Whitepaper

InfoGuard Threat Intelligence Insights 2025

Eine Analyse der Bedrohungslage - inklusive Prognose und Handlungsempfehlungen

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Stand: Mai 2026

Executive Summary

Cyberangriffe werden nicht raffinierter, sondern effizienter. Die umfassende Analyse des Jahres 2025 zeigt: Angriffe folgen zunehmend einem skalierbaren, automatisierten und arbeitsteilig organisierten Modell. Der entscheidende Moment bleibt dabei der Initial Access. Phishing, kompromittierte Identitäten und unzureichend abgesicherte Remote-Zugänge zählen weiterhin zu den häufigsten und zugleich wirksamsten Einstiegsvektoren.

Gleichzeitig verschiebt sich der Fokus der Angreifer klar auf Identitäten. Bereits einzelne kompromittierte Zugangsdaten reichen aus, um weitreichende Kontrolle über Systeme und Daten zu erlangen. Auffällig ist zudem: Sicherheitsvorfälle entstehen selten durch fehlende Schutzmechanismen, sondern durch mangelnde Sichtbarkeit und verspätete Reaktion. Organisationen mit ausgereiftem Monitoring und getesteter Incident Response begrenzen Schäden signifikant.

Dabei zeigen sich klare branchenspezifische Unterschiede: Während einige Sektoren Angriffe frühzeitig erkennen und entsprechend reagieren, greifen andere häufig erst ein, wenn der Impact bereits eingetreten ist. Vor diesem Hintergrund liegt der Schlüssel zur Cyberresilienz nicht in der Investition in zusätzliche Monitoring- und Detektionswerkzeuge, sondern in der Fähigkeit, Angriffe frühzeitig zu erkennen und gezielt zu steuern.

Der Bericht leitet daraus sieben zentrale Handlungsfelder für 2026 ab: von einer konsequenten Absicherung von Identitäten («Identity First») über verkürzte Patchzyklen und eine weitergedachte Zero-Trust-Architektur bis hin zu einer erweiterten Sichtbarkeit über Identitäten, Cloud und APIs. Ergänzt wird dies durch die systematische Vorbereitung auf den Ernstfall – etwa durch getestete Incident-Response-Prozesse, belastbare Backup-Strategien und eine gezielte Reduktion von Risiken in der Supply Chain. Diese Handlungsfelder bilden die Grundlage, um Cyberrisiken nicht nur zu reduzieren, sondern im Ernstfall kontrolliert zu beherrschen.

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Inhaltsverzeichnis

1 Rückblick 2025

2 Einstiegsvektoren

- **2.1** Phishing
- **2.2** Ungesicherte Remote-Zugänge
- **2.3** Schwachstellen
- **2.4** Supply Chain
- **2.5** Fehlkonfiguration

3 Sektortrends

- **3.1** Monitoring
- **3.2** Readiness

4 Gefahren

- **4.1** Ransomware
- **4.2** Business E-Mail Compromise
- **4.3** Identitäts-Diebstahl
- **4.4** Staatliche Akteure
- **4.5** KI-unterstützte Angriffe

5 Die sieben zentralen Handlungsempfehlungen für 2026

6 Fazit

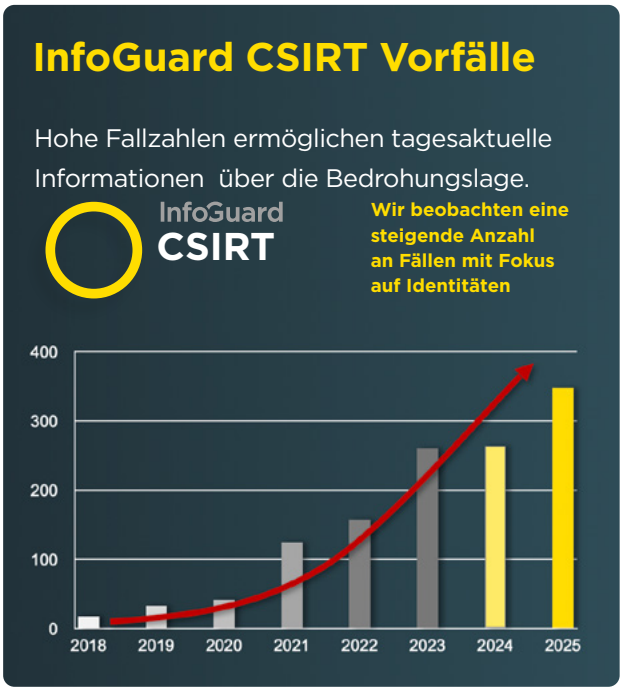
- **6.1** Von reaktiver Sicherheit zu proaktiver Cyberresilienz

1. Rückblick 2025

Die aktuelle Bedrohungslage verschärft sich weiter. Besonders deutlich zeigt sich dies in der operativen Realität der Incident Response. Im Jahr 2025 bewältigte das InfoGuard CSIRT über 350 Cybervorfälle, was einem substanziellen Anstieg von rund 20 Prozent gegenüber dem Vorjahr entspricht. Bereits im ersten Halbjahr zeichnete sich diese Entwicklung ab: Komplexe Angriffe nahmen gegenüber der Vorperiode um beachtliche 115 Prozent zu.

Diese Entwicklung ist kein statistischer Ausreisser, sondern Ausdruck eines strukturellen Wandels. Die steigenden Fallzahlen spiegeln ein zunehmend dynamisches und belastbares Lagebild wider.

Auffällig ist dabei, dass 2025 kaum neue Angriffsmethoden hervorbrachte. Stattdessen beschleunigte sich die Industrialisierung von Cyberangriffen deutlich. Angreifer agieren effizienter, schneller und in hochgradig skalierbaren, arbeitsteiligen Strukturen. Automatisierung, der Handel mit kompromittierten Zugängen durch Initial-Access-Broker, KI-gestützte Angriffswerkzeuge sowie professionalisierte Ransomware-Ökosysteme senken die Eintrittsbarrieren weiter – und führen dazu, dass sich Cyberangriffe zunehmend wie ein Dienstleistungsmodell organisieren lassen.



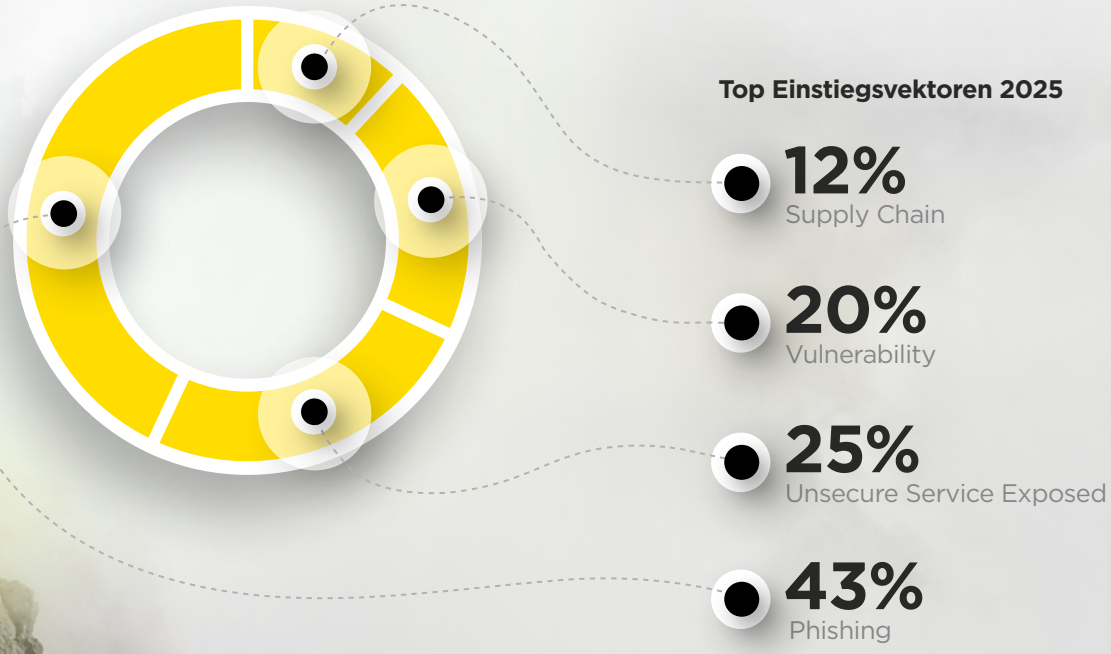
Source InfoGuard Intelligence

2. Einstiegsvektoren

Der Initial Access blieb die kritischste Phase jeder Angriffskette. Gelingt Angreifern der Zugang ins Unternehmensnetzwerk, verschiebt sich der Fokus unweigerlich von Prävention hin zur Schadensbegrenzung

In 43 Prozent der vom InfoGuard-CSIRT bearbeiteten Sicherheitsvorfälle erfolgte der Erstzugang über Phishing. Innerhalb der vergangenen fünf Jahre hat sich dieser Anteil mehr als verdoppelt und als dominanter Angriffsvektor etabliert. Verantwortlich dafür dürfte insbesondere der zunehmende Einsatz von LLMs auf Angreiferseite sein, die personalisierte und kontextuell überzeugende Angriffe ermöglichen. Ein gegenteiliger Trend zeigt sich bei der Ausnutzung von Schwachstellen: Während Phishing stark zunimmt, ist ihr Anteil in fünf Jahren auf nur 20 Prozent gefallen. Ein möglicher Grund dafür ist eine bewusstere Exponierung von Services gegenüber dem Internet. Organisationen haben aus früheren Sicherheitsvorfällen gelernt und exponieren Workloads nicht mehr direkt im Internet, sondern schützen sie über vorgeschaltete Authentifizierungsportale. Beunruhigend blieb jedoch die hohe Zahl von Sicherheitsvorfällen, bei welchen exponierte Services noch immer ausschliesslich durch einfache Benutzername-Passwort-Kombinationen geschützt sind. Ein Sicherheitsniveau, das heutigen Angriffsrealitäten nicht mehr standhält.

Im Vergleich zu den Vorjahren nahm die Zahl der Vorfälle, die über die Supply Chain erfolgen, weiter zu. Viele Unternehmen sind sich dieses Risikos immer noch nicht ausreichend bewusst und unterschätzen die damit verbundenen Gefahren.



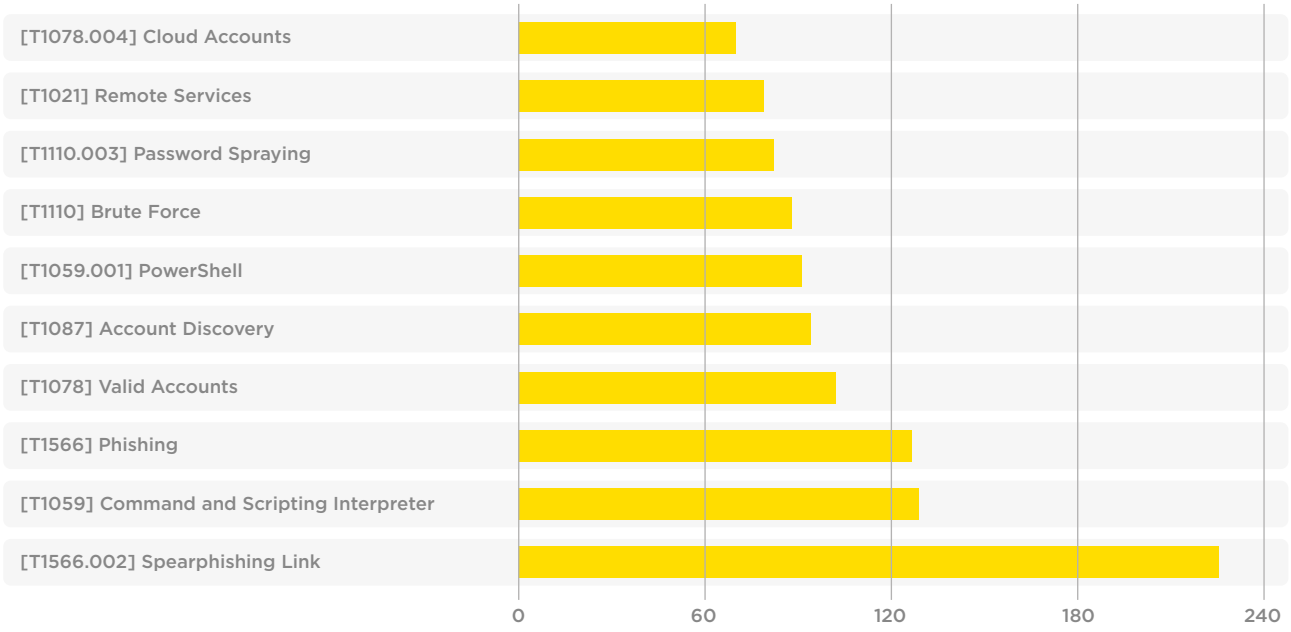
2.1 Phishing

Phishing blieb im Berichtszeitraum der dominierende Einstiegsvektor für Cyberangriffe. Gleichzeitig erreichte die Qualität der Angriffe eine neue Eskalationsstufe: personalisierte Inhalte, KI-generierte Texte, Deepfake-Sprachnachrichten und die präzise Nachbildung interner Kommunikationsstile.

Credential Harvesting verlagerte sich zunehmend auf Cloud-Dienste wie Microsoft 365 (M365) und Google Workspace. MFA-Bypass-Techniken wie der Diebstahl von Session-Tokens oder Adversary-in-the-Middle-Kits wurden nicht mehr als Ausnahme, sondern als etablierter Standard beobachtet. Phishing ist weniger ein Awareness-Problem als vielmehr eine Frage der Identitätssicherheit. Entsprechend überrascht es nicht, dass sich ein erheblicher Anteil, der im InfoGuard MDR Service 2025 detektierten True-Positive-Sicherheitsvorfälle gezielt gegen Identitäten richtete. Typische Angriffsmethoden sind Spearphishing, Phishing, Brute Force und Password Spraying, mit welchen Angreifer versuchen, systematisch Kontrolle über lokale und Cloud-basierte Accounts zu erlangen.

Die Folgen erfolgreicher Phishingangriffe waren meist nicht isoliert, sondern kaskadierend: weitere Phishingkampagnen, die Datenexfiltration aus SharePoint- und OneDrive-Umgebungen, Versand gefälschter Rechnungen oder die gezielte Entwendung sensibler E-Mail-Verläufe.

Häufigste True-Positive-Detektionen im Security Operations Center (SOC)



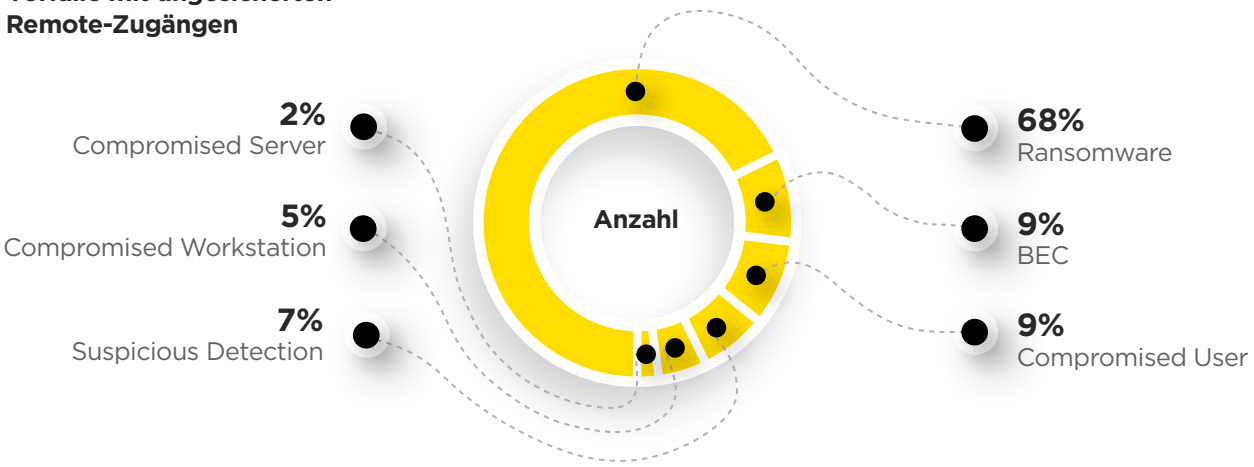
2.2 Ungesicherte Remote-Zugänge

Offene oder schlecht abgesicherte VPN-, RDP- und Remote-Management-Zugänge blieben ein bevorzugter Einstiegspunkt für Ransomware-Akteure mit besonders gravierenden Folgen: In 68 Prozent der beobachteten Vorfälle führte der Zugriff über solche Zugänge direkt zu einer Ransomware-Kompromittierung.

Das grösste Sicherheitsversäumnis blieb die fehlende Multifaktor-Authentifizierung. Sie ermöglicht es Angreifern, mit minimalem Aufwand und maximaler Wirkung in Unternehmensnetzwerke einzudringen. Schwache, wiederverwendete oder nur temporär gesetzte Passwörter verstärken diese Angriffsfläche zusätzlich und erleichtern so, Benutzerkonten durch Brute-Force-Angriffe zu kompromittieren. InfoGuard beobachtete in zahlreichen Unternehmen fehlende Einschränkungen bei den Benutzerkonten, welche Remote-Zugänge nutzen dürfen. In einigen Fällen liess sich der Eintrittspunkt auf technische oder temporäre Benutzerkonten zurückführen. Diese waren mit schwachen Passwörtern geschützt und konnten in einigen Fällen über exponierte Legacy-Protokolle kompromittiert werden, die kaum oder keine Schutzmechanismen bieten.

Initial Access Broker professionalisierten den Handel mit kompromittierten Zugängen. Unternehmen wurden zunehmend nicht mehr direkt angegriffen, sondern als fertige Eintrittspunkte gehandelt und weiterverkauft.

Vorfälle mit ungesicherten Remote-Zugängen



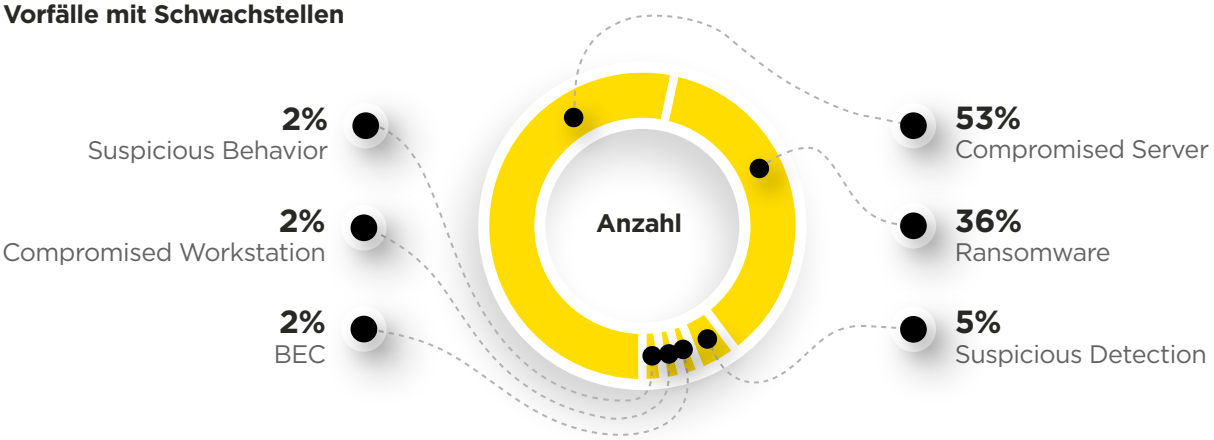
2.3 Schwachstellen

2025 war geprägt von der massiv beschleunigten Ausnutzung neu publizierter RCE-Schwachstellen. Das Zeitfenster zwischen der Veröffentlichung einer CVE und der aktiven Exploit-Nutzung schrumpfte in vielen Fällen von Wochen auf wenige Tage oder sogar Stunden. Der zunehmende Einsatz von Agentic AI auf Angreiferseite dürfte diese Entwicklung künftig weiter verschärfen und klassische, oft träge Patchprozesse strukturell überfordern. Besonders betroffen waren Edge Devices und remote exponierte Services wie:

- Ivanti
- SonicWall
- SAP
- Microsoft SharePoint
- WordPress Plugins

Exploit-Kits waren häufig bereits kurz nach Veröffentlichung einer Schwachstelle verfügbar – teilweise schneller, als Organisationen ihre Risikoanalyse abschliessen konnten. Zu spätes Patchen vermittelte zahlreichen Unternehmen eine trügerische Sicherheit, da Systeme zum Zeitpunkt des Patchings nicht selten bereits kompromittiert waren. Angreifer konnten ihre Aktivitäten dadurch unbemerkt fortsetzen und zeitlich verzögert operationalisieren. In 53 Prozent der Vorfälle, bei welchen eine Schwachstelle als Eintrittspunkt genutzt wurde, führte dies zu einem kompromittierten Server. Schnelle Detektion und Reaktion entschieden dabei über den weiteren Verlauf: In vielen Fällen konnte rasches Eingreifen laterale Bewegungen verhindern. Dennoch mündeten 36 Prozent der Vorfälle in einen erfolgreichen Ransomware-Angriff, mit teilweise erheblichen operativen und finanziellen Auswirkungen auf den Geschäftsbetrieb.

Vorfälle mit Schwachstellen



2.4 Supply Chain

Statt ihre Ziele direkt anzugreifen, nutzten Angreifer zunehmend den Zugang über die Supply Chain und instrumentalisierten gezielt bestehende Vertrauensbeziehungen als Einfallstor.

Beobachtet wurden unter anderem die Ausnutzung ungesicherter Fernwartungszugänge, bösartige Software-Updates sowie über Google Ads beworbene Business Software, die in einem Bundle mit Fernwartungssoftware oder Trojanern bereitgestellt wurde. Zudem entwickelten sich unzureichend eingeschränkte und überwachte S2S-VPN-Verbindungen zu Partnern zunehmend zu einem strukturellen Risiko, da sie Angreifern direkten Zugriff auf interne Netzwerke ermöglichen. Besonders gefährdet für gezielte Supply-Chain-Angriffe waren Unternehmen in der Finanz- und Versicherungsbranche wie auch im Sektor Information und Kommunikation. Diese Organisationen verfügen oft über ein starkes Sicherheitsdispositiv zur Abwehr und Erkennung von Angriffen. Für Angreifer entsteht dadurch ein strategischer Vorteil: Der Weg über die Lieferkette ist oft weniger sichtbar, weniger geschützt und operativ effizienter als ein direkter Angriff auf das eigentliche Ziel.

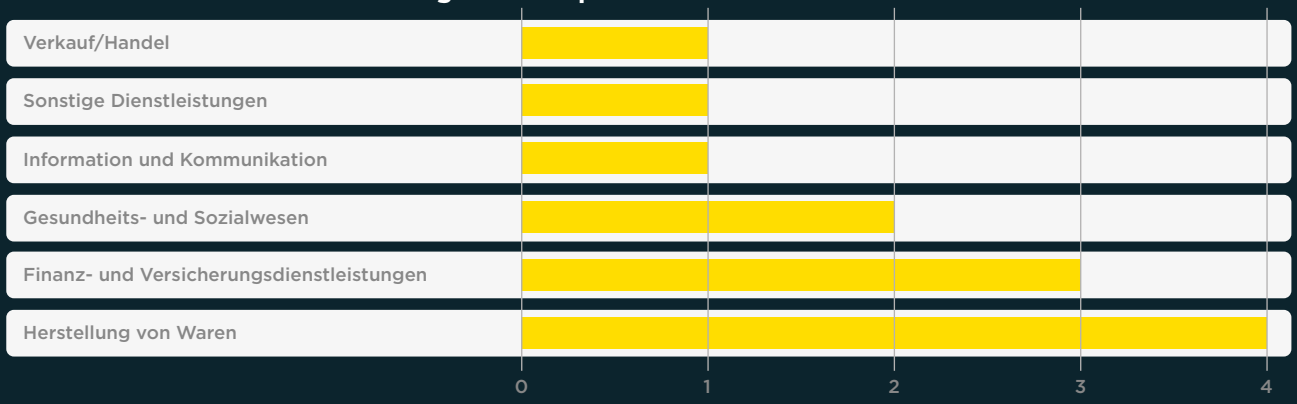
Supply-Chain-Vorfälle pro Sektor

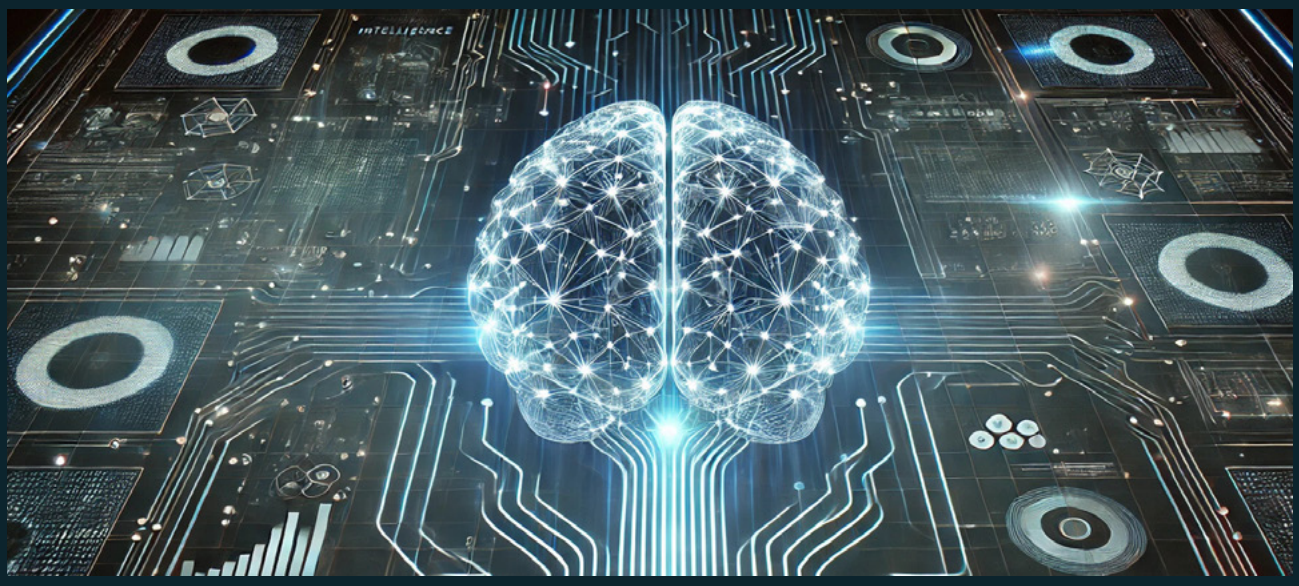
2.5 Fehlkonfiguration

Ein oft unterschätzter Einfallsvektor blieben Fehlkonfigurationen. Sie entstehen selten durch einzelne gravierende Fehler, sondern vielmehr durch eine Vielzahl kleiner, alltäglicher Versäumnisse.
Die Ursachen reichen von mangelndem Know-how über Zeitdruck und Ablenkung im Arbeitsalltag bis hin zu einer unzureichenden Auseinandersetzung mit sicherheitsrelevanten Änderungen, etwa in Patchnotes oder Systemupdates. Hinzu kommen fehlende Prozesse zur Qualitätssicherung, die sicherstellen würden, dass Änderungen konsistent geprüft und dokumentiert werden.
InfoGuard beobachtete im Berichtszeitraum eine Vielzahl unterschiedlichster Fehlkonfigurationen. Dazu gehörten unter anderem verwaiste DNS-Pointer auf Cloud-Ressourcen, die von Angreifern übernommen werden konnten, sowie unbeabsichtigte Deaktivierungen von Authentifizierungsmechanismen. Ebenso wurden gegenüber dem Internet exponierte Management-Interfaces und die unbeabsichtigte Exponierung interner Datenbestände festgestellt.

Fehlkonfigurationen lassen sich keinem bestimmten Sektor eindeutig zuordnen. Auffällig war jedoch, dass betroffene Unternehmen häufig über komplexe, hybride Infrastrukturen mit zahlreichen Schnittstellen und externen Dienstleistern verfügen. In vielen Fällen liess sich die Ursache auf ein strukturelles Governance-Defizit zurückführen, da klare Zuständigkeiten für die Umsetzung, Kontrollmechanismen und unzureichende Dokumentation von Änderungen fehlten.

Sicherheitsvorfälle durch Fehlkonfigurationen pro Sektor





3. Sektortrends

3.1 Monitoring

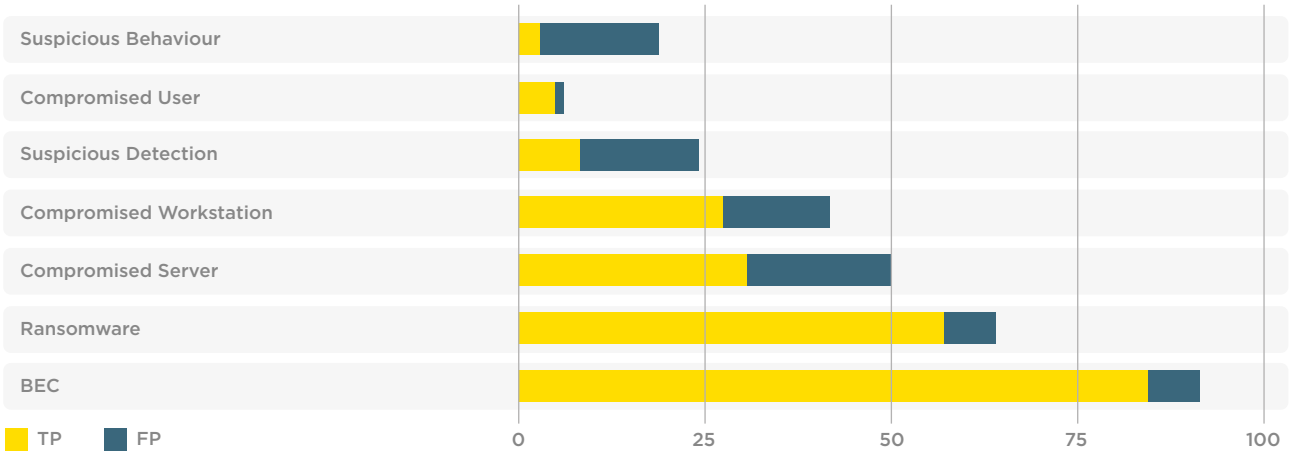
InfoGuard beobachtete im vergangenen Jahr, dass Organisationen bei Verdacht oder Hinweisen auf eine Kompromittierung zunehmend früher und gezielter externe Expertise beizogen – ein klares Zeichen wachsender Sensibilität gegenüber Cyberrisiken.

Organisationen mit ausgereiftem Monitoring und etablierten Response-Prozessen reduzieren den Impact eines Angriffs nachweislich und entscheidend. Der Unterschied liegt dabei weniger in der Verhinderung eines Angriffs als in der Geschwindigkeit und Qualität der Erkennung sowie der anschliessenden Reaktion.

Zu den vom InfoGuard-CSIRT bearbeiteten False-Positive-Alarmen zählen beispielsweise:

- Überprüfung verwundbarer, exponierter Systeme, um auszuschliessen, dass ein System bereits vor der Patchung kompromittiert wurde.
- Unterstützung bei der Analyse unbekannter Detektionen aus der eingesetzten Monitoring-technologie.
- Unzureichender Kontext in der Monitoringtechnologie zur abschliessenden und belastbaren Bewertung eines möglichen Security Incidents.
- Zweitmeinung oder Validierung selbst durchgeführter Analysen.
- Unterstützung bei der Analyse möglicher lateraler Bewegungen aus einem kompromittierten Partnernetzwerk.

False-Positive-Rate pro Vorfalltyp



Auffällig ist die sektorale Verteilung: Besonders häufig wurde das InfoGuard-CSIRT bei False-Positive-Alarmen in den Branchen Energie und Wasser, Finanz- und Versicherungsdienstleistungen, Gesundheits- und Sozialwesen, Informatik und Kommunikation wie auch in der öffentlichen Verwaltung, Verteidigung und bei Sozialversicherungen zur Unterstützung beigezogen. Diese Häufung ist kein Zufall, sondern ein Indikator für vorhandene und funktionierende Monitoring-Strukturen, die Angriffe bereits in einem frühen Stadium sichtbar machen.

Demgegenüber melden sich Organisationen in den Bereichen Herstellung, Handel, Verkehr sowie im Baugewerbe immer noch erst zu einem späteren Zeitpunkt. Dann nämlich, wenn Angreifer ihre Ziele bereits erreicht haben und der Schaden sich abzuzeichnen beginnt. Monitoring wird hier weniger als kontinuierliche Fähigkeit verstanden, sondern als reaktive Massnahme im Ereignisfall.

Für die frühzeitige Erkennung von Angreifern sind insbesondere folgende Faktoren entscheidend:

- Einsatz von «Endpoint Detection and Response»-Technologie statt rein signatur basierter Antivirus-Lösung
- Ergänzung durch «Identity Detection and Response»-Technologie
- Logkorrelation über mehrere Quellen, insbesondere Firewall, Proxy, VPN, VDI Logs

Gleichzeitig identifizierten wir klare Defizite in der Sichtbarkeit:

- Fehlende oder zu kurz aufbewahrte Firewall- und (VPN-)Authentication-Logs
- Eingeschränkte Transparenz in SaaS- und PaaS-Diensten ohne SSO-Integration
- Fremdsysteme und Appliances ohne integriertes Security-Monitoring
- Schatten-IT sowie temporäre Cloud-Workloads bei Cloudanbietern

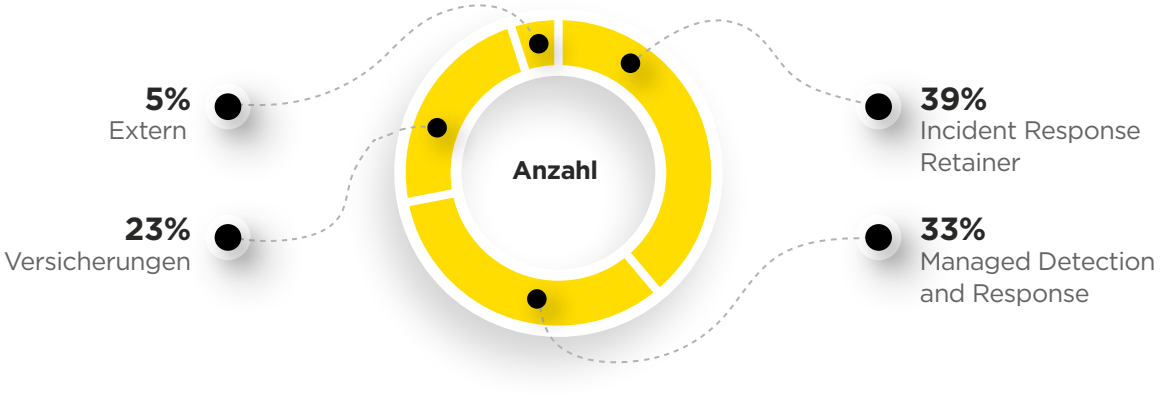
Das zentrale Muster ist klar erkennbar: Angriffe scheiterten im Berichtszeitraum selten an fehlenden Schutzmechanismen, sondern daran, dass sie zu spät erkannt wurden oder im Rauschen der Systeme untergingen.

3.2 Readiness

Das InfoGuard-CSIRT unterstützt Unternehmen in jeder Ausgangslage. Bei bestehenden Kunden – etwa mit «Incident Response Retainer» oder «Managed Detection and Response» – besteht durch strukturiertes Onboarding bereits vor einem möglichen Vorfall eine operative Einsatzbereitschaft, sodass im Ernstfall ohne Zeitverlust gehandelt werden kann. Anders stellt sich die Situation bei Unternehmen, die über Versicherungen oder als Neukunden Kontakt aufnehmen: Hier variiert die Maturität der Incident-Response-Readiness teilweise erheblich mit direkten Auswirkungen auf Reaktionsgeschwindigkeit und Schadensausmass.

In der Praxis identifizierte das InfoGuard-CSIRT bei vielen Organisationen wiederkehrende Lücken in der Incident Readiness. Bemerkenswert ist dabei weniger das Fehlen von Konzepten, sondern deren mangelnde Umsetzbarkeit im Ernstfall. Die Behebung der identifizierten Lücken würde in zahlreichen Fällen eine schnellere und effektivere Reaktion ermöglichen und den entstandenen Schaden signifikant reduzieren.

Kundenbeziehung



Typische Lücken in der Praxis:

- **Validierung einer Ransomware-sicheren Backup-Aufbewahrung:**
  In einigen Fällen stellte sich heraus, dass unternehmenskritische Backups ausschliesslich auf einem NAS gespeichert waren und damit für Angreifer direkt erreichbar und löschbar blieb. Ohne zusätzliche Schutzmechanismen wie Air-Gapping oder Immutable Storage wird die vermeintliche Sicherheitskopie selbst zum Risiko.

- **Fehlende oder ungeübte Incident-Response-, Business-Continuity- und Backup-Recovery-Pläne:**
  Zwar investieren viele Organisationen Zeit in Incident-Response-, Business-Continuity- und Recovery-Pläne. In der Praxis zeigte sich jedoch häufig, dass diese Pläne nie unter realistischen Bedingungen getestet wurden. Ohne regelmässige Übungen – etwa in Form von Tabletop Exercises (TTX) – bleibt ihre Wirksamkeit im Ernstfall ungewiss.

- **Nicht verfügbare Notfalldokumentation im Incident-Fall:**
  Insbesondere bei Ransomware-Angriffen zeigt sich ein wiederkehrendes Muster: Zentrale Informationen wie Notfallkontaktlisten, Zugangsdaten, Lizenzen oder Wiederanlaufpläne sind im entscheidenden Moment nicht verfügbar, da sie selbst verschlüsselt wurden. Kritische Dokumente müssen daher bewusst offline und unabhängig von der produktiven Infrastruktur aufbewahrt werden.

- **Unzureichende Log-Aufbewahrung und forensische Sichtbarkeit:**
  Für die forensische Aufarbeitung eines Incidents sind Logs wie etwa Endpunkt-Logs, Firewall-Logs oder Antivirus-Logs oft die einzige verlässliche Informationsquelle. Fehlen diese Daten oder werden sie nicht langfristig aufbewahrt, ist eine fundierte forensische Aufarbeitung kaum möglich. Dies erschwert nicht nur die Ursachenanalyse, sondern verzögert ebenfalls den sicheren Wiederanlauf. Eine zentrale, manipulationssichere und möglichst Ransomware-resistente Speicherung relevanter Logs ist daher essenziell. Moderne EDR- und XDR-Lösungen bieten hierfür bereits integrierte Möglichkeiten zur erweiterten und sicheren Log-Aufbewahrung. Kritische Dokumente müssen daher bewusst offline und unabhängig von der produktiven Infrastruktur aufbewahrt werden.

Das zentrale Muster zeigt sich deutlich: Nicht die Existenz von Sicherheitsmassnahmen entscheidet über den Erfolg im Ernstfall – sondern deren Verfügbarkeit, Praxistauglichkeit und unmittelbare Nutzbarkeit unter Stressbedingungen.

4. Gefahren

4.1 Ransomware

Ransomware gehörte gemessen am potenziellen Impact im Berichtszeitraum zu den markantesten Cyberbedrohungen für Unternehmen, woran sich auch in der nahen Zukunft nichts ändern wird. Ein erfolgreicher Angriff führt selten zu kurzfristigen Störungen, sondern zieht sich oft über Wochen oder Monate, bis der operative Normalbetrieb wiederhergestellt ist.

Im Vergleich zu den Vorjahren zeigte sich jedoch eine markante Entwicklung: Zunehmend verzichteten Angreifer auf die Verschlüsselung und beschränkten sich auf die Exfiltration sensibler Daten. Diese Angriffe bleiben oft unentdeckt, bis Angreifer mit der Veröffentlichung exfiltrierter Daten drohen und so maximalen Druck aufbauen.

Ransomware-Angriffe erfolgen in der Regel opportunistisch und selten gezielt. Nicht das einzelne Unternehmen steht im Fokus, sondern dessen Verwundbarkeit. Diese Dynamik spiegelt sich auch in der sektorübergreifenden Verteilung der Vorfälle wider.

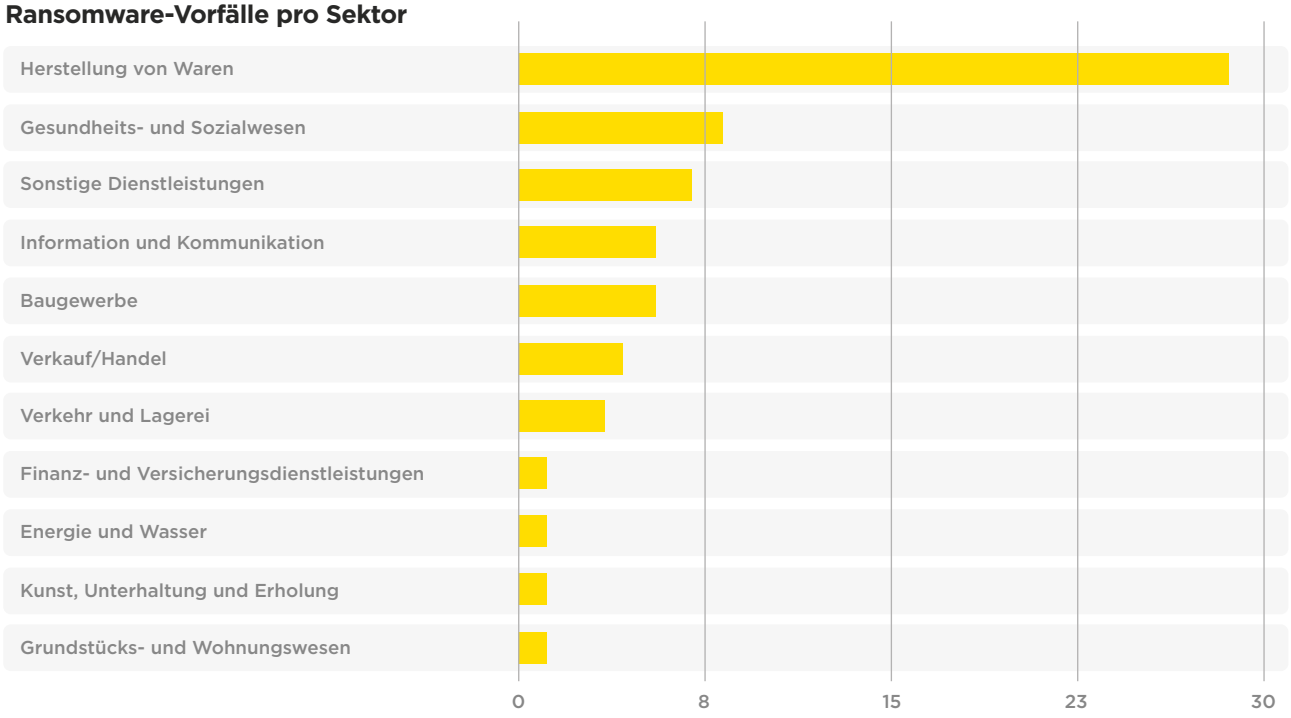
Der überwiegende Teil der vom InfoGuard-CSIRT verzeichneten Vorfälle entfiel auf den Bereich der produzierenden Unternehmen. Im Vergleich zu stärker regulierten Branchen unterliegt dieser Sektor geringeren verbindlichen Anforderungen an Cyberresilienz, was sich unmittelbar in der Angriffsfläche widerspiegelt.

Darüber hinaus betreiben produzierende Unternehmen häufig heterogene, historisch gewachsene IT-Landschaften mit langen Lebenszyklen, in denen Applikationen und Systeme weitergeführt werden, obwohl sie aus Sicherheitssicht bereits kritisch sind.

Besonders relevant ist zudem die enge Verzahnung von IT- und OT-Infrastrukturen. Produktionsumgebungen sind oft über herstellerspezifische Wartungszugänge angebunden, die nicht konsequent segmentiert oder überwacht werden. Ein erfolgreicher Angriff auf die IT kann sich dadurch direkt und ohne Umwege auf die operative Produktion auswirken. Mit entsprechend gravierenden Folgen.

Die zentrale Erkenntnis: Ransomware ist längst nicht mehr nur ein IT-Sicherheitsproblem. Sie entwickelt sich zunehmend zu einem geschäftskritischen Risiko mit unmittelbaren Auswirkungen auf Lieferketten, Produktion und Marktverfügbarkeit.

Ransomware-Vorfälle pro Sektor

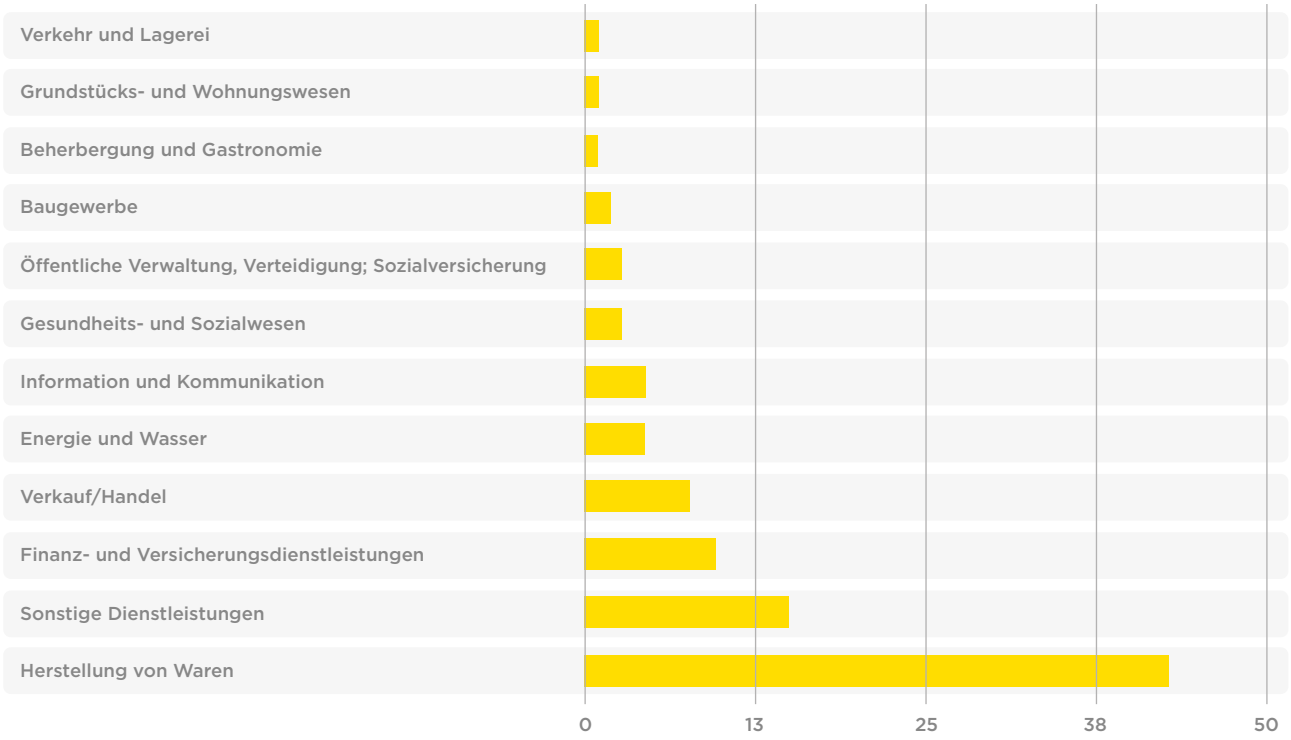


4.2 Business E-Mail Compromise (BEC)

Vor dem Hintergrund von LLMs, InfoStealern und zunehmenden Credential-Leaks steigt die Zahl der Fälle von Business E-Mail Compromise weiter und messbar an. Der überwiegende Teil kompromittierter E-Mail-Accounts steht im Zusammenhang mit Phishing-Angriffen. Am häufigsten nutzten Angreifer dabei «Adversary-in-the-Middle»-Angriffe, um zusätzlich die Multifaktor-Authentifizierung gezielt und systematisch zu umgehen. Um solche Angriffstaktiken künftig technisch zu unterbinden, sollten phishing-resis-tente Verfahren wie Passkeys oder FIDO2 konsequent und flächendeckend implementiert werden. Der unmittelbare Schaden eines Business E-Mail Compromise bleibt in den meisten Fällen überschaubar. Oft werden gekaperte Konten lediglich mit einer Weiterleitungsregel ausgestattet, um die Kompromittierung zu verbergen und anschliessend weitere Geschäftspartner über gezielte Phishingkampagnen zu kompromittieren.

Das InfoGuard-CSIRT verzeichnete jedoch auch mehrere Fälle, in denen es Angreifern gelang, Rechnungen zu manipulieren, sodass einige Unternehmen erhebliche und unmittelbar wirksame finanzielle Verluste erlitten. In einzelnen Fällen übertraf der finanzielle Schaden sogar typische Ransomware-Zahlungen. Neben Zahlungsbetrug beobachtete das InfoGuard-CSIRT auch Threat-Akteure, die über kompromittierte M365-Accounts Unternehmensdaten aus OneDrive und SharePoint exfiltrierten und Unternehmen mit der Veröffentlichung dieser Daten unter Druck setzten. Die meisten BEC-Vorfälle verzeichnete das InfoGuard-CSIRT im Sektor der Warenherstellung. Dies dürfte unter anderem auf die zahlreichen Lieferantenbeziehungen sowie den Umstand zurückzuführen sein, dass Rechnungen in diesem Sektor häufig per E-Mail verarbeitet werden. Gleichzeitig zeigen sich hier typische strukturelle Schwächen: fehlende Multifaktor-Authentifizierung, unzureichendes Identity-Monitoring und mangelnde Transparenz über Kommunikationsprozesse – Faktoren, die solche Angriffe nicht nur begünstigen, sondern oft auch zu spät erkannt werden.

Business E-Mail Compromise pro Sektor



Die Zeitspanne zwischen Kompromittierung und Entdeckung eines Zahlungsbetrugs ist häufig länger als die Aufbewahrungsdauer der für eine forensische Untersuchung relevanten Logs.

In einzelnen Fällen konnte das InfoGuard-CSIRT den Zeitpunkt der Kompromittierung nicht mehr eindeutig rekonstruieren.

4.3 Identitäts-Diebstahl

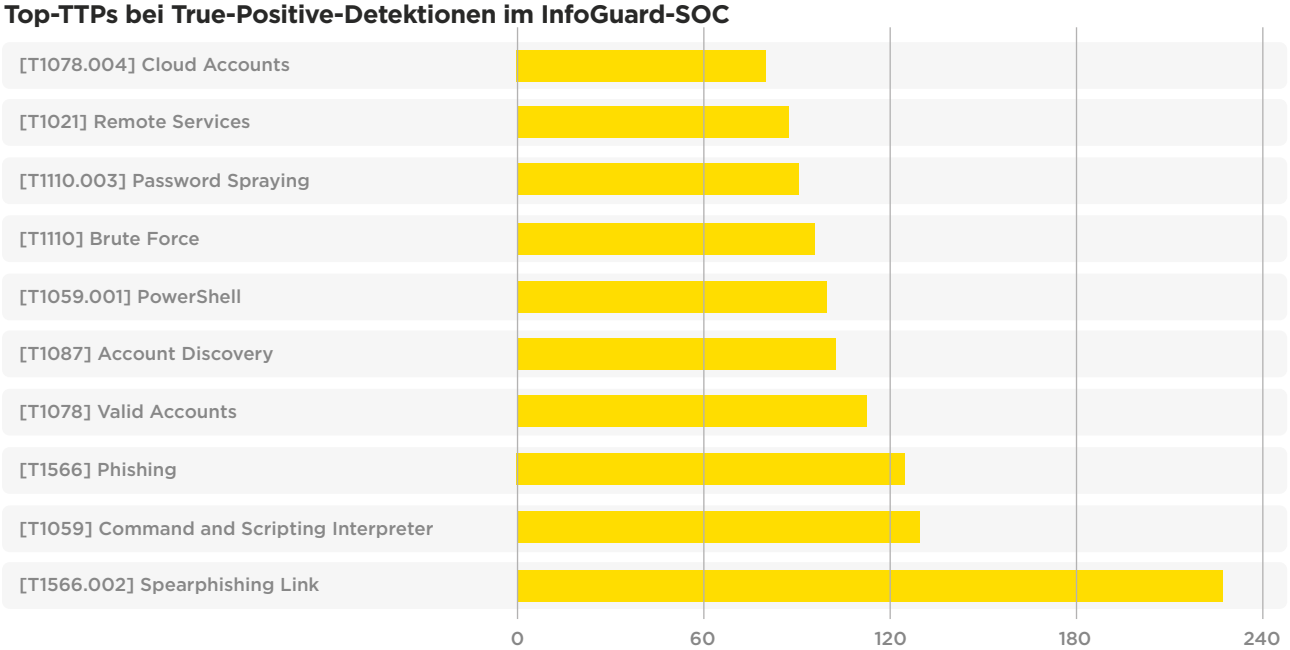
Im Berichtzeitraum verzeichneten das InfoGuard-SOC und das InfoGuard-CSIRT, dass ein Grossteil der Angriffe direkt gegen Identitäten abzielte. Entsprechend beziehen sich die meisten True-Positive-Detektionen im Security Operations Center (SOC) auf TTPs, die im Zusammenhang mit Identitäten stehen, wie etwa Spearphishing-Links, Phishing, Valid Accounts, Account Discovery, Brute Force, Password Spraying, Remote Services und Cloud Accounts. Um solche Angriffe effizient und frühzeitig zu erkennen, sollte das Monitoring um IDR (Identity Detection and Response) erweitert und Identitäten als eigenständige Schutzdomäne systematisch überwacht werden. Gleichzeitig ist es entscheidend, möglichst alle Unternehmens-Accounts über eine zentrale SSO-Lösung zu verwalten, um Transparenz, Kontrolle und Durchsetzbarkeit von Sicherheitsrichtlinien zu erhöhen. Weiter beobachtete das InfoGuard-SOC verschiedene Angriffsmöglichkeiten, über die Angreifer Identitäten übernehmen können.

Folgende Angriffsmuster traten dabei besonders häufig in Erscheinung:

- ClickFix-Infostealer, Social Engineering mittels bekannter Captcha-Dialoge
- Über Suchmaschinen beworbene Unternehmenssoftware mit eingebautem Infostealer
- Social Engineering gegen Entscheider:innen über manipulierte Online-Meeting-Executables mit Schadcode
- Social Engineering auf Entwickler:innen, die unbemerkt bösartigen Code auf Unternehmenssystemen ausführen
- LLM-optimierte Phishing-E-Mails mit hoher sprachlicher und kontextueller Glaubwürdigkeit

Das InfoGuard-CSIRT beobachtete zunehmend, dass Passwörter und Tokens auf privaten Endgeräten entwendet und anschliessend von Angreifern gegen Unternehmen verwendet wurden. Diese Entwicklung verschiebt die Angriffsfläche zunehmend in den nicht kontrollierbaren Bereich ausserhalb der Unternehmensinfrastruktur. Für Organisationen ergibt sich daraus eine klare Konsequenz: Die Gültigkeit von Zugangstoken auf unternehmensfremden Geräten sollte möglichst kurz gehalten oder vollständig unterbunden werden, solange phishingresistente MFA-Mechanismen nicht flächendeckend eingesetzt werden. Andernfalls entsteht ein persistenter Zugangspfad, der sich klassischen Schutzmechanismen weitgehend entzieht.

Top-TTPs bei True-Positive-Detektionen im InfoGuard-SOC



4.4 Staatliche Akteure

Das InfoGuard-CSIRT beobachtete 2025 mehrere erfolgreich durchgeführte Angriffe staatlicher Akteure. Wie im InfoGuard Threat Intelligence Report Q1/2026 analysiert, stehen diese Spionageaktivitäten zunehmend im Kontext geopolitischer Spannungen und zielen auf die langfristige Positionierung in kritischen Infrastrukturen und strategisch relevanten Industrien ab. Besonders im Fokus standen Behörden, die Rüstungsindustrie, Energieversorger und die Telekommunikation. Finanziell motivierte staatliche Akteure richteten ihren Fokus vor allem auf Finanzunternehmen, insbesondere auf Kryptobanken.

Staatliche Akteure verfügen bekannterweise über «unlimitierte» Ressourcen, um den Einstieg in Unternehmensnetzwerke zu erlangen, sowie über die Fähigkeit, hochgradig spezialisierte, individuell angepasste Malware zu entwickeln, die im Netzwerk des Opfers oftmals vollständig unentdeckt bleibt. Dennoch zeigt die Praxis: Auch diese Akteure nutzen für den initialen Zugang häufig bekannte Schwachstellen, jedoch schneller, gezielter und konsequenter als klassische Angriffsgruppen. Innerhalb kompromittierter Netzwerke nutzten staatliche Akteure wiederholt Malware und Angriffsvektoren, die von modernen EDR-Lösungen nicht zuverlässig erkannt wurden oder gezielt umgangen werden konnten. Dabei ist davon auszugehen, dass diese Akteure mit gängigen Monitoring-Lösungen vertraut sind, deren Funktionsweise kennen und Angriffe entsprechend darauf abstimmen.

Für betroffene Organisationen ergibt sich daraus eine klare Konsequenz: Standardisierte Sicherheitsarchitekturen allein bieten keinen ausreichenden Schutz gegen hochentwickelte Angreifer. Stattdessen ist eine Kombination verschiedener XDR-Technologien erforderlich, wie etwa Endpoint, Network, Identity und Cloud Detection and Response, ergänzt durch individuell entwickelte, organisationsspezifische Detektionsmechanismen, die staatliche Akteure bei Test mit Off-the-Shelf-Technologien nicht ohne Weiteres berücksichtigen können.

4.5 KI-unterstützte Angriffe

KI war im Berichtzeitraum noch kein magischer Gamechanger für Angreifer, aber ein klar messbarer Effizienz- und Skalierungs-Booster.
Aus der Perspektive der Cyber Defence bleibt der Einsatz von KI auf Angreiferseite nach wie vor nachzuweisen. Dennoch deuten verschiedene Entwicklungen auf eine klar verstärkte Nutzung hin: Die steigende Erfolgsquote bei Phishingangriffen sowie die beschleunigte Kompromittierung von Edge Devices lassen darauf schliessen, dass Angreifer LLMs gezielt zur Erstellung einwandfreier und kontextbezogener Phishingmails einsetzen, die im Vergleich zu den Vorjahren eine neue Qualitätsstufe erreicht haben. Bei der Exploitation von Edge Devices unterstützt KI sowohl bei der Erstellung von Exploits, FUD-Malware und Webshells als auch bei der Skalierung und Automatisierung von Angriffen durch Agentic AI.

Der Zenit dessen, was Angreifer mit KI erreichen können, ist bei weitem noch nicht erreicht. Für die Verteidigung bedeutet dies, dass neue Angriffsmethoden frühzeitig erkannt und organisatorische wie technische Abwehrmechanismen kontinuierlich angepasst werden müssen.

Besonders deutlich zeigt sich der Wandel im Bereich Social Engineering: Deepfake-Voice- und Video-Calls zwingen Organisationen dazu, klassische Vertrauensmechanismen grundlegend zu hinterfragen. Stimmen und Gesichter verlieren ihre Funktion als verlässliche Identitätsmerkmale. In virtuellen Interaktionen sollte die Authentizität des Gegenübers daher systematisch verifiziert werden. Dies kann beispielsweise durch zusätzliche, unabhängige Authentifizierungsfaktoren oder klar definierte Verifikationsprozesse erfolgen.

5. Die sieben zentralen Handlungsempfehlungen für 2026

Die Analyse der Vorfälle durch das InfoGuard-CSIRT und das InfoGuard-SOC zeigt klar, in welchen Bereichen Unternehmen ihre Cyberresilienz gezielt und prioritär stärken müssen. Der Fokus sollte dabei auf den folgenden sieben Handlungsfeldern liegen:

1. Identity First

Identitäten sind der zentrale und am häufigsten ausgenutzte Angriffsvektor moderner Cyberangriffe. Unternehmen sollten daher für sämtliche externen und sensiblen internen Dienste konsequent Multifaktor-Authentifizierung einsetzen. Phishingresistente MFA-Methoden wie Passkeys oder FIDO2, strenge Conditional Access Policies sowie ein Monitoring von Zugriffstokens helfen, Accountübernahmen frühzeitig zu erkennen und wirksam zu verhindern.

2. Patchzyklen verkürzen

Unternehmen sollten ihre Patchzyklen kurz halten und sicherheitskritische Updates am Perimeter ohne zeitliche Verzögerung implementieren. Nach jeder Patchung sollten Systeme gezielt auf bereits erfolgte Kompromittierungen überprüft werden, um trügerische Sicherheit durch vermeintlich geschlossene Schwachstellen zu vermeiden.

3. Zero Trust forcieren

Zero Trust endet nicht am Perimeter. Auch wenn MFA oder ZTNA eingesetzt werden, dürfen sich Angreifer nach einer Kompromittierung nicht frei im Netzwerk bewegen können. Konsequente Netzwerksegmentierung, überwachte Zonenübergänge und regelmässige Re-Authentifizierungen von Benutzeridentitäten sind dabei zentral für die Eindämmung lateraler Bewegungen.

4. Monitoring-Erweiterung

Lag der Fokus in den vergangenen Jahren hauptsächlich auf der Überwachung von Endpunkten (EDR) und Netzwerken (NDR), muss das Monitoring heute auch Identitäten, Cloudressourcen und exponierte APIs umfassen. Nur eine ganzheitliche Sicht auf alle relevanten Angriffsflächen verhindert blinde Flecken und verkürzt die Zeit bis zur Detektion signifikant.

5. Incident Response testen

Unternehmen sollten ihre Incident-Response-Fähigkeiten regelmässig mit Tabletop Excercises (TTX) trainieren. In praxisnahen Angriffsszenarien können Teams den Ernstfall unter vermeintlich realistischen Bedingungen durchspielen, technische und organisatorische Schwachstellen identifizieren und Massnahmen zur Stärkung der Cyberresilienz gezielt ableiten, um die Handlungsfähigkeit im Krisenfall sicherzustellen.

6. Backup-Strategie validieren

Backups müssen auch einem Ransomware-Angriff standhalten. Unternehmen sollten daher prüfen, ob Angreifer Backups löschen oder manipulieren können. Ist ein vollständiger Schutz nicht gewährleistet, sind immutable oder physisch getrennte Offline-Backups zwingend erforderlich. Gleichzeitig müssen funktionierende Disaster-Recovery-Prozesse regelmässig getestet und verifiziert werden.

7. Supply-Chain-Risiko minimieren

Software-Updates, Wartungs- und Lieferantenzugänge sollten konsequent überwacht und eingeschränkt werden. Gleichzeitig sollte der Einsatz unternehmensfremder Software technisch kontrolliert, validiert oder konsequent unterbunden werden, um indirekte Angriffswege über vertrauenswürdige Dritte zu reduzieren.

6. Fazit

Cyberangriffe folgen 2026 keiner neuen Logik – aber einer neuen Konsequenz. Nicht die Raffinesse der Angriffe hat sich grundlegend verändert, sondern ihre Geschwindigkeit, Skalierung und Präzision in der Ausnutzung bestehender Schwächen. Die Analyse zeigt klar: Angreifer nutzen keine exotischen Zero-Days als primären Einstieg, sondern systematisch Identitäten, Fehlkonfigurationen, unzureichend gesicherte Remote-Zugänge und blinde Flecken im Monitoring. Gleichzeitig verschieben sich Angriffe zunehmend in Bereiche, die sich der direkten Kontrolle von Organisationen entziehen – etwa in Lieferketten, Cloud-Dienste oder private Endgeräte.

Die eigentliche Herausforderung liegt damit nicht in der Verhinderung von Angriffen, sondern in der Fähigkeit, Kompromittierungen frühzeitig zu erkennen, richtig einzuordnen und entschlossen zu handeln.

Organisationen, die über diese Fähigkeiten verfügen, reduzieren den Schaden signifikant, unabhängig davon, ob ein Angriff erfolgreich war oder nicht. Unternehmen hingegen, denen diese Sichtbarkeit fehlt, erkennen Angriffe oft erst dann, wenn der operative Betrieb bereits beeinträchtigt ist oder Daten abgeflossen sind.

Die zentrale Leitthese lautet daher:

Cyberresilienz entsteht nicht durch mehr Cyber-Defence-Tools, sondern durch konsequente Sichtbarkeit, kontextbasierte Analyse und operative Handlungsfähigkeit im entscheidenden Moment.

6.1 Von reaktiver Sicherheit zu proaktiver Cyberresilienz

Um Angriffe frühzeitig zu erkennen und gezielt zu steuern, benötigen Organisationen einen kontinuierlichen, aktuellen Blick auf die eigene Bedrohungslage – abgestimmt auf Infrastruktur, Branche und individuelle Risiken. Genau hier setzt moderne Threat Intelligence an: Sie macht versteckte Angreifer sichtbar, identifiziert neue Angriffsmuster und übersetzt globale Erkenntnisse in konkrete Massnahmen für die eigene Umgebung.

Mit den Threat-Intelligence-Services von InfoGuard prüfen Sie gezielt, ob bereits eine Kompromittierung vorliegt, identifizieren versteckte Bedrohungen durch proaktives Threat Hunting und erhalten fundierte Einblicke in aktuelle Angriffe, Akteure und Taktiken.

Erkennen Sie Angreifer, bevor sie Schaden anrichten – und schaffen Sie die Grundlage für fundierte, proaktive Sicherheitsentscheidungen. Wir freuen uns auf einen unverbindlichen Austausch mit Ihnen.

Mehr über Threat Intelligence erfahren.

Die fünf zentralen Takeaways

1. Identity ist der neue Perimeter
Angriffe beginnen heute nicht mehr am Netzwerk, sondern bei Identitäten. Priorisieren Sie den Schutz von Accounts, Tokens und Zugriffen – mit phishingresistenter MFA, SSO und aktivem Identity Monitoring. Einzelne kompromittierte Zugangsdaten reichen aus, um weitreichende Schäden zu verursachen.

2. Geschwindigkeit schlägt Prävention
Angreifer sind schneller als klassische Sicherheitsprozesse. Verkürzen Sie Patchzyklen konsequent und prüfen Sie Systeme aktiv auf bereits erfolgte Kompromittierungen – auch nach dem Patchen. Reaktive Sicherheit erzeugt trügerische Sicherheit.

3. Sichtbarkeit entscheidet über den Schaden
Angriffe scheitern selten infolge fehlender Schutzmechanismen, sondern daran, dass sie zu spät erkannt werden. Erweitern Sie Ihr Monitoring auf Identitäten, Cloud und Logs und sorgen Sie für ausreichende Datenhaltung zur Analyse. Wer früh sieht, kann handeln.

4. Incident Readiness ist ein Business-Thema
Im Ernstfall zählt nicht, ob Pläne existieren, sondern ob sie im Ernstfall erreichbar sind und funktionieren. Testen Sie Incident Response, Backup und Recovery regelmässig unter realistischen Bedingungen. Ungetestete Konzepte versagen unter Stress.

5. Cyberrisiken entstehen zunehmend ausserhalb der eigenen Kontrolle
Supply Chains, Cloud-Dienste und private Endgeräte erweitern die Angriffsfläche massiv. Reduzieren Sie Abhängigkeiten, kontrollieren Sie Zugänge und überwachen Sie externe Verbindungen konsequent. Vertrauen ist kein Sicherheitskonzept.

Cyberattacken zählen zu den grössten operationellen Unternehmensrisiken.

Sorgen Sie vor und schützen Sie Ihr Unternehmen rund um die Uhr vor Cyberangriffen – schnell, professionell und zuverlässig. Kontaktieren Sie uns jetzt für ein unverbindliches Gespräch.

Alles über wirkungsvolle Cyber Defence erfahren.

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Ihre Cybersicherheit
Unsere Leidenschaft & Expertise

Cyber Defence & Incident Response sind entscheidend, aber nur zwei Aspekte einer umfassenden und erfolgreichen Cybersicherheit. Unser 360°-Cyber-Security-Ansatz umfasst zudem Cloud Security, Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen, Penetration Testing & Red Teaming sowie Security Consulting Services. Die SOC-Services werden aus dem ISO 27001-zertifizierten und ISAE 3000 Typ2 überprüften Cyber Defence Center (CDC) in der Schweiz sowie aus Deutschland erbracht – mit 24/7 Betrieb und durchgehend personeller Besetzung.

2001
Erfahrung und Expertise seit über 25 Jahren

100%
eigenständig

350+
Sicherheits-expert*innen

6
Standorte in Baar, Bern, Frankfurt, München, Düsseldorf und Wien

24/7
Echtzeit-überwachung und Notfall-Intervention

2x SOC in CH & DE
24/7 Security Operations Center in der Schweiz und Deutschland

CSIRT Computer Security Incident Response Team
BSI-qualifizierter APT-Response-Dienstleister und FIRST-Mitglied

ISO 27001
ISO 14001
ISAE 3000 Typ 2

Haben Sie einen Sicherheitsvorfall?
Wir unterstützen Sie jederzeit schnell, kompetent und erfahren.

+41 41 749 24 24

DE +49 896 142 9677
AT +43 1 442 0177
investigations@infoguard.ch

Baar (Hauptsitz)
InfoGuard AG, Lindenstrasse 10, 6340 Baar, Schweiz, +41 41 749 19 00, info@infoguard.ch, infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Schweiz
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

Frankfurt
InfoGuard Deutschland GmbH
Frankfurter Straße 233
63263 Neu-Isenburg
Deutschland
+49 6102 7840 0
info@infoguard.de
infoguard.de

München
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 München
Deutschland
+49 896 142 9660
info@infoguard.de
infoguard.de

Düsseldorf
InfoGuard Deutschland GmbH
Am Gierath 20A
40885 Ratingen
Deutschland
+49 2102 5789 800
info@infoguard.de
infoguard.de

Wien
InfoGuard GmbH
Kohlmarkt 8-10
1010 Wien
Österreich
+43 1 442 0170
info@infoguard.at
infoguard.at