daten sichert und Geschäftskontinuität und Compliance mit Cloud-basierten Lösungen der nächsten Generation gewährleistet.

Unser Flaggschiffprodukt 365 Total Protection ist die umfassendste Cloud-Sicherheitslösung für Microsoft 365 auf dem Markt und umfasst E-Mail-Sicherheit, Compliance, Governance und Backup.

WAS IST DER CYBERSECURITY REPORT?

Der Cybersecurity Report von Hornetsecurity ist eine jährliche Analyse der aktuellen Bedrohungslandschaft, die auf realen Daten basiert, die vom Security Lab von Hornetsecurity gesammelt und ausgewertet werden. Hornetsecurity verarbeitet jeden Monat mehr als 6 Milliarden E-Mails. Durch die Analyse der in diesen E-Mails identifizierten Bedrohungen, kombiniert mit einem tiefgehenden Verständnis der allgemeinen Bedrohungslandschaft, deckt das Security Lab wichtige Sicherheitstrends und Aktivitäten von Angreifern auf. Außerdem können fundierte Prognosen für die Zukunft der Microsoft-365-Sicherheitsbedrohungen erstellt werden, sodass Unternehmen entsprechend handeln können. Die Ergebnisse und Daten aus dem Jahr 2025 sowie Prognosen für 2026 finden Sie in diesem Report.

WAS IST DAS SECURITY LAB?

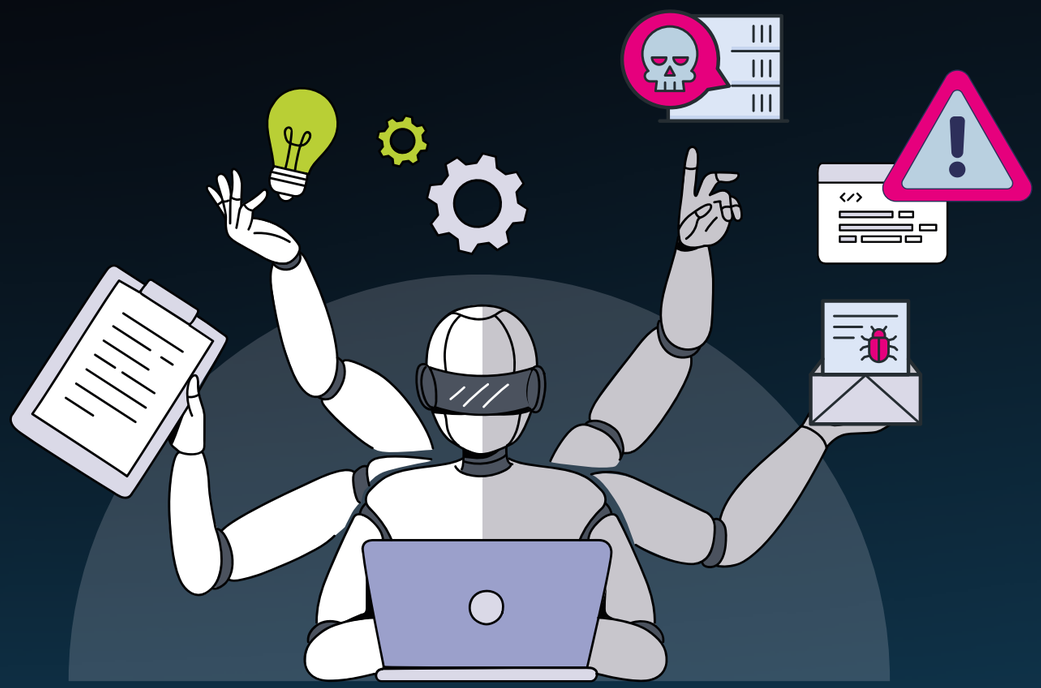
Das Security Lab ist eine Abteilung von Hornetsecurity, die forensische Analysen der aktuellsten und kritischsten Sicherheitsbedrohungen durchführt und auf die E-Mail Sicherheit in der Microsoft-365-Umgebung spezialisiert ist. Dieses multinationale Team aus Sicherheitsexperten verfügt über umfassende Erfahrung in der Sicherheitsforschung, Softwareentwicklung und Data Science.

Ein tiefgreifendes Verständnis der Bedrohungslandschaft, gewonnen durch die Untersuchung realer Phishing-Angriffe, Malware, Ransomware-Gruppen und mehr, ist entscheidend für die Entwicklung wirksamer Gegenmaßnahmen. Die detaillierten Erkenntnisse des Security Labs bilden die Grundlage für die Next-Gen-Cybersicherheitslösungen von Hornetsecurity.

VERWENDUNG DIESES BERICHTS

Dieser Bericht besteht aus fünf Hauptabschnitten:

- Kapitel 1 enthält die Zusammenfassung der wichtigsten Ergebnisse.
- Kapitel 2 konzentriert sich auf die aktuelle Bedrohungslage der Microsoft-365-Plattform.
- Kapitel 3 behandelt die zentralen Herausforderungen und Diskussionen rund um die größten Bedrohungen und Trends aus dem Jahr 2025.
- Kapitel 4 beinhaltet Prognosen des Security Labs zu Cybersecurity-Gefahren im Jahr 2026 sowie Empfehlungen und Leitlinien, um Ihr Unternehmen bestmöglich zu schützen.
- Kapitel 5 listet alle Quellen und weiterführende Links auf, die in diesem Bericht verwendet wurden.



BALANCING INNOVATION AND THREAT:
THE DUAL NATURE OF AI

KAPITEL 1
ZUSAMMENFASSUNG

Das Jahr 2025 war geprägt von Beschleunigung. Bedrohungsakteure nutzten Automatisierung, künstliche Intelligenz und Social Engineering in bisher nie dagewesener Geschwindigkeit, während Verteidiger bemüht waren, Governance-, Resilienz- und Awareness-Programme entsprechend anzupassen. Unsere Analysen im Hornetsecurity-Ökosystem, basierend auf mehr als 6 Milliarden monatlich verarbeiteten E-Mails, bestätigen eine einfache Wahrheit: Die Angriffsfläche wächst schneller, als die meisten Organisationen sie absichern können.

E-Mails bleiben der konstanteste Angriffsvektor für Cyberbedrohungen, doch die Taktiken haben sich weiterentwickelt. Mit Schadsoftware versehene E-Mails nahmen im **Jahresvergleich um 131 %** zu, begleitet von einem Anstieg bei **Betrugsversuchen (+34,7 %)** und **Phishing-Angriffen (+21 %)**. Angreifer setzen zunehmend auf präzise Tarnung statt auf Masse. Sie nutzen legitime Infrastrukturen, verschleierte URLs und unauffällige HTML-Techniken, um sowohl Sicherheitsfilter als auch menschliche Aufmerksamkeit zu umgehen. Gleichzeitig sind bösartige TXT- und alte DOC-Anhänge, die lange als harmlos oder veraltet galten, erneut zu wichtigen Infektionsvektoren geworden. Dies verdeutlicht, dass selbst vermeintlich „risikoarme" Dateitypen nicht mehr ignoriert werden dürfen.

Auch Ransomware erlebte 2025 ein aggressives Comeback. Nach mehreren Jahren relativen Rückgangs gaben **24 % der Unternehmen** an, Opfer eines Angriffs geworden zu sein – ein Anstieg um 29 % im Vergleich zum Vorjahr. Unveränderliche Backups und verbesserte Notfallwiederherstellungspläne haben die Quote der Lösegeldzahlungen auf nur 13 % der Fälle reduziert, doch die Angreifer reagierten mit neuen Strategien: Sie diversifizierten ihre Einfallstore und Ziele. Phishing, kompromittierte Zugangsdaten und Endpunkt-Exploits sind mittlerweile gleichrangige Infiltrationswege. Neue „Ransomware 3.0"-Varianten konzentrieren sich zudem weniger auf Verschlüsselung, sondern zunehmend auf Manipulation der Datenintegrität. Dadurch wird nicht nur die Verfügbarkeit beeinträchtigt, sondern auch das Vertrauen in die Daten selbst untergraben.

Künstliche Intelligenz hat beide Seiten der Sicherheitslage verändert. CISOs sind optimistisch, aber vorsichtig: **61 % glauben, dass KI das Risiko von Ransomware direkt erhöht hat**. Die Bedenken der CISOs gegenüber KI sind vielfältig und reichen von automatisiertem Phishing über Deepfake-Imitationen bis hin zu Model Poisoning. Das Missbrauchspotenzial von KI ist inzwischen zu einem prägenden Merkmal der Bedrohungslandschaft geworden. Doch auch die Verteidigungsseite holt auf: **68 % der Unternehmen investieren bereits in KI-gestützte Erkennung und Analytik**. Die Herausforderung für Organisationen und Sicherheitsteams im Jahr 2026 liegt in der Governance, also darin, KI-Fähigkeiten zu nutzen, ohne die Risiken zu verstärken.

Das Security Lab von Hornetsecurity prognostiziert, dass das kommende Jahr von einer **weiterhin unkontrollierten Einführung von KI-Tools** in Unternehmen geprägt sein wird – oft schneller, als Rechts- oder Sicherheitsteams diese bewerten können. In Verbindung mit der zunehmenden **Nutzung agentischer KI als Waffe** wird dies bestehende Schwachstellen verstärken und gleichzeitig neue schaffen, die sich herkömmlichen Schutz- und Eindämmungsmodellen entziehen. Auch Identität bleibt einer der zentralen Angriffsvektoren: Adversary-in-the-Middle-Kits, kompromittierte Browser-Erweiterungen und OAuth-Missbrauch zeigen, dass Zugangsdaten und Identitäten nach wie vor das schwächste Glied in modernen Cloud-Umgebungen sind.

Trotz dieser zunehmenden Komplexität gibt es Gründe für Optimismus, denn auch Organisationen entwickeln sich stetig weiter. Die Einführung von **Zero-Trust-Prinzipien, unveränderlichen Backup-Technologien** und **Phishing-resistenter Multi-Faktor-Authentifizierung (MFA)** wird zunehmend zum Standard. Sicherheitsbewusstsein, das früher oft nur als Compliance-Pflicht galt, ist zunehmend Teil der Unternehmenskultur. Der Weg nach vorn ist klar: Resilienz statt Perfektion ist das neue Erfolgskriterium. Unternehmen, die Cybersicherheit als integralen Bestandteil der Geschäftskontinuität und nicht nur als IT-Thema betrachten, werden in der Bedrohungslandschaft des Jahres 2026 am besten aufgestellt sein.

SMART DEFENSE:
HOW AI SHIELDS YOUR INBOX

KAPITEL 2
DIE SICHERHEITSLAGE IN DER BRANCHE

E-MAIL-SICHERHEITSTRENDS

E-Mails bleiben das Fundament der geschäftlichen Kommunikation und sind, wie unsere Daten zeigen, nach wie vor das Hauptziel von Angreifern. Die Veränderungen in Klassifizierung und Bedrohungstypen im Jahr 2025 zeigen zwei parallele Entwicklungen: Erstens experimentieren Angreifer mit neuen Dateiformaten und niedrigschwelligen Zustellmethoden (insbesondere ein Anstieg bei TXT- und alten DOC-Dateien). Zweitens bleibt Social Engineering ein durchgehend wirksames Mittel, um Systeme zu kompromittieren.

Kurz gesagt: Sowohl Quantität als auch Qualität der Angriffe verändern sich. Während sich das Volumen klassischer Spam-Mails nach einer Phase der Normalisierung stabilisiert hat, nehmen hochwirksame Methoden wie Malware, Betrug und Phishing deutlich zu. Diese Kombination – gefährlichere Inhalte, die in großem Umfang verbreitet werden – erhöht die Wahrscheinlichkeit, dass selbst gut geschützte Organisationen Vorfälle erleben, sofern sie ihre Erkennungsmechanismen, Benutzeraufklärung und Wiederherstellungsprozesse nicht anpassen.

Spam, Malware und Advanced-Threat-Kennzahlen

Die wichtigsten Zahlen sind eindeutig: **Malware** verzeichnete den größten relativen Anstieg (+130,92 %), gefolgt von **Betrugsversuchen** (+34,70 %) und **Phishing** (+20,97 %). Diese drei Kategorien machen den Großteil der Risiken aus, die zu operativen Auswirkungen wie Datendiebstahl, Verschlüsselung und Geschäftsstörungen führen. Gleichzeitig zeigten Kategorien mit traditionell geringerem Geschäftsrisiko – etwa legitime Nachrichten, transaktionale oder kommerzielle E-Mails – nur moderate Veränderungen. Das deutet darauf hin, dass böswillige Akteure ihre Bemühungen zunehmend auf Angriffsformen mit höherem Ertragspotenzial konzentrieren.

Zentrale Erkenntnisse:

- **Zunahme bösartiger Nutzlasten:** Ein Anstieg der Malware-Klassifizierung um 131 % bedeutet, dass mehr E-Mails aktive Schadkomponenten (oder zumindest Indikatoren dafür) enthalten, statt harmloseren Inhalten. Erkennungsstrategien müssen daher grundsätzlich von einer böswilligen Absicht ausgehen.
- **Zunahme von Betrugsversuchen und fortgeschrittenen Social-Engineering-Angriffen:** Der Anstieg von Betrugsversuchen (+34,7 %) in Kombination mit Phishing (+21,0 %) zeigt, dass Angreifer ihre Täuschungsstrategien und Rendite optimieren. Sie erstellen überzeugendere, individuell zugeschnittene Betrugsnachrichten, vermutlich unterstützt durch generative KI-Technologien.
- **Zunahme sogenannter „Dirty Commercial"-E-Mails erschwert Erkennung durch heuristische Filter:** Der Anstieg verdächtiger oder minderwertiger Werbe-E-Mails (+17,72 %) deutet darauf hin, dass Angreifer E-Mail-Marketingvorlagen als Tarnung einsetzen, um einfache Inhaltsfilter zu umgehen und sich unauffällig unter legitimen Marketing-Kommunikation mischen.
- **Gezielte Spear-Phishing-Anteile nehmen ab, aber sie verschwinden nicht**. Der Anteil verdächtiger oder Spear-Phishing-E-Mails ist um 9,75 % zurückgegangen, was wahrscheinlich auf eine Verlagerung hin zu stärker automatisiertem oder massenhaft eingesetztem Phishing und Zugangsdatendiebstahl hindeutet, der klassische Spear-Phishing-Erkennung umgeht. Hier ist Vorsicht geboten, denn trotz geringerer Häufigkeit bleibt der Schaden solch zielgerichteter Angriffe hochwirksam.

E-MAIL-KLASSIFIZIERUNGSKATEGORIEN

Kategorie	Anpassung YoY 2025 vs. 2024
Malware	+130.92 %
Scam	+34.70 %
Phishing	+20.97 %
Verdächtige kommerzielle E-Mails (Dirty Commercial Emails)	+17.72 %
Kommerzielle E-Mail	+2.37 %
Legitime Nachrichten	+3.38 %
Transaktional	+3.19 %
Spam	+0.03 %
Social	-8.05 %
Verdächtige/ Spear-Phishing-E-Mail	-9.75 %
Professionelle kommerzielle E-Mails	-13.73 %
Rückläufer (Bounce)	-18.69 %

Hinweis: Die Berechnungen berücksichtigen und korrigieren Veränderungen in der Stichprobengröße von Jahr zu Jahr.

KATEGORIEBESCHREIBUNGEN

Spam
Unerwünschte Massen-E-Mails, die an eine große Anzahl von Empfängern gesendet werden, typischerweise zu Werbe- oder böswilligen Zwecken.

Phishing
Betrügerische E-Mails, die Empfänger dazu verleiten sollen, vertrauliche Informationen wie Passwörter, Kreditkartennummern oder persönliche Daten preiszugeben.

Kommerzielle E-Mails
Legitime Marketing- oder Werbe-E-Mails, die von Unternehmen an Kunden oder Interessenten gesendet werden, häufig mit Produktankündigungen oder Angeboten.

Legitime Nachrichten
Authentische, nicht-werbliche E-Mails, die zwischen Einzelpersonen oder Organisationen im Rahmen normaler Kommunikation ausgetauscht werden.

Professionelle kommerzielle E-Mails
Hochwertige, oft stark zielgerichtete und personalisierte Marketing-E-Mails, die typischerweise in B2B-Kampagnen eingesetzt werden.

Transaktional
E-Mails, die durch Benutzeraktionen oder Systemereignisse ausgelöst werden, z. B. Bestellbestätigungen, Passwortzurücksetzungen oder Konto-Benachrichtigungen.

Social
E-Mails, die von sozialen Medien stammen, einschließlich Benachrichtigungen, Freundschaftsanfragen und Aktivitätsmeldungen.

Rückläufer
E-Mails, die nicht an den Empfänger zugestellt werden können, z. B. aufgrund ungültiger Adressen, voller Postfächer oder Serverprobleme.

Verdächtige kommerzielle E-Mails (Dirty Commercial Emails)
Marketing-E-Mails, die gegen Compliance-Vorgaben oder Best Practices verstoßen, oft schlecht formatiert oder irreführend gestaltet.

Scam
E-Mails mit betrügerischer Absicht, häufig mit gefälschten Angeboten, angeblichen Lotteriegewinnen oder Identitätsbetrug.

Malware
E-Mails, die bösartige Anhänge oder Links enthalten, welche darauf abzielen, schädliche Software auf dem Gerät des Empfängers zu installieren.

Verdächtige/Spear-Phishing-E-Mails
Hochgradig zielgerichtete Phishing-Versuche, die sich an bestimmte Personen oder Organisationen richten und persönliche Details nutzen, um glaubwürdig zu wirken.

ANGRIFFSTECHNIKEN IN E-MAIL-ANGRIFFEN 2025

Die Bedrohungslandschaft 2025 zeigt eine deutliche Verschiebung hin zu „**Evasion-first**"-Taktiken: Angreifer konzentrieren sich weniger auf auffällige Einzelangriffe, sondern darauf, Sicherheitsfilter und menschlichen Verdacht hinsichtlich verdächtiger E-Mails zu umgehen. Zu den führenden Techniken gehören: Header-Fälschung, subtile HTML-Manipulationen, Nutzung legitimer Hosting-Dienste und URL-Verschleierung. Diese Methoden sind darauf ausgelegt, bösartige Absichten in scheinbar harmlose E-Mails einzubetten. Das erklärt, warum heute weniger offensichtliche Spear-Phishing-Beispiele, aber mehr erfolgreiche Zugangsdatendiebstähle und mehrstufige Angriffe beobachtet werden: Die E-Mail ist nicht mehr der Endpunkt des Angriffs, sondern der Einstiegspunkt.

Wichtige Beobachtungen:

- Manipulation von Headern und Metadaten dominiert: Bei Spam-Attacken finden sich besonders häufig gefälschte From-Angaben und manipulierte Header und zeigen, dass Spoofing und Manipulation von Metadaten weiterhin kostengünstige, aber wirkungsvolle Methoden sind, um naive Filter zu überwinden und menschliches Vertrauen zu erwecken.
- Missbrauch legitimer Infrastrukturen nimmt zu: Kampagnen über renommierte Hosting-Plattformen zu versenden lässt bösartige E-Mails so erscheinen, als kämen sie von vertrauenswürdigen Quellen. Diese Taktik erhöht die Zustellbarkeit und verringert den unmittelbaren Verdacht von Filtern.
- URL-Verschleierung ist allgegenwärtig: URL-Verkürzung, nicht-ASCII-Zeichen, exotische TLDs (Top-Level-Domains) und Domain-Fuzzing sind einfache Mittel, um das Ziel zu verbergen und Blocklisten oder visuelle Prüfungen zu umgehen.
- HTML-/MIME-Tricks zielen darauf ab, Detektoren zu verwirren, nicht Leser. Leere <a>-Tags, mehrteilige Nachrichten und das Einfügen von Schrift in Größe 0 sind darauf ausgelegt, Signatur- und schlüsselwortbasierte Scanner zu täuschen, während die Nachricht für für Empfänger lesbar bleibt.
- Automatisierte, groß angelegte Umgehungsversuche sind effektiver als gezielte, kleine Angriffe: Angreifer können viele Kampagnen ausrollen, die einzeln harmlos erscheinen, aber zusammen Zugangsdaten abgreifen, Konten kompromittieren oder Downloads ermöglichen.

DIE 10 HÄUFIGSTEN TECHNIKEN BEI E-MAIL-ANGRIFFEN 2025

Rang	Technik
1	Manipulation des From-Headers
2	Manipulation des „Spamcause"-Headers
3	Nutzung legitimer Hosting-Plattformen zum Versand von Kampagnen
4	Verwendung exotischer oder nicht existenter TLDs
5	URL-Verkürzung
6	Leeres HTML-<a>-Tag
7	Mehrteilige (Multi-Part) E-Mails
8	URLs mit Nicht-ASCII-Zeichen
9	Zufallsdomains/URL-Fuzzing
10	Zero-Font-Technik (Schriftgröße 0)

BESCHREIBUNGEN DER TECHNIKEN

1. Manipulation des From-Headers
Angreifer fälschen den From-Header in E-Mails, um vertrauenswürdige Absender zu imitieren und Empfänger glauben zu lassen, die Nachricht sei legitim.

2. Manipulation des „Spamcause"-Headers
Manipulation von Headern in Spam-Attacken, um Spam-Filter zu umgehen und bösartige E-Mails als harmlos erscheinen zu lassen.

3. . Nutzung legitimer Hosting-Plattformen zum Versand von Kampagnen
Verwendung renommierter Hosting- oder E-Mail-Dienste (z. B. Cloud-Plattformen), um Phishingkampagnen oder schädliche Inhalte zu versenden und die Erkennung zu erschweren.

4. Verwendung exotischer oder nicht existenter TLDs
Verwendung ungewöhnlicher oder gefälschter Top-Level-Domains (z. B. .xyz, .club), um betrügerische URLs zu erstellen, die legitim wirken.

5. URL-Verkürzung
Einsatz von URL-Verkürzungsdiensten (z. B. bit.ly), um das tatsächliche Ziel bösartiger Links zu verbergen und die Erkennung zu erschweren.

6. Leeres HTML-<a>-Tag
Einbetten leerer Anker-Tags in HTML-E-Mails, um Spam-Filter zu verwirren oder bösartige Links zu verschleiern.

7. Mehrteilige (Multi-Part) E-Mails
Versenden von E-Mails mit mehreren MIME-Teilen (z. B. Text und HTML), um die Erkennung durch Sicherheitstools zu umgehen.

8. . URLs mit Nicht-ASCII-Zeichen
Einfügen spezieller oder Unicode-Zeichen in URLs, um visuell irreführende Links zu erzeugen (z. B. Homoglyphen-Angriffe).

9. Zufallsdomains / URL-Fuzzing
Generierung zufälliger oder leicht veränderter Domains, um domainbasierte Filter und Erkennungssysteme zu umgehen.

10. Zero-Font-Technik
Einfügen von E-Mail-Text in Schriftgröße 0 (zero-size font), um schlüsselwortbasierte Filter zu manipulieren und gleichzeitig die Lesbarkeit für Menschen zu erhalten.

VERWENDUNG VON ANHÄNGEN UND TYPEN IN ANGRIFFEN

Die Trends bei Dateianhängen 2025 zeigen eine deutliche Verschiebung in der Strategie zur Verbreitung von Malware. Die am schnellsten wachsenden Dateiträger sind TXT (+181,39 %) und DOC (+118,25 %), während ZIP und moderne Office-Formate (DOCX, XLSX) ebenfalls vertreten sind, jedoch moderater wachsen. Veraltete oder früher populäre Vektoren (HTML, RAR, HTM, XLS) sind zurückgegangen, während ICS und SHTML als neue Einträge in unserer Top-10-Liste auftauchen. Das deutet darauf hin, dass Angreifer vermehrt nach übersehenen oder unzureichend inspizierten Dateitypen suchen, ebenso nach Kalenderdateien oder Server-Side-Include-Vektoren.

Wichtige Erkenntnisse:

» **TXT- und alte DOC-Dateien sind Alarmzeichen:** TXT-Dateien, die oft als geringes Risiko eingestuft werden, werden als Staging-Artefakte missbraucht (z. B. mit verschleierten URLs oder Skripten). Alte DOC-Dateien (mit Makro-Unterstützung) bleiben attraktiv, da viele Umgebungen Makros noch zulassen oder nicht ausreichend überprüfen.

» **Archive sind WEITERHIN relevant:** ZIP-Dateien (+29,82 %) bleiben ein Mittel zum Bündeln von Schadcode und zur Umgehung von Filtern; komprimierte Archive sind nach wie vor eine zuverlässige Taktik für Angreifer.

» **Aufkommen von ICS und SHTML ist nennenswert:** Kalendereinladungen (ICS) und Server-Include-Varianten (SHTML) stellen nicht-traditionelle Angriffsvektoren dar, die einige Mailfilter und Nutzererwartungen umgehen können, besonders bei Empfängern, die Kalendereinträge akzeptieren oder HTML-Inhalte in der Vorschau öffnen.

» **Der Rückgang von HTML-, HTM-, RAR- und XLS-Dateien spiegelt wahrscheinlich eine verbesserte Abwehrlage wider,** zeigt aber auch, dass Angreifer auf weniger überwachte Kanäle ausweichen, anstatt E-Mail als Angriffsvektor aufzugeben.

DATEITYPEN FÜR SCHADSOFTWARE 2025

Dateityp	Angepasste Veränderung (YoY) 2025 vs. 2024
TXT	+181.39%
DOC	+118.25%
ZIP	+29.82%
DOCX	+11.69%
XLSX	+7.85%
PDF	-3.32%
HTML	-27.44%
RAR	-36.93%
HTM	Nicht mehr in den Top 10 enthalten
XLS	Nicht mehr in den Top 10 enthalten
ICS	Neuer Eintrag 2025
SHTML	Neuer Eintrag 2025

Hinweis: Die Berechnungen berücksichtigen und korrigieren Veränderungen in der Stichprobengröße von Jahr zu Jahr.

DATEITYP-DEFINITIONEN

PDF
Portable Document Format – Weit verbreitetes Dokumentenformat; Angreifer betten häufig bösartige Links oder Skripte in PDFs ein.

DOC
Microsoft Word-Dokument (veraltet) – Älteres Word-Dateiformat; kann Makros enthalten, die schädlichen Code ausführen.

DOCX
Microsoft Word-Dokument (modern) – Aktuelles Word-Format; unterstützt eingebettete Inhalte (z. B. Makros/Skripte), die ausgenutzt werden können.

XLS
Microsoft Excel-Tabelle (veraltet) – Älteres Excel-Format; häufig Ziel makrobasierter Angriffe.

XLSX
Microsoft Excel-Tabelle (modern) – Aktuelles Excel-Format; kann schädliche Makros oder Links enthalten.

TXT
Reine Textdatei – Einfache Textdateien; Angreifer nutzen sie, um Phishing-Inhalte oder als Text getarnte Skripte zu verbreiten.

HTML
HyperText Markup Language-Datei – Webseitendatei; wird oft in Phishing-E-Mails mit eingebetteten bösartigen Links verwendet.

HTM
HyperText Markup Language-Datei (Variante) – Die ältere Dateinamenerweiterung für HTML-Inhalte; genutzt für Webinhalte und Phishing-Schadsoftware.

SHTML
Secure HTML File – Eine HTML-Variante, die Server-Side-Includes unterstützt; kann für bösartige Weiterleitungen oder Server-seitige Angriffspfade missbraucht werden.

ZIP
Komprimierte Archivdatei – Häufig zum Bündeln mehrerer Dateien verwendet; Angreifer verstecken Malware in komprimierten Archiven.

RAR
Komprimierte Archivdatei (Alternative) – Ähnlich wie ZIP, nutzt ein anderes Kompressionsformat; wird ebenfalls zur Verbreitung von Malware eingesetzt.

ICS
Kalenderdatei – iCalendar-Format; Angreifer missbrauchen bösartige Kalendereinladungen, um Phishing-Links oder Schadsoftware zu verbreiten.

DAS WIEDERAUFLEBEN VON RANSOMWARE IM JAHR 2025

Nach drei Jahren rückläufiger Entwicklung steht Ransomware nun wieder ganz oben auf der Liste der Cybersicherheitsprobleme. Daten von Hornetsecurity zeigen, dass im Jahr 2025 **24 % der Unternehmen angaben, Opfer eines Ransomware-Angriffs geworden zu sein** – ein deutlicher Anstieg gegenüber **18,6 %** im Jahr 2024. Diese Umkehrung ist ein Warnsignal für die Bedrohungslage nach der Pandemie und zeigt, dass sich Angreifer immer schneller weiterentwickeln.

Trotz jahrelanger Aufklärungskampagnen und Schulungsprogramme bleibt Ransomware ein kritisches Geschäftsrisiko, gerade weil sie sich an unsere Abwehrmaßnahmen anpasst. Bedrohungsakteure kombinieren nun **KI-gestützte Automatisierung** mit bewährten Social-Engineering-Methoden, um eine größere Reichweite, Präzision und Hartnäckigkeit zu erzielen.

AUTOMATISIERUNG, KI UND DAS NEUE RANSOMWARE-PLAYBOOK

Angreifer nutzen zunehmend **generative KI und Automatisierung**, um Schwachstellen zu identifizieren, überzeugendere Phishing-Köder zu entwickeln und mehrstufige Angriffe mit minimaler menschlicher Überwachung durchzuführen. Dies macht Ransomware-Aktivitäten leider skalierbarer und persönlicher.

Einige wichtige Datenpunkte:

- **61 %** der CISOs glauben, dass KI das Risiko von Ransomware-Angriffen direkt erhöht hat.
- **77 %** identifizieren KI-generiertes Phishing als eine neue und ernsthafte Bedrohung.
- **68 %** investieren derzeit in KI-gestützte Erkennungs- und Schutzfunktionen.

Das Ergebnis ist ein Wettrüsten, bei dem beide Seiten auf maschinelles Lernen setzen: die eine Seite mit dem Ziel zu täuschen, die andere, um zu verteidigen.

EINSTIEGSPUNKTE: PHISHING VERLIERT AN BEDEUTUNG, ENDPUNKTE GEWINNEN

Phishing ist mit **46 %** der Befragten zwar **nach wie vor der führende Infektionsvektor**, verliert jedoch an Dominanz. Angreifer diversifizieren ihre Vorgehensweisen:

Vector	2024	2025	Δ
Phishing/Email-basiert	52.3 %	46 %	-6,3 pp
Kompromittierte Zugangsdaten	~20 %	~25 %	+5 pp
Ausgenutzte Schwachstellen	–	12 %	n/a
Endpunkt-kompromittierung	–	26 %	n/a

pp = „Prozentpunkt"

Die Daten zeigen eine deutliche Verschiebung hin zu **Identitätsdiebstahl und Kompromittierung von Endpunkten**, insbesondere in hybriden und Remote-Arbeitsumgebungen, in denen **BYOD** („**Bring your own device**") **und Patch-Lücken** nach wie vor weit verbreitet sind. Ransomware ist nicht mehr nur ein E-Mail-Problem, sondern ein Problem des gesamten Ökosystems.

SCHULUNGSMÜDIGKEIT UND DIE FALLE DER „FALSCHEN COMPLIANCE"

Unternehmen investieren nach wie vor stark in Sensibilisierungsschulungen. 74 % bieten solche Schulungen an, doch 42 % davon halten sie für unzureichend.

Viele Programme bleiben reine Pflichtübungen: jährlich, wenig motivierend und schnell vergessen. Das Ergebnis ist das, was Hornetsecurity als *„falsche Compliance"* bezeichnet. Dabei handelt es sich um die Illusion von Vorbereitung ohne tatsächliche Verhaltensänderungen.

Kleine und mittlere Unternehmen (KMU) sind am stärksten betroffen. Viele arbeiten mit minimalem IT-Personal und veralteter Infrastruktur und sind auf ausgelagerte Anbieter oder nicht gepatchte Cloud-Tenants angewiesen. Zwar **geben immer mehr KMU an, über einen DR-Plan („Disaster Recovery Plan") zu verfügen**, doch bedeutet Bereitschaft auf dem Papier nicht immer auch Widerstandsfähigkeit in der Praxis.

WIEDERHERSTELLUNG UND WIDERSTANDSFÄHIGKEIT: DER SILBERSTREIF AM HORIZONT

Allerdings verbessern sich die Wiederherstellungsfähigkeiten trotz zunehmender Angriffe spürbar:

- **62 %** der Unternehmen verwenden mittlerweile **unveränderliche Backup-Technologien**. Dabei handelt es sich um Systeme, bei denen Daten nach dem Schreiben nicht mehr verändert oder verschlüsselt werden können– nicht einmal von Administratoren oder einem kompromittierten Administratorkonto während eines Angriffs.
- **82 %** haben einen **Disaster-Recovery-Plan** implementiert, der sich zunehmend zum neuen Standard für die operative Widerstandsfähigkeit entwickelt.
- Eine weitere gute Nachricht ist, dass nur **13 %** der Opfer im Jahr 2025 das Lösegeld gezahlt haben, gegenüber **16,3 %** im Jahr 2024.

Die Botschaft ist klar: Unternehmen lernen, sich ohne Verhandlungen zu erholen.

Bei den Versicherungen sieht es jedoch anders aus. **Die Versicherungsdeckung für Ransomware** sank von **54,6 %** im Jahr 2024 auf **46 %** in diesem Jahr, da die Prämien und Ausschlüsse stiegen und das Vertrauen in die Auszahlungsbereitschaft der Versicherer sank. Diese Marktkorrektur deutet darauf hin, dass Unternehmen Risiken nicht länger auslagern können. Sie müssen Sicherheit in ihre Systeme integrieren und Resilienz in ihrer Unternehmenskultur verankern.

GOVERNANCE: DIE STRATEGIE HINKT DER BEDROHUNGSREALITÄT NOCH HINTERHER

Cybersicherheit ist mittlerweile ein Thema auf Vorstandsebene, aber viele Unternehmen haben noch Nachholbedarf hinsichtlich der operativen Anforderungen an die Governance im Zeitalter von Ransomware. Nur wenige Vorstände führen **Cyber-Krisensimulationen** durch, und **funktionsübergreifende Playbooks** sind eher die Ausnahme als die Regel.
Da **KI-gesteuerte Fehlinformationen** und **Deepfake-Erpressung** immer plausibler werden, ist Kommunikationsbereitschaft nun Teil der Cybersicherheit und glücklicherweise keine nachträgliche PR-Maßnahme mehr.

AUSBLICK: DIE WIDERSTANDSFÄHIGKEIT NIMMT ZU, ABER AUCH DIE BEDROHUNGEN

Die Daten für 2025 zeichnen ein differenziertes Bild: Ransomware-Angriffe nehmen zu, aber auch unsere Fähigkeit, uns davon zu erholen. Unternehmen, die diese neue Welle überstehen werden, sind diejenigen, die **Resilienz als Strategie** und nicht als Compliance betrachten.

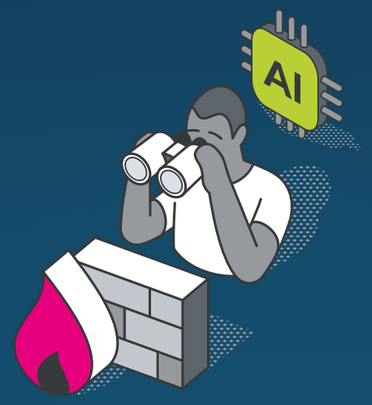
Unveränderliche Backups, gut getestete Wiederherstellungspläne und sinnvolle Benutzerschulungen sind nicht mehr optional, sondern die Mindestanforderung für eine funktionierende Verteidigung.

Angreifer stehen nicht still, und Verteidiger können das auch nicht. Die Herausforderung für 2026 wird nicht darin bestehen, Ransomware vollständig zu verhindern, sondern sicherzustellen, dass die **Geschäftskontinuität auch im Ernstfall erhalten bleibt**.

CISO-PERSPEKTIVEN: DAS GLEICHGEWICHT ZWISCHEN CHANCEN UND RISIKEN VON KI

Künstliche Intelligenz verändert die Cybersicherheit, und zwar nicht nur als Verteidigungsinstrument, sondern auch als strategische Frage. Die CISO Insights-Umfrage 2025 von Hornetsecurity wollte herausfinden, wie Sicherheitsverantwortliche in der Praxis mit KI umgehen: Wo funktioniert sie, wo birgt sie Risiken und welche Herausforderungen stehen einer verantwortungsvollen Einführung im Weg?

Die Ergebnisse sind komplex. CISOs sind enthusiastisch, vorsichtig und in vielen Fällen noch am Experimentieren. KI ist allgegenwärtig, aber Vertrauen, Governance und Verständnis haben leider noch nicht aufgeholt.



EINFÜHRUNG: SCHNELLES WACHSTUM, UNEINHEITLICHE GOVERNANCE

Die meisten befragten CISOs berichten von **umfangreichen Experimenten mit KI**, aber eine strukturierte Einführung ist nach wie vor selten. Einige Unternehmen integrieren KI in Arbeitsabläufe wie Triage, Anreicherung von Bedrohungsdaten und Ticketmanagement, während andere ihre Nutzung vollständig einschränken.

Ein CISO eines globalen Finanzunternehmens merkte an: *„Wir sehen in den letzten zwei Jahren eine Einführung von über 75 % innerhalb unseres Unternehmens."* Im Gegensatz dazu bemerkte ein virtueller CISO: *„Vor zwei Jahren gab es noch keine Beschränkungen für alle KI-Dienste. Im vergangenen Jahr haben wir begonnen, mehr Prozesse und interne LLMs einzuführen."*

Diese Variabilität zeigt die zentrale Herausforderung: Die Einführung von KI schreitet schneller voran als die KI-Governance, ähnlich wie bei früheren innovativen Trends im Technologiebereich. Viele Führungskräfte haben begonnen, die Kontrolle zu zentralisieren und interne Tools zu entwickeln, während andere weiterhin reaktiv agieren und eher auf Compliance setzen, als Innovationen voranzutreiben.

Shadow IT, einst ein bekanntes Ärgernis, wurde durch KI zu **Shadow AI** umdefiniert. Nicht genehmigte Tools, Browser-Erweiterungen und SaaS-Integrationen schaffen neue, undurchsichtige Risiken. Ein CISO fasste es so zusammen: *„Sicherheitsbedenken hinsichtlich KI haben die Gefahren von Shadow IT verstärkt."*

BEWUSSTSEIN DER ENDNUTZER: DER NEUE MENSCHLICHE RISIKOFAKTOR

Wenn ein Unternehmen nur so stark ist wie sein am wenigsten vorbereiteter Mitarbeiter, hat KI diese Messlatte gesenkt. CISOs sind sich einig, dass **das Bewusstsein der Endnutzer für KI-Risiken gefährlich gering ist**. Während einige wenige Unternehmen eine starke Compliance-Kultur vorweisen können und sich selbst mit „5 von 5" bewerten, schätzen die meisten CISOs das Bewusstsein eher mit *„1 oder 2 von 5"* ein.

Das Hauptproblem? Mitarbeiter nutzen öffentliche KI-Tools begeistert, ohne sich der Auswirkungen auf die Sicherheit oder Compliance bewusst zu sein. Ein virtueller CISO fasste zusammen: *„Die Menschen haben die Risiken nicht verstanden, insbesondere wenn sie Unternehmensinformationen in einer öffentlichen KI teilen."*

Der Konsens: Die Bemühungen um Sicherheitsbewusstsein im Unternehmen haben nicht mit der Einführung von KI Schritt gehalten. Eine gezielte, szenariobasierte Schulung ist heute genauso wichtig wie Firewalls und Filter.

VERSTÄNDNIS DER FÜHRUNGSKRÄFTE: DIE BEWUSSTSEINSLÜCKE AN DER SPITZE

CISOs heben zudem **eine große Diskrepanz im Verständnis der Führungskräfte** für KI-bezogene Risiken hervor. Unsere Umfrage ergab die größte Streuung der Antworten auf diese Frage, die von „tiefem Bewusstsein" bis zu „keinem wirklichen Verständnis" reichten. Die mittlere Antwort war ein zurückhaltendes „die Führungskräfte kennen die Risiken einigermaßen". Es ist klar, dass die Fortschritte uneinheitlich sind und von Unternehmen zu Unternehmen stark variieren.

Einige Unternehmen gehen gemeinsam voran. Ein CISO aus dem deutschen Technologiesektor führte die Fortschritte auf gemeinsame Initiativen der Rechts- und Sicherheitsabteilungen zurück: „Das Management beginnt, die Probleme im Zusammenhang mit der KI-Sicherheit zu verstehen." Andere berichten jedoch vom Gegenteil. „Das Management sieht die Produktivitätssteigerungen, aber nicht die Risiken", sagte ein virtueller CISO.

Dieses ungleiche Bewusstsein stellt CISOs vor eine doppelte Verantwortung: Sie müssen sich gegen externe Bedrohungen verteidigen und gleichzeitig die *Führungskräfte intern aufklären*.

AUFKOMMENDE BEDROHUNGEN: DEEPFAKES, MODEL POISONING UND DATENLECKS

Fast alle befragten CISOs sind sich einig, dass **der Missbrauch von KI in den nächsten 12 Monaten eine große Quelle für Cyberrisiken sein wird**.

Zu den dringendsten Anliegen gehören:

- **Synthetischer Identitätsbetrug** unter Verwendung von KI-generierten Dokumenten oder Anmeldedaten
- **Stimmenklone und Deepfake-Videos**, die zur Identitätsfälschung und zum Betrug verwendet werden
- **Model Poisoning**, bei dem bösartige Daten interne KI-Systeme beschädigen
- **Offenlegung sensibler Daten** durch den Missbrauch öffentlicher KI-Tools durch Mitarbeiter

Ein CISO warnte: „Wir sind am meisten besorgt über Model Poisoning-Angriffe, da wir unsere eigenen Modelle intern betreiben." Ein anderer merkte an: „Das größte Risiko der KI ist die freiwillige Weitergabe von Unternehmensdaten an öffentliche Systeme."

KI ist sowohl zu einem Werkzeug als auch zu einem Ziel geworden, und die Angriffsfläche wächst eindeutig schneller, als vielen bewusst ist.

EINFÜHRUNG DURCH DAS SICHERHEITSTEAM: SORGFÄLTIG, KONTROLLIERT UND TAKTISCH

Im Bereich der Sicherheitsmaßnahmen ist der Einsatz von KI zwar noch begrenzt, nimmt aber zu. CISOs beschreiben begrenzte Einsätze, die sich auf **spezifische Aufgaben mit geringem Risiko** konzentrieren. Dazu gehören beispielsweise die Klassifizierung von Tickets oder die Anreicherung von Bedrohungsdaten. Ein CISO aus dem Finanzsektor berichtete von einem praktischen Erfolg:
„KI hat sich für kundenbezogene Ticketnotizen als großartig erwiesen. Sie sind prägnant und unvoreingenommen."
Dieser „vorsichtige Optimismus" ist charakteristisch für das Jahr 2025. Sicherheitsteams begrüßen die Automatisierung, sind jedoch weiterhin vorsichtig, sich zu sehr auf undurchsichtige Systeme oder unausgereifte Modelle zu verlassen.

HERAUSFORDERUNGEN BEI DER IMPLEMENTIERUNG: DIE PRAKTISCHEN HINDERNISSE

Der Weg zu einer verantwortungsvollen Einführung von KI ist alles andere als einfach. Unsere CISO-Umfrage ergab, dass folgende Aspekte zu den größten Hindernissen gehören:

- **Unsicherheit hinsichtlich der Risiken** und des potenziellen Missbrauchs von KI
- **Compliance- und rechtliche Auflagen**
- **Budgetbegründung und Nachweis der Kapitalrendite**
- **Integrationsprobleme** mit älteren Tools
- **Fachkräftemangel** in den Bereichen KI und Datenwissenschaft
- **Akzeptanz durch die Führungsetage**

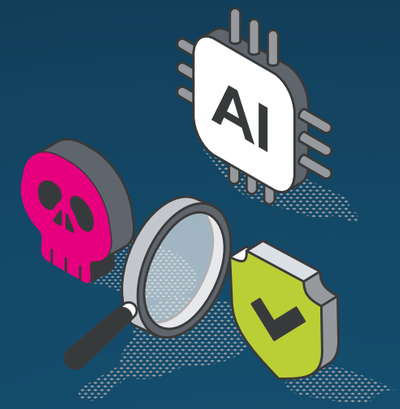
Ein CISO erklärte: *„Uns fehlen nach wie vor Fähigkeiten und spezialisierte Experten im Bereich KI."* Ein anderer fügte hinzu: *„Das Erkennen eines Port-Scans durch das Lesen von zehn Zeilen Logs bringt nicht viel."*

Trotz der Hürden bleiben CISOs pragmatisch: KI ist kein Hype, sondern eine unvermeidliche Entwicklung. Die Einführung wird jedoch weiterhin von Fall zu Fall erfolgen, bis Transparenz, Kompetenzen und Governance mit den Ambitionen Schritt halten können.

VON DER NEUGIER ZUR LEISTUNGSFÄHIGKEIT

KI in der Cybersicherheit ist nicht mehr experimentell, aber auch noch nicht vollständig ausgereift. In allen Branchen verlagert sich der Fokus von *„Was kann KI leisten?"* zu *„Wie steuern wir sie?"*

Das kommende Jahr wird zeigen, ob Sicherheitsteams KI von einem Risiko in einen zuverlässigen Verbündeten verwandeln können.



NO ONE IS IMMUNE:

THREATS TARGET EVERY ORGANIZATION

KAPITEL 3

EINE ANALYSE DER WICHTIGSTEN SICHERHEITSVORFÄLLE UND CYBERSICHERHEITSNACHRICHTEN DES JAHRES 2025

Es ist wichtig, große Cybersicherheitsvorfälle, von denen Unternehmen betroffen sind, als Lerninstrument zu nutzen und zu untersuchen, wie Ihr Unternehmen mit einem ähnlichen Angriff umgegangen wäre und wie Sie Ihre Widerstandsfähigkeit in Zukunft verbessern können. Seit Veröffentlichung unseres letzten Berichts Ende 2024 mangelt es nicht an Beispielen. Hier sind die elf wichtigsten Vorfälle, die wir ausgewählt haben.

OKTOBER 2024 – INTERNET ARCHIVE-HACK UND DDOS-ANGRIFF

Anfang Oktober 2024 wurde die gemeinnützige Organisation Internet Archive (bekannt für die Wayback Machine) Opfer eines erheblichen Datenlecks, von dem über 31 Millionen Benutzerkonten betroffen waren. Die Angreifer verschafften sich Zugriff auf eine 6,4 GB große Datenbank, die unter anderem die E-Mail-Adressen, Benutzernamen und Bcrypt-gehashte Passwörter der Benutzer enthielt. Etwa zur gleichen Zeit startete eine Hacktivisten-Gruppe namens BlackMeta eine Reihe von Distributed-Denial-of-Service-Angriffen (DDoS) auf die Websites des Archivs und legte diese vorübergehend lahm. Dieser Vorfall machte Schwachstellen im Konfigurationsmanagement des Archivs deutlich (eine exponierte GitLab-Konfigurationsdatei war Berichten zufolge der Angriffsvektor).

Daraus lassen sich zwei Schlussfolgerungen ziehen: Selbst wenn Sie eine gemeinnützige Organisation sind oder „zu unbedeutend, um angreifbar zu sein", sind Sie immer ein Ziel. Außerdem sollten Sie immer die Konfiguration der Code-Repositorys Ihrer Entwickler überprüfen, da eine unzureichende MIS-Konfiguration sich später negativ auf Sie auswirken könnte.

DEZEMBER 2024 – HACKERANGRIFF AUF DAS US-FINANZMINISTERIUM DURCH CHINESISCHE APT

Ende Dezember 2024 gab das US-Finanzministerium bekannt, dass es Opfer eines staatlich geförderten Cyberangriffs geworden war, der der chinesischen Regierung zugeschrieben wurde. Angreifer, die mit einer chinesischen APT-Gruppe (Advanced Persistent Threat) in Verbindung stehen, nutzten eine Schwachstelle in der Lieferkette aus, indem sie eine Identitäts- und Fernsupport-Plattform von BeyondTrust, einem vom Finanzministerium genutzten Anbieter, kompromittierten. Durch den Erwerb eines BeyondTrust-Administrationsschlüssels konnten die Hacker aus der Ferne auf die Arbeitsplätze mehrerer Mitarbeiter des Finanzministeriums zugreifen und nicht klassifizierte Dokumente stehlen. Beamte des Finanzministeriums bezeichneten dies als „schwerwiegenden Cybersicherheitsvorfall" und benachrichtigten die US-Cybersicherheitsbehörden (CISA) am 8. Dezember 2024, kurz nachdem BeyondTrust sie über den Einbruch informiert hatte. Der Vorfall, der kurz nach anderen Angriffen mit Verbindungen zu China auf US-Ziele erfolgte, verschärfte die Spannungen und führte zu einer dringenden Überprüfung der Sicherheit des Zugriffs durch Dritte und der Cyberabwehrmaßnahmen der Regierung.

Die wichtigste Lehre daraus ist, das eigene Bedrohungsmodell und die damit verbundenen Abhängigkeiten genau zu verstehen. Wenn Sie eine Sicherheitslösung implementiert haben, sollten Sie sich fragen, wo sich der „Hauptschlüssel" für diese Sicherheitslösung befindet. Was passiert, wenn er kompromittiert wird, und wie können Sie dies erkennen, bevor es zu spät ist?

JANUAR 2025 – KRITISCHE VPN-ZERO-DAY-EXPLOITS (IVANTI & SONICWALL)

Im Januar 2025 nutzten Angreifer aktiv kritische Zero-Day-Schwachstellen in zwei beliebten Fernzugriffsprodukten für Unternehmen aus, was weltweit zu Sicherheitswarnungen führte. Ivanti (Pulse Secure) gab bekannt, dass seine Connect Secure VPN-Appliance eine kritische Schwachstelle zur Umgehung der Authentifizierung enthielt, die in großem Umfang ausgenutzt wurde. Dieser Zero-Day, der die Ausführung von Remote-Code ohne Anmeldung ermöglichte, wurde bereits im Dezember 2024 genutzt, um mindestens 17 Organisationen (darunter Nominet, die britische Domain-Registrierungsstelle) zu infiltrieren. Mandiant-Forscher brachten die Ivanti-VPN-Exploits aufgrund der verwendeten Tools und Malware mit einem in China ansässigen Bedrohungsakteur in Verbindung.

Etwa zur gleichen Zeit warnte SonicWall, dass ein Zero-Day-Exploit in seiner VPN-Serie Secure Mobile Access (SMA) 1000 in ähnlicher Weise von Angreifern ausgenutzt wurde. Microsoft und CISA bestätigten, dass die SonicWall-Sicherheitslücke, die ebenfalls die Ausführung von nicht authentifiziertem Remote-Code ermöglichte, für Angriffe genutzt worden war, wobei es auch später im Juli zu Vorfällen kam. Diese aufeinanderfolgenden VPN-Sicherheitslücken zeigten das alarmierende Potenzial für Angreifer, vertrauenswürdige Fernzugriffssysteme zu missbrauchen, was weltweit dazu führte, dass Unternehmen in aller Eile kritische Patches und Abhilfemaßnahmen veröffentlichten.

Dies sind nur zwei Beispiele für einen Trend der letzten Jahre, bei dem die Technologien, die eigentlich zum Schutz des Netzwerks gedacht sind (Firewalls, VPN-Geräte), oft so schlecht konzipiert und gewartet sind, dass sie Angreifern als einfacher Zugangspunkt die Unternehmensumgebung dienen. Unabhängig von der Größe Ihres Anbieters müssen Sie von ihm höhere Standards verlangen. Sicherheitstechnologien zu beschaffen, die am Ende Schwachstellen schaffen, statt Sie zu schützen, darf keine Option sein.

MÄRZ 2025 – SPIONAGEKAMPAGNE GEGEN ROUTER VON JUNIPER NETWORKS

Im März 2025 enthüllte das Cybersicherheitsunternehmen Mandiant eine laufende Spionagekampagne, die auf Netzwerkinfrastruktur abzielte. Eine mit China verbundene APT-Gruppe (UNC3886) hatte eine neu entdeckte Schwachstelle im Junos OS von Juniper Networks, dem Betriebssystem für Juniper-Router, ausgenutzt. Seit Mitte 2024 nutzten die Angreifer diese Zero-Day-Sicherheitslücke, um sich Zugang zu Routern von Unternehmen und möglicherweise auch von Behörden zu verschaffen, und implantierten dann maßgeschneiderte Backdoor-Malware auf den Geräten. Diese versteckten Hintertüren ermöglichten es den Hackern, den Netzwerkverkehr zu überwachen, und sie konnten sich möglicherweise unbemerkt weiter in Netzwerke hineinbewegen. Juniper hat die Schwachstelle nach ihrer Entdeckung gepatcht, aber der Vorfall weckte Vergleiche mit früheren Angriffen auf Lieferketten und Infrastrukturen. Er unterstrich, dass fortgeschrittene Angreifer nun direkt auf Netzwerkrouter und Firewalls abzielen, um langfristige Spionage zu betreiben und dabei die traditionelle Endpunktsicherheit zu umgehen.

Diesen Vorfall sollten Sie dringend mit Ihrem Netzwerkteam besprechen. Router und Switches sind Teil der IT-Infrastruktur Ihres Unternehmens und werden nach ihrer Installation meist vergessen, solange sie funktionieren. Dies macht sie auch zu einem idealen Versteck für Angreifer, insbesondere da Sie auf ihnen keine Endpoint Detection and Response (EDR) ausführen können. Achten Sie daher darauf, sie auf Konfigurationsänderungen zu überwachen und sie auf dem neuesten Stand zu halten.

JUNI 2025 – UNFI-RANSOMWARE-ANGRIFF STÖRT DIE LEBENSMITTELVERSORGUNGSKETTE

Im Juni 2025 zeigte ein Ransomware-Angriff auf United Natural Foods, Inc. (UNFI), ein führendes Lebensmittelvertriebsunternehmen, die realen Auswirkungen von Cyberangriffen auf Lieferketten. UNFI, bekannt als Hauptvertriebspartner von Whole Foods und anderen Lebensmittelhändlern, entdeckte am 5. Juni unbefugte Aktivitäten in seinen IT-Systemen. Um die Bedrohung einzudämmen, nahm das Unternehmen die betroffenen Systeme vom Netz, wodurch es vorübergehend nicht mehr in der Lage war, Bestellungen zu bearbeiten und Lieferungen durchzuführen. Infolgedessen kam es bei einigen Lebensmitteleinzelhändlern zu Produktengpässen und Lieferverzögerungen. Die Störung hielt mehrere Tage an und UNFI erklärte, dass der Vorfall zu anhaltenden Betriebsverzögerungen und zusätzlichen Kosten führen würde. Die Auswirkungen auf die Lebensmittelversorgungskette erregten die Aufmerksamkeit der Regulierungsbehörden und machten deutlich, dass im Vertriebs- und Fertigungssektor stärkere Cyberabwehrmaßnahmen erforderlich sind, da selbst kurze Ausfälle Kettenreaktionen für die Verbraucher nach sich ziehen können.

Wenn Ihr Unternehmen Dienstleistungen innerhalb eines größeren Verbunds von Firmen anbietet und entsprechend Teil eines größeren Unternehmensnetzwerks ist, in dem ein Ausfall Kettenreaktionen bis hin zur Öffentlichkeit oder kritischen Infrastruktur auslösen kann, muss Ihre Risikomodellierung dies berücksichtigen und nicht nur die unmittelbaren Auswirkungen, die ein Cyberangriff auf Ihren eigenen Betrieb haben kann. Denn in den Augen der Öffentlichkeit (und der Aufsichtsbehörden) werden Sie für diese weiterreichenden Auswirkungen verantwortlich gemacht.

JULI 2025 – SCADER SPIDER-HACKS (FLUGGESELLSCHAFTEN UND EINZELHANDEL – QANTAS-VERSTOSS)

In einigen Berichten über verschiedene Vorfälle der letzten Jahre wurde „Scattered Spider" als Hackergruppe bezeichnet. Das ist nicht ganz zutreffend, da es sich eher um einen losen Zusammenschluss vieler verschiedener Akteure mit ähnlichen Taktiken handelt. Daher ist es genauer, von „Scattered Spider-ähnlichen" Techniken zu sprechen. Ihr Ansatz stützt sich stark auf Social Engineering, wobei (oft ausgelagerte) Helpdesk-Mitarbeiter dazu gebracht werden, Zugangsdaten zurückzusetzen. Es geht weniger darum, Computer zu hacken, als vielmehr darum, Menschen zu hacken. Ein weiterer bemerkenswerter Unterschied zu vielen anderen Bedrohungsakteuren besteht darin, dass sie jung sind, in westlichen Ländern leben und englische Muttersprachler sind, was vorhersehbar dazu geführt hat, dass viele von ihnen in den letzten ein bis zwei Jahren verhaftet wurden.

Anfang 2025 wurde Scattered Spider mit Angriffen auf große britische Einzelhändler (Marks & Spencer, Co-op, Harrods) und Versicherungsunternehmen wie Aflac in Verbindung gebracht. Im Juli 2025 richtete die Gruppe ihre Aufmerksamkeit auf den Luftfahrtsektor. Qantas Airways, Australiens nationale Fluggesellschaft, gab bekannt, dass eine von ihr genutzte Contact-Center-Plattform eines Drittanbieters kompromittiert wurde, wodurch die Daten von etwa 6 Millionen Kunden offengelegt wurden. Zu den gestohlenen Daten gehörten Namen, Kontaktdaten, Geburtsdaten und Vielfliegernummern, jedoch keine Finanzinformationen. Qantas bestätigte, dass es mit einem Erpressungsversuch im Zusammenhang mit dem Datenleck konfrontiert war, und Cyber-Ermittler stellten fest, dass der Angriff die typischen Merkmale der Taktik von Scattered Spider aufwies. Etwa zur gleichen Zeit wurden Berichten zufolge auch WestJet (Kanada) und Hawaiian Airlines (USA) von ähnlichen Vorfällen betroffen.

Die wichtigste Lehre aus diesen Angriffen ist, dass Sie Ihre Helpdesk-Verfahren überprüfen sollten, insbesondere im Hinblick auf das Zurücksetzen von Anmeldedaten („Ich habe mein Telefon verloren"), vor allem bei Konten mit erweiterten Berechtigungen. Alle üblichen wissensbasierten Verifizierungsdetails (Mitarbeiter-ID, Name des Vorgesetzten, Mädchenname der Mutter usw.) sind Informationen, die aus LinkedIn und anderen sozialen Medien gewonnen werden können und nicht sicher genug sind. Als ersten Schritt sollten Sie verlangen, dass jede Wiederherstellung eines privilegierten Kontos persönlich in einer Niederlassung des Unternehmens erfolgt.

JULI 2025 – RANSOMWARE-ANGRIFF AUF INGRAM MICRO

In der ersten Juliwoche 2025 wurde Ingram Micro, eines der weltweit größten IT-Vertriebsunternehmen, durch einen kritischen Ransomware-Angriff offline geschaltet. Am 4. Juli tauchten Berichte auf, dass Ingram Micro einen größeren Systemausfall erlitten hatte; das Unternehmen bestätigte bald darauf, dass es von einem Ransomware-Vorfall betroffen war und viele Systeme proaktiv offline genommen hatte, um diesen einzudämmen. Der Angriff beeinträchtigte den weltweiten Betrieb von Ingram und legte die Online-Bestell- und Logistiksysteme des Unternehmens für fast eine Woche lahm. Bis zum 10. Juli hatte der Distributor alle Geschäftsabläufe wiederhergestellt, jedoch nicht ohne erhebliche Auswirkungen auf Wiederverkäufer und Partner, die auf die Lieferkettendienstleistungen von Ingram angewiesen sind. Cybersicherheitsjournalisten identifizierten eine relativ neue Ransomware-Gruppe namens SafePay als Urheber des Angriffs.

Im Gegensatz zu UNFI verfügt Ingram Micro über keine breite öffentliche Präsenz. Die Lehre daraus: Wenn Ihr Unternehmen für den reibungslosen Betrieb vieler anderer Organisationen von entscheidender Bedeutung ist, kann eine Unterbrechung (in diesem Fall von mehr als einer Woche) schwerwiegende Auswirkungen auf Dritte haben und zu erhöhtem Zahlungsdruck führt – das sollten Sie in Ihrer Bedrohungsanalyse berücksichtigen.

JULI 2025 – „TOOLSHELL"-ZERO-DAY-ANGRIFFE AUF MICROSOFT SHAREPOINT

Im Juli 2025 warnten Sicherheitsforscher vor einer anhaltenden Welle von Cyberangriffen, die neue Zero-Day-Schwachstellen in lokalen Microsoft-SharePoint-Servern ausnutzen und zusammenfassend als „ToolShell" bezeichnet wurden. Bis zum 23. Juli waren weltweit durch diese Exploit-Kette über 400 SharePoint-Server kompromittiert worden. Wir haben hier einen Blogbeitrag mit weiteren Details zum SharePoint-Hack veröffentlicht. Die Angriffe ermöglichten unbefugten Zugriff und die Ausführung von Code auf SharePoint-Hosts, wodurch Angreifer effektiv einen Fuß in die Unternehmensnetzwerke der Opfer setzen konnten. Es wurde über eine Vielzahl von Betroffenen berichtet, darunter Unternehmen aus dem privaten Sektor und mindestens einige US-Regierungsbehörden; sogar das US-Energieministerium bestätigte, dass es „minimal betroffen" war. Die Threat-Intelligence-Teams von Microsoft führten die Aktivitäten auf mehrere staatlich geförderte chinesische Gruppen (mit den Codenamen Linen Typhoon, Violet Typhoon und Storm-2603) zurück, die die Exploits schnell übernommen hatten, sobald sie bekannt wurden. Unabhängig davon nutzten Kriminelle, die mit einer neuen Ransomware namens Warlock in Verbindung stehen, ToolShell ebenfalls, um in Unternehmen einzudringen und Malware zu verbreiten. Microsoft veröffentlichte Patches für die SharePoint-Sicherheitslücken und forderte zusammen mit Behörden wie der CISA alle Organisationen auf, sofort Updates durchzuführen.

Die Schlussfolgerung hier ist, sorgfältig zu prüfen, ob Sie sich weiterhin auf lokale Software (von beliebigen Anbietern) verlassen wollen, da diese Systeme oft nicht im Fokus der Anbieter stehen, sondern ihre SaaS-Angebote priorisieren. Falls Sie lokale Systeme benötigen, stellen Sie sicher, dass diese nicht öffentlich zugänglich sind. Schützen Sie sie mit einem VPN oder noch besser mit einer cloudbasierten SASE-Lösung. Sie müssen außerdem sicherstellen, dass Sie über ein Patch-Programm verfügen, um diese Server auf dem neuesten Stand zu halten.

AUGUST 2025 – SALESLOFT+DRIFT

Ende August 2025 wurde bekannt, dass Salesloft, eine Integration für Salesforce (und Slack/Pardot), kompromittiert worden war, woraufhin Salesforce die Drift-Integration in diesen Systemen deaktivierte. Der Angriff begann bereits im Juni 2025 mit der Kompromittierung des Salesloft-GitHub-Kontos, gefolgt vom Zugriff auf die AWS-Umgebung, in der die Angreifer OAuth-Token für die Kundenumgebungen von Drift erlangten. Diese Art von Supply-Chain-Angriff, bei dem die Kompromittierung eines einzelnen Anbieters den Angreifern potenziell Zugriff auf Hunderte von Opferorganisationen verschafft, ist besonders gefährlich. OAuth-Token sind äußerst mächtig; sobald sie in die Hände Krimineller gelangen, schützt Sie in der Regel nur noch deren Widerruf und die Deaktivierung der Integration – nicht MFA oder das Zurücksetzen von Zugangsdaten. Die Liste der Opfer ist lang und umfasst BeyondTrust, Cloudflare, CyberArk, Nutanix, Palo Alto Networks, Qualys, Rubrik, Tenable und Zscaler.

Die Reaktion auf Vorfälle ist schwierig: Wenn Sie betroffen sind, müssen Sie feststellen, auf welche Daten die Integration Zugriff hatte, welche zusätzlichen Anmeldedaten in diesen Daten verfügbar sein könnten und dann alle betroffenen Anmeldedaten zurücksetzen. Je nach Inhalt der exfiltrierten Daten besteht außerdem das Risiko einer Offenlegung oder Geldstrafen. Die Lehre daraus ist genau das, was wir bereits in unserem Bericht des vergangenen Jahres hervorgehoben haben: Nicht-menschliche Identitäten und Integrationen über APIs und OAuth in der Cloud und bei Ihren verschiedenen SaaS-Anbietern müssen auf anomale Aktivitäten überwacht werden. Dies ist Teil der Identitätsstruktur, wird jedoch häufig nicht überwacht und ist daher für Angreifer besonders attraktiv.

SEPTEMBER 2025 – JAGUAR LAND ROVER

Am Montag, den 1. September 2025, kam die Produktion von Jaguar Land Rover (JLR) in allen Werken in Großbritannien, der Slowakei, Brasilien und Indien zum Erliegen. Da diese Situation noch andauert und zum Zeitpunkt der Berichterstellung nach vier Wochen nur eine begrenzte Produktion wieder aufgenommen wurde, hat dieser Ransomware-Angriff enorme Auswirkungen auf JLR selbst und seine Zulieferer. Technische Details sind noch nicht bekannt, aber die meisten IT-Systeme von JLR wurden an Tata Consultancy Services (TCS) ausgelagert, einem Unternehmen der Tata-Gruppe, die seit 2008 Eigentümerin von JLR ist.

Viele Fertigungsindustrien, darunter auch die Automobilindustrie, bewegen sich in Richtung vollautomatischer Lieferketten, bei denen Teile „just in time" geliefert werden und Konstruktions- und Fertigungsabläufe vollständig digitalisiert sind. Dies kann sehr effizient sein, aber es ist entscheidend, das komplexe Geflecht der gegenseitigen Abhängigkeiten in einem so riesigen System zu verstehen und sicherzustellen, dass Cybersicherheit an jeder Schwachstelle integriert ist. Obwohl JLR über enorme Barreserven verfügt, hat die britische Regierung ein Darlehen in Höhe von 1,5 Milliarden Pfund garantiert, um dem Unternehmen bei der Bewältigung der Folgen zu helfen. Die finanziellen Auswirkungen werden insgesamt auf 1,9 Milliarden Pfund geschätzt, wobei über 5000 Organisationen von dem Angriff betroffen sind. JLR beschäftigt über 34.000 Mitarbeiter und 120.000 in seiner Lieferkette, von denen einige voraussichtlich insolvent gehen werden. Cybersicherheitsversicherungen scheinen nicht vorhanden gewesen zu sein, sodass JRL die gesamten Kosten dieser Katastrophe selbst tragen muss.

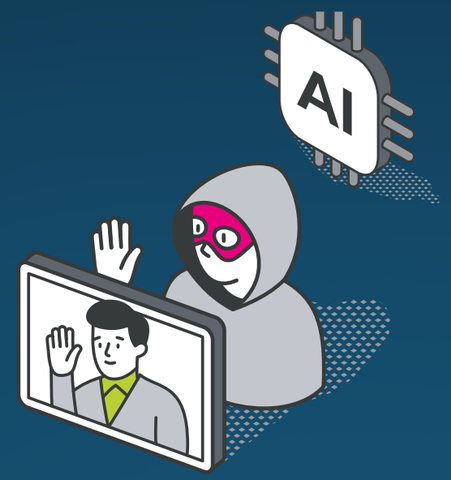
Die Lehre daraus ist eindeutig: Seit einem Jahrzehnt wird in allen Branchen lautstark die digitale Transformation gefordert, und obwohl digitale Prozesse für jedes Unternehmen wichtig sind, können unzureichend abgesicherte IT-Systeme in jedem Bereich des Gesamtsystems enorme Risiken bergen. Stellen Sie sicher, dass Sie über eine Cybersicherheitsversicherung verfügen, die Ihrem Risikoprofil entspricht. Die letzte ernüchternde Erkenntnis ist, dass mit der staatlichen Rettungsaktion zukünftige Angriffe wahrscheinlich auf britische Unternehmen abzielen werden, da diese eher bereit sind zu zahlen.

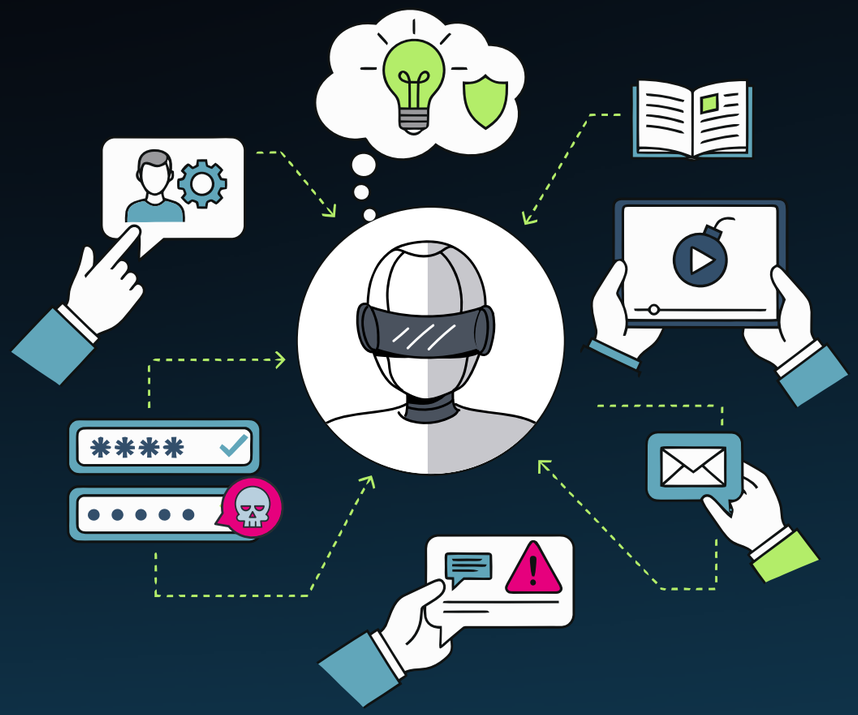
OKTOBER 2025 – F5 VOLLSTÄNDIG KOMPROMITTIERT

Ilm Oktober 2025 gab F5 Networks (ein bedeutender Anbieter von Application Delivery Controllern (ADCs) und Netzwerksicherheitsgeräten) bekannt, dass es Opfer eines hochentwickelten Angriffs durch einen staatlich geförderten Akteur geworden war. Nachfolgende Untersuchungen deuten darauf hin, dass die Angreifer bereits Ende 2023 Zugang erlangten, indem sie ein fälschlicherweise öffentlich zugängliches F5-System ausnutzten und interne Sicherheitsrichtlinien umgingen. Diese Sicherheitslücke ermöglichte es den Hackern, sich dauerhaft und unbemerkt Zugang zu verschaffen, der mindestens 12 Monate lang unentdeckt blieb. Der Vorfall wurde erst im August 2025 entdeckt, woraufhin F5 ihn Mitte Oktober öffentlich machte und damit ernsthafte Bedenken hinsichtlich der Sicherheit der Lieferkette hervorhob, da die Produkte von F5 tief in die Infrastruktur vieler Unternehmen eingebettet sind.

Einmal im Netzwerk, nutzten die Eindringlinge eine maßgeschneiderte Malware-Backdoor namens „BRICKSTORM", um sich lateral durch die virtualisierte Umgebung von F5 zu bewegen und dabei Sicherheitskontrollen zu umgehen. BRICKSTORM, das der mit China in Verbindung stehenden Spionagegruppe UNC5221 zugeschrieben wird, ermöglichte es den Angreifern, nahezu unsichtbar zu bleiben. Teilweise lagen sie über ein Jahr im Ruhezustand, vermutlich um die Aufbewahrungsfrist für Protokolle von F5 zu überdauern und Spuren des ursprünglichen Eindringens zu verwischen. Nach der Reaktivierung exfiltrierten die Angreifer hochgradig sensible Daten, darunter Teile des proprietären BIG-IP-Quellcodes und interne Berichte über nicht veröffentlichte (Zero-Day-)Schwachstellen in den Produkten von F5. Diese gestohlenen Daten verschafften den Hackern Einblick in Sicherheitslücken, die noch nicht gepatcht oder öffentlich bekannt waren – ein Informationsschatz, den Experten mit einem „Generalschlüssel" für potenzielle zukünftige Angriffe auf F5-Geräte weltweit verglichen. Der Vorfall verdeutlicht, wie ein einziger gut ausgeführter Angriff auf einen Kerntechnologieanbieter weitreichende Risiken mit sich bringen kann, da die Plattformen von F5 weltweit zum Schutz und zur Lastverteilung kritischer Anwendungen in Regierungs- und Unternehmensnetzwerken eingesetzt werden.

Die Lehre daraus ist unangenehm und erinnert an den SolarWinds-Hack im Jahr 2020: Selbst der größte Anbieter von Cybersicherheitslösungen kann von einem entschlossenen Angreifer kompromittiert werden und ohne angemessene Überwachung und Protokollierung kann ein solcher Zugriff über lange Zeit unentdeckt bleiben. Die Situation entwickelt sich noch, und obwohl noch nicht genügend technische Details vorliegen, um die langfristigen Auswirkungen in den kommenden Monaten vorherzusagen, sollten Sie, wenn Ihr Netzwerk auf F5-Geräten basiert, sofort alle Systeme aktualisieren und sämtliche Zugangsdaten ändern.





AI-DRIVEN THREATS:

WHEN INNOVATION BECOMES EXPLOITATION

KAPITEL 4

PROGNOSE DER BEDROHUNGSLAGE IM JAHR 2026

HABEN WIR DIE VORHERSAGEN FÜR 2025 RICHTIG GETROFFEN?

Im Bericht des vergangenen Jahres haben wir einige Prognosen darüber getroffen, was das Jahr 2025 für die Cybersicherheit bringen würde, und insgesamt lagen wir damit genau richtig. Wie erwartet sprachen wir über die Risiken generativer KI (GenAI), die auf Large Language Models (LLMs) basieren, und über deren missbräuchliche Nutzung durch Angreifer. Wir können zwar nicht mit Sicherheit sagen, dass eine bestimmte Phishing-E-Mail oder ein anderer Betrugsversuch dadurch begünstigt wurde, dass Angreifer den Köder so attraktiv wie möglich gestaltet haben, aber sowohl OpenAI als auch Anthropic haben weiterhin Berichte über Fälle veröffentlicht, in denen sie eine böswillige Nutzung ihrer Tools festgestellt haben (und anschließend diese Konten gesperrt haben).

Zu den neuartigen Verwendungszwecken gehört der Einsatz von Claude Code zur Automatisierung von Aufklärungsmaßnahmen, zum Sammeln von Anmeldedaten und zum Eindringen in Netzwerke. Die exfiltrierten Finanzdaten wurden ebenfalls von KI analysiert, um die Höhe der Lösegeldforderungen festzulegen. Nordkoreanische IT-Fachkräfte sind mittlerweile eine weit verbreitete Bedrohung. Sie nutzten sowohl Claude als auch ChatGPT, um falsche Identitäten zu erstellen, Lebensläufe automatisiert zu generieren, technische und Programmieraufgaben während des Bewerbungsprozesses zu absolvieren sowie Arbeitsaufgaben nach der Einstellung auszuführen. Obwohl dies eine einfache Vorhersage war, die sich bestätigte, ist es interessant zu beobachten, wie Angreifer KI in verschiedenen Phasen ihrer Angriffe experimentell einsetzen.

Wir haben auch den Einsatz überzeugenderer Deepfakes für Spear-Phishing und Einflussoperationen (IO) vorhergesagt, und auch dies hat sich in den letzten 12 Monaten bestätigt. Neue Versionen von Videobearbeitungstools haben eine Flut von unsauberen KI-generierten Inhalten" mit sich gebracht, die die Fähigkeit gewöhnlicher Nutzer, Fakten von Fiktion zu unterscheiden, trübt – eine Realität, mit der Gesellschaften und Unternehmen auf der ganzen Welt bereits zu kämpfen haben.

Der Bericht des letzten Jahres sagte auch Rechtsstreitigkeiten im Zusammenhang mit KI voraus, und auch hier lagen wir goldrichtig, darunter die Sammelklage gegen Anthropic in Höhe von 1,5 Milliarden Dollar. Aufgrund der sich wandelnden politischen Lage ist es unwahrscheinlich, dass die USA die schlimmsten Aktivitäten der dort ansässigen KI-Unternehmen eindämmen werden, aber die EU hat inzwischen das KI-Gesetz verabschiedet.

Der unaufhaltsame Vormarsch neuer und aktualisierter Regulierungsrahmen setzt sich in den meisten Teilen der Welt fort, und unsere Vorhersage, dass dies die Arbeitsbelastung und die Herausforderungen für Unternehmen (und ihre Lieferanten) erhöhen wird, war ebenfalls zutreffend: Die NIS2-Richtlinie beansprucht Mittel aus dem Personalbeschaffungs- und Notfallbudget, während die Digital Operational Resilience Act (DORA) und die britische Prudential Regulation Authority (PRA) Unternehmen Compliance-Kosten in Höhe von über 1 Million Euro verursachen.

Auch unsere Einschätzung des Ökosystems für freie und quelloffene Software (FOSS) war zutreffend. Im vergangenen Jahr wurden regelmäßig Hunderte bis Tausende bösartige Pakete über NuGet, PyPI, RubyGems und npm gemeldet (allein im August 2025 35.000 bösartige Pakete in npm, Spitzenreiter). Dieser Trend scheint sich zu verschärfen. Wenn Ihr Unternehmen Software intern entwickelt, müssen Sie diese bösartigen Pakete vor der Integration in Anwendungen genau überwachen. Die Zeiten, in denen Entwickler weltweit freiwillig Code zum Wohle der Allgemeinheit zu FOSS beitrugen, könnten bald vorbei sein.

Unsere letzte Prognose zur Verbreitung von speichersicheren Sprachen (Rust / Swift) hat sich ebenfalls bestätigt, wenn auch langsamer als erwartet. Rust wird in Windows-Treibern von Drittanbietern, im Betriebssystemkern (wo etwa 70 % aller CVEs auf Probleme mit der Speichersicherheit zurückzuführen sind) sowie in Hyper-V, Azure und Microsoft 365 eingesetzt. Auch Linux und Android integrieren Rust, was in den letzten sechs Jahren zu einer 52-prozentigen Reduzierung der Speicher-Schwachstellen geführt hat. Apple schlägt unterdessen einen etwas anderen Weg ein, da das Unternehmen mit seiner Memory Integrity Enforcement Kontrolle über die gesamte Hardware und Software hat, aber das Ergebnis ist das gleiche: ausnutzbare Speicherprobleme werden vermieden.

Insgesamt haben sich alle unsere Vorhersagen bewahrheitet, was mehr über die Vorhersehbarkeit von Cyberkriminellen aussagt als über unsere Fähigkeit, Vorhersagen zu treffen.

DIE PROGNOSEN DES SECURITY LAB FÜR 2026

Da KI-Tools immer ausgereifter werden, beschleunigt sich ihre Einführung in Unternehmen, oft schneller, als Governance- oder Sicherheitsrahmenbedingungen angepasst werden können. Diese Beschleunigung wird sowohl durch Initiativen des Managements als auch durch Experimente der Mitarbeiter vorangetrieben, und in einigen Fällen werden täglich neue KI-Lösungen eingeführt. Das Tempo der Innovation hat die Fähigkeit der Rechts-, IT- und Sicherheitsteams übertroffen, jede Implementierung zu bewerten, wodurch kritische Sichtbarkeitslücken entstehen.

Die unkontrollierte Einführung vergrößert effektiv die Angriffsfläche des Unternehmens. Vielen KI-Tools, insbesondere solchen, die auf Large Language Models (LLMs) basieren, fehlt die Trennung zwischen Code und Daten, die in traditionelleren Anwendungen vorhanden ist. Dies führt zu neuen Vektoren für Prompt-Injection, Datenlecks und die unbeabsichtigte Offenlegung sensibler Unternehmensdaten. Der Aufstieg autonomer KI (Agentic AI) verstärkt dieses Risiko noch, da Aktionen ohne menschliche Aufsicht oder festgelegte Genehmigungsketten erfolgen können.

Aktuelle Schwachstellen wie Echoleak in M365 Copilot (Aim Labs) zeigen deutlich, wie ernst diese Risiken sind. Anders als bei klassischen Buffer Overflows oder Code-Injektionen gibt es für LLM-basierte Exploits keine einfachen Gegenmaßnahmen. Selbst wenn Unternehmen die Best Practices aus den OWASP LLM01:2025 Guidelines für Prompt Injection befolgen, sind Unternehmen aufgrund der Unvorhersehbarkeit des Verhaltens von KI-Modellen einem Restrisiko ausgesetzt. Berichte wie „Detecting and Countering Misuse of AI" (August 2025, Anthropic) bestätigen erneut, dass selbst modernste Modelle anfällig für Manipulation und Missbrauch sind.

WAFFENEINSATZ AUTONOMER KI (AGENTIC AI)

Es ist daher nicht verwunderlich, dass autonome KI-Systeme (also Modelle, die mehrstufige Ziele ausführen können) bereits als Waffen eingesetzt werden. Die Grenze zwischen Automatisierung und Instrumentierung ist verschwommen. Angreifer können nun mit minimalem Fachwissen Multi-Vektor-Kampagnen skripten, anpassen und starten, wodurch die Einstiegshürde gesenkt wird. Diese Modelle können jede Phase des Angriffszyklus unterstützen, von der Aufklärung über die Ausnutzung bis hin zur Auswirkung, und folgen dabei durchgängig dem MITRE ATT&CK-Framework.

Online lassen sich zahlreiche Beispiele finden, wie autonome KI bereits Angreiferoperationen beeinflusst. Dazu gehören das Erstellen von Phishing-Ködern, das Umgehen von CAPTCHA-Gates oder das Imitieren von Menschen durch Deepfakes in Form von Sprach- und Videomaterial. Diese Erkenntnisse bestätigen, was viele Verteidiger bereits vermuten: KI verstärkt sowohl die Zugänglichkeit als auch die Geschwindigkeit von Cyberkriminalität.

Trotz der Sicherheitsversprechen großer Anbieter hält der Missbrauch an. Der eigene Bedrohungsbericht von Anthropic vom August 2025 (siehe oben) bestätigt den anhaltenden Missbrauch von Modellen für Aufklärung und Payload-Generierung und untermauert damit die Befürchtung, dass autonome KI-Systeme weiterhin schneller sein werden als Sicherheitsvorkehrungen. Mit LLMs, die in der Lage sind, ganze Angriffsketten autonom zu generieren (vibe coding), sind die Einstiegshürden für ausgeklügelte Exploits so gut wie verschwunden.

RANSOMWARE 3.0: LLM-GESTEUERT UND AUF INTEGRITÄT AUSGERICHTET

Wie bereits in den Ergebnissen unserer Ransomware-Umfrage 2025 beschrieben, befindet sich Ransomware nun in einer neuen Evolutionsphase. Diese Phase ist geprägt von Automatisierung, Autonomie und Datenmanipulation. Für 2026 erwarten wir die Verbreitung von LLM-gesteuerter Orchestrierung, bei der LLMs die Aufklärung, die Generierung von Payloads und die adaptive Umgehung koordinieren. Gleichzeitig verlagern Angreifer den Fokus von reiner Verschlüsselung oder Exfiltration hin zur Manipulation der Datenintegrität: Datensätze werden verfälscht, beschädigt, oder subtil verändert, um Zweifel an der Vertrauenswürdigkeit der Daten selbst zu wecken.

Historisch gesehen hat sich Ransomware stets an die Resilienz der Verteidiger angepasst: von reinen Verschlüsselungsangriffen (Ransomware 1.0) bis hin zu Double-Extortion-Angriffen (Ransomware 2.0). Mit der breiten Einführung unveränderlicher Backups und Cyberversicherungen bringen direkte Verschlüsselungsangriffe immer weniger Gewinn. Der nächste logische Schritt für Cyberkriminelle ist es, das Vertrauen zu untergraben, anstatt nur den Zugriff zu kompromittieren. Manipulierte Daten in Finanzsystemen, Krankenakten oder industriellen Steuerungssystemen führen zu anhaltendem Chaos, regulatorischen Risiken und Reputationsschäden.

Wissenschaftliche Untersuchungen haben bereits Ransomware-Kampagnen nachgewiesen, die autonom von KI orchestriert wurden. Eine Studie der NYU Tandon School of Engineering aus dem Jahr 2025 zeigte, dass LLMs komplette Angriffsketten autonom ausführen können. Dazu gehörten Aufklärung, Exfiltration, Verschlüsselung und Anpassung – und all dies geschah ohne menschliches Zutun. Die Integration von Datenmanipulation in diesen Prozess ist ein natürlicher, aber gefährlicher nächster Schritt.

ATTACKER-IN-THE-MIDDLE-ANGRIFFE WERDEN PHISHING-RESISTENTE MFA ZWINGEND ERFORDERLICH MACHEN

Die Umstellung auf MFA für eine stärkere Authentifizierung in den letzten zehn Jahren war ein guter Schritt, aber die Angreifer haben sich parallel zu unseren Abwehrmaßnahmen weiterentwickelt. Angreifer verwenden Phishing-Kits, darunter das Open-Source-Tool Evilginx, um gefälschte Anmeldeseiten einzurichten, die denen von Microsoft, Google oder Okta nachempfunden sind, und locken dann Benutzer über Phishing-E-Mails oder Teams-Nachrichten dazu, auf einen Link zu diesen Seiten zu klicken. Die Benutzer melden sich auf der gefälschten Seite an; ihre Benutzernamen, Passwörter und MFA-Eingabeaufforderungen werden hinter den Kulissen an die legitime Anmeldeseite weitergeleitet, während der Angreifer das daraus resultierende Token stiehlt und dann auf alles zugreifen kann, worauf der Benutzer Zugriff hat. Dies ist als Attacker-in-the-Middle (AiTM) bekannt.

Die Möglichkeit, die MFA-Abfrage zu verwalten, ist mittlerweile eine „Standardfunktion" dieser Phishing-Kits. Die einzige wirksame Abwehr sind Phishing-resistente MFA-Technologien wie FIDO2-Hardware-Schlüssel, Windows Hello for Business, zertifikatsbasierte Authentifizierung (CBA) und Passkeys, da diese an die legitime Anmeldeseite gebunden sind und auf der gefälschten Seite nicht funktionieren, selbst wenn der Benutzer getäuscht wurde. Sie müssen jedoch nicht nur eine Phishing-resistente MFA einsetzen, sondern diese auch als einzige Anmeldemethode vorschreiben, da die meisten Phishing-Kits mittlerweile auch ein Downgrade von einer stärkeren MFA-Methode zu einer weniger sicheren erzwingen.

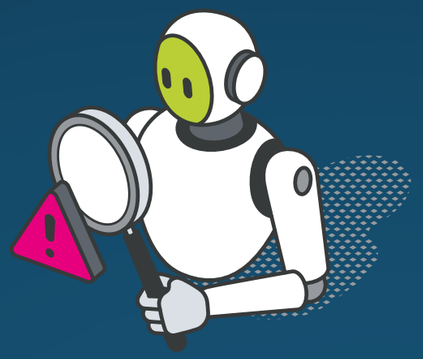
DIE EINFÜHRUNG VON PASSKEYS WIRD DURCH VERWIRRENDE BENUTZERERFAHRUNGEN VERLANGSAMT

Hardware-FIDO-Schlüssel sind zwar eine hervorragende Option für Phishing-resistente MFA, bedeuten jedoch zusätzliche Kosten für jeden Nutzer. Passkeys, bei denen stattdessen der Sicherheitschip eines modernen Smartphone verwendet wird, sind eine Alternative.Wir hatten für dieses Jahr eine schnelle Verbreitung von Passkeys vorausgesagt, die zwar stattgefunden hat, jedoch nicht in dem erwarteten Ausmaß. Der Hauptgrund dafür ist eine fragmentierte Benutzererfahrung, die auf einem iPhone, einem Android-Telefon oder einem Windows-/MacOS-Laptop unterschiedlich aussieht. Darüber hinaus gibt es zwei Varianten: synchronisierbare Passkeys für Verbraucher, die im Apple- oder Google-Konto gespeichert werden und auf verschiedenen Geräten verwendet werden können sowie nicht-synchronisierbare Passkeys für Unternehmen, da die Speicherung von Unternehmensanmeldedaten in persönlichen Cloud-Konten der Endnutzer unzulässig ist. Diese sind an das Smartphone gebunden, auf dem sie erstellt wurden, und im Fall von Microsoft 365 ist die einzige akzeptierte App Microsoft Authenticator. Hinzu kommt die komplizierte Anwendererfahrung, da diese sich zunächst auf ihrem Laptop anmelden, einen QR-Code mit ihrem Smartphone scannen und dann den Anmeldeprozess auf dem Telefon abschließen.

Passkeys sind die Zukunft der Phishing-resistenten MFA, aber die Technologieriesen müssen zusammenarbeiten, um die Anwendererfahrung für Verbraucher und Unternehmen zu vereinheitlichen.

IDENTITÄTSPRÜFUNGS- UND ZURÜCKSETZUNGSPROZESSE WERDEN UNTERNEHMEN WEITERHIN GEFÄHRDEN

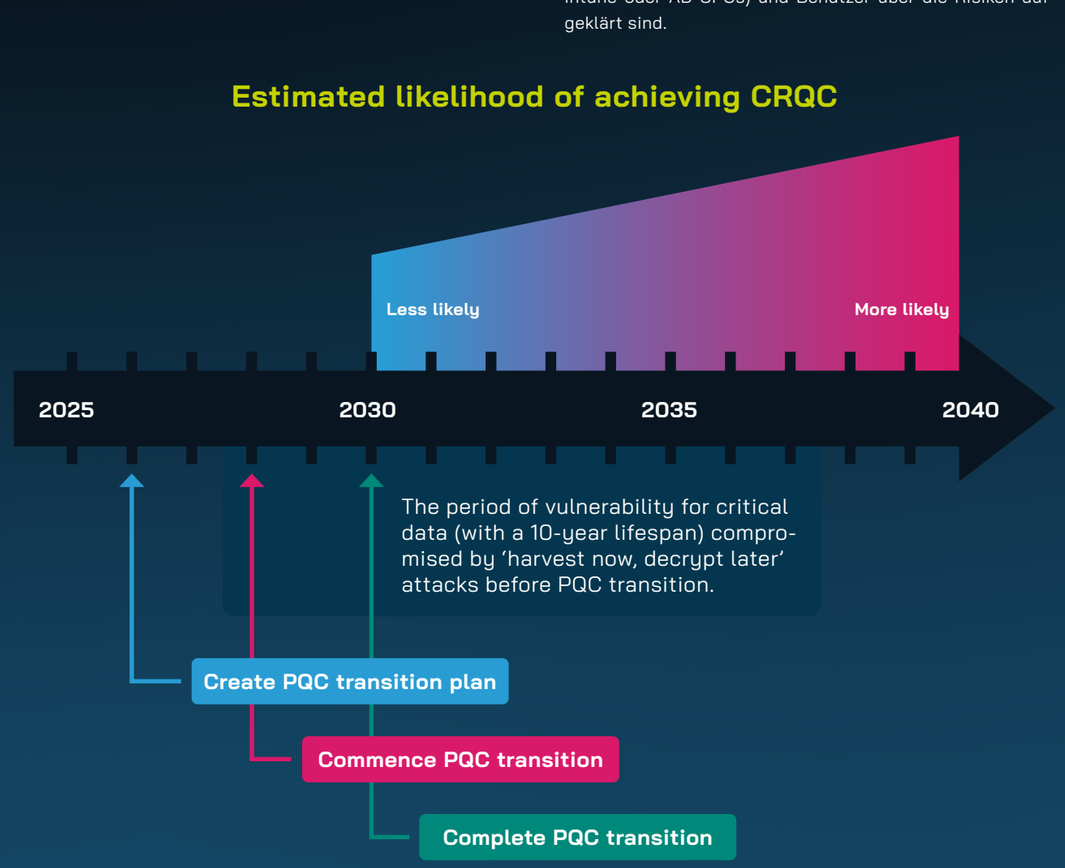
Einige der größten Sicherheitsverletzungen, die wir in letzter Zeit erlebt haben, waren darauf zurückzuführen, dass (oft ausgelagerte) Helpdesk-Mitarbeiter dazu verleitet wurden, Konten für administrative Benutzerkonten zurückzusetzen. Denken Sie daran, dass die Stärke Ihrer Authentifizierung nicht daran gemessen wird, welche Technologie Sie verwenden, wenn alles normal funktioniert, sondern daran, wie schwer es ist, Ihre Registrierungs- und Wiederherstellungsprozesse zu unterlaufen. Wie stellen Sie in der heutigen Welt des Remote-Arbeitens sicher, dass neue Mitarbeiter tatsächlich die Personen sind, die Sie erwarten (und keine nordkoreanischen Eindringlinge)? Wie sieht Ihr Verfahren zur Wiederherstellung von Konten für Benutzer aus, die ihr Passwort vergessen haben, ihr Telefon oder ihren FIDO-Schlüssel verloren, oder deren Laptop gerade kaputt gegangen ist? Verfügen Sie über ein noch sichereres Verfahren für Konten mit hochrangigen Berechtigungen? (Einschließlich der Anforderung einer persönlichen Überprüfung in einer Unternehmensniederlassung). Die Identität ist die neue Firewall, aber Sie müssen die Risikominderung in Ihrem gesamten Identitäts-Workflow ganzheitlich betrachten, angefangen vom Zeitpunkt der Stellenzusage bis zum letzten Arbeitstag.



SAAS-ANWENDUNGEN SIND DIE NEUE ANGRIFFSFLÄCHE
Bestimmte Sicherheitsverletzungen in Unternehmen in den letzten Jahren sind interessant, weil sie das traditionelle Schema „normalen Benutzer kompromittieren – in internes Netzwerk eindringen – Administratorkonten kompromittieren" komplett umgehen. Da Unternehmen immer stärker auf SaaS-Dienste angewiesen sind, werden neue Arten von Angriffen, die nur Cloud-Daten und Identitäten kompromittieren, immer häufiger. Normale Abwehrmaßnahmen wie Endpoint Detection und Response (EDR) sind gegenüber diesen Angriffen meist wirkungslos, da sie zwar im Browser stattfinden, aber keine bösartigen Dateien oder Aktivitäten vorhanden sind, die der Endpunktschutz erkennen kann. Tatsächlich findet ein Großteil der modernen Unternehmens-IT heute in einem Browser statt, der für EDR undurchsichtig ist. Daher empfehlen wir dringend die Verwendung eines Unternehmensbrowsers und/oder spezieller Software zum Schutz im Browser. Mitre hat sogar eine ATT&CK MATRIX für verschiedene SaaS-Angriffe entwickelt.

BROWSER-ERWEITERUNGEN WERDEN IM KOMMENDEN JAHR MEHR UNTERNEHMEN GEFÄHRDEN
Moderne Browser sind heute komplexe Anwendungen – fast schon eigene Betriebssysteme – und verfügen über zahlreiche Schutzfunktionen, die uns sowohl im Privatleben als auch bei der Arbeit weitgehend vor Gefahren im Internet schützen. Doch viele Nutzer verwenden zusätzlich Browser-Erweiterungen, meist aus Gründen der Produktivität oder Bequemlichkeit, aber genau hier lauern versteckte Risiken. Einige dieser Erweiterungen sind unsicher programmiert und beeinträchtigen den eingebauten Schutz des Browsers, andere sind absichtlich bösartig. Dies kann dadurch geschehen, dass sie einen ähnlichen Namen wie ein beliebtes Add-in tragen oder dass Kriminelle eine zuvor harmlose Erweiterung kaufen und sie nachträglich mit Schadcode ausstatten.

Unternehmen sollten daher unbedingt sicherstellen, dass sie eine Übersicht über alle installierten Erweiterungen in den Browsern ihrer Mitarbeiter haben, bösartige oder unerwünschte Add-ons zentral blockieren können (z. B. über Intune oder AD GPOs) und Benutzer über die Risiken aufgeklärt sind.



PROGNOSEN ZUM THEMA QUANTENCOMPUTING
Die meisten Bedrohungen, die wir in diesem Bericht betrachten, sind aktuell, während die Einführung des kryptografisch relevanten Quantencomputers (CRQC) noch einige Jahre entfernt ist. Der Tag, an dem dies geschieht, wird als Q-Day bezeichnet. Dann verfügen Quantencomputer über eine ausreichende Anzahl an Qubits (das Quanten-Äquivalent zu Bits) und sind kostengünstig genug, um mithilfe des Shor-Algorithmus asymmetrische Verschlüsselungsverfahren wie RSA und Diffie-Hellman zu knacken. Gleichzeitig kann der Grover-Algorithmus die Stärke der symmetrischen Kryptografie halbieren (AES-128 wird zu AES-64).

Viele verschiedene Technologieunternehmen, darunter die üblichen Verdächtigen (Google, IBM, Microsoft), investieren derzeit Millionen in verschiedene Arten von Quantencomputern, um herauszufinden, welcher technologische Ansatz ausreichend stabile Qubits liefern wird. Das Hauptproblem liegt in der Stabilität der Qubits: Wenn ein Großteil der Qubits für Fehlerkorrektur benötigt wird, bleibt nur ein kleiner Anteil übrig, der tatsächlich für Berechnungen genutzt werden kann. Quantencomputer werden unsere aktuellen Computer nicht ersetzen, sondern für ganz bestimmte Arten von Berechnungen eingesetzt werden, darunter auch das Knacken heutiger Verschlüsselungsalgorithmen.

Auch wenn CRCQs noch 5 bis 15 Jahre entfernt sind, sollten Unternehmen nicht abwarten, bis sie einsatzbereit sind, sondern bereits jetzt mit der Planung beginnen. Wenn Sie personenbezogene Daten (PII) oder persönliche Gesundheitsdaten (PHI) speichern und beabsichtigen (oder aufgrund von Vorschriften dazu verpflichtet sind), diese länger als fünf Jahre aufzubewahren, sollten Sie jetzt damit beginnen, quantenresistente Verschlüsselungsverfahren zu verwenden. Der Grund dafür ist, dass Behörden weltweit bereits die Strategie „Harvest Now, Decrypt Later" (HDNL) verwenden, um Daten zu speichern, die sie derzeit noch nicht entschlüsseln können, aber zukünftig mit CRCQs entschlüsseln werden können. Darüber hinaus ist die Umstellung kein einfacher Prozess. Unternehmen müssen zunächst jedes System, jedes Gerät und jede Netzwerkkomponente identifizieren, die Verschlüsselung verwendet, dokumentieren, welcher Algorithmus verwendet wird und bewerten, welche Art von Daten gespeichert oder übertragen werden. In manchen Fällen ist es einfach, quantenresistente Algorithmen zu integrieren, in anderen müssen Systeme komplett ausgetauscht oder Prozesse neu gestaltet werden.

Das NIST hat drei quantenresistente Algorithmen standardisiert:

- FIPS 203 definiert ein kryptografisches Schema namens Module-Lattice-Based Key-Encapsulation Mechanism (**ML-KEM**), das aus dem CRYSTALS-KYBER-Vorschlag abgeleitet ist.
- FIPS 204 ist der Module-Lattice-Based Digital Signature Algorithm (**ML-DSA**), der auf dem CRYSTAL-Dilithium-Vorschlag basiert.
- FIPS 205 spezifiziert den Stateless Hash-Based Digital Signature Algorithm (**SLH-DSA**), der aus dem Vorschlag SPHINCS+ abgeleitet wurde.

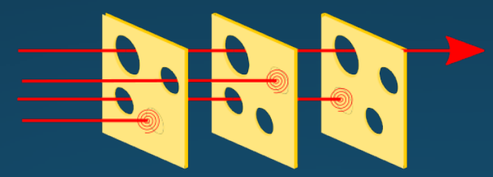
Sie basieren auf Transport Layer Security (TLS) Version 1.3. Beginnen Sie also damit, diese Version überall in Ihrer Umgebung einzuführen.

Was Betriebssysteme angeht, so enthalten die Vorschauversionen von Windows 11 und Windows Server aktualisierte Versionen von SymCrypt, derselben Bibliothek, die auch in Azure und Microsoft 365 verwendet wird. ML-KEM und ML-DSA sind bereits in SymCrypt verfügbar, sowohl unter Windows als auch unter Linux. SymCrypt-OpenSSL bietet die gleiche Unterstützung für OpenSSL. Apple integriert PQC ebenfalls in sein CryptoKit für Entwickler, und iMessage in iOS sowie TLS 1.3 in iOS26 verwenden PQC bereits.

Wenn Sie Ihre eigenen Anwendungen intern schreiben, sollten Sie auf Krypto-Agilität achten, damit Sie bei Updates ganze Verschlüsselungssuiten oder Algorithmen austauschen können.

RISIKEN FÜR UNTERNEHMEN IM JAHR 2026

Cybersicherheit ist kein rein technologisches Problem, sondern in erster Linie ein Menschen- und Prozessproblem. Wie so oft, wenn man sich intensiv mit den neuesten Technologien beschäftigt und die rasanten Entwicklungen rund um GenAI, maschinellem Lernen oder autonomer KI beobachtet, erscheinen die Lösungen meist technischer Natur („Wenn man nur einen Hammer hat, sieht jedes Problem wie ein Nagel aus"). In der Praxis werden Unternehmen jedoch selten allein aufgrund von Technologieausfällen angegriffen, sondern aufgrund einer Kombination aus Fehlern bei Menschen, Prozessen und Technologien. Das Schweizer-Käse-Modell veranschaulicht dieses Prinzip deutlich:



Wenn Sie durch mehrere Schutzschichten und Prozesse Cyber-Resilienz in Ihrem Unternehmen aufbauen, können Sie verheerende Sicherheitsverletzungen mit größerer Wahrscheinlichkeit vermeiden.

Unabhängig von der Größe Ihres Unternehmens werden Sie im Jahr 2026 Ziel von Cyberangriffen sein. Unsere Daten zeigen eindeutig, dass es nicht vor Kriminellen schützt, ein kleines Unternehmen oder eine gemeinnützige Organisation zu sein und erst recht nicht zu glauben, man habe nichts zu bieten, das es zu stehlen lohnt. Wenn Ihr Unternehmen über sensible Daten und Barreserven verfügt, sind Sie ein Ziel. Erstellen Sie ein Programm zur Cyber-Resilienz auf der Grundlage der Zero-Trust-Prinzipien:

- Gehen Sie von einer Sicherheitsverletzung aus – Natürlich bauen Sie starke, mehrschichtige Schutzmaßnahmen auf, aber irgendwann wird eine davon versagen. Fragen Sie sich: Verfügen Sie über Mechanismen, um einen Angriff schnell zu erkennen? Verfügen Sie über isolierte Netzwerke und nur die erforderlichen Berechtigungen, um den Schaden zu minimieren? Verfügen Sie über Mitarbeiter und Prozesse, die im Ernstfall sofort auf die Warnmeldungen reagieren und Angreifer aus dem System zu entfernen, bevor größerer Schaden entsteht?
- Least Privilege – Dies ist möglicherweise das Schwierigste, was es zu beachten gilt: Geben Sie Mitarbeitern nur die Berechtigungen, die sie für ihre Arbeit benötigen, und überprüfen Sie diese regelmäßig, damit sie sich nicht im Laufe der Zeit ansammeln.
- Überprüfen Sie jede Verbindung – Richten Sie eine leistungsstarke Richtlinien-Policy ein (z.B. Conditional Access in Entra ID), die jede Anmeldung und jeden Zugriff auf Anwendungen, Dateien und andere Ressourcen überprüft, um sicherzustellen, dass der Zugriff nicht standardmäßig erlaubt ist, sondern nur dann gewährt wird, wenn die richtigen Bedingungen erfüllt sind.

Bevor Sie Geld für fortschrittliche Sicherheitstools ausgeben, die bestimmte Probleme lösen, sollten Sie zunächst grundlegende Sicherheitsmaßnahmen gemäß der oben genannten Prinzipien umsetzen:

- Implementieren Sie MFA für alle Benutzer. Angesichts der enormen Zunahme von AiTM-Angriffen (Attacker-in-The-Middle) mit integrierter MFA-Umgehung müssen Sie auf Phishing-resistente MFA umsteigen. Dazu gehören Hardware-OAuth-Schlüssel, Windows Hello for Business, zertifikatsbasierte Authentifizierung und Passkeys, die keine Authentifizierung auf gefälschten Anmeldeseiten zulassen, auch wenn der Benutzer selbst getäuscht wurde.
- Verwenden Sie eine starke Endpoint-Schutzlösung auf allen Geräten, auf denen dies möglich ist, und integrieren Sie diese mit Identitäts-, Cloud-Anwendungen und einer E-Mail-Hygiene-Lösung für umfassende eXtended Detection and Response (XDR).
- Schulen Sie Ihre Benutzer darin, Phishing-Versuche zu erkennen, sei es in E-Mails, Teams, Zoom oder WhatsApp. Noch wichtiger ist es aber, eine Sicherheitskultur aufzubauen. Die Annahme, dass sich die IT- oder Sicherheitsabteilung um die gesamte Cybersicherheit kümmern muss, liegt falsch. Jede Person im Unternehmen muss sich verantwortlich fühlen und sich zu Wort melden, wenn etwas gefährlich oder riskant erscheint.
- Patchen Sie Ihre Software mit System. Wenn Sie nicht die Größe Ihrer IT-Abteilung verdoppeln möchten, müssen Sie Prioritäten setzen. Wenden Sie die Prinzipien des Continuous Threat Exposure Management (CTEM) an, um Ihre geschäftskritischen Systeme mit ausnutzbaren Schwachstellen zuerst zu schützen, anstatt zu versuchen, alles gleichzeitig zu patchen, was schlicht unmöglich ist.
- Analysieren Sie Ihre Lieferkette. Mehrere große Sicherheitsverletzungen in den letzten Monaten waren darauf zurückzuführen, dass ausgelagerte Helpdesk-Organisationen Opfer von Social Engineering wurden (Hacking von Personen statt von Computersystemen). Machen Sie sich mit allen ausgelagerten Prozessen vertraut und denken Sie daran, dass Sie zwar eine Funktion auslagern können, nicht aber das damit verbundene Risiko. Untersuchen Sie alle Lieferketten, die für den Betrieb Ihres Unternehmens wichtig sind, und bauen Sie Widerstandsfähigkeit für den Fall auf, dass Sie durch Cybersicherheitsangriffe oder aus anderen Gründen gestört werden.

EINE CYBERRESILIENTE ORGANISATION

Da Cybersicherheit in erster Linie ein Menschen- und Prozessproblem ist, liegt die Lösung nicht in noch mehr Technologie, sondern in einer Veränderung der Unternehmenskultur.

Ein gutes Vorbild liefert die Luftfahrtindustrie, in der jeder Vorfall und jeder Unfall gründlich untersucht wird, nicht um Schuld zuzuweisen, sondern um die Zusammenhänge zwischen Personen, Prozessen und technologischen Faktoren zu identifizieren, die dazu beigetragen haben. Diese Erkenntnisse werden dann genutzt, um mehr/andere Schulungen durchzuführen und Prozesse und Technologien zu ändern, damit sich solche Fehler nicht wiederholen.

Der erste Schritt ist der Aufbau einer Sicherheitskultur, in der sich alle Mitarbeiter sicher fühlen, etwas zu sagen, wenn ihnen etwas auffällt, das nicht stimmt. Dies ist nur möglich, wenn Menschen bei einem Vorfall nicht individuell beschuldigt werden, sondern ihre Fehler als Lernchancen verstanden werden – mit dem Ziel, Prozesse so zu verbessern, dass Fehler unwahrscheinlicher werden. Das bedeutet wiederum, dass Cybersicherheit in der Verantwortung aller liegt, nicht nur der IT- oder Sicherheitsabteilung – denn verschiedene Bereiche des Unternehmens treffen Technologieentscheidungen, die Risiken mit sich bringen, die nicht nur die IT, sondern alle bewältigen müssen. Auch wir in der Sicherheitsbranche müssen besser werden, wenn es um die Kommunikation mit anderen Stakeholdern geht, indem wir es schaffen, technisches „Geek-Speak" in eine Sprache zu übersetzen, die Geschäftsrisiken verständlich macht.

Während Sie in allen Bereichen Ihres Unternehmens Resilienz aufbauen, sollten Sie sich über die Veränderungen in der Bedrohungslandschaft auf dem Laufenden halten, da Angreifer immer innovativer werden, wenn es darum geht, Schwachstellen in unseren Systemen zu finden und auszunutzen.

EINE GANZHEITLICHE SICHERHEITSSTRATEGIE

Wir haben es bereits erwähnt, aber es lohnt sich, es zu wiederholen: Beginnen Sie mit den Grundlagen. Grundlegende Cybersicherheitsprozesse und -technologien dienen der Verteidigung Ihres Unternehmens viel mehr als die neueste punktuelle Lösung für Cybersicherheit. Sie benötigen mehrere Schutzebenen (denken Sie an das Schweizer-Käse-Modell):

Next-Gen Spam-/Malware-Erkennung der nächsten Generation mit ATP für Verhaltensanalysen zum Schutz vor der anhaltenden Flut von E-Mail-basierten Bedrohungen, die wir in dieser Branche beobachten

Sicherheitsschulungen für Endbenutzer, um Mitarbeiter darin zu schulen, Social-Engineering- und Spear-Phishing-Angriffe zu erkennen

Backup- und Wiederherstellungsfunktionen für lokale Daten UND Cloud-Daten, die z.B. in M365 gespeichert sind, um im Fall eines erfolgreichen Ransomware-Angriffs die Geschäftskontinuität sicherstellen sollte

Compliance- und Governance-Funktionen, die zum Schutz vor versehentlichem Datenverlust beitragen und sicherstellen, dass Compliance-Kontrollen eingehalten werden

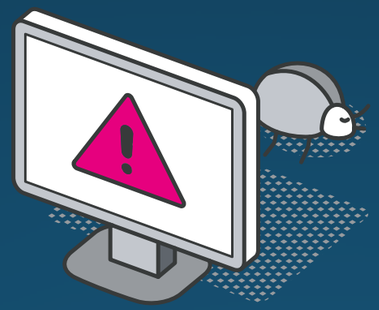
Least Privilege und Freigabekontrolle für Ihre sensiblen Unternehmensdaten, die in SharePoint und OneDrive for Business gespeichert sind

KI-gestützter Cyber-Assistent für E-Mail- und Teams-Kommunikation, der Benutzer hilft, sicher zu bleiben

Weitere Informationen

Cybersicherheit ist nur eine von vielen Herausforderungen, vor denen Unternehmen heute stehen, doch sie zu gering zu priorisieren kann katastrophale Folgen haben (siehe Jaguar Land Rover).

So wie viele Unternehmen Teile ihrer Geschäftstätigkeit an Spezialisten in diesem Bereich auslagern, können Sie von dem fundierten Wissen und den Fähigkeiten profitieren, die wir bei Hornetsecurity seit 2007 entwickelt haben. Arbeiten Sie mit uns zusammen, um Ihr Unternehmen zu schützen.



365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAMER

PLAN 2

INCLUDES 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 3

INCLUDES 1 + 2

- AUTOMATIC BACKUP O M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

PLAN 4

INCLUDES 1 + 2 + 3

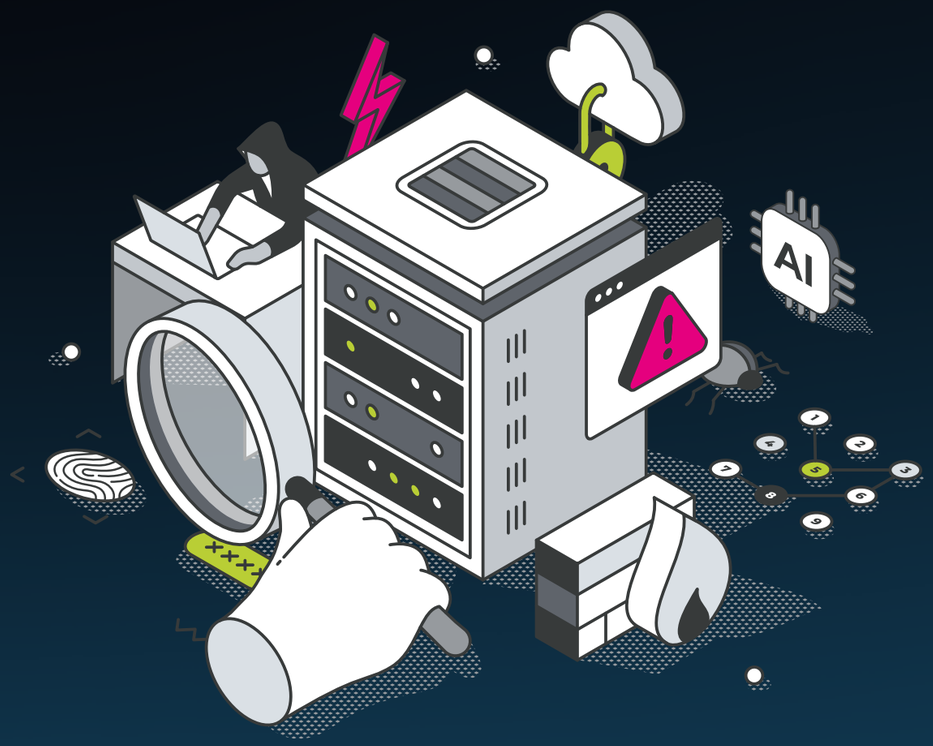
- SECURITY AWARENESS
- PERMISSION MANAGEMENT
- DMARC REPORTING & MANAGEMENT

POWERED BY AI CYBER ASSISTANT

- AI RECIPIENT VALIDATION
- TEAMS PROTECTION
- AI EMAIL SECURITY ANALYST

JETZT DEMO BUCHEN

HORNETSECURITY

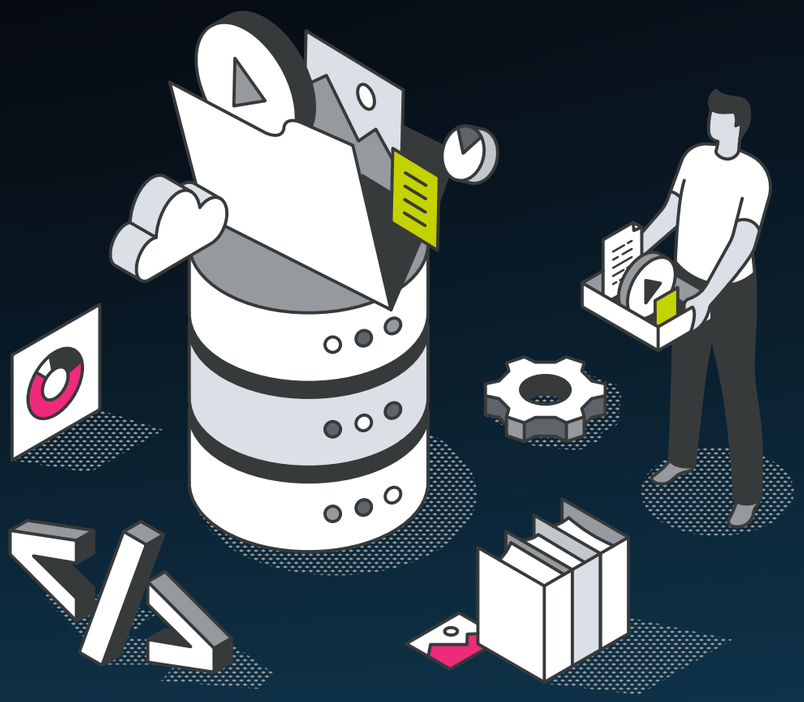


KAPITEL 5

RESSOURCEN

- https://www.hornetsecurity.com/de/blog/ransomware-impact-report-2025-pressemitteilung/
- https://www.hornetsecurity.com/en/blog/ciso-insights/
- https://www.hornetsecurity.com/en/blog/sharepoint-vulnerability/
- https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-june-2025/
- https://www.anthropic.com/news/detecting-countering-misuse-aug-2025
- https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/
- https://www.cnbc.com/2025/09/25/judge-anthropic-case-preliminary-ok-to-1point5b-settlement-with-authors.html
- https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
- https://www.hornetsecurity.com/en/blog/nis2-directive/
- https://www.infosecurity-magazine.com/news/nis2-compliance-strain-budgets/
- https://www.infosecurity-magazine.com/news/dora-compliance-costs-soar/
- https://ossf.github.io/malicious-packages/stats/
- https://techcommunity.microsoft.com/blog/windowsdriverdev/towards-rust-in-windows-drivers/4449718
- https://www.youtube.com/watch?v=uDtMuS7BExE
- https://pentiumsoak.com/the-rise-of-rust-in-the-linux-kernel-transforming-security-stability-in-2025/
- https://medium.com/cybersecurity-and-iot/how-googles-switch-to-rust-programming-is-redefining-android-s-security-a-52-drop-in-memory-29620cd46e0a
- https://security.apple.com/blog/memory-integrity-enforcement/
- https://www.aim.security/post/echoleak-blogpost
- https://genai.owasp.org/llmrisk/llm01-prompt-injection/
- https://arxiv.org/abs/2508.20444v1
- https://github.com/kgretzky/evilginx2
- https://www.proofpoint.com/us/blog/threat-insight/dont-phish-let-me-down-fido-authentication-downgrade
- https://en.wikipedia.org/wiki/North_Korean_remote_worker_scheme
- https://attack.mitre.org/matrices/enterprise/cloud/saas/
- https://postquantum.com/post-quantum/crqc/
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://en.wikipedia.org/wiki/Grover%27s_algorithm
- https://github.com/microsoft/SymCrypt-OpenSSL
- https://developer.apple.com/videos/play/wwdc2025/314/
- https://en.wikipedia.org/wiki/Cryptographic_agility
- https://en.wikipedia.org/wiki/Swiss_cheese_model
- https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/5604/1/g21f.pdf
- https://en.wikipedia.org/wiki/Continuous_Threat_Exposure_Management
- https://www.hornetsecurity.com/en/blog/supply-chain-attacks/
- https://www.hornetsecurity.com/en/services/advanced-threat-protection/
- https://www.hornetsecurity.com/en/services/security-awareness-service/
- https://www.hornetsecurity.com/en/services/365-total-backup/
- https://www.hornetsecurity.com/en/services/vm-backup/
- https://www.hornetsecurity.com/en/services/365-total-protection/
- https://www.hornetsecurity.com/en/services/365-permission-manager/
- https://www.hornetsecurity.com/en/services/ai-cyber-assistant/
- https://www.hornetsecurity.com

HORNETSECURITY



ÜBER DIE AUTOREN

VERFASST VON

ANDY SYREWICZE

Andy verfügt über mehr als 20 Jahre Erfahrung in der Bereitstellung von Technologielösungen in verschiedenen Branchen. Er ist spezialisiert auf Infrastruktur, Cloud und die Microsoft 365 Suite.

Andy ist Träger des Microsoft MVP-Awards im Bereich Sicherheit

PAUL SCHNACKENBURG

Paul Schnackenburg begann seine IT-Karriere, als DOS und 286-Prozessoren noch die neuesten Technologien waren. Heute leitet er Expert IT Solutions, einen MSP an der Sunshine Coast in Australien.

Als angesehener Technologieautor ist Paul in der Community aktiv und schreibt ausführliche Fachartikel mit den Schwerpunkten Cybersicherheit, Microsoft 365 und damit verbundenen Cloud-Diensten.

Er verfügt über MCSE-, MCSA- und MCT-Zertifizierungen.