Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Whitepaper – Threat Intelligence Report Q1/26

Die geopolitische Cyberlage Europas nach «Epic Fury»

Geopolitik trifft Cyber - Wie der Krieg im Iran, Chinas Ambitionen und Russlands hybride Kriegsführung Europa bedrohen.

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Stand: März 2026

Executive Summary

Die geopolitische Lage in Europa hat sich seit dem 28. Februar 2026 fundamental verändert. Mit der militärischen Operation «Epic Fury» (USA/Israel) gegen den Iran ist aus einer latenten Bedrohung ein aktiver Cyberkonflikt geworden – mit direkten Auswirkungen auf europäische Organisationen. Gleichzeitig positionieren sich chinesische APT-Gruppen unbemerkt in kritischen Infrastrukturnetzen. Als ein führender Incident-Response-Spezialist im DACH-Raum sehen wir in der Praxis: Staatliche Cyberangriffe bleiben meist unter dem Radar der Sicherheitssysteme und werden oft erst durch externe Hinweise oder Zufallsfunde sichtbar. Proaktives Threat Hunting durch erfahrene Incident Responder ist derzeit die wirksamste Methode, laufende APT-Kompromittierungen aufzudecken.

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Inhaltsverzeichnis

Die drei Erfolgsfaktoren:

1. Proaktives Threat Hunting
Suchen Sie gezielt nach bereits vorhandenen Kompromittierungen – statt auf Alarme zu warten.

2. Incident-Response-Erfahrung
Lassen Sie APT-Taktiken, Techniken und Angriffsmuster durch ein erfahrenes Incident-Response-Team analysieren.

3. Forensische Tiefenanalyse der Infrastruktur
Identifizieren Sie versteckte Angreiferzugänge in Edge-Systemen, nativen Tools (LOLBins) oder Supply Chains durch gezielte forensische Analysen.

1. Die Cyber-Bedrohungslage in Europa: angespannt wie nie

Die europäische Cyber-Bedrohungslage ist auf einem historischen Höchststand. Laut ENISA Threat Landscape 2025 (Berichtszeitraum Juli 2024 bis Juni 2025) entfielen 76,7 % aller Vorfälle auf DDoS-Angriffe, getrieben durch staatlich gelenkten Hacktivismus. Der öffentliche Sektor war mit 38,2 % am stärksten betroffen, doppelt so hoch wie im Vorjahr. Phishing bleibt mit 60 % der häufigste Initialvektor, wobei über 80 % der Kampagnen nachweislich KI-generierte Inhalte nutzen.

Der CrowdStrike European Threat Landscape Report 2025 zeigt: Ransomware trifft die Region auf Rekordniveau, während staatlich gesteuerte Angriffe (nation-state) um 150 % gestiegen sind. ENISA identifiziert 46 staatlich gesteuerte Intrusion-Sets, die aktiv gegen EU-Mitgliedstaaten operieren. Die Grenzen zwischen Cyberkriminalität, Hacktivismus und Staatsakteuren verschwimmen zusehends. Was früher klar trennbar war, ist heute ein komplexes Ökosystem aus Auftragsarbeit, ideologischer Motivation und staatlicher Instrumentalisierung.

2. Iran: Vom Cyber-Dschihad zur offenen digitalen Front – Lage März 2026

2.1 Der Eskalationspfad: Juni 2025 bis heute

Zum Verständnis der aktuellen Situation ist ein Blick auf den Eskalationspfad notwendig. Der zwölftägige Israel-Iran-Konflikt im Juni 2025 war die erste grosse Probe für Irans koordiniertes Cyber-Ökosystem im Kriegsfall. Das Center for Strategic and International Studies (CSIS) analysierte über 250.000 Telegram-Nachrichten aus mehr als 178 Hacktivist- und Proxygruppen und dokumentierte eine rasche Mobilisierung synchron zu den kinetischen Luftangriffen. Gruppen wie Fatimion Cyber Team, Cyber Fattah und Cyber Islamic Resistance koordinierten Aufklärung, DDoS-Angriffe, Website-Defacement und Datendiebstahl in direkter Abstimmung mit dem militärischen Geschehen – ein Muster, das auf institutionelle Führung hindeutet, nicht auf organischen Hacktivismus.

Parallel dazu setzte die iranische Regierung staatlich gesponserte Ransomware-Kampagnen ein und zahlte Prämien für Infektionen gegen US- und israelische Organisationen. MuddyWater (MOIS) initiierte mit Operation Olalampo eine strukturierte Cyber-Offensive gegen die META-Region (Naher Osten, Türkei, Afrika) mit Überlappungen zu einer parallel laufenden Kampagne namens Red-Kitten – ein Hinweis auf koordinierte Infrastruktur iranisch ausgerichteter Akteure.

2.2 28. Februar 2026: Operation «Epic Fury» und die digitale Reaktion

Am 28. Februar 2026 starteten die USA und Israel die koordinierte Militäroperation «Epic Fury» / «Operation Roaring Lion» mit Strikes auf iranische Führungsstrukturen, IRGC-Einrichtungen und nukleare Infrastrukturen. Innerhalb von Stunden begann Iran eine mehrstufige Vergeltungskampagne – sowohl kinetisch als auch im Cyberraum.

Ein technisch bemerkenswerter Faktor: Die israelische Gegenmassnahme war auch eine der grössten Cyberoperationen der Geschichte gegen Iran selbst und reduzierte die iranische Internetkonnektivität auf 1–4 % (Unit 42 / Palo Alto Networks, März 2026). Das bedeutet: Irans hochspezialisierte APT-Gruppen sind kurzfristig im Inland operativ eingeschränkt. Daraus ergeben sich zwei parallele Bedrohungsszenarien:

- Ausserhalb Irans operierende Zellen und Proxy-Gruppen handeln jetzt mit taktischer Autonomie – ohne direkte Befehlsstruktur aus Teheran. Das macht ihre Aktionen schwerer vorhersagbar.
- Mittelfristig – wenn die Konnektivität wiederhergestellt ist – ist mit einer intensivierten Welle staatlicher APT-Operationen zu rechnen, da die IRGC-Einheiten Zeit hatten, Prioritäten zu setzen und Zugänge zu aktivieren, die schon länger «dormant» vorhanden waren.

2.3
Der «Electronic Operations Room» – koordinierter Cyber-Dschihad

Noch am 28. Februar 2026 wurde der «Electronic Operations Room» gegründet – ein Koordinationsgremium, das pro-iranische Hacktivist-Kollektive in einem strukturierten Cyber-Jihad bündelt. Das Umbrella-Netzwerk «Cyber Islamic Resistance» (auch: Islamic Cyber Resistance Axis) koordiniert Gruppen wie RipperSec, Cyb3rDrag0nzz und zahlreiche weitere für synchronisierte DDoS-Wellen, Datenlöschoperationen und Defacements. Bis Anfang März 2026 wurden über 150 dokumentierte Hacktivismus-Vorfälle gezählt, wobei ca. 60 einzelne Gruppen aktiv sind – darunter auch pro-russische Kollektive (CloudSEK Situation Report, März 2026).

Europol warnte am 6. März 2026 explizit vor einer erhöhten Bedrohung für die EU: «Key risks are an elevated threat of terrorism and violent extremism, increased cyber-attacks targeting EU infrastructure, a rise in conflict-themed online fraud schemes, and the spread of disinformation and influence campaigns.» Frankreich, Deutschland und andere EU-Staaten haben ihre Sicherheitsmassnahmen erhöht, da iranische Netzwerke auch in Europa operativ sind.

2.4
Welche Cyberrisiken entstehen daraus für europäische Organisationen?

Das UK National Cyber Security Centre (NCSC) hat Anfang März 2026 eine explizite Warnung herausgegeben: Auch wenn derzeit kein signifikanter Anstieg direkter Cyberangriffe auf britische Netzwerke zu beobachten ist, warnen die Behörden: Die Lage kann sich jederzeit und mit nur geringer Vorwarnung ändern. Historisch gesehen hat Irans Cyberaktivität Europa immer wieder getroffen – Deutschland, Frankreich, Niederlande, und das vereinigte Königreich – oft als Kollateralschaden oder gezielter Sekundärangriff auf Organisationen mit Nahostbezug.

Das primäre Cyber-risikoprofil für europäische Organisationen im aktuellen Kontext:

- Kritische Infrastruktur (Energie, Wasser, OT/ICS): Iran hat nachweislich ICS/SCADA-Systeme als Ziele priorisiert. Die Schwachstelle CVE-2025-1960 in Schneider Electric EcoStruxure WebHMI ist bereits in iranisch-affiliierten Kampagnen ausgenutzt worden.
- Rüstung, Luft- und Raumfahrt, Telekommunikation: UNC1549 (Tortoise Shell) war im zweiten Halbjahr 2025 der viertaktivste iranische Akteur mit Fokus auf genau diese Sektoren.
- Regierungsstellen und diplomatische Einrichtungen: MuddyWater verbrachte 8 Monate unentdeckt in einem nahöstlichen Regierungsnetzwerk – ähnliche Muster sind bei europäischen Stellen zu erwarten.
- Supply-Chain-Risiko: Organisationen, die israelische OT-Komponenten einsetzen (z. B. bestimmte Unitronics-Systeme), gelten als indirekte Ziele nach dem Angriffsmuster der CyberAv3ngers-Kampagnen von 2023–2024.
- Organisationen mit Iran-nahen Mitarbeitern oder Diaspora: Iranische Akteure führen aktiv Verfolgungsoperationen gegen Regime-Gegner in Europa durch, inklusive physischer Bedrohungen nach Cyber-Kompromittierung.

2.5 Typische Angriffstechniken iranischer Cyberoperationen

Irans Cyberarsenal ist heterogen: Es reicht von hochkomplexen APT-Kampagnen bis zu kriminell genutzten Ransomware-Frameworks. Das Besondere ist die strukturelle Vermischung: Staatlich gesteuerter Zugang wird für kriminelle Zwecke monetarisiert, während gleichzeitig plausible Abstreitbarkeit staatlicher Beteiligung gewahrt bleibt. Sicarii – eine seit Dezember 2025 aktive RaaS-Operation – hat einen kritischen Defekt: Die Malware löscht ihre eigenen Entschlüsselungsschlüssel nach der Verschlüsselung, was eine Wiederherstellung dauerhaft unmöglich macht, unabhängig von einer Lösegeldzahlung (Halcyon, März 2026).

Technisch operieren iranische Gruppen bevorzugt über: Ausnutzung von VPN-Gateways und Firewalls (Pulse Secure, Fortinet, Palo Alto, F5, Citrix), ASPX-Webshells auf exponierten Servern, Living-off-the-Land-Techniken (LOLBins) für Persistenz und laterale Bewegung sowie KI-gestützte Spear-Phishing-Kampagnen mit hohem Personalisierungsgrad.

3. China: Stille Präsenz in staatlichen Netzwerken – eine unterschätzte Bedrohung

Während der Iran mit lautem Hacktivismus und politisch aufgeladenen Operationen auffällt, agiert China nach dem gegenteiligen Prinzip: maximale Stille, minimale Spuren, langfristige Positionierung. Dieser Paradigmenwechsel ist in den letzten zwei Jahren immer deutlicher geworden: China verschiebt seinen Fokus von klassischer Industrie- und IP-Spionage hin zu staatlichen Organisationen und kritischer Infrastruktur.

Volt Typhoon – die bekannteste chinesische APT-Gruppe für Infrastruktur-Targeting – wurde in einigen US-Netzwerken über fünf Jahre unentdeckt betrieben. CISA-Direktorin Jen Easterly formulierte es klar: Was bisher gefunden wurde, ist «wahrscheinlich nur die Spitze des Eisbergs.» Volt Typhoon nutzt ausschliesslich Living-off-the-Land-Techniken – keine Malware, nur native Systemtools. Das macht traditionelle signaturbasierte Erkennung weitgehend wirkungslos.

In Europa sind chinesische Cyberoperationen längst angekommen: Die niederländischen Dienste MIVD und AIVD bestätigten 2024 den ersten öffentlich attribuierten chinesischen Angriff auf das Verteidigungsministerium («Coathanger»-Malware für Fortinet FortiGate). Tschechien machte APT31 im Mai 2025 für die Kompromittierung des Aussenministeriums während der EU-Ratspräsidentschaft 2022 verantwortlich. Die EU-Aussenbeauftragte Kaja Kallas erklärte, die EU sei «bereit, Peking Kosten aufzuerlegen».

Salt Typhoon – eine weitere chinesische Gruppe – infiltrierte die Telekommunikationsinfrastruktur von über acht US-Anbietern, darunter CALEA-Abhörsysteme, und blieb in einigen Umgebungen bis zu drei Jahre unentdeckt. Das FBI informierte über 600 Organisationen in mehr als 80 Ländern über mögliche Kompromittierungen. ENISA warnt 2025 explizit vor sechs chinesischen APT-Gruppen (APT27, APT30, APT31, Ke3chang, GALLIUM, Mustang Panda) als «bedeutende und andauernde Bedrohungen für die EU». CrowdStrike identifiziert Vixen Panda als «die produktivste Bedrohung für europäische Regierungs- und Verteidigungseinrichtungen» (November 2025).

Der geopolitische Rahmen: Chinas zunehmende Abkopplung vom Westen und sein Anspruch auf Taiwan machen diese Positionierung strategisch: «Pre-Positioning» bedeutet, Zugänge zu kritischer Infrastruktur anzulegen, die im Ernstfall eines Taiwan-Konflikts aktiviert werden könnten – zur Ablenkung, Demoralisierung oder direkten Sabotage westlicher Unterstützungsstrukturen. Ein chinesischer Beamter deutete bei einem geheimen Treffen in Genf im Dezember 2024 an, dass die Infrastruktur-Hacks direkt mit der US-Militärunterstützung für Taiwan zusammenhingen.

4. Russland: Hybride Kriegsführung als Dauerzustand

Russland bleibt laut ENISA 2025 die aktivste staatlich gelenkte Bedrohung für die EU. APT28 (Fancy Bear, GRU) hat 2024 die SPD-Zentrale, tschechische Regierungsstellen und die Deutsche Flugsicherung (DFS) angegriffen, wobei letzteres allein Kosten von ca. 9 Mio. Euro verursachte. Frankreich machte im April 2025 die Gruppe APT28 für Cyberangriffe auf ein Dutzend Einrichtungen seit 2021 verantwortlich. Zu den betroffenen Zielen zählten unter anderen auch Strukturen der Olympischen Spiele 2024.

Sandworm (APT44) operiert mit seiner «BadPilot»-Kampagne seit 2022 global und war bis Dezember 2025 für destruktive Wiper-Angriffe auf Wind- und Solarparks sowie Kraftwerke in Polen verantwortlich – der erste bestätigte destruktive Angriff auf eine EU-Energieinfrastruktur. APT29 (Cozy Bear) nutzt weiterhin raffinierte Social-Engineering-Angriffe gegen EU-Diplomaten, zuletzt mit gefälschten Weinverkostungseinladungen und der neuen WINELOADER-Backdoor. Prorussischer Hacktivismus durch NoName057(16) – im Juli 2025 durch Europol/Eurojust in «Operation Eastwood» teilweise zerschlagen – hat in Deutschland allein 14 mehrtägige DDoS-Wellen gegen ca. 230 Organisationen verursacht.

5. Die unbequeme Wahrheit: Wie staatlich gesteuerte Cyberangriffe tatsächlich entdeckt werden

Im Alltag eines Incident Responders bestätigt sich immer wieder, was die Daten zeigen: Staatliche APT-Angriffe werden selten durch eigene Sicherheitssysteme erkannt. Mandiant M-Trends 2025 (basierend auf 450.000+ Untersuchungsstunden) zeigt: 57 % aller Kompromittierungen wurden durch externe Quellen entdeckt – nicht durch das eigene SOC oder die eigene Sicherheitsinfrastruktur. Nur 43 % der Fälle wurden intern detektiert.

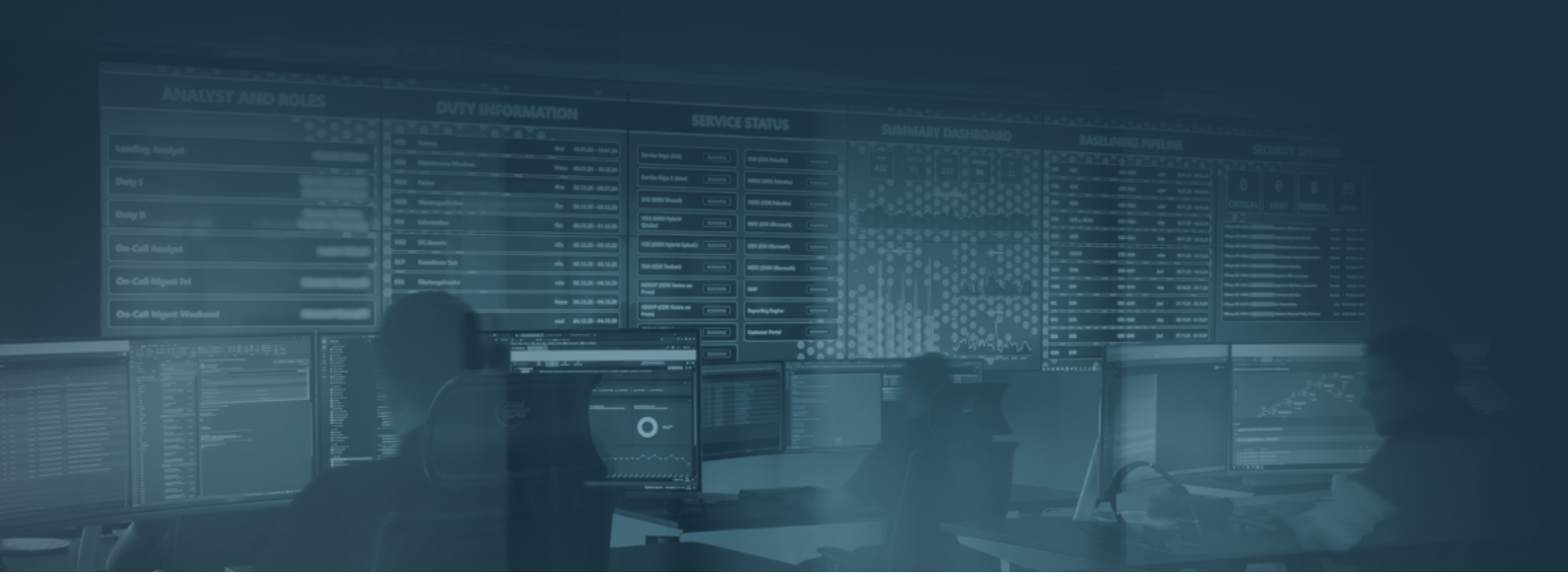
Die mediane Verweildauer (Dwell Time) eines Angreifers im Netzwerk lag 2024 global bei 11 Tagen – in der EMEA-Region sogar bei 22 Tagen. Das bedeutet: Ein Angreifer bewegt sich im Schnitt fast drei Wochen unbemerkt durch Netzwerke, bevor eine Kompromittierung entdeckt wird. Bei Intrusionen, die erst durch externe Hinweise auffliegen, steigt die Dwell Time auf 26 Tage.

5.1 Warum viele Cyberangriffe nicht entdeckt werden? Dafür gibt es drei strukturelle Ursachen:

- LOTL-Techniken: 62 % aller Bedrohungserkennungen 2024 nutzten keine Malware (CrowdStrike). Angreifer verwenden native Systemtools – PowerShell, WMI, WMIC – die signaturbasierte Systeme schlicht nicht als bösartig flaggen.
- Blinde Flecken an Perimetern: 44 % der im Jahr 2024 ausgenutzten Zero-Days zielten auf Edge-Geräte wie VPNs und Firewalls – Systeme, auf welchen typischerweise kein EDR installiert ist (Mandiant M-Trends 2025).
- Supply-Chain-Kompromittierungen: Drittanbieter-bezogene Breaches haben sich 2025 laut Verizon DBIR auf 30 % aller Fälle verdoppelt. Die Kontrollen beim Endopfer werden vollständig umgangen.

Das Präzedenzbeispiel schlechthin ist Volt Typhoon: Über fünf Jahre operierte die Gruppe unentdeckt in US-Infrastrukturen. Entdeckt wurde sie nicht durch ein SIEM, nicht durch ein EDR – sondern durch dedizierte Threat-Hunting-Teams der CISA, die aktiv nach Kompromittierungsindikatoren gesucht haben. Der SolarWinds-Angriff (Verweildauer 8–9 Monate, 18.000 kompromittierte Organisationen) flog auf, weil FireEye beim Untersuchen eines anderen Sicherheitsvorfalls zufällig auf die Supply-Chain-Kompromittierung stiess.

Auch in realen Incident-Response-Einsätzen zeigt sich dasselbe Muster: Nation-State-Vorfälle werden fast nie durch Alarme der eigenen Sicherheitssysteme aufgedeckt. Sie werden meist im Zuge eines anderen Cybervorfalls entdeckt. Etwa wenn ein Incident-Response-Team im Zusammenhang mit einem Ransomware-Angriff gerufen wird und sich in der Analyse dann ein zweiter, deutlich älteren Zugangspfad zeigt. Nicht selten erfolgt die Entdeckung auch durch Hinweise von aussen: Ein CERT, eine Behörde oder ein ausländischer Partner meldet, dass die eigene Infrastruktur als Command-and-Control-Relay missbraucht wird. Das sind keine Ausnahmen, das ist der Normalfall.



6. Threat Hunting durch Incident Responder: Der proaktive Ausweg

Wenn reaktive Detektion systematisch versagt, braucht es einen anderen Ansatz: proaktives Threat Hunting. Threat Hunting ist die hypothesengetriebene, aktive Suche nach bösartiger Aktivität, die bestehende Sicherheitskontrollen umgangen hat – ohne auf einen Alarm zu warten. Der Unterschied liegt im grundlegenden Ansatz:

Statt «Wir reagieren, wenn etwas auffällt» gilt «Wir gehen davon aus, dass wir bereits kompromittiert sein könnten und suchen systematisch danach.»

Warum sind gerade Incident Responder die besten Threat Hunter? Weil sie wissen, wie Angreifer denken und agieren. IR-Teams kennen die Taktiken und Techniken realer Angreifer aus zahlreichen Einsätzen und verfügen über forensische Untersuchungskompetenz bei der Analyse subtiler Anomalien. Gleichzeitig verstehen sie Persistenzmechanismen, die herkömmliche Sicherheitsteams oft übersehen. Aus demselben Grund gelang es dem Threat-Hunting-Team der CISA – einem Kreis erfahrener Incident Responder – die Gruppe Volt Typhoon zu entdecken, während automatisierte Sicherheitssysteme versagten. Threat Hunting durch erfahrene Incident Responder erhöht in der aktuellen Lage die Chance, laufende APT-Angriffe zu entdecken – ob iranisch, chinesisch oder russisch.

Die zentrale Frage jeder Lagebeurteilung: «Sind wir kompromittiert?»

Incident Response beantwortet die Frage «Sind wir kompromittiert?» – forensisch, systematisch und mit Kenntnis der Taktiken, Techniken und Verfahren staatlicher Angreifer-TTPs.

IR-Teams suchen gezielt nach:

- LOTL-Artefakten und anomalem Verhalten nativer Systemtools, das durch signaturbasierte Systeme nicht detektiert wird.
- Dormante Backdoors und C2-Channels in Perimeter-Geräten, Edge-Systemen und OT/ICS-Umgebungen.
- Persistenzmechanismen nach iranischem, chinesischem und russischem TTP-Muster (MITRE ATT&CK-basiert).
- Supply-Chain-Kompromittierungen und vertrauensmissbräuchlichen Zugangspfaden über Drittanbieter.
- Daten-Staging und Exfiltrations-Vorbereitung, oft wochenlang vor dem eigentlichen Angriff.

Fazit

7. Proaktive Aufklärung statt reaktiver Sicherheit

Die geopolitische Lage hat sich in wenigen Wochen deutlich verschärft. Iranische Cybermobilisierung, chinesisches Pre-Positioning in kritischen Infrastrukturen und russische hybride Kriegsführung erhöhen den Cyberdruck auf Europa spürbar.

Organisationen sollten deshalb nicht darauf warten, bis Angriffe sichtbar werden oder externe Stellen auf eine Kompromittierung hinweisen. Die Erfahrung aus zahlreichen Incident-Response-Einsätzen zeigt: Staatlich gesteuerte Angriffe bleiben häufig lange unentdeckt und operieren gezielt im toten Winkel klassischer Sicherheitskontrollen.

In der aktuellen Bedrohungslage gewinnt ein Ansatz an Bedeutung, der über reaktive Sicherheitsmechanismen hinausgeht: die gezielte, hypothesengetriebene Suche nach bereits vorhandenen Kompromittierungen. Proaktives Threat Hunting schafft Transparenz darüber, ob und wo sich Angreifer bereits in einer Infrastruktur bewegen.

Gerade in Phasen geopolitischer Spannungen kann dieser Perspektivwechsel entscheidend sein. Nicht zusätzliche Sicherheitstools schaffen Klarheit, sondern die systematische Analyse durch erfahrene Incident Responder, die nach genau den Spuren suchen, die Angreifer bewusst verborgen halten.

Wenn Sie Ihre Sicherheitslage im aktuellen geopolitischen Umfeld fundiert bewerten wollen, freuen wir uns auf den unverbindlichen fachlichen Austausch mit Ihnen.

Mehr über Threat Intelligence erfahren.

8. Die Realität aus der Praxis: 350 Cybervorfälle in einem Jahr

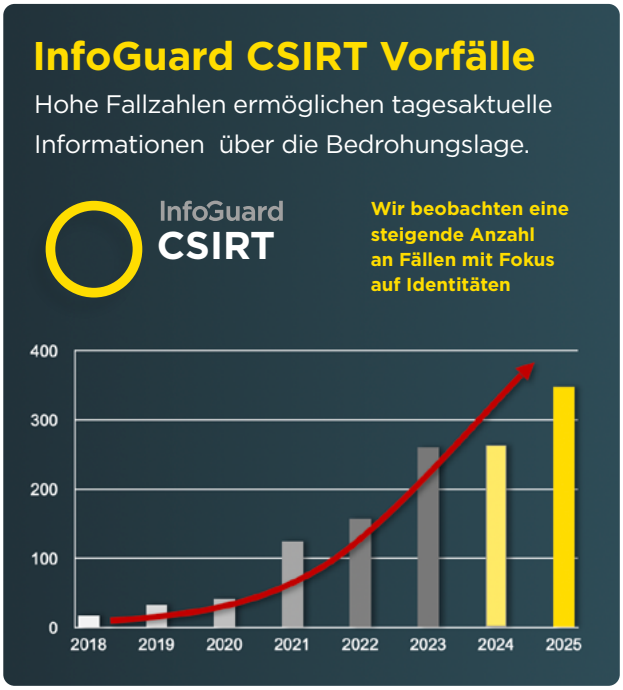
Die aktuelle Bedrohungslage spitzt sich in der Tat weiter zu, was sich in der operativen Realität der Incident Response besonders deutlich zeigt.

Im Jahr 2025 bewältigte das InfoGuard CSIRT über 350 Cybervorfälle, was einem substanziellen Anstieg von rund 20 Prozent gegenüber dem Vorjahr entspricht. Diese Eskalation wurde bereits im ersten Halbjahr greifbar, als komplexe Angriffe bereits um beachtliche 115 Prozent gegenüber der Vorperiode zunahmen.

Diese Entwicklung ist kein statistischer Ausreisser, sondern Ausdruck eines strukturellen Wandels, der sich in unseren Fallzahlen widerspiegelt und ein tagesaktuelle Lagebild zeigt.

Besonders deutlich zeigt sich eine Verschiebung hin zu Identitäten als primärem Angriffsziel. Bereits einzelne kompromittierte Zugänge genügen, um weitreichende Kontrolle über die Netzwerkinfrastrukturen von Organisationen, unabhängig von ihrer Grösse, zu erlangen. Gleichzeitig entstehen Sicherheitsvorfälle selten durch fehlende Schutzmechanismen, sondern durch mangelnde Sichtbarkeit und verspätete Reaktion.

Die Konsequenz ist grundlegend: Cyberangriffe entwickeln sich von einzelnen Vorfällen zu einem skalierbaren, industriellen Geschäftsmodell. Oder anders gesagt: Nicht die Angriffe nehmen zu, sondern ihre Effizienz.



Source InfoGuard Intelligence

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.

Kontaktieren Sie uns jetzt.

Quellen & Referenzen

- Palo Alto Networks Unit 42: Threat Brief – March 2026 Escalation of Cyber Risk Related to Iran (März 2026)
- Europol: Elevated terrorism threat in EU amid Iran conflict (6. März 2026)
- CloudSEK: Situation Report Middle East Escalation 27 Feb – 1 March 2026
- CSIS: Beyond Hacktivism – Iran's Coordinated Cyber Threat Landscape (2025/2026)
- Canadian Centre for Cyber Security: Iranian Cyber Threat Response Bulletin (Februar 2026)
- Halcyon: Iranian Use of Cybercriminal Tactics in Destructive Cyber Attacks 2026 Updates
- Arctic Wolf: Heightened Cyber Risk Following February 2026 US/Israel-Iran Escalation
- Nozomi Networks: Iranian APT Activity During Geopolitical Escalation (März 2026)
- The Register: Iran's cyberwar has begun (März 2026)
- ENISA Threat Landscape 2025 (Oktober 2025)
- Mandiant M-Trends 2025 (Google Cloud)
- CrowdStrike 2025 European Threat Landscape Report
- CISA Advisory AA24-038A: PRC State-Sponsored Actors / Volt Typhoon (2024)
- BSI Lagebericht zur IT-Sicherheit in Deutschland 2024

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 Beset-

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
247 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
Graben 19
1010 Wien
Österreich
+43 1 442 0170
info@infoguard.at
infoguard.at