

CYBERSECURITY

Trends – Technologien – Abwehrstrategien

2026

CHF 20.–



Der CISO als Multitalent in der Cyberabwehr

Die Universalgelehrten der IT



**Das Aufgabenfeld
und das Verant-
wortungsgebiet von
CISOs sind derzeit
im Umbruch.**

Coen Kaat,
stv. Chefredaktor

Was zeichnet gute CISOs aus? Ist es wichtiger, dass sie die aktuelle Versionsnummer der Firmware auf jeder Firewall im Unternehmen kennen? Oder sollten sie lieber das Business so innig verstehen, dass sie nur noch von Wertschöpfungsketten träumen? Natürlich ist die Antwort nicht so einfach, wie man es vielleicht gerne hätte. Die Welt – im Gegensatz zur klassischen IT – ist nicht binär. Und moderne CISOs sollten nicht entweder Techies oder Businessexperten sein, sondern beides – und auch noch viel mehr. Sie müssen zudem Sales-Spezialisten, Marketingprofis, Politik-Versteher, Kommunikationstalente, Risiko-Management-Beherrscher und HR-Genies sein. Oder kurz gesagt: Die guten CISOs von heute müssen die Universalgelehrten der IT-Welt sein. Denn das Aufgabenfeld und das Verantwortungsgebiet von CISOs sind derzeit im Umbruch, wie aus dem Interview mit Andy Schneider ab Seite 14 hervorgeht. Schneider ist derzeit

Field CSO EMEA Central bei Palo Alto Networks und war zuvor selbst jahrelang in verschiedenen Unternehmen als CISO tätig.

Die künstliche Intelligenz und die digitale Souveränität bringen gewiss Bewegung in die Rolle des CISOs. Einer der Haupttreiber ist aber die zunehmende Regulierung. Mit ihr steigen auch die Verantwortung und der Druck auf CISOs. Um dem standhalten zu können, braucht das ohnehin schon lange Rezept dafür, was gute CISOs ausmacht, vielleicht noch eine weitere Zutat: eine Prise Optimismus. Denn für die CISOs werde sich dieser Wandel lohnen, erklärt Schneider im Interview.

Das hier vorliegende Special zum Thema Cybersecurity deckt noch viel mehr ab als die sich verändernde Rolle von CISOs. So lesen Sie etwa ab Seite 8, wo die Schweiz punkto digitaler Souveränität steht. Weshalb das Posten von Kinderfotos im Netz seit dem Aufkommen von KI ein noch grösseres Problem geworden ist, erfahren Sie ab Seite 42. Und wie Unternehmen teure Fehler rund um Security Operations Center vermeiden, lesen Sie ab Seite 54.

Übrigens: Die aktuelle Ausgabe des Cybersecurity-Specials ist eine ganz besondere: 2026 feiert SwissCybersecurity.net nämlich das 5-jährige Bestehen. Am 15. Februar 2021 lancierte die Redaktion das News- und Infoportal für Cybersecurity und Cybercrime. Mehr zum Jubiläum lesen Sie im Dossier ab Seite 18. Die Jubiläumsbeiträge im Dossier blicken auf die Entwicklungen der vergangenen Jahre zurück und geben auch einen Ausblick darauf, was noch kommen könnte.

Ich wünsche viel Vergnügen bei der Lektüre – und: Bleiben Sie wachsam!



Coverbild: FRisaFitri - stock.adobe.com; Gemini

INTRO

Editorial	01
Inhaltsverzeichnis	02–03
Impressum	03

MARKET

Studie	04
Schweizer KMUs verlieren Vertrauen in ihre Cybersicherheit	
Messe	05
Die IT-SA 2025 hat die Messlatte höher gelegt	
Dossier kompakt	06–07
Cyber-Schuld und digitale Souveränität	
Swiss Cyber Security Days	08–09
Die digitale Souveränität der Nischen	

PEOPLE

News	10–13
Company Profile	12
Axel Egger Advisory	
Live	14–16
Andy Schneider, Palo Alto Networks	

5 JAHRE CYBERSECURITY.NET

Auftakt	18
Jubiläum	19
5 Jahre SwissCybersecurity.net	
Wenn Angriffe denken lernen	20–21
Cyberabwehr unter KI-getriebenem Angriffstempo	
Cyberangriffe 2026	22–23
Automatisiert, identitätsbasiert und KI-beschleunigt	
Von Creeper zu Morris zu Zeus	24–26
Eine kleine Geschichte der Malware	
Verschlüsselung	27–29
Die Kunst, so zu schreiben, dass fast niemand es versteht	
Testimonials	30–33
Wir feiern fünf Jahre SwissCybersecurity.net	

THREATS

Das Who's who der Malware	34–35
Company Profile	36
Consulteer Incyber	
Datenschutz	37
KI-Brille von Meta leitet intime Videos nach Kenia	
Cyberisiken im Finanzsektor	38
Handlungsbedarf bleibt bestehen	
Peripheriegeräte	39
Schwachstelle für kritische Systeme	
Dossier kompakt	40–41
KI-Agenten	
Deepfakes	42–43
So verschärft KI das Problem von Kinderfotos im Netz	

DEFENSE

Das kleine IT-Security-Glossar	44–45
Studie	47
So beflügelt KI das MSP-Geschäft 2026	
Studie	48
Warum KI-generierte Passwörter nur scheinbar sicher sind	
Kolumne	49
Sicherheit beginnt bei der Führung	
Marktübersicht	50–51
Wer schützt was?	
Dossier kompakt	52–53
Die Bilanz der Schatten-KI	
Webinar	54–55
Wie Unternehmen teure Fehler bei SOC's vermeiden	

TRENDS

Was Sicherheitsexperten den Schlaf raubt	56–57
Report	59
KI-Angriffe setzen auf Masse statt Klasse	
Studie	60
LLMs durchbrechen Anonymität im Netz	
Kolumne	61
Ein Gesellschaftsvertrag für die digitale Welt	
Company Profile	62
Netrics	
Studie	63
Schweizer verschwitzen Datenschutz bei KI	
Kolumne	64
Asymmetrie in der Cybersicherheit	

IMPRESSUM

Verlag

Netzmedien AG / Heinrichstrasse 235 /
CH-8005 Zürich / Tel. +41 44 355 63 63

Redaktion: desk@netzmedien.ch

Verlag: info@netzmedien.ch

Anzeigen: inserate@netzmedien.ch

Aboservice: abo@netzmedien.ch

Druck: Werner Druck Basel gedruckt in der
schweiz

Erscheinungsweise

Eine Publikation der Reihe «IT for ...»

Erscheint als Eigenbeilage zu «Netzwoche» und «IT-Markt»

Einzelausgabe (Schweiz): CHF 20.–

Auflage: 15 500 Ex.

Partnerplattformen

netzwoche

netzwoche.ch

IT-MARKT

it-markt.ch

ICTjournal

ictjournal.ch

Sie erreichen alle Mitarbeiter telefonisch unter
+41 44 355 63 + jeweilige Endziffern oder
per E-Mail: vorname.nachname@netzmedien.ch

Chefredaktor & Verleger: Marc Landis (mla) (+36)

Head of Sales Support, Leiterin Projekte & Awards: Seraina Frehner (+35)

Key Account Manager: Konstantinos Georgiou (+33)

Senior Sales Consultant: Reto Rudin (+39)

Sales Consultant: Michael Frey (+66)

Senior Sales Consultant W-CH: Supannika Chavanne

Sales Support: Patrizia Zbinden (+69)

Buchhaltung: Christina Frischknecht (+30)

Grafik/Layout: Samantha Maurer (+65)

Redaktion Deutschschweiz

Coen Kaat (cka), stv. Chefred. IT-Markt (+64)

Joël Orizet (jor), stv. Chefred. Netzwoche (+68)

Susanne Löbe, CvD/Korrektorat/Layout (+61)

René Jaun (rja), Redaktor (+68)

Dylan Windhaber (dwi), Redaktorin (+68)

Chiara Binder (cbi), Praktikantin

Valentina Graziano (vgr), Praktikantin (+38)

Andreas Huber (ahu), Praktikant (+38)

Seraina Huber (shu), Praktikantin

Redaktion Westschweiz

Yannick Chavanne (ych), leitender Redaktor

Alexia Muanza (amu), Redaktorin

Marie-France Porres, Korrektorat

Copyright 2026 Netzmedien AG

Die Wiedergabe von Artikeln, Bildern und Inseraten, auch auszugsweise
oder in Ausschnitten, ist nur mit Genehmigung des Verlags erlaubt.

Sofern nicht anders vermerkt, stammen die Bilder von den Herstellern der
abgebildeten Produkte oder wurden zur Verfügung gestellt.

Schweizer KMUs verlieren Vertrauen in ihre Cybersicherheit

Zwei von fünf Schweizer KMUs fühlen sich gut auf einen Angriff vorbereitet – das sind deutlich weniger als vor einem Jahr. Laut der Studie «KMU Cybersicherheit 2025» verpassen es viele KMUs, organisatorische Massnahmen umzusetzen und Cybersecurity zu priorisieren. Autor: René Jaun

Schweizer KMUs sollten mehr tun für ihre Cybersicherheit. Wie gross der Handlungsbedarf ist, zeigt die Studie «KMU Cybersicherheit 2025» von der Allianz Digitale Sicherheit Schweiz (ADSS), Die Mobiliar, Digitaliswitzerland, der Fachhochschule Nordwestschweiz (FHNW), HES-SO Valais-Wallis, Information Security Society Switzerland (ISSS), der Schweizerischen Akademie der Technischen Wissenschaften (SATW), der Swiss Internet Security Alliance (SISA) und Yougov Schweiz. Die sechste Ausgabe dieser Untersuchung stützt sich auf eine Yougov-Umfrage unter 515 IT-Entscheidern von Schweizer Unternehmen mit bis zu 49 Angestellten. Zudem befragte Yougov 336 IT-Dienstleister.

Bei der Frage, wie KMUs ihre eigene Cybersicherheit bewerten, hat sich im Vergleich zum Vorjahr kaum etwas verändert: Über die Hälfte der Befragten (52 Prozent) fühlt sich eher oder sehr sicher vor Cyberkriminalität, nur eine kleine Minderheit (9 Prozent) fühlt sich eher oder sehr unsicher. Stark verändert – und zwar zum Negativen – hat sich die Selbstbewertung zur Resilienz, also wie gut vorbereitet und geschützt man sich einschätzt. Im Vorjahr hielten sich über die Hälfte der Befragten (55 Prozent) für eher oder sehr gut geschützt. 2025 waren es nur noch zwei Fünftel (42 Prozent). Der Mittelwert sank von 3,5 auf 3,3 auf der Fünferskala. «Die Befragten fühlen sich also unverändert mehrheitlich sicher, aber signifikant schlechter vorbereitet und geschützt», fassen die Autoren zusammen. Beunruhigenderweise sinkt 2025 auch die Priorität des Themas stark, wie es weiter heisst: 2024 beurteilte noch knapp die

Hälfte das Thema Cybersicherheit als (sehr) wichtig; 2025 war es nur noch ein Drittel. Dementsprechend planen 2025 auch signifikant weniger Befragte, ihre Sicherheitsmassnahmen zu erhöhen (40 Prozent) als im Vorjahr (48 Prozent).

Es fehlen organisatorische Massnahmen

Die Selbsteinschätzung von KMUs zur Resilienz täuscht nicht: «KMUs fühlen sich nicht nur nicht resilient, sie sind es effektiv auch nicht», sagte Simon Seebeck, Leiter des Kompetenzzentrums Cyber Risk der Mobiliar, an einer Medienkonferenz zur Studie. Konkret seien Unternehmen eher gut beim Umsetzen technischer Massnahmen. Zwei Drittel der Befragten greifen laut Seebeck auf solche zurück, also etwa auf Firewalls. Es besteht aber auch hier Verbesserungsbedarf, wie die Zahlen zeigen: So setzen 53 Prozent der Befragten eine Multi-Faktor-Authentifizierung ein. Passwort-Manager nutzen 42 Prozent der befragten KMUs.

Doch richtig schlecht sieht es bei organisatorischen Massnahmen aus: 5 von 10 Massnahmen seien von jeweils nur einem Drittel der Befragten umgesetzt worden; dazu gehören ein Notfallplan für die Geschäftsfortführung, ein Sicherheitskonzept, regelmässige Schulungen für Mitarbeitende und Sicherheitsevaluationen der IT-Zulieferer und Partner. Nur 2 von 5 Unternehmen führen zudem regelmässige Sicherheits-Audits durch.



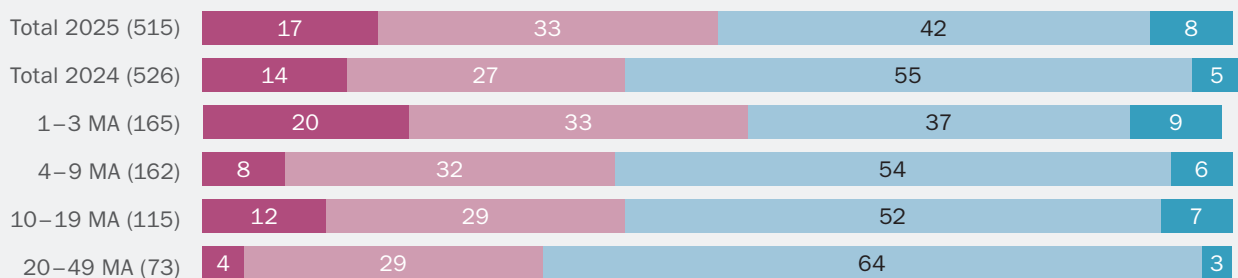
Den vollständigen Artikel finden Sie online
swisscybersecurity.net

WAS SCHÄTZEN SIE: WIE GUT SIND SIE VOR CYBERANGRIFFEN GESCHÜTZT UND AUF EINEN ANGRIFF VORBEREITET?

■ (sehr) schlecht ■ neutral ■ (sehr) gut ■ weiss nicht / keine Angabe

Anzahl Mitarbeitende (MA)

(Angaben in Prozent)



Quelle: cyberstudie.ch

Die IT-SA 2025 hat die Messlatte höher gelegt

Vom 7. bis 9. Oktober 2025 hat die IT-SA Expo & Congress stattgefunden. Die Fachmesse brach alle bisherigen Rekorde bezüglich der Anzahl der Aussteller und Teilnehmenden. Vor Ort waren auch mehrere Schweizer Aussteller. Wie sie die IT-SA erlebt haben, sagen sie im Podium. Autor: Coen Kaat

Am 9. Oktober ist die letztjährige Ausgabe der IT-SA Congress & Expo zu Ende gegangen. Der Veranstalter der Fachmesse für IT-Security zeigt sich zufrieden und meldet neue Rekordzahlen. An die IT-SA 2025 kamen demnach an drei Messetagen 28 267 Fachbesucherinnen und -besucher aus 64 Ländern – ein Wachstum von fast 10 Prozent im Vergleich zum Vorjahr. Die Anzahl der Aussteller kletterte ebenfalls um rund 10 Prozent: In diesem Jahr zeigten 993 Unternehmen und Organisationen, was sie in puncto IT-Security zu bieten haben.

Das Besucherplus «und die um über 22 Prozent gestiegene internationale Beteiligung zeigen, wie wichtig die IT-SA für den internationalen Dialog zur Cybersicherheit geworden ist», sagt Veranstaltungsleiter Thimo Holst. «Hier trifft sich die Cybersecurity-Community, um den länderübergreifenden Herausforderungen der digitalen Sicherheit gemeinsam zu begegnen.» Die globale Vielfalt der Branche zeigte die Messe unter anderem mit Gemeinschaftsständen aus Israel, den Niederlanden, Österreich, Tschechien und dem US-Bundesstaat Virginia.

Der «Athene Startup Award UP25@it-sa» ging dieses Jahr an Infrafon aus Freiburg im Breisgau. «Das Unternehmen überzeugte mit einer innovativen Lösung zur sicheren Zugangskontrolle in regulierten Umgebungen», wie es in der Mitteilung heisst. Auf den Plätzen 2 und 3 kamen Onekey aus Düsseldorf und Nenna.ai aus Berlin.

Die Quantität und Qualität der Gäste

«Die IT-SA entwickelt sich zu einer starken europäischen Alternative zu grossen US-amerikanischen Veranstaltungen», sagt Alain Favre-Victoire, Head of Certificate Services bei Swisssign. Dem stimmt auch Hendrik Flierman, Sales Director Security Solutions bei Swisssbit, zu: «Wer in Europa im Bereich Cybersicherheit mitspielen will, kommt an der IT-SA kaum vorbei.» Man spüre, dass «Aussteller und Veranstalter viel investieren, um den Teilnehmenden etwas zu bieten», sagt Désirée Poffet, Chief Marketing Officer bei Avantec.

Marc Bütikofer, Head of Innovation Airlock bei Ergon Informatik, war nach eigenen Angaben vor allem von der «Qualität und Quantität der Messegespräche» beeindruckt. Palo Stacho, Managing Director von Cyberdise, zählt das «proaktive Vorgehen der



Die IT-SA 2025 zählte 28 267 Fachbesucherinnen und -besucher aus 64 Ländern.

Besuchenden und das Interesse der Laufkundschaft» zu seinen Highlights an der IT-SA 2025. «Viele Diskussionen sind von Buzzwords zu echten Umsetzungsfragen übergegangen», sagt auch Denis Matosevic, Head of Sales DACH bei Exeon Analytics.

Die nächste Ausgabe der IT-SA Expo & Congress findet vom 27. bis 29. Oktober 2026 wieder im Messezentrum Nürnberg statt. Um die Wartezeit zu verkürzen, können registrierte User die Forenbeiträge der jüngsten Ausgabe weiterhin auf der Onlineplattform «IT-SA 365» kostenlos abrufen.

ONLINEPODIUM: DIE IT-SA 2025 AUS SCHWEIZER SICHT

Die IT-SA 2025 hat fast 1000 Aussteller zusammengebracht – darunter auch mehrere Schweizer Unternehmen. Wie sie die Messe erlebt haben und weshalb die IT-SA auch für Schweizer Fachbesuchende spannend ist, sagen sie online im Podium. Die Teilnehmenden des Podiums: Marc Bütikofer von Airlock (Ergon Informatik), Alain Favre-Victoire von Swisssign, Hendrik Flierman von Swisssbit, Denis Matosevic von Exeon Analytics, Désirée Poffet von Avantec und Palo Stacho von Cyberdise.



Hier geht es zum
IT-SA-Podium
swisscybersecurity.net

Cyber-Schuld und digitale Souveränität – ein strategischer Handlungsdruck

In den vergangenen 20 Jahren haben viele Unternehmen eine erhebliche «Cyber-Schuld» aufgebaut. Gemeint sind Sicherheitsmassnahmen, die hätten umgesetzt werden sollen, jedoch unterblieben sind. Dieser Rückstand schwächt die Resilienz der Organisationen.

Zu Cyber-Schulden zählen grundlegende Schutzmassnahmen wie Multi-Faktor-Authentifizierung, regelmässige Backups, Endpoint-Management sowie klar definierte Sicherheitsverantwortlichkeiten und die Sensibilisierung der Mitarbeitenden. Dieser Rückstand schwächt die Resilienz der Organisationen in einem Umfeld, das von industrialisierten Bedrohungen und wachsendem regulatorischen Druck geprägt ist. Cyber-Schulden sind längst nicht mehr nur ein technischer Verzug. Sie stellen ein strategisches Risiko für die Geschäftskontinuität, die Reputation und die Wettbewerbsfähigkeit dar.

Der Aufstieg der künstlichen Intelligenz verschärft die Lage zusätzlich. Mitarbeitende nutzen KI zur Analyse oder Generierung von Inhalten, ohne sich der Risiken im Zusammenhang mit dem Abfluss sensibler Informationen oder von Geschäftsgeheimnissen bewusst zu sein. Wo Technologien ausserhalb klarer Governance-Strukturen eingeführt werden, vergrössert sich die Angriffsfläche erheblich.

Informationssicherheit ist nicht mehr allein eine Frage von Firewalls oder der IT. Sie ist Gegenstand einer integrierten Governance, die Risikomanagement, Technologiestrategie, re-

Der Autor

Eduardo Geraldí, CTO, Spie ICS

gulatorische Compliance und Unternehmenskultur miteinander verbindet.

Von der Compliance zur Führungsverantwortung

In Europa verschärft die NIS-2-Richtlinie die Verpflichtungen wesentlicher und wichtiger Einrichtungen und nimmt die Unternehmensleitung unmittelbar in die Verantwortung. In der Schweiz steht das Informationssicherheitsgesetz (ISG) in derselben Dynamik. Die Geschäftsleitung muss heute ihre Fähigkeit nachweisen, Cyberrisiken zu steuern und kritische Geschäftsprozesse zu schützen.

Gefordert ist ein ganzheitlicher Risikoansatz, der interne Systeme wie auch die gesamte Lieferkette einschliesslich Lieferanten und Partner systematisch erfasst und steuert. In diesem Kontext wird die Business Impact Analysis (BIA) zu einem zentralen Instrument, um kritische Abhängigkeiten zu identifizieren, Prioritäten zu setzen und Sicherheitsinvestitionen konsequent an den strategischen Zielsetzungen auszurichten.

Digitale Souveränität und OT-Risikomanagement

In der Industrie steigern Digitalisierung und KI die Effizienz und Prognosefähigkeit. Doch die zunehmende Konzentration sensibler Betriebs- und Produktionsdaten in externen Cloud-Diensten wirft Fragen der digitalen Souveränität, der technologischen Abhängigkeit und der rechtlichen Exponierung auf.

Digitale Souveränität bedeutet deshalb, Transparenz über Datenstandorte, eingesetzte KI-Systeme und anwendbare Jurisdiktionen zu haben. Ebenso entscheidend sind Exit-Strategien und belastbare Alternativen bei regulatorischen oder geopolitischen Einschränkungen. Die risikobasierte Inventarisierung und Klassifizierung kritischer Daten wird zur strategischen Kernaufgabe.

Cybersicherheit, Business Continuity und operative Souveränität konvergieren zunehmend. Sicherheit entwickelt sich vom technischen Schutzmechanismus zum strategischen Hebel für unternehmerische Resilienz und nachhaltiges Kundenvertrauen.



Das Dossier finden
Sie auch online

swisscybersecurity.net

Bild: photo for everything - stock.adobe.com

«Sicherheit ist ein Geschäftsrisiko, kein reines IT-Thema»

Cyber-Schulden, Cloud-Abhängigkeiten und der sichere Umgang mit KI gehören heute zur Unternehmensrealität. Im Interview ordnet Eduardo Geraldi, CTO bei Spie ICS, ein, wie das Thema Sicherheit im Unternehmen verankert wird und Exit-Strategien für Cloud- und KI-Dienste sinnvoll aufgebaut werden können. Interview: Dylan Windhaber



Eduardo Geraldi,
CTO, Spie ICS.

Wie können Unternehmen konkret ihre «Cyber-Schulden» priorisieren und schrittweise abbauen, ohne den laufenden Betrieb zu gefährden?

Eduardo Geraldi: Sie lassen sich nur strukturiert und risikobasiert abbauen. Zunächst braucht es Transparenz über Systeme, Schwachstellen und Risiken. Darauf aufbauend wird eine an Standards orientierte Cyber-Roadmap erstellt und in einem realistischen Umsetzungsplan in den Betrieb integriert, mit Fokus auf die grundlegenden Sicherheitsmassnahmen. Entscheidend ist ein ganzheitlicher Ansatz entlang von People, Process und Technology.

Wie kann die Verantwortung für Informationssicherheit von einer rein technischen Aufgabe zu einer dauerhaften Führungsaufgabe im gesamten Unternehmen transformiert werden?

Damit sie zur Führungsaufgabe wird, braucht es einen Perspektivenwechsel: Sicherheit ist ein Geschäftsrisiko, kein reines IT-Thema. Sie muss auf Ebene der Geschäftsleitung strategisch verankert und sichtbar gemacht werden. Diese Visibilität entsteht durch gezielte Awareness sowie durch klar definierte Security-KPIs, die regelmässig rapportiert werden und eine wirksame Steuerung ermöglichen.

Welche Kriterien und Prozesse sollten bei der Entwicklung von Exit-Strategien für Cloud- und KI-Dienste berücksichtigt werden, um digitale Souve-

ränität gegenüber regulatorischen und geopolitischen Risiken zu gewährleisten?

Exit-Strategien für Cloud- und KI-Dienste müssen frühzeitig, bereits bei der Anbieterauswahl, berücksichtigt werden. Zentrale Kriterien sind Datenportabilität in standardisierten Formaten sowie die Vermeidung von proprietären Abhängigkeiten, insbesondere bei KI-Modellen. Vertraglich sind klare Regelungen zu Kündigung, Datenhaltung, Datenbearbeitung, Datenrückgabe, Löschung und Unterstützung beim Exit entscheidend. So lassen sich regulatorische und geopolitische Risiken gezielt kontrollieren und digitale Souveränität sichern.

In welchem Umfang und mit welchen Instrumenten sollten Lieferanten und Partner in die Business Impact Analysis eingebunden werden, um kritische Abhängigkeiten frühzeitig zu identifizieren und zu steuern?

Lieferanten und Partner sollten konsequent risikobasiert in die Business Impact Analysis eingebunden werden, mit Fokus auf kritische Drittparteien. Abhängigkeiten in den Geschäftsprozessen müssen frühzeitig transparent gemacht und bewertet werden. Dies idealerweise bereits vor der Beschaffung durch ein strukturiertes Security- und Risiko-Assessment. Ergänzend unterstützen standardisierte Assessments, Audits, Zertifizierungen sowie klare vertragliche Sicherheitsanforderungen dabei, kritische Abhängigkeiten von Anfang an gezielt zu steuern.

Wie lässt sich die Nutzung von KI-Tools durch Mitarbeitende so regulieren, dass Innovationspotenziale erschlossen werden, gleichzeitig aber das Risiko von sensiblen Datenabflüssen und Geschäftsgeheimnissen minimiert wird?

KI-Tools sollten nicht verboten, sondern verantwortungsvoll ermöglicht werden. Klare Leitlinien sind entscheidend, insbesondere, welche Daten verwendet werden dürfen und wie mit sensiblen Informationen umzugehen ist. Gleichzeitig sollten Unternehmen geprüfte und freigegebene Tools bereitstellen, um Schatten-IT-/KI zu vermeiden. Zentral ist dabei die Sensibilisierung der Mitarbeitenden sowie der Einsatz technischer Schutzmassnahmen wie Data Loss Prevention und Zugriffskontrollen. Der Schlüssel liegt in einer klaren Governance, die KI-Nutzung kontrolliert ermöglicht und so Innovation und Sicherheit in Einklang bringt.

SCSD 2026 – die digitale Souveränität der Nischen

Mitte Februar haben in Bern die Swiss Cyber Security Days 2026 stattgefunden. Das Thema: die digitale Souveränität. Bundeskanzler Viktor Rossi ordnete die Lage in der Verwaltung ein und BACS-Direktor Florian Schütz sagte, wie man Souveränität in den Nischen schaffen kann. Autor: Coen Kaat

Die Swiss Cyber Security Days (SCSD) haben Bern am 17. und 18. Februar 2026 wieder zur «City of Cybersecurity» gemacht, jedenfalls wenn es nach SCSD-Präsident Nik Gugger geht. Denn Bern sei der Ort, wo «die digitale Frontlinie auf Diplomatie trifft, wo Innovation auf Souveränität trifft und wo die geopolitische Zukunft der Cybersicherheit gestaltet wird», wie er in seiner Begrüssungsrede sagte. Die SCSD standen in diesem Jahr unter dem Motto «Digital Sovereignty – The New Frontier»; ein Thema, das stark geprägt ist von aktuellen geopolitischen Spannungen. «Wir leben in Zeiten grosser Umbrüche», sagte SCSD-Programmdirektor Nicolas Mayencourt in seiner Auftaktrede. «Und die zentrale Frage lautet: Wer wird die Regeln der neuen Weltordnung festlegen?»

Die digitalen Räume seien nicht mehr neutral; sie seien strategisch und politisch – «und sie sind entscheidend für unsere Zukunft», sagte Mayencourt. Empörung oder Angst seien keine guten Strategien in dieser neuen Realität – weder für Europa noch für die Schweiz. Die SCSD sollen daher auf eine sehr praktikable Weise die Perspektiven von Politik, Wirtschaft und Forschung zusammenbringen und den Diskurs mehr auf Möglichkeiten und Lösungen lenken, damit die Gespräche nicht bei den Risiken allein verharren.

Keine rasche oder vollständige Abkehr von Microsoft beim Bund

Zunächst musste aber das Problem beschrieben werden. Bundeskanzler und Ehrengast Viktor Rossi brachte es in seiner Rede schnell auf den Punkt: «Die Bundesverwaltung ist abhängig von externen Anbietern und auch von grossen ausländischen Konzernen.» Dies treffe nicht nur auf die Bundesverwaltung zu, sondern vermutlich auf jede Verwaltung und praktisch jedes Unternehmen. «Und das wissen wir auch schon lange.» So habe sich der damals noch neue Informatikrat des Bundes 1999 in seiner ersten Sitzung bereits mit der Einführung von Windows 2000 auseinandergesetzt und über die Gefahren und Risiken der steigenden Abhängigkeit von Microsoft-Produkten diskutiert.

«Eine rasche und vollständige Abkehr des Bundes von Microsoft oder von M365 ist weder realistisch noch zwingend», sagte Rossi. Denn die Bundesverwaltung stehe nicht auf einer grünen Wiese mit der Möglichkeit, von Grund auf neu zu bauen. Zwar müssten Abhän-

gigkeiten gezielt reduziert werden, aber dies gehe nur schrittweise. Einer dieser Schritte ist eine Machbarkeitsstudie, welche die Bundeskanzlei derzeit durchführt. Mit dieser will sie testen, inwiefern Open-Source-Lösungen als BCM-Alternative und für die Bearbeitung sensibler Dokumente infrage kommen.

«In diesem Prozess tauschen wir uns auch mit Pionieren aus», sagte Rossi und nannte beispielhaft das deutsche Bundesland Schleswig-Holstein. Dieses habe in den vergangenen sieben Jahren den Wechsel zu Open-Source-Büroumgebungen zu 80 Prozent vollzogen. «Das zeigt: Grundsätzlich ist eine Umstellung möglich, sie ist aber aufwendig, teuer und dauert seine Zeit.»

Austauschbare Softwareanbieter werden wünschenswert

In seiner Rede adressierte Rossi auch Softwarehersteller und -lieferanten. «Entwickeln Sie Produkte, die austauschbar sind mit anderen Produkten von anderen Lieferanten», sagte er. «Mir ist schon klar, als Firma machen Sie sich damit in einem ersten Schritt ersetzbar, aber ich bin überzeugt, genau das kann eben auch ein strategischer Vorteil und ein Business Case werden, der sich lohnen kann.» Die Vermeidung von Abhängigkeiten könnte zum Verkaufsargument werden.

«Souverän ist nicht, wer sich abschottet, sondern wer Abhängigkeiten kennt, wer Wahlmöglichkeiten schafft und sie dort, wo sinnvoll, auch gezielt reduziert», kam Rossi zum Schluss. Das Thema gehe alle etwas an – vom Bund über die Kantone und Gemeinden bis zu den Bürgerinnen und Bürgern. «Und deshalb braucht es auch von allen einen Einsatz.»

Die Schweiz muss den Vergleich nicht scheuen

Das Lagebild in der Schweiz, wenn es um digitale Souveränität geht, präsentierte Florian Schütz, Direktor des Bundesamts für Cybersicherheit (BACS). «Ganz so schlecht stehen wir nicht da», sagte er. Es gibt gemäss Schütz «ein oder zwei Dinge, die wir in der Schweiz ganz gut machen». Die Selbstkritik helfe dabei, besser zu werden, aber geisseln müsse die Schweiz sich nicht. Schütz plädierte dafür, nicht nur auf Regulierungen zu setzen, sondern auch Anreizsysteme zu schaffen. Einen eigenen Schweizer Tech-Stack bauen könne die Schweiz wohl nicht. «Und wenn sie es könnte, sollte sie es wahrscheinlich auch nicht tun», sagte er. Er schlug einen anderen Weg vor: «Abhängigkeiten können Souveränität geben.» Um Wahlfreiheit zu haben, braucht die Schweiz laut dem BACS-Direktor Firmen, die IT- und Cyber-





Viktor Rossi,
Bundeskanzler
und Ehrengast
an den SCSD
2026.

Schütz den Raum. Es werde viel von Europa gesprochen. «Ja, die Schweiz ist in Europa», sagte er und räumte ein, dass der Kontinent durchaus Chancen habe. Europa sei der zweitgrösste IT-Markt der Welt und wachse erst noch schneller als die USA.

Der BACS-Direktor plädierte allerdings dafür, in die Nischen zu gehen, statt mit den Tech-Giganten konkurrieren zu wollen. «Wir vergessen sehr oft, dass man auch Souveränität herstellen kann, indem man in diesen Nischen interessante Produkte anbietet.» Die Schweiz biete etwa IT-Produkte an, die beim Entladen von Hochseeschiffen zum Einsatz kommen. «Hier gibt es nur wenig Konkurrenz», sagte er. Für gewisse Komponenten in den

security-Produkte global vermarkten und so Abhängigkeiten schaffen können.

Um sein Argument zu illustrieren, brachte er die Halbleiterfertigung als Beispiel. Aktuell gibt es gemäss dem BACS-Direktor zwei Firmen weltweit, die Sub-3-Nanometer-Chips produzieren können – eine hat ihren Sitz in Taiwan, die andere in Südkorea. Und wie viele Firmen gibt es, die Maschinen herstellen, die diese Chips produzieren? Eine, ASML, und die hat ihren Sitz in den Niederlanden, wie Schütz erklärte. Wer produziert die dafür benötigten Linsen? Wieder nur eine Firma: Zeiss mit Sitz in Deutschland. In Japan komme aber Konkurrenz auf. Und die Software für diese Maschinen komme aus den USA. «Das ist eine globale Lieferkette», sagte Schütz, und alle seien abhängig voneinander. Versuche, diese verteilte Supply Chain zu regionalisieren, das Wettrennen um «Tech Supremacy», führten nun zu globalen Spannungen. Und auch zu Cyberattacken – denn «man muss diese Maschinen ja irgendwie kopieren» und wenn man die entsprechenden Daten stiehlt, spart man den Forschungsaufwand.

Wo die Schweiz Souveränität schaffen kann

«Die Frage ist jetzt, wie man sich da positionieren möchte?», fragte

dafür benötigten Kränen gebe es nur einen oder zwei Anbieter weltweit. Die nächsten Nischen, die es zu besetzen gelte, seien Quantenkryptografie und KI. Und die Schweiz habe in diesen Bereichen «dominante Forschungsergebnisse», sagte Schütz.

Aber nur innovativ zu sein, genüge nicht. «Es geht auch darum, dass wir beginnen, Firmen aufzubauen, die skalieren und einen globalen Markt bedienen können», sagte Schütz. Firmen, deren Angebote auch von staatlicher Seite genutzt werden können.



Florian Schütz,
Direktor des
Bundesamts für
Cybersicherheit.

Proofpoint ernennt neuen Regionalleiter für die Schweiz und Österreich

dwi. Das Cybersicherheitsunternehmen Proofpoint ernennt Douglas Chechele zum neuen Regionalleiter für die Schweiz und Österreich. Er trat die Stelle unter der neuen Bezeichnung Director Sales Alps Anfang Januar 2026 an, wie seinem LinkedIn-Profil zu entnehmen ist. In seiner neuen Funktion soll Chechele die allgemeine Geschäftsstrategie des Unternehmens in der Alpenregion vorantreiben, wie Thomas Mierschke, Area Vice President DACH bei Proofpoint, auf Anfrage mitteilt. Zudem verantwortet Chechele die Stärkung der Beziehung zu Kunden und Partnern sowie die Fortsetzung der Investitionen in einen für Proofpoint strategisch wichtigen Markt.

Chechele bringt laut Mierschke über zwei Jahrzehnte Erfahrung in den Bereichen Unternehmens-IT und Cybersicherheit mit. Vor seinem Wechsel zu Proofpoint arbeitete Chechele gemäss seinem LinkedIn-Profil vier Jahre als Sales Manager Major Accounts bei Check Point Software Technologies in Spreitenbach. Davor hatte er von 2016 bis 2022 das Schweizer Geschäft des Softwareherstellers Veeam geleitet.

Chechele tritt gemäss Mierschke die Nachfolge von Roger Gomol an. Dieser hatte die Stelle mit der vorherigen Bezeichnung



Douglas Chechele,
Regionalleiter für die
Schweiz und Österreich,
Proofpoint.

als Country Manager seit Juni 2024 inne. Der neue Regionalleiter Chechele schreibt auf Anfrage, dass strukturelle Veränderungen bei Proofpoint dazu geführt hätten, dass er die Geschäfte im Alpenraum nun unter dem Titel des Director Sales weiterführt und es einen Country Manager in diesem Sinne nicht mehr gebe.



Den vollständigen
Artikel finden Sie
online

swisscybersecurity.net

Check Point bestimmt Nachfolger für beförderten Schweiz-Chef

cka/nki. Check Point Software Technologies hat Marco Pierro zum neuen Country Manager für die Schweiz ernannt. Er übernahm die Funktion am 1. Oktober 2025, wie das israelische Cybersecurity-Unternehmen mitteilt. In seiner neuen Rolle soll Pierro die Expansion des Geschäfts in der Schweiz vorantreiben, Kundenbeziehungen stärken und Partnerschaften ausbauen. Er berichtet an Lothar Geuenich, Vice President Central Europe/DACH. «Ich freue mich darauf, mit unseren Schweizer Kunden und Partnern zusammenzuarbeiten, um das digitale Vertrauen zu stärken, Innovationen voranzutreiben und Sicherheit zu einem nahtlosen Bestandteil des Erfolgs jedes Unternehmens zu machen», lässt sich der neue Schweiz-Chef zitieren.

Pierro tritt die Nachfolge von Alvaro Amato an. Nach vier Jahren als Schweiz-Chef übernahm er Anfang April die Rolle des Director Globals für EMEA und Asien.

Laut Mitteilung bringt Pierro über 20 Jahre Erfahrung in den Bereichen Cybersecurity und Channel-Management mit. Zuletzt war er als Country Manager bei Arrow ECS Switzerland tätig. In dieser Funktion arbeitete er bereits mit Check Point zusammen. «Marcos fundierte Kenntnisse des lokalen Marktes und seine



Marco Pierro,
Country Manager
Schweiz, Check Point.

ausgeprägte Partnerorientierung machen ihn zum idealen Leiter für den Ausbau unserer Präsenz in der Schweiz», sagt Geuenich. Die Schweiz sei für Check Point zu einem wichtigen Innovationszentrum geworden. Insbesondere seit der Übernahme von Lakera und der Eröffnung eines globalen AI Security Centers in Zürich ergänzt er.



Den vollständigen
Artikel finden Sie
online

swisscybersecurity.net

Agora Secureware ernennt CEO

vgr. Thomas Blaser hat Anfang Januar 2026 die Funktion als CEO bei Agora Secureware übernommen. Mit ihm ernannte das Tessiner Softwareunternehmen erstmals einen CEO, wie Agora Secureware auf Anfrage mitteilt. Da das Unternehmen im Aufbau war, hatte es bisher «eine Geschäftsleitung in anderer Konstellation», weshalb es keinen direkten Vorgänger gab. Blaser soll nun als Geschäftsführer die strategische Positionierung von Agora Secureware und dessen Kollaborations- und Dokumentenaustauschplattform «Trust Room» weiter vorantreiben.

Der Berner Oberländer bringe über 20 Jahre Führungserfahrung im Finanzdienstleistungssektor sowie aus Transformations- und Militärprojekten mit. Er sei unter anderem in leitenden Positionen bei der UBS und Julius Bär tätig gewesen, wo er für grössere Organisationseinheiten, Transformationsprojekte und die strategische Marktentwicklung zuständig gewesen sei. Zuletzt habe er über zwölf Jahre für die Schweizer Armee gearbeitet. Dort wirkte er seit 2022 im Militärstrategischen Stab des Chefs der Armee als Oberstleutnant, wie seinem LinkedIn-Profil zu entnehmen ist. Zudem verfügt Blaser laut Mitteilung über ein Diplom in Betriebswirtschaft, hat einen Executive MBA der University of Rochester in den USA sowie der Nyenrode Business Universiteit in den Niederlanden. «Er vereint unternehmerisches



Thomas Blaser, CEO,
Agora Secureware.

Denken, regulatorische Erfahrung und technologische Affinität in idealer Weise und wird eine entscheidende Rolle dabei spielen, Agora konsequent weiterzuentwickeln, um unsere Position als führende Schweizer Plattform für sichere digitale Zusammenarbeit und digitale Unabhängigkeit nachhaltig zu stärken», sagt Nagi Moustafa, Präsident des Verwaltungsrats bei Agora Secureware.



Den vollständigen
Artikel finden Sie
online

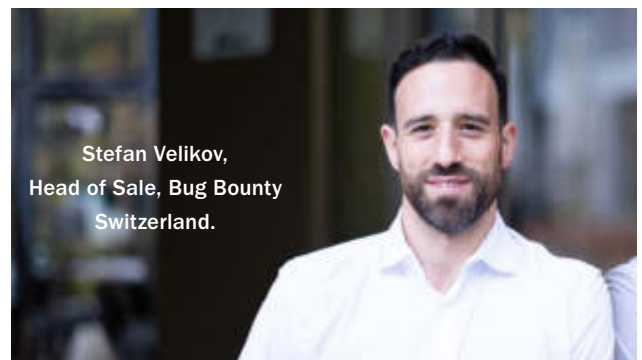
swisscybersecurity.net

Bug Bounty Switzerland erweitert GL

cbi. Stefan Velikov ist seit Anfang Februar 2026 Head of Sales bei Bug Bounty Switzerland. Als neues Mitglied der Geschäftsleitung soll er das Unternehmen mit tragfähigen Strukturen und reproduzierbaren Prozessen in der Verkaufsorganisation unterstützen, wie es in einer Mitteilung heisst. Velikovs Aufgabe sei zudem, Bug Bounty Switzerland auf dem Weg vom Start-up- zum Scale-up-Unternehmen sowie bei der internationalen Expansion systematisch zu begleiten. Zudem soll er das Sales-Team des Unternehmens weiterentwickeln sowie bis 2027 ausbauen. Ziel sei es, der Nachfrage nach dem Cyber Resilience Shield, einem im Jahr 2024 lancierten Produkt zum Schutz für Unternehmen, nachzukommen.

Der neue Head of Sales verfügt laut Mitteilung über Know-how für komplexe Verkaufsprozesse. Er habe 2017 das Unternehmen Viabz gegründet und bis zum Verkauf im Jahr 2022 skaliert. Er sei zudem gut im Schweizer Venture- und Start-up-Ökosystem vernetzt.

Wie das Unternehmen auf Anfrage mitteilt, hat man die Rolle des Head of Sales neu geschaffen. Zuvor habe COO und Co-Founder Florian Badertscher die Position ad interim wahrgenommen. Mit der neuen Sales-Organisation möchte Bug Bounty Switzerland laut Mitteilung einen Schritt weiter gehen, um Se-



Stefan Velikov,
Head of Sale, Bug Bounty
Switzerland.

curity-Testing neu zu definieren. «Stefan stösst in einer entscheidenden Phase zu uns – in einem Moment, in dem wir uns als Unternehmen wandeln und sich zugleich die Art und Weise verändert, wie Sicherheitstests im Zeitalter der künstlichen Intelligenz durchgeführt werden», lässt sich Sandro Nafzger, CEO und Mitgründer von Bug Bounty Switzerland, in der Mitteilung zitieren.



Den vollständigen
Artikel finden Sie
online

swisscybersecurity.net

Kompetenz in Datensicherheit

In einer digitalen Welt, in der Daten das Fundament jedes Unternehmens sind, ist Datensicherheit kein Luxus, sondern eine absolute Notwendigkeit.



Axel Egger, CEO, Axel Egger Advisory GmbH.

In einer vernetzten Welt ist der Schutz Ihrer IT-Infrastruktur und Daten unerlässlich. Wir erarbeiten mit Ihnen massgeschneiderte Lösungen, die Ihre Kronjuwelen im normalen Betrieb nicht nur zuverlässig sichern, sondern auch bei unbefugter Verwendung ihren Inhalt nicht preisgeben.

Von der Erstellung über die Verarbeitung, bei Verwendung, Speicherung, Archivierung und Löschung sorgen wir dafür, dass Ihre Daten und die damit zusammenhängenden Prozesse stets sicher und gesetzeskonform sind. Auf dem Weg dahin begleiten wir Sie strategisch und operativ. Unter Berücksichtigung Ihrer Unternehmensstrategie, von der Konzeption, Überprüfung und Einhaltung des Datenschutzes engagiert, individuell und loyal.

Künstliche Intelligenz

Unser Motto: Starten statt warten. Jetzt anfangen, in KI-Modelle zu investieren, Optimierungen durchführen und mit den gewonnenen Erfahrungen im Unternehmen einen echten Nutzen erzielen. Inzwischen stehen in verschiedenen Bereichen erprobte Standardmodelle zur Verfügung, die – angepasst an Ihr Unternehmen – gesetzeskonformen Datenschutz und -sicherheit gewährleisten. Auch wenn es oft suggeriert wird: Eine Abkürzung gibt es nicht.

Zero Trust

Beim Thema Cybersicherheit fokussieren wir uns auf die Sicherheit Ihrer Unternehmensdaten, zugrundeliegend auf dem Zero-Trust-Ansatz. Daten werden so geschützt, dass sie im normalen Betrieb und gemäss Autorisierung zugänglich bleiben, im Ernstfall durch Malware, Phishing, Datendiebstahl und andere Bedrohungen zum einen unverändert und zum anderen bei einem Datenabgang nicht verwendbar sind.

Zero Trust heisst: niemals blind vertrauen, immer in Echtzeit für jede Aktion verifizieren. Dieser Ansatz unterstützt die Agilität des Geschäftsalltags mit einer angepassten Dynamik im IT-technischen Bereich. Keine Diskrepanz und (langes) Warten, bis die Berechtigungen (endlich) an die veränderten Gegebenheiten angepasst sind. Das Thema KI ist zum einen Chefsache und zum anderen kann individuelle und Organisationserfahrung durch nichts ersetzt werden.

Als Ihr Partner im Bereich Security und Softwareberatung bieten wir Ihnen fundiertes technisches und betriebswirtschaftliches Know-how, strategische Weitsicht und praxisnahe Lösungen. Und zum Schluss noch ein Wort zur Souveränität: Wir sind der Meinung, dass man aufgrund der derzeitigen geopolitischen Lage das Kind nicht mit dem Bade ausschütten sollte, und vertreten daher den Ansatz: regional, wo immer möglich, global, wo nötig.

Unsere Mission:

Sicherung Ihrer Geschäftstätigkeit.

Das LinkedIn-Profil, Posts und Artikel zum Thema finden Sie hier:



Das Company Profile finden Sie auch online
swisscybersecurity.net



Axel Egger Advisory GmbH

Langmattstrasse 4
5200 Brugg
079 66 19 56
a.egger@egger-advisory.ch
egger-advisory.ch

Cisco Schweiz ernennt neuen Cybersecurity-Chef

cbi. Cisco Schweiz hat Nicolas Capitoni per Oktober 2025 zum neuen Cybersecurity-Chef ernannt. Capitoni bringt über 15 Jahre Erfahrung in der Branche mit und soll für die Schweiz eine zentrale Funktion im Bereich Cybersicherheit übernehmen, wie das Unternehmen mitteilt.

Bis September 2025 arbeitete er laut seinem LinkedIn-Profil als Board Advisor bei Exeon Analytics, und davor für Wipro und Open Systems in verschiedenen Positionen. Bei Wipro habe Capitoni den Bereich Cybersecurity & Risk Services geleitet und die Markteinführungsstrategie wie auch den Ausbau strategischer Beziehungen zu global tätigen Unternehmen vorangetrieben, schreibt Cisco. Zudem ist er Podcast-Host, Keynote-Speaker und Advisor verschiedener Security-Start-ups.

Für den neuen Cybersecurity-Chef Schweiz ist gemäss Cisco eine enge und vertiefende Zusammenarbeit mit bestehenden Partnern geplant sowie eine Erweiterung des Cisco-Ökosystems mit neuen Partnerschaften. Der Fokus liege auf umsetzbaren Lösungen für



Nicolas Capitoni,
Head of Cybersecurity,
Cisco Schweiz.

Use Cases, wobei Capitoni eng mit Matthias Wick, CTO Cisco Schweiz, und Niema Nazemi, Partner Lead Cisco Schweiz, zusammenarbeite.

Wie das Unternehmen auf Anfrage mitteilt, übernimmt Capitoni das Ruder von Roman Stefanov, der gemäss seinem LinkedIn-Profil seit August 2025 bei Okta die neu geschaffene Stelle als Regional Director Alps and Eastern Europe innehat.



Den vollständigen
Artikel finden Sie
online

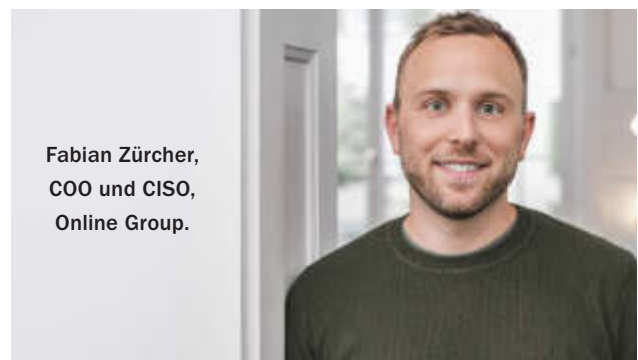
swisscybersecurity.net

Online Group besetzt CISO und COO in Personalunion

rja. Fabian Zürcher heisst das neue Geschäftsleitungsmitglied des Microsoft-Partners Online Group. Das Beratungsunternehmen befördert ihn zum COO und CISO in Personalunion. Man unterstreiche damit die strategische Bedeutung von Betriebsexzellenz und Informationssicherheit, teilt die Online Group mit.

In seiner Doppelrolle als COO und CISO verantwortet Zürcher die operative Steuerung und Weiterentwicklung der Operationsorganisation und die Sicherstellung höchster Qualitätsstandards in Services und Prozessen. Er trägt zudem die Verantwortung für die Informationssicherheit und Compliance im Rahmen der ISO-27001-Zertifizierung und soll die Unternehmenskompetenzen in den Bereichen Cloud Security, Infrastructure und Managed Services ausbauen. Zürcher stiess im September 2024 zur Online Group und leitete zuletzt den Bereich «Cloud Security & Infrastructure». In dieser Rolle habe er massgeblich dazu

beigetragen, die Kompetenz in den Bereichen Cloud Security und Cloud Infrastructure weiterzuentwickeln. Ganz besonders hebt das Unterneh-



Fabian Zürcher,
COO und CISO,
Online Group.

men hervor, dass Zürchers Team die ISO-27001-Zertifizierung erfolgreich bei der Online Group eingeführt habe.

«Informationssicherheit und operative Exzellenz sind die Grundlage für nachhaltige Kundenbeziehungen. Ich freue mich darauf, gemeinsam mit unseren Teams die Organisation weiterzuentwickeln und unsere Position als führender Microsoft-Partner mit ISO-27001-Zertifizierung auszubauen», sagt Zürcher.



Den vollständigen
Artikel finden Sie
online

swisscybersecurity.net

«Gute CISOs müssen einen grossen Spagat machen können»

IT-Spezialist, Businessexperte, Kommunikator, Diplomat – es gibt wenig, was ein CISO nicht können muss. Wie sich die Anforderungen an CISOs durch KI und digitale Souveränität ändern und wie sie damit umgehen sollten, sagt Andy Schneider von Palo Alto Networks. Interview: Coen Kaat

Was zeichnet einen guten beziehungsweise eine gute CISO aus?

Andy Schneider: Ein guter oder eine gute CISO kann technische Probleme und Herausforderungen in den Businesskontext übersetzen – es geht also nicht primär um die Technologie, sondern darum, welche Anforderungen das Unternehmen hat. Die konkreten Bedürfnisse unterscheiden sich stark von Unternehmen zu Unternehmen: Ein Automobilhersteller auf Sparkurs erfordert eine andere Herangehensweise als ein junges Start-up, das schnell skalieren will. Gleichzeitig muss ein CISO nicht nur überzeugend vor dem Verwaltungsrat sprechen, sondern die besprochenen Themen anschliessend in konkrete Massnahmen und technische Lösungen herunterbrechen können. Das ist ein grosser Spagat, aber gute CISOs müssen diesen machen können.

Stark verallgemeinert lässt sich sagen, dass CISOs in der Regel in zwei Gruppen eingeteilt werden können: Techies, die Management-Fähigkeiten dazugelernt haben, oder Manager, die sich Security-Expertise angeeignet haben. Was müssen diese beiden Gruppen noch voneinander lernen?

Beide Wege führen zum Ziel. CISOs brauchen eine fundierte Security-Expertise; sie brauchen aber auch Führungsfähigkeiten. Letztlich geht es aber primär um Menschen, Zahlen und das Business und weniger um Firewalls oder andere Security-Themen. Das Business zu verstehen und zu beherrschen, ist viel wichtiger. Dies hängt natürlich von der Grösse und Komplexität des Unternehmens ab. Was die beiden voneinander lernen können? Also der Techie kann das Business vom Manager lernen. Am besten setzt er sich mit dem CFO zusammen, um zu verstehen, wie ein Geschäftsbericht überhaupt entsteht, welche Kennzahlen relevant sind und welche strategischen Ziele das Unternehmen verfolgt.

Und die andere Seite – der Manager?

Auf der anderen Seite – und das sehe ich oft – stehen CISOs, denen es an technischen Skills mangelt. Sie werden fast schon zu «Compliance-CISOs», wie ich sie nenne. Statt die Hintergründe und Risiken zu verstehen, beschränken sie sich darauf, Checklisten abzuhaken. «Wir brauchen eine Firewall?» – gekauft, erledigt. «Wir brauchen SASE?» – gekauft, erledigt. Aber die feinen Unterschiede und Details, auf die es am Ende eben doch ankommt, bleiben ihnen verborgen. Ein reiner Business-CISO ist genauso verloren wie ein reiner Tech-CISO – es braucht echte Hybrid-CISOs, die sowohl die Technologie als auch das Geschäft verstehen.

Gibt es noch einen dritten Weg?

In meiner Funktion als Field CSO spreche ich mit vielen CISOs; dabei habe ich viele kennengelernt, die als Quereinsteiger zu dieser Rolle gekommen sind. Ich habe kein Muster gefunden, das besagt, dass die besten CISOs Informatik studiert haben oder HSG-Alumni sein müssen. Quereinsteiger haben oft den Vorteil, dass sie mit einem unvoreingenommenen Blick beginnen können, weil sie nicht zu technikbelastet sind. Das finde ich immer wieder spannend.

Woher kommen diese Quereinsteiger?

Die kommen aus Bereichen wie dem Marketing oder auch aus dem Sales und wechseln dann in eine CISO-Rolle. Das kann sinnvoll sein, denn wer aus der Technik kommt, neigt oft dazu, dem Marketing skeptisch gegenüberzustehen. Dasselbe gilt auch für Personen mit einem reinen Business-Hintergrund. Aber Security muss man intern vermarkten können – es muss den Mitarbeitenden sozusagen verkauft werden. Deswegen sind Marketing- und Sales-Fähigkeiten für einen CISO fast schon essenziell, aber das vergessen viele Business- und Techie-CISOs oft.

Muss ein CISO heutzutage mehr Diplomat, mehr Kommunikator oder mehr Tech-Experte sein?

In erster Linie muss er Kommunikator sein, weil er mit einer Vielzahl von Stakeholdern sprechen muss. Und an zweiter Stelle stehen die diplomatischen Fähigkeiten, weil man Allianzen schmieden muss – auch mit Personen, die man vielleicht nicht gern hat. CISOs müssen die Entscheider im Unternehmen identifizieren und sie

ZUR PERSON

Andy Schneider ist Chief Security Officer EMEA Central bei Palo Alto Networks. Mit über 20 Jahren Erfahrung in der IT-Branche setzt er sich für die Stärkung der Cyberresilienz bei C-Level-Führungskräften ein, agiert als deren enger Berater und etabliert zukunftsweisende Thought-Leadership-Themen in der Branche.



«Die Verantwortung und die Haftbarkeit im Ernstfall rückt immer mehr in Richtung CISO.»

Andy Schneider, Field CSO EMEA Central, Palo Alto Networks

LIVE

für die eigenen Sicherheitsinitiativen gewinnen können. Nur so lassen sich Massnahmen erfolgreich umsetzen. Dieser Human-Factor ist nicht neu, gewinnt jedoch zunehmend an Bedeutung – das zeigt auch eine aktuelle Studie von Palo Alto Networks. Der CISO wird immer mehr zu einer Corporate-Rolle, die viel breiter aufgestellt ist.

Wie hat sich das Profil des CISOs in den vergangenen fünf bis zehn Jahren verändert?

Durch die Zunahme von Regulierungen wie beispielsweise NIS-2 ist der Druck auf den CISO gestiegen. Die Verantwortung und die Haftbarkeit im Ernstfall verlagern sich immer mehr in Richtung CISO. Einen Präzedenzfall, in dem ein CISO angeklagt wurde, gibt es bislang aber nicht. Derzeit liegt die Verantwortung meist noch beim CEO. Delegiert dieser jedoch sauber, haftet der Nächste in der Nahrungskette – und das wäre dann der CISO. Diese gestiegene Verantwortung und die Haftbarkeit wirken sich auf die Art und Weise aus, wie man Entscheidungen trifft. Das Denken wird langfristiger und ergebnisorientierter; sich hinter reinen Checklisten zu verstecken, reicht dann nicht mehr. Das ist der eine Treiber, der die Funktion des CISOs verändert.

Und der andere Treiber?

Die Angriffe hören nicht auf. In den vergangenen 20 Jahren haben wir zwar zahlreiche neue Abwehrtechnologien eingeführt, aber gleichzeitig sind genauso viele – wenn nicht sogar mehr – Angriffe aufgetreten. Unternehmen realisieren nun, dass es nicht genügt, einfach ISO-27001-konform zu sein. Unternehmen müssen schauen, dass sie auch sicher sind. Dafür brauchen sie kompetente CISOs, die nicht nur die Compliance im Blick haben, sondern den Spagat zwischen Technik und Business machen können.

Wie hat das Aufkommen von generativer KI die Aufgaben des CISOs verändert?

Noch ist die KI nicht vollständig angekommen, aber die Aufgaben des CISOs befinden sich wegen ihr bereits im Wandel. Angreifer nutzen immer häufiger KI – etwa für Deepfakes, für Phishing-Attacken oder für Schadprogramme, die auch schon KI-Elemente haben können. Diese Entwicklungen beschleunigen sich kontinuierlich. Auf der Abwehrseite kann man nicht einfach abwarten und zusehen: Die Verteidigung muss ebenfalls schneller werden. Mit

ausschliesslich menschlichen Spezialisten ist eine effiziente Abwehr schon nicht mehr möglich. KI wird hier deshalb eine enorm wichtige Rolle spielen. Zugleich führen Unternehmen verzweifelt KI-Projekte ein, weil sie sich dadurch Effizienzgewinne erhoffen. Auch hier kommt der CISO also nicht darum herum, sich mit KI-Modellen zu beschäftigen.

Inwiefern sind KI-Systeme anders zu schützen als herkömmliche IT-Systeme?

Eine KI kann man nicht einfach patchen und anschliessend wieder sicher verwenden. Wenn ein KI-Modell eine Schwachstelle hat, muss ich sechs Monate warten, bis ein neues Modell bereitsteht. Hier braucht es einen anderen Security-Ansatz. Deswegen sind derzeit alle CISOs gefragt, Sicherheitsarchitekturen so umzusetzen, dass auch KI-Modelle geschützt sind. Dieser Wandel ist vergleichbar mit der Revolution, die durch das Aufkommen von SaaS-Modellen ausgelöst wurde.

Ein weiteres aktuelles Thema ist die digitale Souveränität. Hierbei handelt es sich primär nicht um ein technologisches, sondern um ein politisches Thema. Wie viel internationale Politik muss ein CISO verstehen, um seine Aufgaben optimal erfüllen zu können?

Er muss sich gewiss damit beschäftigen. Politik ist immer sehr kurzfristig und auch emotional aufgeladen. CISOs müssen unterscheiden können, was die allgemeine Gefühlslage ist und was bloss von der Politik genutzt wird, um irgendwelche Eigeninteressen zu pushen. Deshalb empfehle ich jedem CISO, ein klassisches Risikomanagement zu betreiben. Es bestehen zwar Risiken im Zusammenhang mit der digitalen Souveränität, doch die Wahrscheinlichkeit, von einer Ransomware getroffen und erpresst zu werden, ist um ein Vielfaches höher. CISOs müssen den politischen Diskurs beiseitelassen und Risiken nüchtern priorisieren können. Nur so kann ein CISO die Geschäftsleitung oder den Verwaltungsrat richtig briefen. Wenn wir uns emotional auf ein Thema versteifen, verlieren wir das grosse Ganze aus den Augen. Für CISOs muss aber das Business immer an erster Stelle stehen.

Ich fasse kurz das Anforderungsprofil eines CISOs zusammen: Techie, Businessexperte, Sales-Spezialist, Marketingprofi, Politik-Versteher, Kommunikationstalent und Risiko-Management-Beherrscher. Gibt es auch Fähigkeiten, die ein CISO nicht unbedingt besitzen muss?

Wow, das ist eine gute Frage. Die Funktion des CISOs ist tatsächlich eine sehr krasse Generalistenrolle. Es kommen sogar noch mehr Aspekte als die aufgezählten hinzu: So muss ein CISO auch People- und HR-Fähigkeiten mitbringen, wenn er ein Team führt. Zudem müssen CISOs ihre Mitarbeitenden motivieren und auf die



«Die Funktion des CISOs ist eine sehr krasse Generalistenrolle.»

Andy Schneider, Field CSO EMEA Central, Palo Alto Networks

Security-Reise mitnehmen können. Das macht diese Rolle so anspruchsvoll.

Wie wird sich die Rolle des CISO in den nächsten fünf bis zehn Jahren verändern?

CISOs werden sich einen echten Platz am Tisch verdienen. Aufgrund strengerer Regularien werden sie stärker in Haftung genommen. Somit werden auch Versicherungen für CISOs immer relevanter. Diese Entwicklung wirkt sich natürlich auch auf die Gehälter aus. Gleichzeitig löst sich die CISO-Funktion zunehmend aus der reinen IT-Abteilung. Gewisse Technologien und Verantwortungsbereiche, die heute noch zur IT gehören, wandern in den Aufgabenbereich des CISO. Das führt dazu, dass die Teams und auch die Budgets wachsen – aber damit nimmt auch die Verantwortung zu, die CISOs übernehmen müssen. Die USA sind schon an diesem Punkt angekommen und bei uns beginnt die Maschinerie nun langsam anzuschlagen und in diese Richtung zu lenken.



axians

IN DER SCHWEIZ **VERANKERT.**
360° **VERNETZT.**
IN DER DIGITALEN ÄRA **ZUHAUSE.**



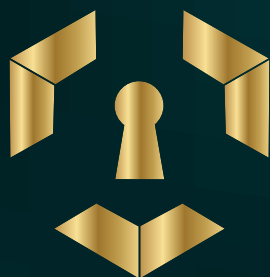
Cyber Security in der KI-Ära.

Axians zeigt Ihnen, wie Sicherheit zum strategischen Erfolgsfaktor wird.

THE **BEST OF ICT** WITH
A HUMAN TOUCH.

JETZT AI SECURITY
PLAYBOOK RUNTERLADEN





**SWISSCYBER
SECURITY.NET**
BY IT-MARKT netzwoche

Bild: Wow Design Studio - stock.adobe.com; Netzmedien

Dies ist erst der Anfang

cka. Cybersecurity ist heute omnipräsent. Einerseits sorgen häufige Cyberattacken auf grosse und auch kleine Unternehmen dafür, dass man dieses Thema nicht vergisst. Und andererseits zwingt die aktuelle politische Lage Unternehmen dazu, sich intensiver mit der digitalen Souveränität und somit auch mit Fragen zum Datenschutz und zur IT-Sicherheit zu befassen. Dass man Cybersecurity ernst nehmen und Massnahmen ergreifen sollte, darüber sind sich die Schweizer KMUs heutzutage weitgehend einig, wie die Studie «KMU Cybersicherheit 2025» zeigt.

2021 war dies noch anders, wie Vorläufer derselben Studie zeigten. Das Bewusstsein war zwar mancherorts da – aber Massnahmen packten die Unternehmen deutlich seltener an. Damals dominierte noch immer die Haltung: «Cyberkriminelle

interessieren sich doch nicht für mein kleines Unternehmen.» Das waren die Rahmenbedingungen, als die Netzmedien vor fünf Jahren das Portal SwissCybersecurity.net lancierten – das Schweizer News- und Infoportal für Cybersecurity. Anlässlich des Jubiläums blicken die Redaktion und Gastautoren in verschiedenen Beiträgen darauf zurück, was sich in den vergangenen Jahren im Cyberbereich verändert hat – und zeigen, wohin sich die Branche noch entwickeln wird. KI-Malware, Quantenverschlüsselung oder auch Cyber-Biosecurity – egal, was noch kommen mag, eines ist klar: SwissCybersecurity.net wird auch diese künftigen Entwicklungen mit News, Hintergründen, Interviews und weiteren bekannten, aber auch neuen Formaten begleiten. Die vergangenen fünf Jahre waren erst der Anfang.

SwissCybersecurity.net feiert dieses Jahr seinen 5. Geburtstag

Das auf Cybersecurity und Cybercrime spezialisierte Portal SwissCybersecurity.net wird fünf Jahre alt. Seit 2021 veröffentlicht die Redaktion täglich aktuelle News, Analysen und Praxistipps rund um Cybersecurity und Cybercrime. Blog, Bedrohungsradar und Partner wie SATW und iBarry machen das Portal zur Anlaufstelle für CISOs, CSOs und Co. Autorin: Dylan Windhaber

Am 15. Februar 2021 hat das auf Informationstechnologie spezialisierte Fachmedienunternehmen Netzmedien AG den Schalter auf «On» gestellt – und SwissCybersecurity.net ging online. Seit fünf Jahren berichtet die Netzmedien-Redaktion auf diesem Portal täglich über News rund um die Themen Cybersecurity und Cybercrime: von aktuellen Warnungen über kriminelle Machenschaften bis zu neuen Strategien zur Abwehr von Ransomware, DDoS-Attacken und Co. Abgesehen von aktuellen News finden Interessierte auf SwissCybersecurity.net seit der Lancierung auch weiterführende Hintergrundberichte im Dossier Cyberwissen. Dies erweitert den Umfang von einer reinen News- zu einer umfassenden Informationsplattform rund um Cyberthemen. Hier finden CISOs, CSOs und IT-Security-Verantwortliche von Schweizer Unternehmen die für sie relevanten News und Hintergrundinformationen.

Neue und bekannte Formate

Das neue Portal musste nicht bei null starten, denn es baute auf der Vorarbeit der Netzmedien-Publikationen «Netzwoche» und «IT-Markt» auf. Die Zugriffszahlen auf entsprechende News belegten die Relevanz des Themas Cybersicherheit. «Die Idee, ein dediziertes Portal aufzubauen, war so naheliegend wie selbstverständlich», lässt sich Coen Kaat, stellvertretender Chefredaktor von «IT-Markt» und SwissCybersecurity.net, zitieren. Kaat war verantwortlich für die Konzeption und Umsetzung des Projekts; seit dem Launch von SwissCybersecurity.net prägt er das Portal auch weiterhin federführend. Unter anderem schreibt er zudem den seit 2018 regelmässig erscheinenden Blog «Was IT-Security-Experten den Schlaf raubt». Ursprünglich unter dem Banner von «IT-Markt» gestartet, fand der Blog auf SwissCybersecurity.net eine neue Heimat.

Zu den bekannten Formaten wie dem Blog gesellten sich bald neue hinzu. So erschien 2022 die erste Ausgabe des Bedrohungsradars. Darin teilen seither monatlich Schweizer Branchenexpertinnen und -experten ihre Einschätzung dazu, welche Entwicklungen die aktuelle Bedrohungslandschaft der

Schweiz gerade prägen. Denn nur wer weiss, welche Gefahren lauern, kann diesen effektiv entgegentreten.

Starke Partnerschaften

«Zu den Highlights der ersten fünf Jahre gehören sicher die Partnerschaften mit der Schweizerischen Akademie der Technischen Wissenschaften (SATW) sowie mit der Plattform iBarry von der Swiss Internet Security Alliance (SISA)», sagt Kaat. Die SATW und SwissCybersecurity.net vertiefen in einem gemeinsamen Newsletter jeweils ein Fokusthema und bilden dieses in unterschiedlichen Facetten ab. Als Medienpartner beteiligt sich SwissCybersecurity.net an der Erstellung und der Streuung von Content für iBarry. Die Plattform soll die Schweizer Bevölkerung über aktuelle digitale Bedrohungen informieren und so grössere technische oder finanzielle Schäden abwehren.

«Fünf Jahre nach dem Start hat sich SwissCybersecurity.net als feste Grösse in der Schweizer Cybersecurity-Branche etabliert», sagt Kaat. «Mit unserem Anspruch, relevante Informationen einzuordnen, Wissen zu vertiefen und Orientierung in einem zunehmend komplexen digitalen Umfeld zu bieten, sind wir auch für die Zukunft gut aufgestellt», sagt Kaat. «Auf die nächsten fünf Jahre!»

FÜNF JAHRE SWISSCYBERSECURITY.NET

SwissCybersecurity.net feiert das fünfjährige Bestehen mit einem Jubiläumsdossier, das sie auf den nachfolgenden Seiten lesen können. Die Jubiläumsartikel umfassen technologische Rückblicke, Analysen aktueller Marktentwicklungen, einen Ausblick auf kommende Trends sowie Testimonials von Leserinnen, Lesern und Kunden von SwissCybersecurity.net. Das Jubiläumsdossier mit allen Beiträgen in voller Länge finden Sie hier auch online.

Hier geht es zum Dossier:



Wenn Angriffe denken lernen: Cyberabwehr unter KI-getriebenem Angriffstempo

Nicht der Alarm schreckt den CIO auf, sondern die Erkenntnis, dass der Angriff längst läuft. Systeme fallen aus, der CISO meldet verdächtige Aktivitäten, Zuständigkeiten sind unklar. Währenddessen verschärft sich die Lage weiter.

Was vor fünf Jahren reaktiv beherrschbar schien, greift heute zu kurz. Cyberangriffe eskalieren nicht mehr linear, sondern adaptiv, während Entscheidungsfenster von Stunden auf Minuten schrumpfen. Die Cyberabwehr steht damit am Wendepunkt. Die zentralen Faktoren dieser veränderten Angriffsdynamik? Im Folgenden eine Einordnung.

Wenn reine Abwehr nicht mehr genügt

Situationen wie diese sind längst keine Ausnahme mehr. In der Cyberabwehr markieren sie die Verschiebung vom Technologiefokus zur operativen Entscheidungsfähigkeit auf Führungsebene.

Heutige Cyberangriffe verlagern sich vom Rand des Netzwerks in den laufenden Betrieb: gesperrte Konten, ungewohnte Zugriffe, eine sprunghafte Zunahme der Alarme – und die Frage, ob es sich um eine Fehlkonfiguration, eine Störung oder um einen koordinierten Angriff handelt. Während noch abgeklärt wird, verschiebt sich die Lage.

Hier stösst klassisches Abwehrdenken an seine Grenzen. Prävention bleibt Pflicht, ihr Wirkungshorizont jedoch begrenzt. Passen Cyberkriminelle Taktik und Ziel während eines laufenden Angriffs an, versagen sequenzielle Abläufe, lange Eskalationsketten und unklare Entscheidungsbefugnisse. Cyber Defence wird damit zur organisatorischen Disziplin: Wer früh einordnen, priorisieren und begrenzen kann, bleibt handlungsfähig.

Cyber Defence vor fünf Jahren: ein Modell seiner Zeit

Noch vor einigen Jahren galten Sicherheitsvorfälle als beherrschbare Ausnahmefälle. Cyberangriffe liessen sich erkennen, eingrenzen und sequenziell abarbeiten. Prävention stand im Zentrum, Detektion und Reaktion setzten ereignisbezogen ein. Dieses Abwehrmodell folgte einer stringenten Logik. Angriffsketten verliefen weitgehend sequenziell, Eskalationen entlang klar definierter Stufen. Zuständigkeiten liessen sich geordnet aktivieren, Entscheidungen aufgrund konsistenter Lagebeurteilungen treffen. Für die damalige Bedrohungsdynamik funktionierte dieser Ansatz. Cyber Defence war damit primär eine technisch-prozessuale Disziplin. Stabilität, Kontrolle und Regelmäßigkeit standen im Vordergrund – passend zu einer Angriffswelt, die Zeit für Einordnung und Reaktion liess.



Den Beitrag finden
Sie auch online
swisscybersecurity.net



Der Autor

Reinhold Zurfluh, Head of Marketing,
Infoguard

Beschleunigung durch die Ökonomisierung des Cybercrime

Cybercrime ist heute nach den USA und China die drittgrösste Volkswirtschaft. Der globale Schaden erreicht heute Dimensionen, die klassische kriminelle Märkte wie den Drogenhandel übersteigen. Das Big Business folgt inzwischen industriellen Logiken: Initialzugänge werden vermarktet, Angriffe automatisiert, Erpressung und Monetarisierung ausgelagert. Ransomware-as-a-Service, Partnerprogramme und spezialisierte Rollen senken die Eintrittshürden und erhöhen Tempo, Reichweite und Anpassungsfähigkeit.

Cyberkriminalität wird damit ökonomisch steuerbar. Aufwand, Ertrag und Risiko lassen sich kalkulieren, Forderungen am Umsatz der Opfer ausrichten, Vorgehen iterativ schärfen. Angreifende operieren nicht mehr statisch, sondern passen ihr Vorgehen während des laufenden Geschehens situativ an – abhängig davon, welche Abwehrmassnahmen greifen und wo neue Angriffsflächen entstehen. Diese Ökonomisierung markiert den strategischen Wendepunkt: Sie beschleunigt Angriffe zugunsten der Cyberkriminellen.

Cyber Defence im Betrieb: vom Schutz zur Entscheidungsfähigkeit

Mit der Beschleunigung der Angriffe verlagert sich Cyber Defence grundlegend. Abwehr findet nicht mehr punktuell im Ereignisfall statt, sondern fortlaufend. Das Security Operations Center (SOC) übernimmt dabei eine zentrale Rolle – nicht als reine Überwachungsstelle, sondern als permanenter 24/7 personell besetzter Entscheidungs- und Reaktionsraum. Noch vor wenigen Jahren beschränkte sich das SOC primär auf Monitoring und Alarmierung. Heute begleitet es Angriffe aktiv. Detektion, Reaktion und Wiederherstellung greifen dabei ineinander und sind nicht mehr isoliert zu betrachten. Pre-Breach- und Shift-Left-Ansätze verlagern den Fokus darauf, Risiken früh zu



Bild: hobonski - stock.adobe.com

erkennen, bevor Angriffe greifen. Voraussetzung dafür ist die ganzheitliche Sichtbarkeit über die Angriffsfläche hinaus: von IT- und OT-Umgebungen über Cloud-Dienste bis zu Identitäten. Künftig wirkt die Cyberabwehr nur, wenn Erfahrungen aus laufenden Angriffen unmittelbar in legitimierte Entscheidungen einfließen. Analyse und Entscheidung erfolgen parallel, nicht als Ausnahme, sondern als neue operative Normalität.

KI als Game-Changer: Human-AI-Teaming als Zukunftsmodell

Zunehmende Geschwindigkeit und Komplexität moderner Angriffe lassen sich ohne Automatisierung nicht mehr bewältigen. KI wird damit zur operativen Voraussetzung. Sie beschleunigt, filtert, strukturiert Informationen und schafft Entscheidungsgrundlagen – entscheidet jedoch nicht. Diese Verantwortung bleibt beim Menschen. Denn Kontextverständnis, Erfahrung und Verantwortung lassen sich nicht in Algorithmen übersetzen.

Entscheidungen in der Cyberabwehr betreffen die operative Stabilität ebenso wie Haftung und Vertrauen. Die Verantwortung für ihre Folgen ist deshalb nicht an Maschinen delegierbar. Mensch und Maschine – ein Team? Der Begriff Human-AI-Teaming steht für eine klare Arbeitsteilung: KI liefert Übersicht und Tempo, der Mensch trifft legitimierte Entscheidungen. Wo dieses Zusammenspiel bewusst gestaltet ist, entsteht zeitgemässe Resilienz. Transparenz, Nachvollziehbarkeit und Human-in-the-Loop sind dabei keine Zusatzoptionen, sondern Voraussetzung wirksamer Cyber Defence unter Echtzeitbedingungen.

Führung und Governance: der unterschätzte Faktor

Eskalierende Angriffe verlangen Handlungsfähigkeit. Und sie fordern Führung. Wer entscheidet? Wer kommuniziert? Was hat Priorität, wenn die Lage unklar ist?

Diese Verantwortung ist heute klar auf Führungsebene verankert und Teil wirksamer Governance. Anders als noch vor einigen Jahren wird Cyberresilienz auch regulatorisch explizit eingefordert. Vorgaben wie NIS-2, DORA oder der Cyber Resilience Act (CRA) verankern Verantwortung explizit in der obersten Führungsebene. Führung definiert Zuständigkeiten, legitimiert Entscheidungsbefugnisse und stellt sicher, dass Cyber Defence und Incident Response vorbereitet und überprüft sind, bevor Zeitdruck entsteht. Regulatorik setzt den Rahmen und erhöht den Druck, garantiert jedoch keine Handlungsfähigkeit. Zentral ist, ob Entscheidungslogiken, Zuständigkeiten und Eskalationswege im Ernstfall tragen. Hier zeigt sich der Unterschied zwischen formaler Governance und gelebter Führung. Tabletop-Übungen und Krisensimulationen klären, ob strategische Führung, Governance, Krisenorganisation und Incident Response im Ernstfall wirken, denn Handlungsfähigkeit entsteht nicht in Dokumenten, sondern in geübten Entscheidungen.

Ausblick: Cyber Defence als lernendes System

Die Angriffsdynamik der Gegenwart lässt kaum Raum für Verzögerung. Angriffe sind schneller, präziser und zunehmend KI-gestützt. Die Folge: Entscheidungsfenster schrumpfen, Unsicherheit wird zum Normalzustand. Cyber Defence ist damit kein Projekt mit Enddatum, sondern ein fortlaufender Lernprozess.

Damit verschiebt sich der Anspruch an die Führung. Handlungsfähigkeit entsteht dort, wo Rollen geklärt, Abläufe etabliert und Entscheidungen nachvollziehbar getroffen werden – selbst wenn Lageeinschätzungen unvollständig bleiben und Zeit der limitierende Faktor ist. Die heutige Bedrohungslage erfordert daher ein Zusammenspiel der Kräfte. Mensch, Prozesse und Technologie müssen ineinandergreifen – nicht starr, sondern lernfähig.

Cyberresilienz von morgen entscheidet sich heute

Wie resilient Organisationen morgen sind, hängt davon ab, wie konsequent sie Cyber Defence heute organisieren. Ein 24/7-SOC – durchgehend personell besetzt – bildet dabei den Dreh- und Angelpunkt, wo menschliche Expertise und KI-gestützte Unterstützung zusammenwirken. Human-AI-Teaming steht nicht für Automatisierung um jeden Preis, sondern für die gezielte Entlastung und Schärfung menschlicher Entscheidungen. Erkenntnisse aus realen Vorfällen, Übungen und neuen Angriffsmustern fliessen dabei kontinuierlich in die tägliche Abwehrarbeit ein.

Cyberresilienz entsteht dort, wo dieses Lernen nicht zufällig bleibt, sondern strukturell verankert ist. Die Fähigkeit der Cyber Defence, künftiger verhaltensbasierter Angriffsdynamik standzuhalten, entscheidet sich daran, ob Organisationen kontinuierliche Anpassung institutionalisieren und der Gegenseite so auf Augenhöhe begegnen.

Cyberangriffe 2026 – automatisiert, identitätsbasiert und KI-beschleunigt

Die Cyberbedrohungslandschaft hat sich in den vergangenen fünf Jahren weiter professionalisiert, erweitert und automatisiert. Die Techniken haben sich strukturell verändert, viele Trends und Ziele sind jedoch gleich geblieben.

Die grundlegenden Motivationen der Angreifer sind unverändert: Profit und Informationsgewinn. Verändert hat sich die Umgebung. Ein Unternehmen besteht längst nicht mehr aus klar abgegrenzten Netzsegmenten hinter einer Firewall, sondern aus Identitäten, Cloud-Diensten, SaaS-Plattformen und APIs. Dadurch entstehen Sicherheitsvorfälle immer häufiger durch Fehlkonfigurationen oder falsche Annahmen.

Die Automatisierung durch KI erlaubt es den Angreifern, schneller und weiter zu skalieren. Schweizer Unternehmen stehen dabei vermehrt im Fokus. Die hohe Kaufkraft, gepaart mit einer dichten KMU-Landschaft, macht die Schweiz zu einem idealen Ziel für skalierbare Angriffe.

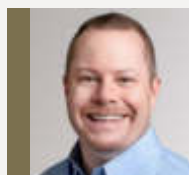
Vertrauen als Vektor

Die effektivste Methode im Jahr 2026 ist nicht der direkte digitale Einbruch, sondern die Ausnutzung von Vertrauen. Supply-Chain-Angriffe auf Softwarehersteller und IT-Dienstleister erlauben es Angreifern, Schadcode über offizielle Prozesse und Updates zu verteilen. Vorfälle wie Solarwinds haben längst gezeigt: Fällt ein IT-Dienstleister, fallen hunderte Kunden gleichzeitig. Der jüngste Notepad++-Angriff zeigte, dass dies auch 2026 weiterhin sehr beliebt ist.

Ein anderer Weg ist, sich als Angreifer einfach mit gestohlenen Zugangsdaten einzuloggen. Allgemein haben kompromitierte Identitäten weiter an Gewicht gewonnen, gerade im Cloud-Umfeld. Deshalb bleibt auch Infostealer-Malware bei den Angreifern sehr beliebt. Die grosse Menge an gestohlenen Credentials wird über Initial Access Brokers verkauft oder direkt für Ransomware ausgenutzt. Einige sprechen deshalb scherzhaft von RDP als dem «Ransomware-Delivery-Protokoll» statt dem Remote-Desktop-Protokoll, weil es so häufig als Initialvektor genutzt wurde.

Generell nutzen Angreifer bei ihren Cyberattacken immer weniger klassische Malware. «Living off the Land», also das Missbrauchen legitimer Tools, die sich bereits auf dem Zielsystem befinden, erfreut sich grosser Beliebtheit. Legitime Fernwartungstools werden als Backdoors installiert und ermöglichen so den kompletten Zugriff ohne auffällige Malware. Dies macht die Erkennung durch AV/EDR schwieriger. Teilweise wird aber auch einfach die DER-Sicherheitslösung ausgeschaltet, um unentdeckt zu bleiben.

Ein weiteres populäres Ziel sind Netzwerk-Devices wie DSL-Modems, VPN-Gateways und Firewalls. Zum einen sind diese



Der Autor

Candid Wüest, Principal Security Advocate, Xorlab

Geräte direkt dem Internet ausgesetzt, zum anderen werden sie selten durch Sicherheitssoftware überwacht – ein ideales Ziel für Cyberkriminelle.

Im Cybercrime-Massengeschäft boomen Low-Effort-Angriffe. Techniken wie «ClickFix» verleiten Nutzer durch täuschend echte Browser-Meldungen dazu, bösartige Skripte manuell zu kopieren und auszuführen. Die Nutzer machen also die ganze Arbeit und infizieren sich unbewusst selbst, während sie glauben, eigentlich ein Captcha zu lösen.

Künstliche Intelligenz

Natürlich kommen wir nicht darum herum, auch über die Entwicklung von und die Risiken durch KI zu sprechen. Der November 2022 markiert einen Wendepunkt, als plötzlich mit ChatGPT ein Large Language Model (LLM) den breiten Markt erreichte. KI und ML gab es zwar schon vorher, aber Chatbots wurden erstmals zum Alltagstool. Wir befinden uns 2026 an dem Punkt, an dem KI vom Buzzword zum Standardwerkzeug geworden ist – ob wir es wollen oder nicht.

Dies bringt neue Herausforderungen mit sich: Data Poisoning, Privacy-Probleme, Halluzinationen und Voreingenommenheit sind nur einige davon. Ein grosses ungelöstes Problem sind Prompt Injections. Vereinfacht gesagt hat das KI-Modell Mühe, zwischen Befehlen und Daten zu unterscheiden, weil beides Text ist. Dadurch können Angreifer eigene Befehle in E-Mails und Dokumenten verstecken. Ein weisser Text auf weissem Grund reicht teilweise schon aus, um dem KI-Agenten mitzuteilen, dass er die anderen Befehle ignorieren und interne Finanzdaten senden soll. In Zukunft wird die KI also eventuell zum Mittäter, und der Angreifer fragt die sensiblen Daten einfach ab, statt sie selbst zu suchen. Die Einbindung von KI-Agenten in alle Prozesse und die Erweiterung mit Berechtigungen und Tools vergrössern dieses Risiko weiter, wie Openclaw kürzlich demonstrierte.



Den Beitrag finden
Sie auch online
swisscybersecurity.net

Bild: NpicArt - stock.adobe.com



Die generative KI hat auch das Phishing-Niveau massiv angehoben. Inhalte sind meistens weiterhin bekannte Paket-Benachrichtigungen oder angebliche Swisspass-Login-Fehler. Dank LLMs fehlen jedoch häufig die früher typischen Rechtschreibfehler als Warnsignal.

- **Deepfakes:** Ein kurzes Youtube-Snippet des CEOs reicht aus, um mittels Sprachklon Finanzmitarbeitende zu Zahlungen zu bewegen. Der Kanton Schwyz berichtete über einen solchen Vorfall im Januar 2026.
- **Personalisiertes Phishing:** KI scannt LinkedIn und andere Profile, um überzeugende personalisierte E-Mails zu verfassen.
- **Token Hijacking:** Angreifer zielen vermehrt auf Session Tokens statt auf Passwörter. Mittels aktiver Proxys wird selbst die Zwei-Faktor-Authentifizierung (2FA) ausgehebelt.

KI gegen KI

Da KI-Modelle immer besser im Programmieren werden, werden sie auch beliebter bei der Erstellung von Malware. Es gibt zahlreiche Beispiele, bei denen KI-Modelle beim Erstellen von Malware geholfen haben. So wurde Voidlink, ein komplexes Malware-Framework, innerhalb weniger Wochen mithilfe von KI entwickelt. Es existieren auch erste KI-powered-Malware-Varianten, die KI zur Laufzeit nutzen, um sich dynamisch anzupassen. Lamahug, Promptlock und Quitevault sind Beispiele dafür. Glücklicherweise sind die meisten Samples noch rudimentär und nutzen das Potenzial der KI noch nicht voll aus. Sie lassen sich deshalb weiterhin mit traditionellen Methoden erkennen. Mit durchschnittlich 5 Millionen neuen Malware-Samples pro Monat stieg die Anzahl bis jetzt nicht exponentiell, sondern ist seit 2023 sogar gefallen.

Frontier-Modell-Betreiber wie Google und Anthropic berichten, dass Angreifer, inklusive staatlicher Akteure, KI bereits für Reconnaissance, Automatisierung und den Rest der Cyber Kill Chain einsetzen. Im November 2025 berichtete Anthropic über GTG-1002, eine chinesische APT-Gruppe, die das Claude-

Modell nutzte, um Angriffe zu 85 Prozent zu automatisieren. Die KI fungierte als Orchestrator bestehender Penetrationstest-Tools, um Schwachstellen zu finden und gezielt auszunutzen. Gleichzeitig scheiterte das Modell häufig an eigenen Halluzinationen. Klar ist, dass Penetrationstests und Schwachstellensuche stark mit KI automatisiert werden können. Im Februar 2026 fand das Claude-Opus-4.6-Modell über 500 neue Schwachstellen in verschiedenen Softwarepaketen. Die Angriffsgeschwindigkeit hat sich von Tagen auf Minuten verkürzt. Verteidigung wird damit zum Kampf KI gegen KI.

Fazit für die Zukunft

Wer heute nur auf rein manuellen Schutz setzt, hat gegen die schnelle, KI-gesteuerte Offensive verloren. Die Verteidigung der nächsten Dekade muss proaktiver und automatisierter werden, um Schritt halten zu können. Die Techniken sind nicht grundlegend neu, aber die Attacks erschlagen durch Volumen und Geschwindigkeit. Agentic AI bringt zusätzliche Non-Human-Identitäten mit sich, die bewertet und abgesichert werden müssen. Zero Trust und Identity First bedeuten, dass Vertrauen für jeden Workflow und jede Identität kontinuierlich neu verifiziert wird.

Auch Themen wie Post-Quantum-Kryptografie, Secure-Enterprise-Browser, Datensouveränität und die Regulierungen werden uns selbstverständlich vermehrt beschäftigen.

In Zukunft verteidigen wir keine Endgeräte mehr, sondern Identitäten, Prozesse und Workflows. KI kann uns helfen, schneller zu reagieren, kann aber auch viele neue Probleme herbeiführen. Ein umfassendes Threat Modeling hilft, Risiken früh sichtbar zu machen und gezielt zu reduzieren. Es gibt zahlreiche wirksame Massnahmen, von Behaviour Anomaly Detection bis Security by Design. Die Schutzmethoden sind bekannt, werden jedoch noch nicht überall umgesetzt.

Cyberkriminalität hat uns in den letzten fünf Jahren beschäftigt und wird uns leider auch in Zukunft weiter begleiten.

Von Creeper zu Morris zu Zeus – eine kleine Geschichte der Malware

Malware ist keine Erfindung des 21. Jahrhunderts. Seit mindestens 40 Jahren ärgert sie User und Admins. Aber welcher Schädling fing damit an? Diese Frage lässt sich nicht so einfach beantworten, denn es gab viele, die in einem bestimmten Bereich die ersten waren. Eine Übersicht der verschiedenen Premieren in der Malware-Welt. Autor: Coen Kaat

Die Cyberkriminalität floriert. Bis 2025 verursachen Cyberkriminelle weltweit Schäden in Höhe von rund 10,5 Billionen US-Dollar. Aktuell wachsen die Kosten jährlich um 15 Prozent, wie eine Analyse von Cybersecurity Ventures zeigt. Kein Wunder, dass Anfang 2024 auch das WEF Cyberangriffe als eines der fünf grössten Risiken der nächsten Jahre bezeichnete. Es ist davon auszugehen, dass die Bedrohungslage – zumindest in den nächsten Jahren – noch schlimmer werden wird.

Blickt man aber zurück statt nach vorn, taucht man in eine völlig andere Welt ein. Die Anfänge von Malware lassen nämlich kaum erahnen, welch monströse Ausmasse diese technischen Spielereien annehmen werden. Die ersten Computerwürmer und -viren wurden nämlich nicht entwickelt, um Schaden anzurichten.

Die Geschichte der Malware beginnt in den 1940er-Jahren mit einer Frage: Kann sich ein Computercode, also ein mechanischer Organismus, genauso verhalten wie ein biologisches Virus? Kann er andere Maschinen infizieren, diese beschädigen, sich selbst replizieren und neue Wirte finden? Den Denkanstoss für diese Diskussion lieferte der ungarisch-US-amerikanische Mathematiker John von Neumann. Dieser vertiefte seine Gedanken im 1966 veröffentlichten Artikel «Theory of Self-Reproducing Automata».

1971

Die ersten Würmer

Es sollte nur fünf Jahre dauern, bis aus der Theorie schliesslich Praxis wurde. 1971 entwickelte Bob Thomas vom US-amerikanischen Unternehmen BBN den wohl ersten Computerwurm. Sein Programm namens Creeper war eigentlich ein Machbarkeitsnachweis, um zu zeigen, dass Computerprogramme sich selbst replizieren und sich auf andere Rechner ausbreiten können. Der Wurm verbreitete sich über das Arpanet, dem Vorläufer des Internets, von einem PDP-10-Mainframe des Herstellers DEC zum nächsten. Übrigens: Die Fähigkeit, sich selbst zu replizieren, wurde von Ray Tomlinson hinzugefügt, der später als «Vater der E-Mail» bekannt wurde. Gemäss Tomlinson wurden höchstens 28 Maschinen infiziert – und diese waren alle Teil des Experiments. Entsprechend richtete Creeper auch keinen Schaden an. Er blendete lediglich die Nachricht «I'm the Creeper: Catch me if you can» ein. Streng genommen erfüllte der Wurm somit nicht alle Kriterien, die von Neumann aufgelistet hatte.

Im darauffolgenden Jahr wurde der zweite Computerwurm geschrieben: Reaper. Dieser wurde von Tomlinson 1972 entwickelt, um sich über das Arpanet zu verbreiten, Creeper aufzuspüren und ihn zu löschen. Somit war der zweite Computerwurm bereits ein sogenannter Nematode – ein Computerwurm, der andere Computerwürmer fressen soll.

1975

Der erste Trojaner

Nur wenige Jahre nach dem ersten Computerwurm entstand auch der erste Trojaner – allerdings wohl unabsichtlich und ohne böse Hintergedanken. Der Programmierer John Walker schrieb die Software Animal. Diese versuchte anhand von 20 Fragen zu erraten, an welches Tier der Benutzer beziehungsweise die Benutzerin gerade denkt. Aufgrund der hohen Nachfrage wollte Walker die Verteilung der Software vereinfachen. Also programmierte er die Subroutine namens Pervade. Dieses Unterprogramm war effektiv in einem anderen Programm versteckt, installierte sich automatisch und führte zudem weitere Aktionen aus, ohne sich bemerkbar zu machen, oder anders gesagt: ein Trojaner. Während man ahnungslos Animal spielte, legte Pervade eine Kopie der Animal-Software in allen Verzeichnissen ab, in denen noch keine Kopie vorhanden war.

1982

Die erste unkontrollierte Verbreitung

Die Folgen der ersten Schädlinge hielten sich in Grenzen. Aber sie hatten den Damm gebrochen. In den darauffolgenden Jahren kamen immer mehr vergleichbare Programme auf. Die nächsten Schädlinge, die für Aufsehen sorgten, entstanden jedoch nicht mehr aufgrund eines akademischen Interesses: Die Zeit der Scriptkid-dies war angebrochen. Junge Studierende und Schüler, die sich für die Grenzen des Machbaren und Erlaubten im Bereich der Informatik interessierten. Zu den frühen Beispielen in diesem Bereich gehört Elk Cloner. Der Schädling wurde 1982 vom damals 15-jährigen Schüler Rich Skrenta in Pennsylvania entwickelt. Elk Cloner gilt als das erste Computervirus, das sich unkontrolliert verbreitete. Es handelte sich um ein sogenanntes Bootsektor-Virus (ein Virus, das beim Start eines Rechners aktiv wird) für den Apple II. Um sich zu verbreiten, infizierte Elk Cloner 5,25-Zoll-Disketten. Grossen Schaden richtete auch Elk Cloner nicht an. Betroffene mussten infizierte Rechner neu star-



Bild: fadi - stock.adobe.com

ten, um sie wieder normal zu nutzen. Auf nicht schreibgeschützten Apple-DOS-Disketten ohne Standard-Image überschrieb Elk Cloner allerdings die reservierten Spuren. Steckten hinter dem ersten Computervirus in freier Wildbahn böse Absichten? Auf seiner Website verneinte der Entwickler dies in einem unterdessen gelöschten, aber vielzitierten Blogeintrag. «Nein, nicht böswillig. Es war ein Scherz, kombiniert mit einem Hack. Ein wunderbarer Hack», schrieb er.

Übrigens: Der wichtigste Unterschied zwischen einem Computervirus und einem Computervirus liegt in der Art, wie sie sich verbreiten. Ein Wurm kann unabhängig agieren und sich selbstständig vermehren; ein Virus hingegen muss sich an Host-Dateien oder -Programme anhängen.

1986

Das erste MS-DOS-Virus

Vier Jahre nach dem Apple-Virus kamen auch MS-DOS-Systeme ins Zittern. 1986 folgte Brain, das erste sich unkontrolliert verbreitende Computervirus für MS-DOS-Systeme. Brain (beziehungsweise dessen Vorläufer Ashar) war auch die erste Malware mit rudimentären Stealth-Features – obwohl die erste Antivirenlösung erst im Jahr darauf auf den Markt kam. Brain verlangsamte das Diskettenlaufwerk und blockierte 7 Kilobytes an Speicherplatz.

Hinter der Malware steckten die pakistanischen Brüder Basit Farooq Alvi und Amjad Farooq Alvi. Diese hatten ihre Kon-

taktdaten im Virus eingefügt – mit der Aufforderung, dass sich Betroffene an die Brüder wenden sollten, um das Virus wieder zu entfernen. Wie sie gegenüber dem «Time Magazine» sagten, wollten sie mit Brain lediglich ihre Softwarelösung vor Raubkopien schützen. Allerdings wird auch spekuliert, dass sie damit die Bekanntheit ihres Unternehmens steigern wollten. Die beiden Brüder führen noch immer einen Internetprovider und ICT-Dienstleister namens Brain Telecommunication und werben damit, dass die Firma «von den Machern des ersten PC-Virus» gegründet wurde. Übrigens: Brain war zudem die Inspiration für den mittlerweile verstorbenen John McAfee, ins Security-Geschäft einzusteigen. Seine Anti-Virus-Lösung, eine der ersten Anti-Virus-Lösungen überhaupt, wurde entwickelt, um Brain-Infektionen abzuwehren.

1987

Das erste zerstörerische Virus

Die Schäden dieser Erstlinge waren noch immer mehrheitlich unbeabsichtigt oder überschaubar.

Daher gehen die Meinungen auseinander, ob es sich dabei wirklich um die ersten echten Beispiele von Malware handelt. Die Kehrtwende in der Malware-Geschichte kam 1987. In dem Jahr wurde in Jerusalem ein neuartiges Computervirus entdeckt und nach der Stadt benannt. Dieser Schädling wurde ganz klar mit dem Ziel entwickelt, zu zerstören. Das Virus aktivierte sich immer an einem Freitag, dem 13. Daraufhin löschte es alle Programmdateien und infizierte wiederholt .exe-Dateien, bis sie zu gross für den Computer wurden. So reduzierte das Virus etwa eine halbe Stunde nach dem Start der infizierten Programme die Rechenleistung befallener Computer. Der hartnäckige Schädling war auch Mitte der Neunzigerjahre noch immer aktiv. Als Windows-Systeme die alten DOS-Geräte verdrängten, nahmen sie dem Jerusalem-Virus jedoch auch den Lebensraum. Gemäss der Definition, wie sie von Neumann aufgestellt hatte, war Jerusalem also wohl die erste echte Malware.

1988

Die erste Verurteilung

Mit dem Morris Worm folgten 1988 gleich zwei Premieren. Dieser wurde nach seinem Entwickler Robert Morris benannt, einem Studenten an der Cornell University und Sohn eines gleichnamigen NSA-Kryptografen. Der Morris Worm ist wohl der erste Wurm, der sich über das Internet verbreiten konnte. Gemäss Opswat infizierte er in nur 15 Stunden rund 2000 Rechner. Laut einer Schätzung sollen rund 10 Prozent aller damals mit dem Internet verbundenen Computer dem Morris Worm zum Opfer gefallen sein. Gemäss seinem Entwickler sollte der Wurm eigentlich keinen Schaden anrichten. Aufgrund eines Designfehlers legte er jedoch infizierte Rechner lahm. Der Wurm prüfte zwar, ob eine Maschine bereits infiziert ist. Aber um falsch-positive Ergebnisse und mögliche Abwehrmassnahmen zu umgehen, legte der Wurm trotzdem in 14 Prozent der Fälle eine Kopie von sich an. Computer konnten also mehrfach infiziert werden. Weil jede Infektion zusätzliche Rechenleistung frass, brachte dies die Rechner zum Abstürzen. Den Schädling zu beseitigen, dauerte bis zu zwei

Tage. Die zweite Premiere, die auf den Morris Worm zurückzuführen ist: Robert Morris ist die erste Person, die nach dem Computer Fraud and Abuse Act von 1986 wegen einer Straftat verurteilt wurde. Die Folgen für Morris: drei Jahre auf Bewährung, 400 Stunden gemeinnützige Arbeit und eine Geldstrafe von 10 050 Dollar zuzüglich der Kosten für die Bewährungsaufsicht. Insgesamt also rund 13 326 Dollar Strafe.

1989

Die erste Ransomware

Im Vergleich zu den Cyberbedrohungen, die noch kommen sollten, wirken all diese Erstlinge fast schon harmlos. Das Schadenspotenzial, das sich bereits abzeichnete, lockte aber eine neue Art von Entwicklern an: finanziell motivierte Kriminelle. Eine der gängigsten Waffen von Cyberkriminellen heutzutage ist Ransomware. Diese Schadprogramme dringen in Rechner ein, verschlüsseln Daten und behaupten, dass sie diese nur gegen eine Lösegeldzahlung freigeben (tatsächlich ist eine Zahlung jedoch keine Garantie dafür, dass man die Daten zurückerhält). Spätestens mit Wannacy 2017 begann die Blütezeit der Ransomware. Erstaunli-

cherweise war die erste Ransomware zu dem Zeitpunkt schon fast 30 Jahre alt. Der Biologe Joseph Popp entwickelte 1989 den ersten Verschlüsselungstrojaner. Die Malware mit dem Namen Aids Info Disk verschlüsselte alle Dateien auf dem Laufwerk C und blendete anschliessend eine Nachricht ein. Diese forderte die Opfer auf, die «PC Cyborg Corporation» zu kontaktieren und ihre Lizenz zu erneuern. Konkret bedeutete dies, 189 Dollar an ein Postfach in Panama zu schicken. Popp verbreitete die Malware via Floppy Disks, die er per Post verschickte. Er wurde zwar wegen elffacher Erpressung angeklagt, aber nicht verurteilt, da er aufgrund seines Verhaltens nach der Verhaftung für geistig unzurechnungsfähig erklärt wurde.

2007

Der erste Banking-Trojaner

Die Zeit der Scriptkiddies war damit noch nicht vorbei. Jugendlicher Leichtsinn respektive technische Neugier führten zu vielen weiteren Erstlingen. Wie etwa Concept 1995, das erste Virus, das Microsoft-Macros ausnutzte. Aber spätestens in den 2000er-Jahren wurden die Cyberkriminellen zur dominanten Kraft in der Malware-Szene. Mit ihnen kam ein neuer Fokus, der wiederum zu neuen Formen von Schadprogrammen führte. Gesellschaftliche Aktivitäten verlagerten sich parallel zunehmend in den digitalen Raum. So wurde der Cyberraum auch für Cyberkriminelle zunehmend spannender. Wohin auch immer sich die Gesellschaft entwickelte, Cybercrime folgte ihr. Die wachsende Popularität von E-Banking etwa führte 2007 zum ersten E-Banking-Trojaner: Zeus. Das Schadprogramm war zwar nicht die erste Malware, die Informationen stahl, aber sie war der erste Infostealer, der es spezifisch auf Bank- und andere Online-Finanzdaten abgesehen hatte.

2025

Das unentdeckte Land

Im digitalen Äther fanden die Cyberkriminellen ein regelrechtes Schlaraffenland vor. Das Geschäft mit Ransomware und Co. ist schon seit Jahren dermassen lukrativ, dass sich eine veritable Schattenwirtschaft entwickelt hat – inklusive Arbeitsteilung, Marketingkampagnen und einer indirekten Vertriebskette. Und mit dem Aufkommen der künstlichen Intelligenz bahnt sich die nächste Entwicklung an. Wie sich diese Technologie auf die Malware-Welt auswirken wird, ist noch nicht klar. Tools wie ChatGPT und Co. werden unerfahrenen Malware-Entwicklern sicher helfen. Es ist also davon auszugehen, dass das Volumen an Malware durch KI stark zunehmen wird. Dafür greifen KI-Tools aber lediglich auf Code zurück, der bereits irgendwo in irgendeiner Form existiert. KI wird daher nicht zwangsläufig zu neuen, noch schrecklicheren Formen von Schadprogrammen führen. Aber wenn uns die Vergangenheit eines gezeigt hat, dann wohl, dass Akademiker, Tech-Nerds und Cyberkriminelle gar keine KI-Tools brauchen, um innovative Wege zu finden, um IT zu stören und zu zerstören.



Den Artikel finden
Sie auch online

swisscybersecurity.net

heimg - stock.adobe.com



Die Kunst, so zu schreiben, dass fast niemand es versteht

Seit der Mensch zu schreiben gelernt hat, will er auch verbergen, was er geschrieben hat. Mit dem Computer änderte sich die Art zu verschlüsseln jedoch grundlegend. Am Horizont bahnt sich aber schon die nächste Umwälzung an: Was heute als sicher gilt, könnte schon bald von Quantencomputern geknackt werden. Autor: Coen Kaat

Etwas so aufzuschreiben, dass keiner es versteht, ist nicht schwierig. Mit ein bisschen Kreativität und einer ordentlichen Portion Willkür schafft man sogar sehr schnell eine unknackbare Verschlüsselung. Bedauerlicherweise ist dies jedoch genauso unnütz wie einfach. Die wahre Kunst ist es nämlich, etwas so zu verschlüsseln, dass niemand es lesen kann – ausser den Personen, für welche die Nachricht bestimmt ist.

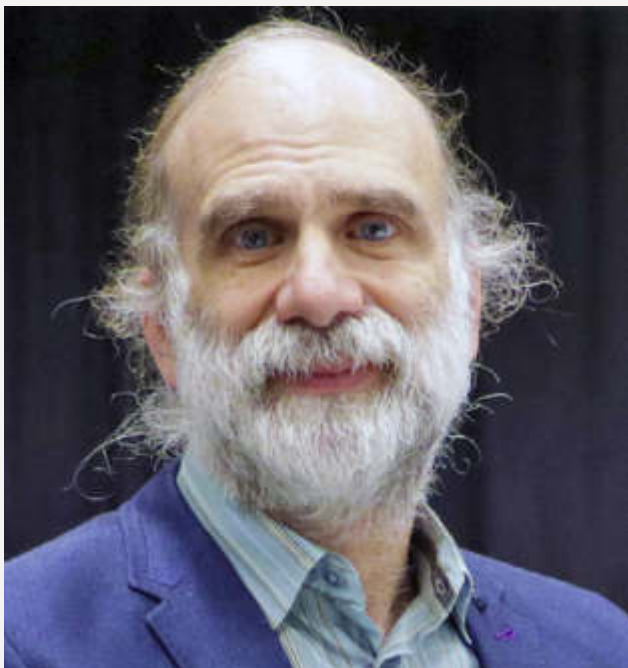
Damit das Gegenüber eine verschlüsselte Nachricht auch wieder entschlüsseln kann, benötigt der Chiffriervorgang, also die Verschlüsselung, eine gewisse Systematik. Je systematischer der Prozess ist, desto einfacher ist auch die Entschlüsselung durch Unbefugte. Mit dieser Zwickmühle befasst sich die Menschheit schon seit tausenden Jahren – wohl schon seit der Mensch gelernt hat, etwas aufzuschreiben. So gibt es etwa Beispiele alt-ägyptischer religiöser Texte, die (wohl um gewisse Tabus zu wahren) verschlüsselt niedergeschrieben wurden.

Ein bekanntes Beispiel, das auch heute noch eine gewisse Relevanz besitzt, ist die sogenannte Caesar-Chiffre. Dabei handelt es sich um ein simples Substitutionsverfahren, das Gaius Iulius Caesar gemäss Sueton schon vor über 2000 Jahren nutzte. Um eine Nachricht zu verschlüsseln, werden die Buchstaben um einen bestimmten Wert im Alphabet verschoben – dieser Wert ist der Schlüssel. Nimmt man also den Schlüssel 5, wird aus dem Ursprungstext «SWISSCYBERSECURITY.NET» neu «XBNXXHDG-JWXJHZWNYD.SJY» oder auch «XBNXX HDGJW XJHZW NYDSJY», wenn man es – wie bei verschlüsselten Botschaften üblich – we-

niger offensichtlich niederschreiben will. Um daraus wieder einen lesbaren Klartext zu machen, muss man die Buchstaben des Chiffrats, also des verschlüsselten Textes, wieder um den Wert 5 verschieben – einfach in die andere Richtung.

Die Caesar-Chiffre findet sogar in der digitalen Welt noch Verwendung, und zwar als ROT13. Dabei werden die einzelnen Buchstaben um den Wert 13 verschoben. Diese Methode gehört etwa zu den Basis-Tools vieler Linux- und Unix-Betriebssysteme – und auch Windows XP nutzte ROT13 für gewisse Registrierungsschlüssel. Ferner wird das Verfahren vor allem bei Onlineforen genutzt, um etwa Spoiler oder Pointen zu verschleiern. Der Wert 13 ist kein Zufall. Da das lateinische Alphabet aus 26 Buchstaben besteht, lässt sich ein Text mit demselben Algorithmus ver- und auch wieder entschlüsseln. Denn in beiden Fällen verschiebt man das Alphabet um jeweils 13 Stellen.

Eine echte Verschlüsselung bietet die Caesar-Chiffre und somit auch ROT13 nicht. Da auch hier wieder gilt: Der Geheimtext lässt sich leicht knacken – auch ohne technische Hilfsmittel. Je länger das Chifftrat, desto einfacher ist es, die Botschaft zu entschlüsseln. Dafür muss man lediglich wissen, wie oft bestimmte Buchstaben in einer Sprache vorkommen. Der häufigste Buchstabe in deutschen Texten ist gemäss Duden etwa das «e» mit über 12 Prozent. Darauf folgen «n» und «r» mit jeweils über 8 Prozent. Um den Text zu knacken, muss man nur die Buchstaben zählen. Da ROT13 überhaupt keinen echten Schutz bietet, ist das Verfahren daher in gewissen Kreisen selbst zur Pointe geworden.



Bruce Schneier, Sicherheitsexperte.

Etwa, wenn man sich über eine schwache Verschlüsselung lustig machen will.

Von DES zu AES

Mit dem Aufkommen des Computers änderten sich diese jedoch grundlegend. War man zuvor noch daran gebunden, die Buchstaben an sich zu verschlüsseln, wirkt die moderne, IT-basierte Verschlüsselung auf der Ebene der einzelnen Bits. Das heisst, dass etwa auch Bilder mit denselben Methoden verschlüsselt werden können wie Texte.

Eine der wichtigsten Fragen bei modernen Verschlüsselungsverfahren ist, ob man einen symmetrischen oder asymmetrischen Schlüssel verwendet. Bevor der Mensch seine eigene Rechenleistung mit dem Computer zu steigern begann, waren alle Verschlüsselungsverfahren symmetrisch. Das heisst, dass eine codierte Nachricht stets mit demselben Schlüssel entschlüsselt wurde, den man zuvor auch benutzte, um den Text zu verschlüsseln.

Computer wurden zwar schon seit dem Zweiten Weltkrieg für die Entschlüsselung von geheimen Botschaften genutzt. Dennoch dauerte es fast 30 Jahre, bevor die ersten computergestützten Verschlüsselungsverfahren aufkamen, die eine weite Verbreitung erreichten. Zu den frühesten Beispielen gehört die symmetrische Verschlüsselung DES. Die Abkürzung steht für Data Encryption Standard. Das Verfahren wurde in den 1970er-Jahren von IBM entwickelt und 1976 als Standard zugelassen. Auch die NSA, der Auslandsgeheimdienst der Vereinigten Staaten, wirkte daran mit. Kritische Stimmen behaupteten damals, die NSA kompromittiere die Sicherheit des Standards, damit sie die Verschlüsselung insgeheim knacken könnte.

Tatsächlich machten die Optimierungen der NSA den Standard besser. Die akademische Gemeinschaft brauchte einfach

zwei Jahrzehnte, um dies zu erkennen, wie der Cybersecurity-Experte Bruce Schneier später sagte. «Das bedeutet, dass die Nationale Sicherheitsbehörde in den 70er-Jahren dem Stand der Technik um zwei Jahrzehnte voraus war», verriet er 2004 in einem Interview mit «Cnet». Diesen Vorsprung, sagte er, habe die akademische Gemeinschaft jedoch schon fast wieder aufgeholt.

Während 30 Jahren war DES der Standard im Bereich der Verschlüsselungstechnologie. Das Verfahren setzte jedoch auf eine relativ kurze Schlüssellänge von lediglich 56 Bit. Dies war ebenfalls dem NSA zu verdanken. Das heisst, dass es insgesamt 72 057 594 037 927 936 mögliche Schlüssel gibt. Das mag nach viel klingen. Für einen Computer ist es aber nur eine Frage der Zeit, bis er mit einer Brute-Force-Attacke, also dem systematischen Ausprobieren aller möglichen Schlüssel, eine Nachricht entschlüsselt. 1997 wurde DES daher im Rahmen eines Wettbewerbs erstmals öffentlich geknackt.

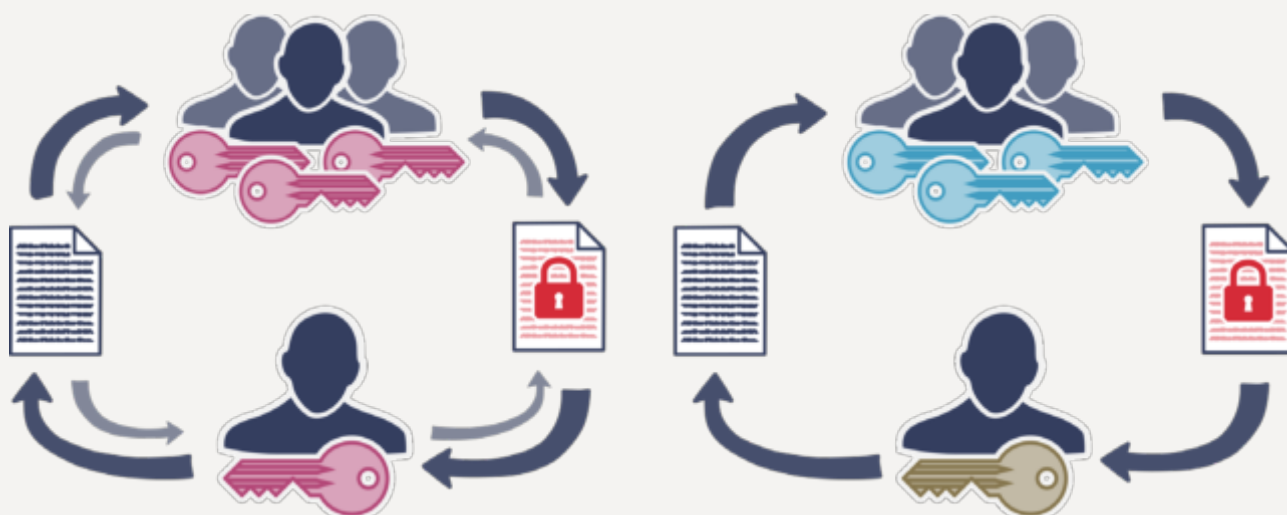
Im Jahr 2000 wurde DES schliesslich von AES abgelöst – dem Advanced Encryption Standard, auch bekannt als Rijndael. Der neue Standard ist ebenfalls symmetrisch, verwendet aber deutlich längere Schlüssellängen von 128, 192 oder 256 Bit. Eine korrekt implementierte, volle Verschlüsselung mit AES kann mit den heutigen Mitteln nicht geknackt werden. Jedenfalls sind gegenwärtig keine praktischen Angriffsmöglichkeiten bekannt.

Bei der Verschlüsselung wird der Text in einzelne Blöcke von 128 Bit aufgeteilt. Die Blöcke werden in einer Tabelle dargestellt und in mehreren aufeinanderfolgenden Runden verschlüsselt. Jede Runde erhält einen eigenen Schlüssel, der aus dem Originalschlüssel berechnet wird. In einer Runde werden zunächst alle Bytes ausgetauscht. Was dabei durch was ersetzt wird, bestimmt die sogenannte S-Box. Anschliessend werden die Zeilen verschoben und danach die Daten innerhalb der Spalten vermischt, bevor ein neuer Schlüssel generiert wird und der ganze Prozess erneut beginnt.

Das Schlüsselverteilungsproblem

Ein symmetrisches System bedingt natürlich, dass Absender und Empfänger einer Nachricht denselben Schlüssel haben. Bevor man miteinander kommunizieren kann, müssen beide Parteien also zunächst diesen Schlüssel teilen. Und den Schlüssel zu teilen – egal ob digital oder analog – bringt immer das Risiko mit sich, dass dieser in die falschen Hände gerät. Je grösser die Anzahl der Nutzer, desto grösser das Risiko eines Schlüsselverlusts. Und falls das passiert, ist auch die beste Verschlüsselung vollkommen nutzlos.

Asymmetrische Verfahren sollen dieses sogenannte Schlüsselverteilungsproblem lösen. Der erste Schritt: Der Schlüssel wird breit gestreut. Jeder, der eine Nachricht senden will, soll auch einen Schlüssel haben. Aus diesem Grund wird der Schlüssel auch als Public Key bezeichnet. Mit diesem lassen sich Nachrichten allerdings nur verschlüsseln. Um sie zu entziffern, braucht der Empfänger einen anderen Schlüssel, den Private Key. Da dieser nicht genutzt wird, um etwas zu verschlüsseln, kann der Empfänger den privaten Schlüssel für sich behalten und trotzdem verschlüsselt mit anderen Personen kommunizieren.



Bei symmetrischen Verschlüsselungen (links) wird eine Nachricht mit demselben Schlüssel codiert und auch wieder entziffert.

Bei asymmetrischen werden dafür unterschiedliche Schlüssel genutzt: der Public Key und der Private Key.

Diese Form der Verschlüsselung beruht auf sogenannten Falltür-beziehungsweise Trapdoor-Einwegfunktionen. Dabei handelt es sich um mathematische Funktionen, die sich in eine Richtung einfach berechnen lassen. Die Umkehrfunktion ist hingegen schwer oder unmöglich zu berechnen – es sei denn, man besitzt eine gewisse Zusatzinformation. Obwohl dieses Prinzip seit Jahrzehnten genutzt wird, gibt es noch keinen mathematischen Beweis dafür, dass solche Funktionen tatsächlich existieren.

RSA – auf den Schultern von riesigen Primzahlen

Zu den wohl bekanntesten Beispielen einer asymmetrischen Verschlüsselung gehört RSA. Die Methode blickt ebenfalls auf eine rund 50-jährige Geschichte zurück. 1976 publizierten die US-amerikanischen Kryptologen Whitfield Diffie und Martin Hellman ihr Konzept eines asymmetrischen Verschlüsselungssystems mit einem öffentlichen und einem privaten Schlüssel. Was in ihrem Konzept jedoch noch fehlte, war die Einwegfunktion. Diese formulierten später Ron Rivest, Adi Shamir und Leonard Adleman vom Massachusetts Institute of Technology (MIT). Die Methode wird auch heute noch eingesetzt – allerdings schwindet ihre Popularität. Denn jeder Fortschritt in der Rechenleistung von Computern tastet zugleich die Sicherheit von RSA an.

Das Verschlüsselungsverfahren basiert auf Primzahlen, immens grossen Primzahlen. Gegenwärtig liegt die standardmässige Schlüssellänge bei 2048 Bit. Diese Zahlen miteinander zu multiplizieren, ist noch immer relativ einfach. Aber dieses Produkt zu faktorisieren, also zurück in seine Primfaktoren zu zerlegen, ist sehr viel rechenintensiver. Die Umkehrung benötigt folglich Zeit, und sofern sie mehr Zeit braucht als die erwartete Lebensdauer der codierten Nachricht, gilt das System als sicher.

Die Post-Quanten-Kryptografie

Das Problem moderner Verschlüsselungssysteme ist, dass sie in der Regel auf Rechenaufgaben basieren. Die Rechenleistung konventioneller Computer steigt jedoch jährlich. Und die ersten

Gehversuche im Bereich der Quantencomputer stellen diese Leistungen auch noch in den Schatten. Was heisst das nun für Verschlüsselungslösungen? Gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) machen leistungsfähige Quantencomputer praktisch alle heutigen Public-Key-Verfahren unsicher. Symmetrische Verfahren stehen zwar etwas besser da. Der russische IT-Security-Anbieter Kaspersky etwa ist überzeugt, dass AES auch Quantencomputern standhalten könnte. Für die Schlüsselverteilung setzen symmetrische Verfahren jedoch oft auf Public Keys. Das heisst, dass auch hier der Status quo künftig nicht genügen wird. Das heisst aber auch, dass sämtliche bisher verschlüsselten Dokumente ab dem Zeitpunkt nicht mehr geschützt sein werden.

Wann es so weit sein wird, ist schwierig vorherzusagen. Dafür bräuchte es einen Quantencomputer mit Tausenden oder Millionen von Qubits sowie niedrigen Fehlerraten, wie der Europäische Datenschutzbeauftragte (EDSB) in einem aktuellen Bericht schreibt. In absehbarer Zukunft sei dies wohl nicht realistisch. Zum Vergleich: IBM will bis 2023 einen 1121-Qubit-Prozessor lancieren. Die Post-Quanten-Kryptografie befasst sich dennoch schon heute mit der Verschlüsselung in der Ära der Quantencomputer. Die ersten Ansätze für solche Lösungen existieren bereits. Und auch das National Institute of Standards and Technology (NIST) der USA arbeitet schon an einem Standardverfahren. Bis spätestens 2024 soll dieses definiert sein.

Quantencomputer werden die Art, wie Daten verschlüsselt werden, massiv verändern. Was heute als sicher gilt, wird vielleicht schon in wenigen Jahren antiquiert sein. Aber eines ist klar: Im Gegensatz zur Meinung einiger werden Quantencomputer gewiss nicht das Ende der Verschlüsselung sein. Sondern der Anfang einer neuen Form der Cybersecurity.



Den vollständigen Artikel finden Sie online
swisscybersecurity.net

Wir feiern 5 Jahre SwissCybersecurity.net

Seit fünf Jahren berichtet SwissCybersecurity.net täglich über Cybersecurity und Cybercrime: von aktuellen Warnungen über kriminelle Machenschaften bis hin zu neuen Strategien zur Abwehr von Ransomware, DDoS-Attacken und Co. Zum Jubiläum blicken Leserinnen und Leser, Partner und Kunden zurück und teilen ihre Erfahrungen. Autor: Coen Kaat

«Alles Gute zu eurem Jubiläum, SwissCybersecurity.net. Als Lead Advisory Board von iBarry – der Plattform für Internetsicherheit – schätze ich den praxisnahen Austausch sehr. Ich freue mich auf die nächsten gemeinsamen Schritte, um die Bevölkerung für digitale Risiken zu sensibilisieren.»

Marcus Beyer,
Lead Advisory Board iBarry & Security-Awareness-Expert, Swisscom



«Fünf Jahre SwissCybersecurity.net! Ein starkes Fundament für die IT-Branche. Danke für die inspirierende Plattform und die partnerschaftliche Zusammenarbeit. Gemeinsam bauen.»

Simone Böttcher,
Manager of Channel Marketing, Eset

«Herzliche Gratulation zum fünfjährigen Bestehen! Ich schätze den offenen Dialog, das sichere Gespür für relevante Themen und die vertrauensvolle Zusammenarbeit sehr. Als wichtiger Partner der Swiss Internet Security Alliance ist SwissCybersecurity.net für mich eine wertvolle Plattform für den Austausch und die Vernetzung in der Schweizer Cybersecurity-Community.»

Katja Dörlemann,
Präsidentin Swiss Internet Security Alliance (SISA) & Human Centred Security Expert, Switch



«Herzlichen Glückwunsch zu fünf Jahren SwissCybersecurity.net! Danke für euren kontinuierlich starken, relevanten Content und den wertvollen Beitrag zur Schweizer Cyber-Community. Ihr schafft Orientierung, Awareness und Austausch im Markt – weiter so, auf die nächsten fünf Jahre voller Impact!»



Peter Kosel,
Gründer & Talent Community Manager, Cyberunity



«Fünf Jahre SwissCybersecurity.net – herzliche Gratulation an das ganze Team! Von Beginn an hat es zwischen uns gefunkt und seither funktioniert die Zusammenarbeit mit euch schlichtweg hervorragend. Wir schätzen sie sehr und freuen uns auf viele weitere Jahre. Viel Erfolg auf dem weiteren Weg!»

Manuel Kugler,
Programm-Manager Daten & KI / Advanced Manufacturing,
Schweizerische Akademie der Technischen Wissenschaften (SATW)

«Fünf Jahre SwissCybersecurity.net stehen für Orientierung in einem immer komplexeren Cyber-Umfeld. Als IT-Partner für Unternehmen und den öffentlichen Sektor erleben wir täglich, wie zentral diese Orientierung für digitale Souveränität ist. Die Plattform verbindet Expertise, Praxisnähe und Dialog. Genau das braucht die Schweiz, um digital zukunftsstark zu bleiben. Herzliche Gratulation und weiterhin viel Wirkungskraft.»



Martin Kull,
Vice President, Bechtle Holding Schweiz



«Herzlichen Glückwunsch zum Jubiläum! In diesen fünf Jahren, die wir von Anfang an begleitet haben, hat sich SwissCybersecurity.net zu einem festen Bestandteil der Branche entwickelt. Ihr seid mit der Berichterstattung immer am Puls der Zeit. Besonders schätzen wir die offene Zusammenarbeit. Macht weiter so!»

Cornelia Lehle,
Head of Sales, G DATA CyberDefense

«Herzliche Gratulation an das Team von SwissCybersecurity.net! In der heutigen Zeit sind lokale, unabhängige Redaktionen wichtiger denn je. Gerade im Bereich der Cybersecurity, die durch KI zusätzlich befeuert wird, sind einordnende Nachrichten und Hintergrundinformationen äusserst wertvoll.»

Edgar Lehmann,
Chief Financial Officer, SPIE Schweiz



«Herzliche Gratulation zum fünfjährigen Jubiläum! SwissCybersecurity.net ist für mich als CISO eine wertvolle Plattform, um Cyber-Entwicklungen zu verfolgen, Perspektiven zu gewinnen und Risiken realistisch zu bewerten. Praxisnah, unabhängig und relevant für Entscheidungsträger. Viel Erfolg weiterhin!»

Sascha Maier,
Group CISO, SV Group

«Herzlichen Glückwunsch an das ganze Team von SwissCybersecurity.net zu fünf Jahren als verlässliche Referenz für fundierte Cybersecurity-Insights in der Schweiz – mit Substanz, Kontext und fachlicher Tiefe. Danke für Qualität, klare Orientierung und die stets angenehme Zusammenarbeit.»

Sandro Nafzger,
CEO, Bug Bounty Switzerland





«Herzlichen Glückwunsch zum Jubiläum. Ich kann mich noch gut an die ersten Gespräche und eure erste Vorstellung von SwissCybersecurity.net erinnern. Schon damals war ich überzeugt, dass damit eine spannende und qualitativ hochwertige Plattform für alle an Cybersecurity Interessierten geschaffen wird.»

Daniel Schmutz,
Head of Partner Management & Marketing, Adnovum

«Fünf Jahre starke Arbeit! Gerade in der Cybersecurity braucht es Fakten statt Buzzwords. Eure News und Einordnungen sind präzise, relevant und auf den Punkt gebracht. Ich schätze die Inhalte ebenso wie die professionelle, unkomplizierte Zusammenarbeit mit der Redaktion. Herzliche Gratulation und auf viele weitere Jahre!»

Sylvana Zimmermann,
stellvertretende Geschäftsführerin, Jenni Kommunikation



«Herzliche Gratulation zum fünfjährigen Jubiläum! SwissCybersecurity.net steht für Kompetenz, Praxisnähe und Vertrauen. Die Plattform verbindet technisches Know-how und schafft echten Mehrwert. Ein verlässlicher Partner, wenn es um nachhaltige Cybersicherheit geht.»

Marcel Zumbühl,
Co-Präsident, ISSS

Das Who's who der Malware

Die Namen von Schadprogrammen decken ein breites Spektrum ab: von einschüchternd (wie etwa Olympic Destroyer) über kryptisch (Necurs) bis hin zu nerdy (Kirk). Das Who's who der Malware gibt einen schnellen Überblick darüber, was hinter den Namen steckt. Autor: Coen Kaat

Das Botnetz **Andromeda** gehörte zu den grössten seiner Art. Es war vor allem in Europa, Nordamerika und Asien aktiv; in der Schweiz gemäss dem Bundesamt für Polizei (Fedpol) jedoch kaum. Anfang Dezember 2017 zerschlugen Ermittler aus neun Ländern in Zusammenarbeit mit dem FBI das Botnetz.

@
a

Bootkitty kann auf infizierten Rechnern die Firmware auf dem Motherboard beeinflussen. Erstaunlicherweise befällt das UEFI-Bootkit Linux-Systeme. Das Hauptziel des Schädlings besteht darin, die Signaturprüfungsfunktion des Kernels zu deaktivieren und zwei Binärdateien vorzuladen.

/
b

Der Computerwurm **Conficker** tauchte erstmals im Oktober 2008 auf. Er dringt über eine Sicherheitslücke im Serverdienst in Windows-Systeme ein. Noch im selben Monat wurde die Lücke von Microsoft geschlossen. Trotzdem taucht der Wurm auch 15 Jahre später noch auf und infiziert jährlich Millionen von Systemen.

+
c

"
l

Was lange nur ein theoretisches Schreckgespenst war, wurde Ende 2018 bedrohlich real. Die Malware **Lojax** hockt nicht auf der Festplatte oder im Betriebssystem, sondern im UEFI-Modul direkt auf dem Mainboard eines Rechners.



Mehr online

Das Internet – unendliche Weiten. Wir schreiben das Jahr 2016. Dies sind die Abenteuer der Ransomware **Kirk**, die unterwegs ist, um neue Rechner zu infizieren, neue Opfer zu erpressen und sehr viel Lösegeld zu fordern ...

'
k

4
r

2010 haben Unbekannte den Wurm **Ramnit** derart massiv und aggressiv verbreitet, dass heute noch Geräte damit infiziert sind. Obwohl die Behörden 2015 gegen die Drahtzieher vorgegangen sind und gar nicht klar ist, ob überhaupt noch irgendwer die Zügel in der Hand hält.

Olympic Destroyer ist der Name einer breit angelegten Sabotagekampagne. Der Wurm frass sich durch die IT der Organisatoren, Zulieferer und Partner der Olympischen Winterspiele 2018 im südkoreanischen Pyeongchang. Die Drahtzieher stammen vermutlich aus China oder Nordkorea.

9
o

(
h

Die Malware **HeroRAT** infiziert seit Juni 2018 Smartphones. Der mobile Trojaner ist in App-Stores von Drittanbietern zu finden. Die Malware verschafft dem Angreifer kompletten Zugriff auf das Handy. Um unbemerkt zu kommunizieren, nutzt HeroRAT das Protokoll der Messenger-App Telegram.

*
g

Die Ransomware **Gandcrab** gehört zu den aggressiveren Exemplaren ihrer Art. Bekannt wurde sie jedoch vor allem wegen des Streits, den der Entwickler mit dem südkoreanischen Sicherheitsanbieter Ahnlab anzettelte. Ahnlab hatte zuvor ein Tool veröffentlicht, das Gandcrab-Infektionen verhindert.

Der Schädling **Simjacker** kommt über präparierte SMS-Nachrichten auf die Handys seiner Opfer. Die Nachrichten enthalten SIM-Toolkit-Befehle, die auf der SIM-Karte ausgeführt werden. Dort nistet sich die Spyware anschliessend ein. Dies funktioniert nur mit Karten, die mit dem S@T-Browser bestückt sind.

Si
n

Necurs gehört zu den grössten Botnetzen der Welt. Es wird vor allem mit der Ransomware Locky in Verbindung gebracht. Necurs verschwindet immer wieder mal vom Netz. Anfang 2016 glaubten einige sogar, Necurs sei endgültig abgeschaltet worden. Doch das Botnetz kam immer zurück – stärker als zuvor.

Coinhive wurde eigentlich als legitime Alternative zur Werbung konzipiert. Der Dienst lässt sich leicht in Websites einbauen. Wer diese besucht, zahlt mit seiner Rechenleistung, sodass Coinhive nach Kryptowährungen schürfen kann. Oft geschieht dies jedoch ohne Zustimmung des Nutzers.

+
C

Die hochansteckende Ransomware **Wannacry** katapultierte das Thema IT-Security in den Alltag aller. Das Erpresserprogramm befahl im Mai 2017 über 230 000 Computer weltweit. Obwohl Wannacry eine damals schon behobene Schwachstelle ausnutzte, fielen ihr auch im Sommer 2018 noch Rechner zum Opfer.

2
W

Eigentlich will **XMRig** ja nichts Böses. Statt Werbung zu sehen, sollen Website-Besucher mit einem Teil ihrer Rechenleistung zahlen. Skripts wie XMRig nutzen diese, um nach Kryptowährungen zu schürfen. Dies geschieht jedoch leider oft ohne Zustimmung oder Wissen des Nutzers.

-
X

Im August 2016 machten Sicherheitsforscher eine beunruhigende Entdeckung: die Spionageplattform **Projectsauroon** – benannt nach dem Bösewicht aus der Buch- und Filmreihe «Der Herr der Ringe». Ein hochkomplexes Stück Software, das auf langfristige und heimliche Kampagnen ausgelegt ist.

6
y

Oftmals teilen sich Cyberkriminelle die Arbeit: Die einen beschaffen sich Zugang, die anderen infizieren. Die atypische Ransomware **Ymir** hingegen erledigt alles selbst. Sie nutzt zudem eine ungewöhnliche Kombination aus Funktionen, um Schadcode direkt im Speicher auszuführen.

o
p

Industroyer (auch als Crashoverride bekannt) ist der erste bekannte Fall einer Malware, die spezifisch das Stromnetz eines Landes angreift. Zu diesem Zweck infiziert sie industrielle Steuerungssysteme. Das Schadprogramm kam vermutlich auch im Rahmen von Russlands Annexion der Krim zum Einsatz.

8
i

Emotet wurde erstmals 2014 beobachtet. Der E-Banking-Trojaner war zunächst nur in der Schweiz, Deutschland und Österreich aktiv, schwappte aber bald auch in die USA über. Wie seine Artgenossen versteckt sich Emotet gerne in PDFs und anderen E-Mail-Anhängen, die vorgeben, Rechnungen zu sein.

3
e

Mit vollem Namen heisst diese Ransomware **Barack Obama's Everlasting Blue Blackmail Virus** und sie hat einen Heissunger auf .exe-Dateien im Windows-Systemordner. Für gewöhnlich meiden Ransomware-Programme diesen Ordner, um keine ungewollten Systemabstürze zu verursachen.

/
b

Stuxnet (auch bekannt als «RootkitTmphider») wurde speziell für Angriffe auf industrielle Überwachungssysteme von Siemens entwickelt. Beobachtet wurde der Computerwurm erstmals 2009. Unbekannte nutzten ihn, um etwa das iranische Atomprogramm zu stören. Wer dahintersteckte, ist noch nicht geklärt.

S

Sicherheit, die Innovation ermöglicht

Consulteer InCyber unterstützt als erste Schweizer Firma Unternehmen dabei, die Risiken von KI-Systemen umfassend zu managen und zu minimieren. Dabei werden Security Consulting und leistungsfähige Managed Security Services kombiniert, um AI Security zuverlässig zu etablieren.

Das Ziel ist klar: Unternehmen fundierte Antworten auf ihre Cybersecurity-Fragen zu geben. Dafür verbindet Consulteer InCyber strategische Beratung, Architekturkompetenz und operativen Sicherheitsbetrieb in einem konsolidierten Ansatz. Organisationen werden von der Sicherheitsstrategie über Architektur und Integration bis zum laufenden Betrieb begleitet – inklusive Managed Services für SASE (Secure Access Service Edge), WAAP (Web Application & API Protection) und IAM (Identity & Access Management).

Im Fokus stehen die Reduktion von Komplexität, die Konsolidierung von Sicherheitsfunktionen und klare Verantwortlichkeiten im Betrieb. Sicherheit wird dabei ganzheitlich betrachtet: Neben IT-Systemen fließen auch Geschäftsprozesse, organisatorische Strukturen und regulatorische Anforderungen ein – etwa bei OT-Security, im Kontext des Cyber Resilience Act oder bei ISO-27001-Implementierungen. KI-Sicherheit ist eine konsequente Erweiterung dieses Ansatzes. Ziel ist es, KI-Systeme sicher einzusetzen und Risiken frühzeitig zu adressieren, ohne die Innovationsfähigkeit und Agilität zu verlieren.

KI-Sicherheit als neue zentrale Herausforderung

KI verändert, wie Unternehmen Entscheidungen treffen, Prozesse steuern und mit Kunden interagieren. Dabei entstehen neue Risiken: Sensible Daten können über Prompts in öffentliche KI-Modelle gelangen, APIs schaffen zusätzliche Angriffsflächen, und automatisierte KI-Entscheidungen können Prozesse oder Compliance-Anforderungen beeinflussen.

Consulteer InCyber unterstützt Unternehmen dabei, diese Risiken systematisch zu adressieren und KI-Systeme sicher einzusetzen. In der Praxis bedeutet das, den Abfluss sensibler Daten in öffentliche KI-Modelle zu verhindern, eigene KI-Anwendungen und APIs abzusichern und klare Regeln für den Einsatz von KI-Tools zu definieren. So entsteht die notwendige Transparenz und Kontrolle, um künstliche Intelligenz verantwortungsvoll zu nutzen und gleichzeitig die Innovationsfähigkeit zu erhalten.

Sicherheitsarchitektur statt Tool-Vielfalt

Erfolgreiche Cybersecurity hängt nicht von der Anzahl eingesetzter Tools ab, sondern von einer konsistenten Sicherheitsarchitektur.

Für zentrale Disziplinen wie SASE, IAM, WAAP und AI Security arbeitet Consulteer InCyber mit sorgfältig ausgewählten Technologiepartnern, die in ihren Bereichen führend sind. Best-of-Breed-

Technologien werden dabei mit klarer Verantwortung pro Lösung verbunden. So lassen sich komplexe Sicherheitsanforderungen effizient umsetzen und gleichzeitig eine unabhängige, lösungsneutrale Beratung sicherstellen. Technologie, Architektur und Betrieb greifen nahtlos ineinander.

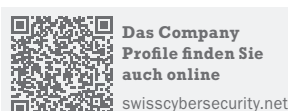


zen und gleichzeitig eine unabhängige, lösungsneutrale Beratung sicherstellen. Technologie, Architektur und Betrieb greifen nahtlos ineinander.

KI sicher betreiben – von der Strategie bis zum Betrieb

KI-Sicherheit entwickelt sich zu einem zentralen Bestandteil moderner Cybersecurity-Strategien. Neben konzeptioneller Beratung ist vor allem die Umsetzung im Betrieb entscheidend. Consulteer InCyber begleitet Organisationen entlang des gesamten Prozesses – von der KI-Sicherheitsstrategie über Architektur und Implementierung bis zum Betrieb moderner Managed Security Services. So lassen sich KI-Systeme verantwortungsvoll einsetzen, regulatorische Anforderungen erfüllen und gleichzeitig Innovationsfähigkeit sichern. Wer verstehen möchte, wie sich KI-Risiken in der Praxis kontrollieren lassen, findet bei Consulteer InCyber erfahrene Ansprechpartner für Strategie, Architektur und Betrieb moderner Sicherheitslösungen.

Weitere Informationen finden Sie hier:



Consulteer InCyber AG

Riedweg 6
CH-6045 Meggen
+41 41 377 22 66
incyber@consulteer.com

About
Consulteer
InCyber:



KI-Brille von Meta leitet intime Videos nach Kenia

Was die KI-Brille von Meta aufnimmt, kann auf den Bildschirmen von Mitarbeitenden eines Meta-Subunternehmers in Kenia landen. Diese müssen mitunter private und intime Videoclips sichten, um die KI zu trainieren. Die Enthüllungen werfen gravierende Fragen zu Datenschutz und Transparenz auf und zeigen eine deutliche Diskrepanz zwischen Werbeversprechen und Realität. Autor: Joël Orizet, Netz-KI Bot



Den vollständigen Artikel finden Sie online

swisscybersecurity.net

Meta vermarktet seine Ray-Ban-Datenbrille als stylischen Allround-Helfer, der mithilfe von Kamera, Mikrophon und KI-Assistent den Alltag erleich-

tern soll. Doch zumindest ein Teil von dem, was diese Brillen aufzeichnen, landet auf den Bildschirmen von Angestellten eines Meta-Subunternehmens in Kenia. Wie eine Recherche der schwedischen Tageszeitungen «Göteborgs-Posten» und «Svenska Dagbladet» zeigt, sichten diese Mitarbeitenden auch äusserst private Inhalte.

Über 30 Angestellte des Meta-Dienstleisters Sama berichteten den Journalistinnen und Journalisten anonym von ihrer Arbeit. In bis zu 10-Stunden-Schichten trainieren sie als sogenannte Daten-Annotatoren die KI. Dabei sichten sie aufgezeichnete Inhalte und versehen sie mit Beschreibungen, Kategorien oder Warnhinweisen. Solche menschlich markierten Daten liefern generativen KI-Systemen die Grundlage, um Inhalte zu erkennen, einzuordnen und darauf zu reagieren.

Die Schilderungen der Angestellten zeichnen ein beunruhigendes Bild. «Wir sehen alles – von Wohnzimmern bis zu nackten Körpern», berichtet eine Person aus dem Team. Andere beschreiben Videos, in denen Menschen die Toilette benutzen oder sich ausziehen – offenbar ohne zu wissen, dass die Brille aufzeichnet. Sie sehen demnach auch sexuelle Handlungen, versehentlich gefilmte Bankkarten oder Personen, die beim Tragen der Brille Pornografie konsumieren.

Eine rein lokale Verarbeitung der Daten ist unmöglich

Die KI-Funktionen erfordern eine aktive Internetverbindung. Eine Analyse des Netzwerkverkehrs belegte eine regelmässige Kommunikation mit Meta-Servern in Europa. Eine rein lokale Verarbeitung der Daten ist demnach nicht möglich.

Um die Brille überhaupt verwenden zu können, müssen User einwilligen, dass ihre Interaktionen mit der KI «manuell (menschlich)」 überprüft

werden können. Diese Datenverarbeitung erfolgt laut Nutzungsbedingungen automatisch und lässt sich nicht abschalten. Eine Wahlmöglichkeit, dieser menschlichen Überprüfung zu widersprechen, ist nicht vorgesehen.

Fachleute für Datenschutz kritisieren diese Praxis scharf. Kleanthi Sardeli von der Wiener Datenschutzorganisation NOYB erklärt gegenüber den schwedischen Zeitungen: «Wenn dies in Europa geschieht, fehlen sowohl die Transparenz als auch die Rechtsgrundlage für die Verarbeitung.» Ihre Organisation ist der Ansicht, dass für die Datennutzung zum KI-Training eine ausdrückliche Zustimmung erforderlich ist. Wie Netzpolitik.org berichtet, droht bei einer weiten Verbreitung der Brillen die kommerzielle Totalerfassung privater und öffentlicher Räume; bald könnte Meta das Gerät zusätzlich mit Gesichtserkennung aufrüsten.

Für die Übermittlung personenbezogener Daten aus der EU in ein Drittland wie Kenia setzt die Datenschutz-Grundverordnung (DSGVO) jedoch hohe Hürden. Derzeit existiert kein Angemessenheitsbeschluss der EU, der Kenia ein mit Europa vergleichbares Datenschutzniveau bescheinigt.

Auch OpenAI setzte übrigens für das Training der KI-Modelle hinter ChatGPT auf den Subunternehmer Sama. Die Firma beschäftigt Mitarbeitende in Kenia, Uganda und Indien, die Texte, Bilder und Videos nach höchst problematischen Inhalten durchsuchen und diese kennzeichnen sollen.

Was die «AI Glasses» von Meta und Ray-Ban aufzeichnen, kann bei Clickworkern in Kenia landen.



Cyberrisiken im Finanzsektor: Handlungsbedarf bleibt bestehen

Auch für das Jahr 2026 liefert der Finma-Risikomonitor klare Warnsignale. Demnach steht die Schweizer Finanzbranche weiter vor wachsenden Cyber-Herausforderungen. Entscheidend ist ein integrierter Ansatz für Schutz, Erkennung, Reaktions- und Widerstandsfähigkeit.

Die Finma legt im Risikomonitor 2025 offen, wo sie die grössten Gefahren für den Schweizer Finanzplatz sieht. Die aktuelle Risikolandschaft ist dabei von erhöhter Komplexität geprägt. Neben finanziellen Risiken nehmen nicht-finanzielle Risiken wie Cyberangriffe an Bedeutung zu. Entsprechend bleibt die Schweizer Finanzbranche auch 2026 ein bevorzugtes Ziel von Cyberkriminellen.

Finanzinstitute sind aufgrund ihrer hohen technologischen Vernetzung und ihrer Abhängigkeiten von externen Dienstleistern einem besonders hohen Risiko ausgesetzt. Gleichzeitig ist das Management von Cyberrisiken bei vielen Instituten noch immer unzureichend koordiniert. Die Organisation und Kontrolle der Cyber-Sicherheitsmassnahmen erfolgt häufig isoliert innerhalb der IT, ohne ausreichende Verankerung in der Governance, im Internen Kontrollsystem (IKS) oder im operationellen Risikomanagement.

Ein modernes Sicherheitskonzept besteht nicht aus einzelnen technischen Massnahmen, sondern aus aufeinander abge-



Der Autor

Tobias Schumacher,
Senior Risk Management Specialist für
Cyberrisiken, Finma

stimmt, risikobasierten Sicherheitsmechanismen. Gerade im Umgang mit externen Dienstleistern gibt es in der Praxis jedoch noch blinde Flecken: Anforderungen werden nicht durchgängig definiert, die Wirksamkeit von Sicherheitsmassnahmen nicht systematisch nachgewiesen und es fehlt oft eine lückenlose Einbindung in das Erkennungssystem. Auch Prüfberichte von Dienstleistern werden oft nicht konsequent auf Cyberrelevanz analysiert. Dadurch entstehen Lücken an zentralen Schnittstellen, die von Angreifern bewusst ausgenutzt werden. Die Fähigkeit, sicherheitskritische Ereignisse schnell zu identifizieren, zu priorisieren und einzudämmen, ist für die Widerstandsfähigkeit eines Instituts essenziell. Zwar verfügen viele Institute über eine SIEM-Lösung (Security Information and Event Management) zur Überwachung, doch fehlen oftmals institutsspezifische Anwendungsfälle, klare operative Zuständigkeiten in kritischen Situationen sowie regelmässige Tests der Reaktionsprozesse. Ohne eine konsistente Integration von Governance, Detektion und Reaktion bleibt die Wirksamkeit einzelner Lösungen begrenzt. Ein Alarm ist ineffektiv, wenn er nicht rechtzeitig bewertet und mit der entsprechenden Entscheidungsbefugnis adressiert wird.

Cyberresilienz ist längst zu einem Schlüsselfaktor für die Stabilität des Schweizer Finanzplatzes geworden. Die Frage lautet nicht mehr, ob oder wann ein Institut zum Ziel eines Cyberangriffs wird. Entscheidend ist, wie widerstandsfähig es in der Bewältigung des Angriffs ist, wie schnell die Erkennung erfolgt, wie wirksam die Eindämmung funktioniert und ob der kritische Geschäftsbetrieb verlässlich fortgeführt werden kann. Die Qualitätsunterschiede liegen nicht in der Technologie, sondern im Zusammenspiel von Governance, Risikokultur, technischem Schutz, Reaktionsfähigkeit und Wiederherstellungskompetenz. Die Institute verfügen über die notwendigen Grundlagen. Entscheidend ist, wie gut sie diese im Ernstfall einsetzen können.

Bild: VibrantVisionsStudio - stock.adobe.com



Den vollständigen
Artikel finden Sie
online
swisscybersecurity.net

Wie Peripheriegeräte zur Schwachstelle für kritische Systeme werden

Peripheriegeräte am digitalen Arbeitsplatz stellen eine unterschätzte Angriffsfläche dar. Das zeigt eine Analyse des Nationalen Testinstituts für Cybersicherheit. Das NTC identifizierte in diversen Geräten insgesamt 60 Schwachstellen, darunter schwerwiegende und kritische. Autorin: Valentina Graziano



EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG

Das NTC gibt fünf allgemeine Empfehlungen zur Reduktion der Risiken beim Einsatz von Peripheriegeräten:

- Standardisierung und sichere Beschaffung über vertrauenswürdige Kanäle
- Aufnahme von Peripheriegeräten in das IT-Lifecycle- und Asset-Management
- Netzwerksegmentierung für netzwerkfähige Geräte wie Konferenzsysteme
- Bevorzugung kabelgebundener Lösungen in Bereichen mit erhöhtem Schutzbedarf
- Sensibilisierung der Mitarbeitenden für physische und organisatorische Risiken

Eine Analyse des Nationalen Testinstituts für Cybersicherheit (NTC) entlarvt Büroarbeitsgeräte als Sicherheitsrisiko. Das Schweizer Institut untersuchte während eines Jahres 30 drahtlose wie auch kabelgebundene Tastaturen, Headsets, Webcams und Konferenzsysteme, wie es in einer Mitteilung heisst. Die Forschenden testeten Produkte, die an Schweizer Arbeitsplätzen häufig anzutreffen sind, insbesondere in kritischen Infrastrukturen eingesetzt werden und von etablierten Herstellern stammen, darunter Logitech, Yealink, Jabra, HP, Eizo und Cherry.

Das NTC entdeckte dabei 60 Schwachstellen, davon 13 schwerwiegende und 3 kritische. Modernere Peripheriegeräte wiesen zwar bei sicherer Konfiguration und aktueller Firmware ein akzeptables Sicherheitsniveau auf. Dennoch steige das Risiko mit zunehmender Komplexität, etwa bei Konferenzsystemen

oder anderen IoT-Geräten und beim Einsatz veralteter Funktechnologien.

Die identifizierten Sicherheitslücken hat das Testinstitut den betroffenen Herstellern gemeldet, woraufhin diese die Schwachstellen «mehrheitlich rasch behoben» haben, wie es in der Mitteilung weiter heisst. In einem Fall habe der Hersteller aber nicht reagiert: «Bei einem drahtlosen Präsentationssystem übergab das NTC den Fall an das Bundesamt für Cybersicherheit (BACS), das daraufhin eine öffentliche Warnung veröffentlichte», wie das Institut schreibt.



Den vollständigen
Artikel finden Sie
online
swisscybersecurity.net

ÜBER DIE ANALYSE

Die Untersuchung erfolgte laut Mitteilung im Rahmen einer gemeinsamen Initiative des NTC mit Unterstützung von Behörden auf Bundes- und Kantonsebene sowie Organisationen aus dem Finanzsektor. Im öffentlichen Bericht der Analyse hat das Nationale Testinstitut für Cybersicherheit bewusst auf technische Details und produktbezogene Schwachstellen verzichtet, wie es schreibt. Weiter heisst es: «Um die Unabhängigkeit der Resultate zu gewährleisten, waren die Hersteller der getesteten Geräte weder an der Auswahl noch an der Durchführung der Tests beteiligt und wurden erst im Rahmen der vertraulichen Meldung zur Behebung der Schwachstellen kontaktiert.»

Schnittstelle für Angreifer

Anhand eines realen Szenarios während einer Videokonferenz veranschaulicht das NTC in der Mitteilung, wie konkret diese Risiken sind. Über Tastaturen werden Passwörter eingegeben und über Mikrofone und Webcams vertrauliche Gespräche übertragen. Unsichere Peripheriegeräte ermöglichen es Angreifern, bestehende Schutzmassnahmen zu umgehen. Die Geräte sind eine kritische Schnittstelle, über die sensible Informationen fließen, wie das NTC erklärt. Die Kosten für professionelle Sicherheitsanalysen würden zudem den Anschaffungspreis solcher Geräte oft um ein Vielfaches übersteigen. Die Prüfstelle spricht von einer «gefährlichen Asymmetrie». «Peripheriegeräte werden in der Praxis oft als reines Zubehör betrachtet und entsprechend nicht systematisch geprüft sowie nicht konsequent in bestehende Sicherheitskonzepte integriert», sagt Tobias Castagna, Leiter Testexperten beim NTC.

Wenn KI-Agenten zu viel dürfen – die «Rule of Two» als Sicherheitsleitlinie

KI-Agenten sind keine Chatbots: Sie handeln autonom, nutzen Werkzeuge und treffen eigenständige Entscheidungen. Doch mit jeder zusätzlichen Fähigkeit steigt das Schadenspotenzial durch Prompt Injection. Ein Denkmodell aus der Forschung hilft, die Grenze zwischen Nutzen und Gefahr zu ziehen.

KI-Agenten sind ein absolutes Hype-Thema. Gleichzeitig sind sie für Nutzerinnen und Nutzer immer einfacher zugänglich: Bereits mit lokalen LLM-Apps, KI-Browsern oder Vibe-Coding-Tools haben sie die Möglichkeit, eigene Agenten zu erstellen und zu nutzen.

Vom Chatbot zum Agenten

Was diese KI-Agenten von Chatbots unterscheidet, lässt sich in einem Wort zusammenfassen: Agency. Im Gegensatz zu einem Chatbot, der lediglich auf Eingaben reagiert, interagiert ein Agent aktiv mit seiner Umgebung: Er ruft APIs auf, delegiert an Subagenten und entscheidet eigenständig über den Lösungsweg. Je mehr Fähigkeiten einem Agenten gegeben werden, desto grösser ist sein Schadenspotenzial.

Wie gefährlich das werden kann, zeigte OpenClaw: ein Agent mit vollem Systemzugriff, bei dem Sicherheitsforscher in 13,4 Prozent aller Skills kritische Schwachstellen fanden. Eine Zero-Click-Schwachstelle in Claude Desktop (CVSS 10/10) bewies zudem, dass auch kommerzielle Produkte nicht vor Prompt Injection gefeit sind.

Simon Willison beschreibt das Kernproblem als «lethal trifecta». Sobald ein Agent erstens Zugang zu vertraulichen Daten hat, zweitens nicht vertrauenswürdige Inhalte verarbeitet und drittens nach aussen kommunizieren kann, kann er dazu verleitet werden, auch private Daten nach aussen zu geben. LLMs können die Herkunft von Anweisungen einfach nicht zuverlässig beurteilen.

Daraus lässt sich die «Rule of Two» ableiten: Ein Agent sollte nicht mehr als zwei dieser drei Fähigkeitsklassen in einer Sitzung vereinen. Solange nur zwei zusammenkommen, bleibt das Risiko beherrschbar.

Das Problem: Leistungsfähigkeit wächst gerade durch die Kombination aller drei Klassen. Wer einschränkt, beschneidet in der Regel auch den Nutzen.

Identität und Gedächtnis als blinde Flecken

Nicht nur die Fähigkeiten selbst sind problematisch, sondern auch die Zugriffsrechte: Persönliche Agenten erben oft die vollen Rechte ihres Nutzers: Vergleichbar mit einem Praktikanten, der am ersten Tag den Generalschlüssel erhält. Statische API-Keys verschärfen das Problem, da sie keine kontextabhängige Zugriffskontrolle ermöglichen. Modernes IAM setzt stattdessen auf kurzlebige Credentials nach dem Just-in-Time-Prinzip.

Das Langzeitgedächtnis wird dabei oft vernachlässigt. Das Gedächtnis als weitestgehend vierte Fähigkeitsklasse kann die

Der Autor

Udo Schneider, Governance, Risk & Compliance Lead, Europe, TrendAI (ein Geschäftsbereich von Trend Micro)

Rule of Two unterlaufen, weil die eingeschleusten Instruktionen erst in einer späteren Sitzung «explodieren»: eine verzögerte Prompt Injection, die zum Zeitpunkt der Einschleusung harmlos erscheint.

Fazit: Pragmatismus statt Verbote

Es gibt keine Universallösung. Prompt Injection bleibt ein grundlegendes, ungelöstes Problem aller LLMs. Die Rule of Two ist dabei eine Ergänzung und kein Ersatz für bewährte Prinzipien wie Least Privilege. In der Praxis bedeutet das: risikobasierte Bewertung statt pauschaler Verbote, differenzierte Agenten mit abgestuften Berechtigungen und ein gesundes Misstrauen gegenüber dem Versprechen, ein einzelner Agent könne alles sicher erledigen. Denn sobald man Werkzeuge eigenständig kombiniert, kann kein Anbieter mehr Schutz garantieren.

KOMBINATION VON AGENTEN-FÄHIGKEITSKLASSEN – ZWEI SIND BEHERRSCHBAR, DREI WERDEN GEFÄHRLICH



Quelle: Trend Micro

«Nachträgliche Sicherheit ist in der Regel nicht erfolgreich»

Agentic AI verändert das Spiel: Statt nur Antworten auszugeben, planen und handeln KI-Agenten eigenständig über mehrere Systeme hinweg – mit mächtigen Tools, Langzeitgedächtnis und hoher Autonomie. Das macht sie extrem nützlich, aber auch zu einem wichtigen Thema für die Cybersecurity. Interview: Dylan Windhaber

Agentic AI ist derzeit in aller Munde. Was genau unterscheidet agentische Systeme von klassischen KI-Anwendungen?

Udo Schneider: Der zentrale Unterschied liegt eben in der «Agency». Ein KI-Agent agiert eigenständig: Er ruft APIs auf, nutzt Werkzeuge, delegiert Aufgaben an andere Agenten und trifft Entscheidungen. Er plant, entscheidet und handelt in mehreren Schritten und Systemen, oft im Namen der User. Ausserdem verfügt er über ein Gedächtnis, das über einzelne Sitzungen hinausgeht und es ihm ermöglicht, aus früheren Interaktionen zu lernen. All dies macht diese Systeme wesentlich leistungsfähiger als herkömmliche KI-Anwendungen, aber auch anfälliger für Risiken.

Welche Sicherheitsprobleme tauchen dabei auf?

Die OWASP-Top-10 für agentische Anwendungen deckt eine breite Vielfalt ab: vom Agent Goal Hijack, also der Manipulation von Agentenzielen durch Prompt Injection, über Tool-Missbrauch und Identitätsprobleme bis hin zu Memory Poisoning und kaskadierenden Fehlern in Multi-Agenten-Systemen. Ein Beispiel: Model Context Protocol, kurz MCP, wird als «USB für KI» beworben. Es ermöglicht aber auch, gefährliche Fähigkeiten in einem einzigen Tool zu kombinieren. Ein Exploit des MCP-Servers von Github hat genau dies gezeigt: Ein einziges Tool konnte öffentliche Issues lesen, auf private Repositories zugreifen und Pull Requests erstellen. Das ist die ideale Kombination für Datenexfiltration.

Woher rühren diese Probleme, und wie kann man sich schützen?

Das Grundproblem liegt in der «Lethal Trifecta»: Sobald ein Agent Zugriff auf vertrauliche Daten hat, nicht vertrauenswürdige Inhalte verarbeitet und nach aussen kommuniziert, kann er zur Datenexfiltration missbraucht werden. Das Hauptproblem dabei ist, dass LLMs nicht zuverlässig erkennen können, woher ein Befehl stammt. Die «Rule of Two» unterbricht diese Angriffskette. Das Langzeitgedächtnis von Agenten kann die Regel jedoch umgehen, wenn sich eingeschleuste Befehle erst in späteren Sitzungen manifestieren. Dann bietet die zeitliche Trennung der Fertigkeiten keinen Schutz mehr.

Gibt es auch konkrete Handlungsanweisungen?

OWASP schlägt für jedes Risiko konkrete Massnahmen vor. Ein zentrales Prinzip ist «Least Agency», das über «Least Privilege»



Udo Schneider,
Governance, Risk &
Compliance Lead,
Europe, TrendAI.

hinausgeht. Es geht dabei nicht nur um minimale Berechtigungen, sondern darum, unnötige Autonomie ganz zu vermeiden. Unnötiges Agentenverhalten vergrössert die Angriffsfläche ohne Nutzen. Dazu gehört auch die Überprüfung von IAM-Systemen: Sie müssen heute in der Lage sein, kurzlebige, aufgabenbezogene Berechtigungen für Agenten auszustellen, statt nur statischer API-Keys. Ebenso werden regulatorische Rahmenbedingungen künftig strengere Anforderungen an agentenbasierte Systeme stellen. So wird der EU AI Act auch Auswirkungen auf Schweizer Unternehmen haben. Darüber hinaus ist zukünftig auch mit spezifisch schweizerischer Gesetzgebung zum Thema zu rechnen.

Was würden Sie abschliessend empfehlen?

Keine Panik! Agentische Systeme sind grundsätzlich verteilte Systeme, ähnlich wie Microservices-Architekturen. Wir wissen, wie man diese Systeme absichert: durch Telemetrie, Zugriffskontrolle, Sandboxing und Zero-Trust-Modelle. Es gibt spezifische Aspekte wie Speicherverwaltung oder Kommunikation zwischen Agenten, aber auch dafür gibt es Lösungen, sowohl Open Source als auch kommerzielle. Wichtig ist, die Sicherheit von Anfang an zu berücksichtigen, auch wenn es in der heutigen Hektik schwierig erscheint. Denn nachträgliche Sicherheit ist in der Regel nicht erfolgreich.



Das Dossier finden
Sie auch online
swisscybersecurity.net

So verschärft KI das Problem von Kinderfotos im Netz

Viele Eltern posten regelmässig Fotos oder Videos ihrer Kinder in den sozialen Medien. Ungewollt entsteht so ein frei zugängliches Onlinearchiv, das zur Erstellung täuschend echter Deepfakes missbraucht werden kann. Autorin: Seraina Huber

Anfang 2026 hat der KI-Chatbot Grok auf dem Kurznachrichtendienst X (ehemals Twitter) für Aufsehen gesorgt: User erstellten mithilfe von KI sexualisierte Bilder von Erwachsenen und Minderjährigen – dies teilweise auf Basis bestehender Fotos. Laut einer Hochrechnung des «Center for Countering Digital Hate» wurden dabei innerhalb von elf Tagen rund 23 000 sexualisierte Kinderbilder generiert. Dies zeigt, wie niedrig die Hürden in diesem Bereich mittlerweile sind.

Der digitale Fussabdruck der Kleinsten

Wenn Eltern Fotos oder Videos ihrer Kinder im Internet veröffentlichen, bezeichnet man dies als «Sharenting» – ein Kofferwort aus «Sharing» und «Parenting». Was auf den ersten Blick wie eine schöne Momentaufnahme wirkt, kann schnell zu einer bleibenden Onlinepräsenz für ein Kind werden.

Eine Studie der Universität Fribourg aus dem Jahr 2023 zeigt, dass rund jeder zehnte Elternteil in der Schweiz regelmässig Bilder seiner Kinder online teilt. 45 Prozent fragen dabei ihre Kinder vor dem Posten nicht um Erlaubnis. Für die Stiftung Kinderschutz Schweiz ist dies problematisch: Ein Kind erhalte so einen digitalen Fussabdruck, «obwohl es diesem wohl in den wenigsten Fällen zugestimmt hat». Geteilte Inhalte könnten dadurch für Mobbing, Cybergrooming, Darstellungen von sexualisierter Gewalt oder Identitätsdiebstahl missbraucht werden. «Eltern sollten sich bewusst sein, dass ihr Verhalten in der digitalen Welt genauso weitreichende Auswirkungen auf ihre Kinder haben kann wie im realen Leben», schreibt die Stiftung.

Michael In Albon, Jugendmedienschutzbeauftragter von Swisscom, sagt zudem, dass viele Eltern ein mangelndes Problembewusstsein hätten. Denn digitale Medien «vergessen nichts», und Inhalte, die öffentlich sind, können somit auch von Personen gesehen werden, die diese missbrauchen. «Vielen Eltern ist nicht wirklich bewusst, wie schnell Inhalte im digitalen Raum zweckentfremdet werden können», sagt In Albon.

KI als Katalysator

Während sich die Risiken von geteilten Kinderinhalten lange vor allem auf die Sichtbarkeit und mögliche Weiterverbreitung

fokussierten, kommt mit KI eine zusätzliche Dimension hinzu. «Die KI funktioniert wie ein Katalysator», sagt In Albon und ergänzt: «Wenn es

früher vor allem darum ging, die Persönlichkeitsrechte des Kindes bestmöglich zu schützen und es nicht der Gefahr auszusetzen, dass es 10 oder 15 Jahre später in der Schule wegen eines alten Fotos gemobbt wird, dann kommt heute die andere Gefahr hinzu, dass Inhalte unter Umständen für pornografische und kinderpornografische Zwecke missbraucht werden.»

Yves Kraft, Head of Security Academy von Oneconsult, erklärt, dass schon wenige, gut ausgeleuchtete und frontal aufgenommene Bilder ausreichen, um ein Gesicht in synthetische Inhalte einzubetten. «Für einfache Bild-Deepfakes können schon 5 bis 20 hochauflösende Fotos ausreichen, sofern unterschiedliche Blickwinkel und Mimik vorhanden sind», sagt er. Die Einstiegshürde sei zudem durch benutzerfreundliche Tools stark gesunken: «Das Risiko liegt weniger in der Technologie selbst als in ihrer breiten Verfügbarkeit.»

Die aufgrund von Sharenting online freie Verfügbarkeit von Kinderbildern und -videos bietet somit eine leicht zugängliche Datenquelle für den Missbrauch durch neue Technologien.

Technologie als Teil der Lösung

Abgesehen von den Risiken, die KI-Technologien mit sich bringen, können sie aber auch helfen, Missbrauch zu erkennen. Kraft nennt dazu einige Beispiele: automatische Erkennung synthetischer Gesichter, Klassifikation sensibler Inhalte vor Veröffentlichung, Monitoring-Plattformen mit Hash-Datenbanken bekannter Missbrauchsbilder und Anomalieerkennung bei Uploads. «Zudem können Kindergesichter proaktiv mit digitalen Signaturen versehen werden, um spätere Manipulationen nachweisbar zu machen», ergänzt er.

Obwohl die meisten KI-Systeme sehr gut im Erkennen von Mustern sind, seien solche Systeme nicht fehlerfrei: «Es gibt auch sehr hohe Vorbehalte gegenüber der Technologie, weil es sehr oft falsch-negative und falsch-positive Zuordnungen gibt», erklärt In Albon. Dies sei auch sehr gefährlich, weil dadurch Personen in Verruf geraten können, die eigentlich nichts falsch gemacht haben.

Zwischen Gesetz und Plattformverantwortung

Rechtlich ist die Lage in gewissen Bereichen eindeutig. Das Schweizer Strafgesetzbuch, Artikel 197, verbietet die Herstellung von kinderpornografischen Inhalten – ungeachtet der Tatsache, ob sie echt oder unecht sind. Sexualisierte Deepfake-



Bild: Prostock-studio - stock.adobe.com



Inhalte mit Kindern sind somit laut In Albon genauso illegal wie Inhalte mit echten Kindern.

Weniger klar geregelt ist es im präventiven Bereich. Ein spezifisches Gesetz gegen Sharenting existiert in der Schweiz nicht, obwohl politische Motionen zur Regulierung von Kinderfotos auf Social Media bereits bis zum Bund gelangt sind. Diese fordern insbesondere, Kinder vor kommerzieller Ausbeutung, beispielsweise durch Influencer-Marketing, zu schützen.

Auch für KI-Tools wie Grok oder sogenannte «Nudifyer-Apps» gibt es gemäss Kinderschutz Schweiz aktuell keine behördlichen Prüfungen auf sexualisierte Gewalt an Kindern. «Es fehlt global an Regulierungen in diesem Bereich», erklärt die Stiftung und findet: «Das Internet und die meisten digitalen Plattformen und Medien wurden nicht für Kinder konzipiert und all diese Lücken gilt es zu schliessen. Es braucht einerseits noch mehr Sensibilisierung, aber gleichzeitig gibt es auch klaren gesetzlichen Handlungsbedarf, damit Kinder und Jugendliche besser geschützt werden können.»

Kraft sieht auch bei Anbietern und Entwicklern von KI-Tools eine klare Mitverantwortung. Sie sollten technologische Schutzmechanismen standardmässig implementieren – etwa Altersfilter, Missbrauchsdetektion, Output-Moderation, Protokollierung auffälliger Nutzung sowie Beschränkungen bei der Generierung sensibler Inhalte. Zusätzlich seien auch Regulierungen sinnvoll: mit Transparenzpflichten, Haftungsregeln und klaren Strafnormen bei Missbrauch.

«Wichtig ist jedoch, Innovation nicht pauschal zu blockieren, sondern gezielt Risikoanwendungen zu adressieren», sagt Kraft und warnt gleichzeitig, dass es ein «Katz-und-Maus-Spiel» bleibe: «Sobald die eine Seite die Nutzung reguliert, findet die andere Seite wieder neue Wege für Missbrauch oder Möglichkeiten, wie die Schutzmechanismen umgangen werden können.»

Laut Kinderschutz Schweiz tragen wir alle die Verantwortung, Kinder und Jugendliche online zu schützen. Es sei aber auch ganz klar, dass soziale Plattformen noch viel stärker in die Verantwortung genommen werden müssten.

Prävention beginnt bei den Eltern

Gemäss In Albon sollten Eltern grundsätzlich keine persönlichen Daten wie Namen, Adressen oder Telefonnummern ihrer Kinder teilen. Wenn Eltern Bilder oder Videos ihrer Kinder trotzdem online posten wollen, empfiehlt er, diese unkenntlich zu machen. Einige Methoden dafür seien beispielsweise die Darstellung mit angeschnittenem Gesicht, nur von hinten oder mit einem «Blur-Effekt». «Am allerbesten wäre natürlich, wenn man das Kind im Kontext des Posts gar nicht thematisiert, weil es in dem Moment oft gar nicht zustimmen kann», sagt er. Zudem sieht In Albon auch bei etwas älteren Kindern, die bereits selbst bewusst entscheiden können, die Eltern in der Verantwortung, ihren Schützlingen «begleitend zur Seite zu stehen».

«Die Förderung der Medienkompetenz bei den Eltern ist einerseits ein löblicher Weg, aber auch ein beschwerlicher Weg», sagt er weiter. «Er braucht extrem lange Überzeugungsarbeit und die Verinnerlichung von Verhaltensweisen, die man unter Umständen so nie gelernt hat.»

Gesetze und technische Schutzmassnahmen setzen bereits einen Rahmen. Und obwohl auch Plattformen Verantwortung tragen sollten, liegt der grösste Hebel laut In Albon akut bei den Eltern: «Sie haben die Möglichkeit, durch ihr eigenes Verhalten Sharenting zu verhindern, indem sie keine Inhalte publizieren.» Die Förderung der Medienkompetenz ist dabei ein entscheidender Ansatz, um Kinder vor den Folgen von Sharenting und den damit verbundenen Deepfake-Risiken zu schützen.

Das kleine IT-Security-Glossar

Spätestens seit Wannacry, Mirai und Spectre sind Cyberbedrohungen omnipräsent und alles spricht von Ransomware, DDoS und Trojanern. Aber was war schon wieder was?

Das IT-Security-Glossar bietet einen schnellen Überblick über die gängigsten

Begriffe. Die Liste wird online laufend aktualisiert. Autor: Coen Kaat

Fileless Malware beziehungsweise **Fileless Attacks** sind Cyberattacken, die rein im Arbeitsspeicher des infizierten Rechners stattfinden. Es werden keine Dateien auf die Festplatte geschrieben, was Analysen erschwert. Ein Neustart leert den Arbeitsspeicher und löscht die Malware in der Regel. Gewisse Fileless Attacks sind jedoch persistent.

&
f

2

W

Die Schadprogramme, die gemeinhin als **Wiper** bezeichnet werden, sollen keine Daten stehlen oder Opfer erpressen. Sie verfolgen nur ein Ziel: Die Festplatte eines infizierten Rechners komplett zu löschen und so alle Daten und Programme böswillig zu vernichten für maximalen Schaden.

Wenn man potenzielle Angreifer auf eine falsche Fährte locken will, kann man **Honeypots** in seinem Netzwerk verteilen. Diese Server sollen auf Angreifer möglichst attraktiv wirken, ohne tatsächlich wichtig zu sein oder bedeutende Informationen zu haben.

(
h

4

r

Eine der fieseren Varianten von Malware. **Ransomware** nistet sich auf einem Rechner ein, verschlüsselt die Dateien und zeigt dem Opfer nur noch einen Sperrbildschirm. Dieser fordert das Opfer auf, ein bestimmtes Lösegeld zu zahlen.

Eine Möglichkeit, eine Website oder einen Onlinedienst vom Netz zu fegen, sind **DDoS-Attacken** – Distributed Denial of Service. Dabei wird eine Website mit so vielen Anfragen überhäuft, dass sie unter der Last zusammenbricht.

\$
d

:
m

Wieso nur ein Passwort, wenn man seine Daten auch hinter mehreren Schutzwällen verbergen kann? Bei einer **Multi-Faktor-Authentifizierung** wird das Passwort durch zusätzliche, unabhängige Faktoren ergänzt. Dabei kann es sich beispielsweise um einen mTAN-Code oder einen Hardware-Schlüssel handeln.

#

S

Stingray ist nicht nur die englische Bezeichnung für Stachelrochen; mit dem Begriff bezeichnet man in der IT Cell-Site-Simulatoren beziehungsweise IMSI Catcher. Diese Geräte imitieren die Signale von Mobilfunkmasten, um eine Verbindung mit Handys aufzubauen und um so Daten zu stehlen.

Eine besonders schwerwiegende Form des Exploits sind die sogenannten **Zero Day Exploits**. Dabei werden Schwachstellen bereits aktiv genutzt, bevor der Hersteller diese mit einem Patch beheben kann. Ihm bleiben folglich «Zero Days», um die Lücken zu schliessen.

%

Z

#

S

Beim **Social Engineering** greift der Cyberkriminelle die Schwachstelle Mensch an. Dem

Opfer werden falsche Tatsachen vorgaukelt, um dessen Vertrauen zu gewinnen. So soll das Opfer zu bestimmten Handlungen motiviert werden – etwa zur Herausgabe von Daten.

Bilder: hrf; S and V Design - stock.adobe.com

Beim **Phishing** werden Internetnutzer über gefälschte Websites betrogen. Oftmals imitieren die Websites bekannte Webauftritte namhafter Unternehmen. Ziel des Phishing ist es, an die Kontodaten der Betroffenen zu gelangen.

o
p

\$
d

DLL-Injection ist eigentlich etwas ganz Normales: Ein Prozess forciert einen anderen Prozess, eine programmfremde Dynamic Link Library (DLL) zu laden. Debugging-Tools etwa verwenden diese Technik. Aber auch Hacker wissen DLL-Injection für sich zu nutzen – zum Beispiel für Fileless Attacks.

Mit «**digitaler Souveränität**» wird die Fähigkeit von Individuen, Unternehmen und Staaten bezeichnet, digitale Technologien möglichst selbstbestimmt und ohne den Einfluss anderer zu nutzen. In der vernetzten Welt wird diese Handlungsfreiheit durch Abhängigkeiten eingeschränkt.

\$
d

5
t

Nach aussen hin wirken **trojanische Pferde** beziehungsweise Trojaner wie nützliche Anwendungen. Im Hintergrund jedoch führt das Programm ganz andere Aufgaben durch und lädt etwa weitere Malware herunter oder zerstört Dateien.

Wer Feuer mit Feuer bekämpfen will, greift auf **Nemato-den** zurück. Dabei handelt es sich um Viren oder Computer, die in Rechner eindringen. Allerdings nicht um diesen zu infizieren, sondern um andere Schadprogramme zu beseitigen.

i
n

Wenn ein Angreifer aus der Ferne auf den Rechner seines Opfers zugreifen und beliebige Codezeilen ausführen kann, spricht man von **Remote Code Execution**. So kann er Einstellungen ändern oder Schadprogramme ausführen. Hierzu nutzen Cyberkriminelle Sicherheitslücken in Hard- und Software aus.

4
r

+
c

Der **CEO-Scam** oder auch CEO-Betrug ist eine Form von Social Engineering. Dabei täuscht der Angreifer dem Opfer etwa in einer E-Mail vor, eine vorgesetzte Person zu sein – wie etwa der CEO. In der Regel läuft es darauf hinaus, dass das Opfer aufgefordert wird, eine Zahlung zu tätigen.

'
k

Sogenannte **Keylogger** speichern sämtliche Tastaturbefehle eines infizierten Rechners. So können Hacker etwa Passwörter oder Kreditkartendaten von nichtsahnenden Nutzern stehlen. Keylogger kommen als Hard- und auch als Software vor.

Zero Trust ist das perfekte Sicherheitskonzept für Paranoide. Bei diesem Ansatz geht man nämlich davon aus, dass jeder User, jedes Gerät und jedes Netzwerk zunächst einmal nicht vertrauenswürdig ist. Alle erhalten nur so viel Zugriffsrechte, wie sie benötigen.

:
m

Malvertising bezeichnet Malware, die über unerwünschte Werbung noch unerwünschteren Bedrohungen auf den Rechnern der Opfer einschleust. Sie wird etwa genutzt, um die Opfer auf Scam-Websites umzuleiten, oder um Adware, Exploit Kits und Ransomware zu installieren.

Brute-Force-Attacken: Was brutal klingt, bezeichnet eigentlich nur blosses Ausprobieren aller Möglichkeiten, bis man die richtige gefunden hat. Gewisse Tools nutzen die Methode, um Login-Daten zu erraten. Dabei klappern sie sämtliche gängigen Wörter und Passwörter ab.

/
b

%
Z



Mehr online

Der Q-Day rückt näher – die aktuelle Kryptografie steht auf der Kippe

Der Q-Day ist nicht mehr nur ein theoretisches Konzept. Das Aufkommen der Quanteninformatik zwingt Unternehmen dazu, bereits heute die Auswirkungen auf die Kryptografie zu antizipieren. Das Inventarisieren der eigenen Krypto-Assets und die Vorbereitung der Migration auf Post-Quantum-Standards wird zu einem entscheidenden Schritt.



Der Autor

Yoann Le Corvic,
Senior Security Engineer,
e-Xpert Solutions

Der Q-Day, jener gefürchtete Zeitpunkt, an dem Quantencomputer Verschlüsselungsverfahren wie RSA und ECC knacken und AES sowie SHA erheblich schwächen werden, zeichnet sich für die Jahre 2030 bis 2040 ab. Unternehmen sollten daher ihre Krypto-Assets sofort inventarisieren, um der Bedrohung «Harvest Now, Decrypt Later (HNDL)» entgegenzuwirken, und die Migration auf die NIST-«Quantum-Safe»-Standards planen.

Auswirkungen und betroffene Bereiche

Asymmetrische Algorithmen wie RSA und ECC kollabieren und müssen ersetzt werden, sobald ein ausreichend leistungsfähiger Quantencomputer verfügbar ist. Symmetrische Algorithmen wie AES und SHA bleiben zwar funktionsfähig, verlieren jedoch etwa die Hälfte ihrer Sicherheitsmarge, was den Einsatz längerer Schlüssel erfordert. Betroffene Bereiche sind:

Kommunikationssicherheit: HTTPS, VPN, SSH basieren auf Algorithmen, die nach dem Q-Day geknackt oder stark geschwächt sein werden.

Langzeitspeicherung von Daten: Zweifellos das wichtigste Thema. Archive, Backups und sensible Daten sind heute noch mit nicht-quantensicheren Verfahren geschützt.

Digitale Identitäten: Sämtliche Prozesse rund um Public-Key-Infrastruktur (PKI) und Zertifikate (essenziell für die Authentifizierung) sind gefährdet.

Die Bedrohung «Harvest Now, Decrypt Later»

Cyberkriminelle sammeln bereits heute verschlüsselte Daten, um sie nach dem Q-Day zu entschlüsseln. Dazu gehören KYC-Archive, Branchengeheimnisse, Medizin- und Finanzdaten. Da diese Daten langfristig wertvoll sind, bleibt das Risiko kritisch – unabhängig vom genauen Zeitpunkt des Q-Days. Deshalb hat das Inventarisie-

ren der Krypto-Assets, die diese Daten schützen, oberste Priorität.

Wer ist betroffen und was ist zu tun?

Alle Branchen sind betroffen, jedoch mit unterschiedlicher Intensität. Unternehmen, die Archive über Jahrzehnte verwalten (Banken, Verteidigungs- und Gesundheitswesen) sind gegenüber der HNDL-Bedrohung am stärksten gefährdet. Auch Unternehmen mit kurzlebigen Daten sollten ein vollständiges Inventar führen.

Wichtig ist es, rechtzeitig zu starten. Denn der Übergang zu post-quantensicherer Kryptografie (PQC) ist ein langfristiges Projekt und kann nicht an einem Tag durchgeführt werden. Es gibt keinen «PQC-Patch», der eine Umgebung sofort quantensicher macht. Folgende Schritte sind wichtig:

Governance: Sensibilisieren Sie das Management, um die nötigen Budgets zu sichern und eine klare Übersicht über die Krypto-Assets zu erhalten.

Inventarisierung: Scannen Sie Netzwerke, PKI, HSM und Anwendungscode, um Zertifikate, Schlüssel und Protokolle zu erfassen.

Priorisierung: Klassifizieren Sie die Assets nach geschäftlichem Risiko, mit Fokus auf den Schutz langfristiger Daten, die besonders von HNDL bedroht sind.

Automatisiertes Management: Setzen Sie auf Certificate-Lifecycle-Management-Tools (CLM), um eine umfassende Sicht auf Ihre Krypto-Assets zu erhalten und deren Verwaltung effizienter zu gestalten.

Schrittweise Implementierung: Mit CLM kann die Migration automatisiert und schrittweise erfolgen, um alle Krypto-Assets quantensicher zu machen. Dies beruht auf der Verwendung neuer asymmetrischer Algorithmen:

- ML-KEM (FIPS 203)
- ML-DSA (FIPS 204)
- SLH-DSA (FIPS 205)
- FN-DSA (FIPS 206 – in Standardisierung)
- Auf der Erhöhung der Schlüssellängen für symmetrische Algorithmen und Hash-Algorithmen (AES-256 / SHA-3)



Bild: ArtemisDiana - stock.adobe.com

Schlüsselrolle der CLM-Tools

CLM-Tools sind echte Alleskönner für die Verwaltung von Krypto-Assets und ermöglichen deren Erkennung, automatische Erneuerung und Überwachung. Sie erleichtern die Migration zu PQC und verhindern gleichzeitig Produktionsausfälle aufgrund ablaufender Zertifikate, die nach wie vor allzu häufig vorkommen. Sie sind zudem eine wirksame Antwort auf die schrittweise Verkürzung der Gültigkeitsdauer von Zertifikaten: 200 Tage ab März 2026, 100 Tage im Jahr 2027 und 47 Tage im Jahr 2029.

Der Umstieg auf Post-Quantum-Kryptografie ist kein Spurt. Mit einer soliden Governance und einer genauen Bestandsaufnahme der Krypto-Assets (Schlüssel, Zertifikate und Algorithmen) können Unternehmen ihre Migration planen und sensible Daten langfristig sichern.



SWISSEXPERTGROUP
YOUR SUCCESS MATTERS

Swiss Expert Group
c/o eb-Qual SA

Oberfeldstrasse 20 | CH-8302 Kloten
+41 43 211 47 20 | info@swissexpertgroup.com
swissexpertgroup.com



Bild: Flash memory - stock.adobe.com

So beflügelt KI das MSP-Geschäft 2026

Acronis hat einen Blick auf die Zukunft von Managed Services Provider geworfen. In seinen Channel-Trends für 2026 beschreibt das Unternehmen, wie die künstliche Intelligenz MSPs Arbeit abnehmen und neue Geschäftschancen ermöglichen kann. Autor: Coen Kaat, Netz-KI Bot

Künstliche Intelligenz wird den strukturellen Wandel von Managed-Services-Providern (MSPs) und Channelpartnern beschleunigen. Dies prognostiziert Acronis in seinen Channel-Trends für 2026. Mit KI könnten Dienstleister ihre Betriebsmodelle neu gestalten und zentrale Workflows automatisieren, teilt der IT-Security-Anbieter mit. Der Fokus verschiebe sich zunehmend in Richtung Sicherheit, Skalierbarkeit und ergebnisorientierte Dienstleistungen. Im Folgenden die prognostizierten Trends.

- **KI automatisiert einen Grossteil der MSP-Workflows:** Der menschliche Aufwand wird halbiert. Die meisten Tier-1-Tickets werden entweder vollständig automatisiert oder durch vorgefertigte Lösungsvorschläge, die Techniker mit wenigen Klicks genehmigen können, bearbeitet. KI-generierte Runbooks, Checklisten, Kundenberichte und Echtzeitprotokolle vereinfachen auch die Dokumentation. KI soll aber auch Geschäftsprozesse (Verträge, Planung, Reporting, Zeiterfassung und Abrechnung) steuern.
- **Intelligente Systeme optimieren Sicherheits- und Geschäftsprozesse:** Um eine Flut von Alerts zu vermeiden, übernimmt KI immer mehr die Triage. So sollen Technikerinnen und Techniker mehr Zeit für übergeordnete Aufgaben haben. Ferner werden KI-Tools proaktiv Patch-Zeitpläne, Konfigurationsänderungen und Schritte zur Vorbeugung von Sicherheitsvorfällen vorschlagen. Datenbasierte Insights sollen zudem Abdeckungslücken aufspüren und so zusätzliche Geschäftsmöglichkeiten aufzeigen.
- **KI treibt ergebnisorientierte Geschäftsmodelle voran:** Ergebnisorientierte Preismodelle werden zum Standard, wie

Acronis schreibt. «Virtuelle KI-Mitarbeiter», die selbstständig Aufgaben von der Ticketbearbeitung bis zur Planung von Behebungsmassnahmen erledigen, befähigen kleine MSPs. So können sie laut Acronis das Serviceniveau grösserer Unternehmen zu einem geringeren Preis anbieten, um ihren Marktanteil und Einfluss zu erweitern.

Partner, die sich auf Produkte konzentrieren, werden es schwer haben – im Gegensatz zu denen, die messbare Ergebnisse liefern. Zugleich erwarten Kunden, dass die Security inklusive ist. Acronis empfiehlt MSPs daher basierend auf diesen Trends:

- den Fokus auf Ergebnisse statt auf Tools zu legen,
- Security-First-Dienstleistungsmodelle einzuführen,
- sich auf vertikale Expertise zu konzentrieren,
- in die Weiterbildung der Kunden zu investieren,
- und Herstellerbeziehungen zu stärken.

MSPs werden KI-Tools schützen und verwalten müssen, so wie sie es bereits mit E-Mail- oder Cloud-Diensten tun. «Die Einführung von KI ist eine neue Chance: MSPs werden KI-gestützte Produkte und Services anbieten, die Kunden dabei unterstützen, KI-Technologien zu implementieren, zu verwalten und zu schützen», sagt Markus Fritz, General Manager DACH bei Acronis. «Mit dieser Rolle entwickeln sich MSPs von reaktiven Problemlösern zu strategischen Partnern, die verändern, wie ihre Kunden arbeiten, und neue Geschäftswerte erschliessen.»



Den vollständigen Artikel finden Sie online

swisscybersecurity.net



Bild: InfiniteFlow - stock.adobe.com

Warum KI-generierte Passwörter nur scheinbar sicher sind

Lang, komplex und mit Sonderzeichen: Passwörter von KI-Modellen sehen sicher aus. Tatsächlich sind sie aber gefährlich vorhersagbar. Eine Untersuchung zeigt, wie KI die Sicherheit von Passwörtern untergräbt und neue Angriffsvektoren entstehen. Autor: Joël Orizet, Netz-KI Bot

Wer einen KI-Assistenten wie ChatGPT, Claude oder Gemini bittet, ein sicheres Passwort zu generieren, erhält auf den ersten Blick ein beeindruckendes Ergebnis: eine lange Zeichenkette, gespickt mit Gross- und Kleinbuchstaben, Ziffern und Symbolen. Doch der Eindruck täuscht: Solche KI-generierten Passwörter sind aufgrund der Funktionsweise grossen Sprachmodellen (LLMs) fundamental unsicher, wie aus einer Untersuchung des IT-Sicherheitsdienstleisters Irregular hervorgeht.

Das Kernproblem liegt in der Architektur der KI. Während ein sicheres Passwort auf echter Zufälligkeit basieren muss, sind Sprachmodelle darauf trainiert, Muster zu erkennen und das wahrscheinlichste nächste Wort oder Zeichen vorherzusagen. Ein starkes Passwort stammt üblicherweise von einem kryptografisch sicheren Zufallszahlengenerator – ein Verfahren, das gezielt unvorhersehbare Zeichenfolgen erzeugt. Ein LLM tut jedoch genau das Gegenteil: Es produziert das, was es für eine plausible und wahrscheinliche Zeichenfolge hält.

In ihren Tests forderten die Forschenden von Irregular führende KI-Modelle wiederholt auf, Passwörter zu erstellen. Die Ergebnisse sind alarmierend. Das Modell Claude Opus 4.6 generierte bei 50 Versuchen nur 30 einzigartige Passwörter. Ein und dasselbe Passwort, nämlich «G7\$kL9#mQ2&xP4!w», wiederholte sich dabei 18 Mal. Andere Modelle wie ChatGPT und Gemini zeigten ähnliche Tendenzen: Die Passwörter begannen überproportional oft mit denselben Buchstaben, nutzten nur eine kleine Auswahl an Sonderzeichen und wiesen klare, wiederkehrende Muster auf.

Die Stärke eines Passworts messen Fachleute in Entropie-Bits. Dieser Wert gibt vereinfacht an, wie viele Versuche ein Angreifer im Schnitt für einen Brute-Force-Angriff – also das systematische Durchprobieren aller Möglichkeiten – benötigt. Ein KI-generiertes Passwort, das laut gängigen Tools eine Entropie von über 100 Bits zu haben scheint (was Billionen von Jahren zum

Knacken bräuchte), besitzt laut der Analyse von Irregular in Wirklichkeit oft nur 20 bis 30 Bits. Das reduziert die benötigte Zeit zum Knacken auf wenige Sekunden oder Minuten.

Die unsichtbare Gefahr durch Coding-Assistenten

Besonders brisant wird das Problem durch den Einsatz von KI-gestützten Programmier-Assistenten. Im sogenannten Vibe-Coding, bei dem die User eine KI ganze Code-Blöcke erstellen lassen, ohne jede Zeile im Detail zu prüfen, generieren diese Agenten oft selbstständig Passwörter für Datenbanken oder Dienste. Statt auf sichere Standardmethoden zurückzugreifen, lassen sie diese häufig direkt vom Sprachmodell erstellen. So gelangen extrem schwache Passwörter unbemerkt in den Quellcode von Anwendungen. Die Forschenden von Irregular fanden bei Suchen auf Plattformen wie Github bereits zahlreiche Beispiele für solche im Code fest verankerten, KI-generierten Passwörter.

Dieses Phänomen eröffnet Angreifenden neue Möglichkeiten. Statt rein zufällige Kombinationen zu probieren, können sie nun spezielle «Wörterbuch-Angriffe» mit den am häufigsten von KIs generierten Passwörtern durchführen. Ein Angreifer, der vermutet, dass ein Dienst mithilfe von KI entwickelt wurde, kann gezielt diese wahrscheinlichen Passwörter testen.

Irregular rät daher dringend davon ab, Passwörter von Sprachmodellen erstellen zu lassen. Stattdessen sollten User auf etablierte Passwort-Manager zurückgreifen. Wer in der Softwareentwicklung auf KI-Assistenten setzt, sollte den generierten Code sorgfältig auf fest einprogrammierte Zugangsdaten prüfen und sicherstellen, dass die KI-Agenten kryptografisch sichere Methoden zur Passwort-Erstellung verwenden.



Den vollständigen Artikel finden Sie online

swisscybersecurity.net

«Kann man Vorfälle ohne Angst melden, wird Kultur zum Schutzschild»

Cyberresilienz ist zur zentralen Führungsaufgabe geworden. Katja Dörlemann, Präsidentin Swiss Internet Security Alliance SISA, Human Centred Security Expert bei Switch, sagt, welche Kompetenzen zählen, wie Sicherheitskultur gelingt und warum Kooperation entscheidend ist. Interview: SISA



Katja Dörlemann, Präsidentin, Swiss Internet Security Alliance (SISA), und Human Centred Security Expert, Switch.

Warum ist Cybersecurity heute eine Kernfrage der Unternehmensstrategie?

Katja Dörlemann: Fast jede Organisation ist digital unterwegs. Ob Kommunikation oder Prozesse – alles findet im digitalen Raum statt. IT-Systeme sind kritisch für den Arbeitsalltag und damit für den Fortbestand jeder Organisation. Zunehmende Komplexität schafft Angriffsfläche für Cyberkriminelle. Cybersecurity ist deshalb eine Kernfrage, weil sie die Geschäftsgrundlage sichert.

Wie gelingen wirkungsvolle Cybersicherheit und eine starke Sicherheitskultur?

Digitalisierung betrifft jeden Arbeitsbereich. Unternehmen müssen klären, welche Daten und Systeme besonders schützenswert sind, wo sie liegen und wer Zugriff braucht. Da der Mensch zunehmend Ziel von Angriffen ist, müssen Mitarbeitende befähigt werden, zum Schutz der Organisation beizutragen. Es braucht klare Regeln, Melde- wege und vernetzte Ansprech- personen. Wenn Mitarbeiten- de wissen, was erwartet wird, und die Umsetzung einfach

ist, integrieren sie sicheres Verhalten in den Arbeitsalltag. Entscheidend ist, dass Führungskräfte dieses Verhalten vorleben: Werden Meldungen belächelt oder sanktioniert, sinkt die Wach- samkeit. Können Vorfälle ohne Angst gemeldet werden, wird Kultur zum aktiven Schutzschild.

Welche Kompetenzen benötigen Führungskräfte, um Cyberrisiken realistisch zu bewerten?

Führungskräfte müssen keine IT-Spezialistinnen und -Spezialis- ten sein. Sie sollten jedoch verstehen, welche IT-Systeme kri- tisch sind und welche Auswirkungen eine tiefe oder hohe Cyber- security-Maturität auf die Organisation hat. Dieses Kontextwis- sen ermöglicht fundierte Entscheidungen. Dafür braucht es Lernbereitschaft und den Mut, Fragen zu stellen.

Security gilt oft als Verhinderer. Wie wird Sicher- heit zum Enabler?

Indem sie von Anfang an mitgedacht wird. Das richtige Sicher- heitsniveau ist ein Wettbewerbsvorteil und reduziert Geschäfts- risiken wie Reputations- und Geldverlust oder Ausfälle. Immer mehr B2B-Kunden fordern Zertifizierungen, auch Cyberversiche- rungen stellen Mindestanforderungen. Sicherheit schafft Ver- trauen und Marktzugang.

Welche Hürden beschäftigen Führungskräfte – und warum ist Kooperation ein Vorteil?

Führungskräfte beschäftigt vor allem, welches Sicherheits- niveau angemessen ist und wo Investitionen den grössten Ef- fekt haben. Hier hilft branchenübergreifender Austausch: Wenn Organisationen Informationen zu Angriffstaktiken oder betrüge- rischen URLs teilen, können alle schneller reagieren und Sys- teme sowie Mitarbeitende gezielt vorbereiten.

Sicherheit gelingt kaum im Alleingang. Wo finden Führungskräfte Impulse und welche Rolle spielt die SISA?

Es gibt verschiedene Organisationen, die Austausch bieten. Die Swiss Internet Security Alliance ermöglicht Zugang zu einem breiten Expertennetzwerk und zu vertrauenswürdigen Informati- onen. Veranstaltungen wie der Swiss Websecurity Day oder der Human Centred Security Day fördern den Dialog. Mit iBarry.ch stellen wir kuratierte Inhalte als Creative Commons zur Verfü- gung, die Organisationen direkt nutzen können.



Das Interview
finden Sie auch
online

[swisscybersecurity.net](https://www.swisscybersecurity.net)

Wer schützt was?

Dass die IT geschützt werden muss, steht ausser Frage – aber mit welcher Lösung? Eine Vielzahl an EDR-, XDR- und weiteren Security-Produkten unterschiedlicher Anbieter schützen heutzutage Unternehmensrechner. Wie Unternehmen die beste Lösung für ihre spezifischen Anforderungen finden, zeigt diese Marktübersicht. Autor: Coen Kaat

Quantensichere Verschlüsselung, Zero Trust und künstliche Intelligenz in der Cyberabwehr – die IT-Security beschäftigt sich oft mit sehr komplexen Themen und solchen, die erst noch relevant werden müssen. Wenn in der Abwehr aber etwas schief läuft, scheitert es in der Regel an den Basics wie etwa an sicheren Passwörtern. Und auch wenn die Devise heutzutage «Assume Breach» lautet (Unternehmen sollten davon ausgehen, dass sich bereits ein Angreifer im eigenen Netzwerk befindet), ist der Perimeterschutz nach wie vor wichtig.

Auf diesem Markt tummeln sich zahlreiche Anbieter mit teilweise sehr ähnlichen Angeboten. Die meisten bieten einen guten Grundschutz für diverse Endgeräte beziehungsweise Anwendungsbereiche, wie die Tabelle zeigt. Wer jedoch, abgesehen von PCs, auch noch Mobilgeräte, Cloud-Anwendungen oder Mail-Server schützen will, muss ein wenig genauer hinschauen; gewisse Anbieter decken diese Kategorien nicht in allen Preismodellen oder mit separaten Produkten ab. Positiv fällt auf, dass alle Anbieter – mit einer Ausnahme – bei der Detektion auf einen hybriden Ansatz setzen. Das

MARKTÜBERSICHT EDR FÜR UNTERNEHMEN*							* Selbstdeklaration der Anbieter ** Separates Produkt
Name des Unternehmens		Acronis	Barracuda	Bitdefender	Check Point	Cisco	CrowdStrike
Name der Plattform		Cyber Protect Cloud	Barracuda Managed XDR	Gravityzone	Check Point Infinity XDR/XPR, Harmony Endpoint	Cisco Secure Endpoint	CrowdStrike Falcon Platform
Unterstützte Betriebssysteme		Windows, MacOS, Linux, Server	Windows, MacOS, Linux, Server, Cloud	Windows, MacOS, Linux, Server und Workstations	Windows, MacOS, Linux, Android, iOS	Windows Workstation, Windows Server, MacOS, Linux	Windows, MacOS, Linux, Server, ChromeOS
schützt	Endpoints / Clients	Ja	Ja	Ja	Ja	Ja	Ja
	Mobilgeräte	Ja	Nein	Ja	Ja	Ja	Ja
	Cloud-Anwendungen	Ja	Ja	Ja	Ja	Ja	Ja
	Mailserver	Ja	Je nach Plan	Ja	Ja	Ja	Ja
Automatisierte Reaktion		Ja	Ja	Ja	Ja	Ja	Ja
Signatur oder Verhaltensbasiert		Beides	Beides	Beides	Beides	Beides	Verhaltensbasiert
Log-Retention / Historie		30 bis 365 Tage	90 / 365 (je nach Plan)	730 Tage	bis zu 90 Tage	30 Tage Standard (unbegrenzt, falls in SIEM integriert)	Standardmässig 7 Tage, aber flexibel bis zu 5 Jahre (1826 Tage)
Integrierte Firewall-Funktionalität		Nein	Je nach Plan	Ja	Ja	Ja	Ja
Ransomware-Schutz		Ja	Ja	Ja	Ja	Ja	Ja
USB Monitoring & Policy Enforcement		Ja	Ja	Ja	Ja	Ja	Ja
Cloud Sandboxing		Nein	Je nach Plan	Ja	Ja	Ja	Ja
Festplattenverschlüsselung		Ja	Nein	Je nach Plan	Ja	Nein	Nein
Threat Hunting & Forensik		Ja	Je nach Plan	Ja	Ja	Ja	Ja
Overhead		Geringe Auslastung	Geringe Auslastung	Geringe Auslastung	Geringe bis mittlere Auslastung	Geringe Auslastung	Geringe Auslastung

heisst, ihre Lösungen setzen auf eine statische signatur- und eine dynamische verhaltensbasierte Detektion. Die Tage der reinen signaturbasierten Erkennung, bei der nicht gelistete Bedrohungen durch die Lappen gehen, sind wohl definitiv vorbei. Lediglich CrowdStrike verzichtet auf eine hybride Erkennung und setzt auf reine Verhaltensanalysen, um Schädlinge aufzuspüren.

Die grössten Unterschiede zwischen den Anbietern finden sich bei der Log-Retention. Die kürzeste Aufbewahrungszeit ist eine Woche, bei anderen Lösungen ist sie unbegrenzt. Oft lässt sich die Zeitspanne konfigurieren, in der Daten zu Ereignissen aufbewahrt werden. Bei gewissen Anbietern ist auch die Art der Daten relevant: So speichert etwa Palo Alto Networks Rohdaten für 30 und Incident-Daten für 180 Tage.

Beim Thema Festplattenverschlüsselung zeigt sich ebenfalls ein gemischtes Bild. Rund die Hälfte der Lösungen bietet keine entsprechende Funktionalität. Etwa ein Drittel der Lösungen bietet die Option an. Und bei zwei weiteren Lösungen ist dies abhängig vom gewählten Preismodell. Was in der Übersicht fehlt, sind

die Angaben zur Preisgestaltung und zu den Schnittstellen. Hier empfiehlt es sich, das Kleingedruckte bei den Angeboten zu lesen. In der Regel wird pro User und Monat abgerechnet. Gewisse Anbieter bieten jedoch eine Standardlizenz, mit der Option, ergänzend noch zusätzliche Features zu buchen. Aber auch der tatsächliche Verbrauch kann die Ausgangslage der Abrechnung bilden. Ein Anbieter, Trend Micro, bietet ein Credit-System an. Die Credits könnten Unternehmen auf alle Lösungen des Anbieters verteilen. Und für diejenigen, die ihre Schutzlösung in andere Produkte integrieren möchten, gibt es gute Neuigkeiten: Alle Unternehmen bieten zahlreiche Integrationsmöglichkeiten oder APIs an. So lassen sich die Schutzlösungen etwa in SIEM-Systeme einbauen. Die kleinen Abweichungen können aber den Unterschied machen. Welche Lösung am besten passt, finden Unternehmen mit dieser Marktübersicht heraus. Die Tabelle basiert auf der Selbstdeklaration der Anbieter.



MARKTÜBERSICHT EDR FÜR UNTERNEHMEN*						
Eset	Fortinet	G Data Cyberdefense	Kaspersky	Palo Alto Networks	Sophos	Trend Micro
Eset Protect und Eset Inspect	FortiEndpoint	G Data 365 MXDR	Next EDR Expert	Cortex-Plattform (XDR/Cloud oder XSIAM)	Sophos XDR	Trend Vision One
Windows, MacOS, Linux, Server (Windows, Linux), Android	Windows, Linux, MacOS	Windows, Linux, MacOS	Windows, MacOS, Linux, Android und iOS	Unified Agent für jedes Betriebssystem	Windows, MacOS, Linux, Server	Windows, MacOS, Linux
Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ja	Nein	Ja	Ja	Ja	Nein**	Ja
Je nach Plan	Nein	Ja	Ja	Ja	Ja	Ja
Je nach Plan	Nein**	Ja	Ja	Ja	Nein**	Ja
Ja	Ja	Ja	Ja	Ja	Ja	Ja
Beides	Beides	Beides	Beides	Beides	Beides	Beides
Individuell (Cloud, On-Prem)	Standard 30 Tage (konfigurierbar)	Unbegrenzt	Bis zu 90 Tage in der Cloud, On-Prem unbegrenzt	Rohdaten 30 Tage und Incident-Daten 180 Tage, Erweiterung möglich	90 oder 365 Tage	Individuell konfigurierbar; maximal 9 Jahre
Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ja	Ja	Ja	Ja	Ja	Ja	Ja
Je nach Plan	Ja	Nein	Ja	Ja	Ja	Ja
Je nach Plan	Nein	Nein	Ja	Ja	Nein**	Nein
Je nach Plan	Ja	Ja	Ja	Ja	Ja	Ja
Geringe Auslastung	Geringe Auslastung	Geringe Auslastung	Mittlere Auslastung	Geringe Auslastung	Geringe Auslastung	Geringe Auslastung

Effizienz frisst Datensouveränität: Die Bilanz der Schatten-KI

Sind Schweizer Unternehmen im KI-Wettrüsten noch sicher aufgestellt? Wenn Schatten-KI und autonome Agenten Daten absaugen, versagt traditionelle IT-Security. Erfahren Sie, warum eine datenzentrierte Architektur 2026 der einzige Weg ist, globale Innovation profitabel und souverän zu nutzen.

Die Schatten-KI hat Schweizer Unternehmen und Behörden längst unterwandert. Aus Erfahrung wissen wir: Mitarbeitende nutzen KI-Chatbots so selbstverständlich, dass herkömmliche Sicherheitsdispositive ausgehebelt werden. Wir erleben aktuell den grössten unkontrollierten Abfluss sensibler Informationen in der Geschichte der Schweiz. Geschäftskritische Daten landen unverschlüsselt in den Trainingsspeichern globaler Hyperscaler. Diese unkontrollierte Preisgabe sensibler Daten ist kein technisches Versäumnis, sondern ein strukturelles Risiko, das die digitale Integrität bedroht. Studien belegen: Über 57 Prozent der Angestellten nutzen bereits private Konten für geschäftliche Zwecke, und ein Drittel lädt sensible Daten in unautorisierte Tools hoch. Wer 2026 noch glaubt, dieses Problem allein durch Verbote zu lösen, verkennt die Realität. Wer heute nur reglementarische Antworten liefert, verkennt die Zeit und handelt grob fahrlässig.

Das Dilemma: Schweizer Organisationen können mit den Investitionen aus dem Silicon Valley nicht mithalten, doch ein Verzicht auf globale Sprachmodelle würde die Innovationskraft unserer Wirtschaft lähmen. Die Lösung ist Souveränität durch Design: Nur ein innovativer technischer Ansatz kann die hohen Anforderungen an digitale Compliance erfüllen. Dies ist längst keine reine IT-Frage mehr, sondern eine strategische Kernaufgabe für Verwaltungsräte und Geschäftsleitungen, da es den

Der Autor

Michael Rieder, Head IT Cloud Consulting, e3

Kern der IT-Sicherheitsarchitektur betrifft. Mit dem revidierten Datenschutzgesetz (revDSG) ist das Haftungsrisiko real, Führungskräfte haften persönlich. KI-Security ist Chefsache. Das gilt es zu tun: Informationsschutz muss neu gedacht werden. 2026 stehen drei strategische Optionen bereit:

- **Option 1: Präventive Barriere:** Fortschrittliche Data Loss Prevention (DLP) blockiert den Zugriff auf nicht autorisierte Plattformen direkt am Endpoint oder spätestens am Perimeter.
- **Option 2: Granulare Kontrolle:** Eine «Sprachpolizei» scannt Anfragen in Echtzeit und blockiert diese nur bei sensiblen Inhalten, während die allgemeine Nutzung erlaubt bleibt.
- **Option 3: Technologische Speerspitze:** Cloud Data Protection Gateways (CDPG) erweitern das Zero-Trust-Modell auf die Datenebene. Daten werden verschlüsselt oder anonymisiert, bevor sie die Infrastruktur verlassen. In Kombination mit Confidential Computing bleiben Daten selbst in der Cloud für Dritte unlesbar.

Data-Centric AI Security Architecture ist das Fundament für unternehmerische Handlungsfreiheit. Nur wer Informationsschutz direkt an Daten verankert, bleibt agil und kann Innovationen sicher adaptieren. Datensouveränität ist die Voraussetzung für sichere Skalierung und eine starke Wettbewerbsposition in der Zukunft. Durch Verschlüsselung und die Neutralisierung von Prompts verlieren ausländische Offenlegungsgesetze wie der US CLOUD Act ihre Wirkung. Innovative Verfahren «Made in Switzerland» schützen Daten in Millisekunden und vermeiden Vendor Lock-in. Wer kryptografische Schlüssel selbst hält, bleibt unabhängig und erfolgreich.

Last but not least: Data-Centric AI Security transformiert IT-Sicherheit vom Kostenfaktor zum strategischen Vertrauensbeweis. 2026 fordern Kunden und Partner den Nachweis der Datenhoheit als Grundlage für Zusammenarbeit. IT-Security wird zum Business-Turbo und Innovationsstreiber. Die entscheidende Frage ist nicht, ob wir KI nutzen, sondern wie resilient die IT-Security-Architektur ist.



Das Dossier finden
Sie auch online

swisscybersecurity.net

«KI braucht keine Verbote, sondern Kontrolle über Datenflüsse»

Im Interview erläutert Michael Rieder, Head IT Cloud Consulting bei e3, wie sich KI mit Zero Trust, lokaler Datenhoheit und granularen Schutzmechanismen sicher in bestehende Prozesse und regulierte Umgebungen integrieren lässt. Interview: Dylan Windhaber

Weshalb lautet die zentrale Frage für Schweizer Unternehmen nicht mehr, ob KI genutzt wird, sondern wie resilient die zugrunde liegende Architektur ist?

Michael Rieder: KI ist längst Teil des Arbeitsalltags. Mitarbeitende nutzen generative Systeme zur Recherche, Analyse oder Texterstellung – oft auch ausserhalb offiziell freigegebener IT-Umgebungen. Dadurch entsteht eine neue Form von Schatten-IT, bei der sensible Unternehmensinformationen in externe KI-Systeme gelangen können, ohne dass Organisationen den Datenfluss kontrollieren. Die entscheidende Frage lautet deshalb heute: Wie nutzen Unternehmen KI und behalten dabei gleichzeitig die Kontrolle über ihre Daten? Das ist keine reine IT-Frage, sondern eine Führungsaufgabe. Unternehmen müssen festlegen, welche Daten genutzt werden dürfen, welche geschützt werden müssen und wie KI verantwortungsvoll in Geschäftsprozesse integriert werden kann. Resiliente Sicherheitskonzepte setzen dabei *direkt* am Datenfluss an – etwa durch Verschlüsselung oder kontrollierte Zugänge zu KI-Diensten.

Welche Rolle spielen hybride oder lokale Komponenten in einer Zero-Trust-Strategie für KI-Anwendungen?

Zero Trust bedeutet, *keinem* System und *keinem* Datenfluss automatisch zu vertrauen. Für KI-Anwendungen führt das häufig zu hybriden Architekturen. Lokale oder hybride Komponenten ermöglichen es, besonders sensible Daten und kryptografische Schlüssel unter eigener Kontrolle zu halten, während KI-Modelle oder Rechenleistung aus der Cloud genutzt werden. Für Unternehmen ist das eine strategische Entscheidung: Welche Daten müssen unter eigener Hoheit bleiben und welche Prozesse können extern laufen? Die Architektur setzt diese Entscheidungen technisch um.

Welche Architektur- und Governance-Strukturen brauchen regulierte Branchen, um KI gesetzeskonform und sicher zu nutzen?

Für regulierte Branchen ist der Einsatz von KI vor allem eine Governance-Aufgabe. Unternehmen müssen verstehen, welche Daten besonders schützenswert sind und unter welchen Bedingungen sie genutzt werden dürfen. Daraus ergeben sich klare Richtlinien für die Nutzung von KI-Tools, transparente Audit- und Logging-Strukturen sowie technische Kontrollen für Datenflüsse. Dazu gehören Datenklassifizierung, zentrale Schlüsselver-

«Unternehmen, die KI nutzen und gleichzeitig die Kontrolle über ihre Daten behalten, schaffen Vertrauen und sichern ihre Wettbewerbsfähigkeit.»

Michael Rieder,
Head IT Cloud Consulting, e3



waltung und Schutzmassnahmen direkt auf Datenebene. Diese Massnahmen lassen sich modular umsetzen – auch für mittelständische Unternehmen.

Wann empfiehlt sich die granulare Schutzoption, also die Kontrolle einzelner Prompts?

Granulare Schutzmechanismen eignen sich besonders dort, wo KI produktiv genutzt werden soll, gleichzeitig aber einzelne sensible Informationen geschützt werden müssen. Inhalte innerhalb eines Prompts können erkannt, anonymisiert oder verschlüsselt werden, bevor sie an ein externes Modell übermittelt werden. So lassen sich Produktivitätsgewinne durch KI nutzen, ohne kritische Daten preiszugeben.

Wie können Unternehmen ihre Daten und Prozesse so gestalten, dass KI-Risiken proaktiv gemanagt werden und Sicherheit zum strategischen Wettbewerbsvorteil wird?

Der wichtigste Schritt ist, Informationsschutz als Teil von Architektur und Unternehmensführung zu verstehen. Unternehmen sollten ihre Daten klassifizieren, sensible Informationen schützen und klare Regeln für den Umgang mit KI etablieren. Der Aufbau einer resilienten Architektur muss dabei kein Grossprojekt sein. Viele Organisationen können mit fokussierten Massnahmen beginnen – etwa indem sie kritische Daten und KI-Zugänge zuerst absichern. Unternehmen, die KI nutzen und gleichzeitig die Kontrolle über ihre Daten behalten, schaffen Vertrauen und sichern ihre Wettbewerbsfähigkeit.

Wie Unternehmen teure Fehler bei Security Operations Center vermeiden

SOC-Projekte scheitern oft nicht an der Technik, sondern an Prozessen und falschen Annahmen für den Betrieb. Was beim Aufbau eines Security Operations Centers oft untergeht und wer ein SOC besser als Service beziehen sollte, erklärten SwissCybersecurity.net und Arctic Wolf in einem Webinar. Autor: Coen Kaat

Build or buy? Sollten Unternehmen selbst ein Security Operations Center (SOC) bauen oder besser für entsprechende Services zahlen? Dieser Frage gingen SwissCybersecurity.net und Arctic Wolf am 26. Juni in einem gemeinsamen Webinar auf den Grund. Eine One-Size-Fits-All-Lösung gibt es nämlich nicht: Beide Optionen haben ihre Vorteile und beide bergen auch Risiken – vor allem, wenn man Aufwand, Kosten oder Ressourcen falsch einschätzt.

Bevor Felix Guggenheim, Senior Sales Engineer bei Arctic Wolf, aufzeigte, wie Unternehmen die für sie richtige Lösung finden, schilderte er die aktuelle Bedrohungslage. Die präsentierten Zahlen zeichnen ein beunruhigendes Bild: Die durch Cyberkriminalität verursachten Schäden nehmen jährlich zu – und das Wachstum beschleunigt sich. 2023 stieg der Betrag im Vergleich zum Vorjahr um 21 Prozent auf 12,5 Milliarden US-Dollar. 2024 wuchs der Verlust sogar um 33 Prozent auf 16,6 Milliarden Dollar.

In derselben Zeit legten die Security-Ausgaben (183 Milliarden Dollar) um 13 Prozent zu. «Was heisst das nun?», fragte Guggenheim und lieferte sogleich eine Antwort: «Wir investieren zwar einerseits immer mehr Geld in die Cyberabwehr, diese Ausgaben scheinen aber nicht effektiv zu sein.» Der Schaden durch Cybercrime wächst schneller als die Investitionen in die Sicherheit.

Wohin fliesst dieses Geld? Viele Unternehmen würden laufend neue Sicherheitstools beschaffen – «natürlich haben sie sich um das Thema Passwörter gekümmert; natürlich haben sie Perimeter-Firewalls im Einsatz; natürlich nutzen sie Endpoint-Security-Lösungen», sagte Guggenheim. Aber die Unternehmen würden jeweils nur Lösungen für punktuelle Probleme erwerben. Daher hinken sie der Security hinterher, statt sie proaktiv zu betreiben. Das Problem liegt laut Guggenheim nicht bei der Beschaffung neuer Tools, sondern beim Betrieb all dieser Technologien. «Das heisst, in den Prozessen, im eigentlichen Alltag, wie ich mit diesen Technologien und der Situation insgesamt umgehe», präzisierte Guggenheim. Genau hier hapert es oft: beim Thema Security Operations.

«Und wo wird Security Operations betrieben? Normalerweise in einem SOC, womit wir beim eigentlichen Thema sind», scherzte Guggenheim. Ein SOC ist nämlich mehr als nur eine Alarmanlage, es soll auch insgesamt zeigen, wie man die Gesamtsicherheit verbessern kann.

Das gehört zu einem SOC

Frameworks wie der ITK-Minimalstandard geben einen Überblick, was alles zu einem SOC gehört. Dieser Minimalstandard bleibt gemäss Guggenheim aber auf einem sehr generischen Level; er empfiehlt daher, auch das BSI-Gesetz anzuschauen. Dieses gehe einen Schritt weiter und gebe auch eine konkrete Umsetzungshilfe. Gemäss dem BSI-Gesetz muss ein SOC im Wesentlichen drei Bereiche abdecken: Protokollierung, Detektion und Reaktion.

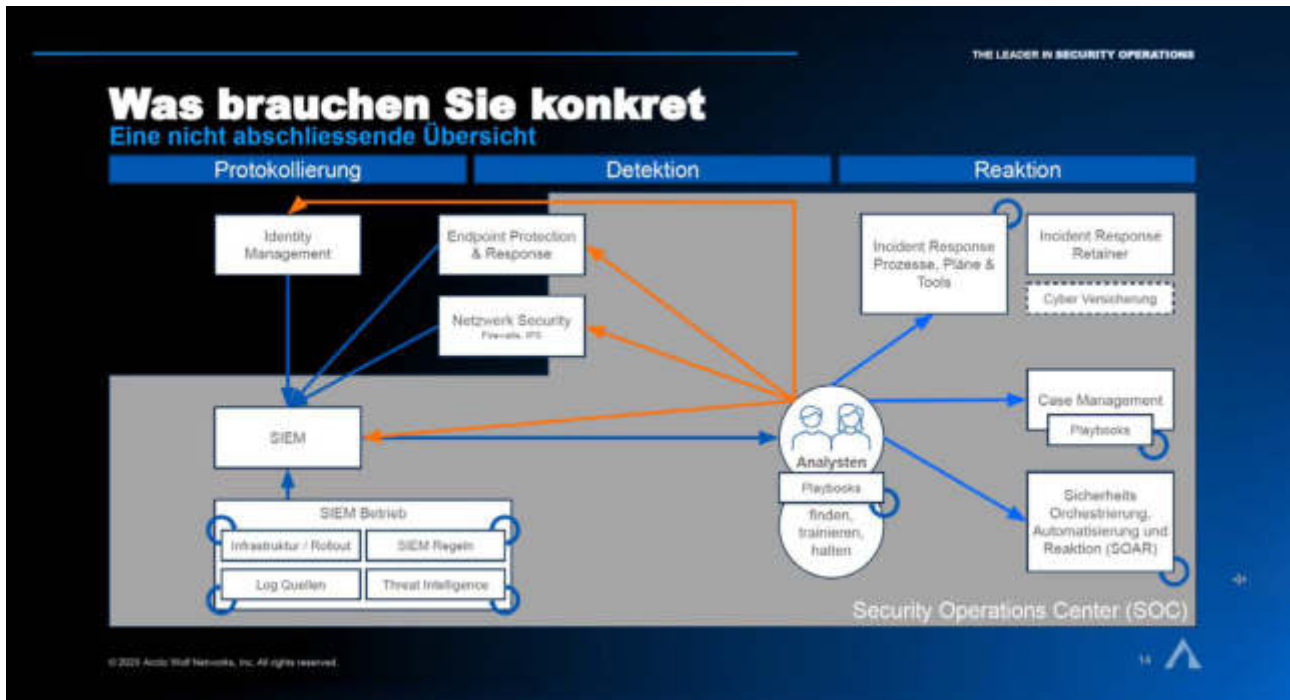
Aufgrund der konkreteren Vorgaben können Unternehmen also nicht einfach etwas annehmen und sich darauf berufen, dass sie es nunmal so verstanden haben. «Ich kann also nicht einfach irgendeinen schwindeligen Open-Source-Server nehmen und wenn die Festplatte voll ist, wird alles wieder gelöscht», sagte Guggenheim. Unternehmen müssen die Daten filtern, normalisieren, aggregieren, korrelieren und verfügbar halten. Eigentlich handle es sich hier also bereits um ein SIEM-System (Security Information and Event Management).

Gemäss Guggenheim geht beim Aufbau eines SOC oft vergessen, dass dieses mehr ist als nur Screens beziehungsweise ein Dashboard. Ein funktionierendes SOC ist eine Kombination aus Menschen, Tools und Prozessen. Wie wichtig diese SOC-Analysten seien, werde oft unterschätzt. Das Problem manifestiert sich dann in der bekannten (und aus Sicht des Risikomanagements berückichtigten) «One-Man-Show»: «Das macht bei uns der Patrick», heisst es dann; ein IT-Mitarbeiter soll nebenbei auch noch die Sicherheitswerkzeuge bedienen. Dies funktioniert nicht, da der IT-Betrieb meist höhere Priorität hat als noch nicht eingetretene Sicherheitsrisiken.

Das gilt es bei einem SOC zu vermeiden

Ein vollständiges SOC erfordert also ein SIEM, Threat Intelligence, Sicherheitstools, qualifizierte Analysten, standardisierte Playbooks, Case Management und Incident-Response-Pläne. Wer ein SOC aufbaut, stösst gemäss Guggenheim möglicherweise auf folgende typische Probleme:

- Finden, Trainieren und Halten der SOC-Analysten
- SOC-Betrieb nur von Montag bis Freitag
- Fehlende Befugnisse und Beratungsgewalt des SOC
- Unterschätzen des Aufwands, das SOC in den vorhandenen Stack und die Prozesse zu integrieren
- Unterschätzen des Aufwands für die Feinabstimmung der Analyse (verheddern in Details)



Das sind die Bestandteile eines SOC. Bild: Screenshot Webinar

- Mangel an Threat-Intelligence-Informationen
- Nur auf Vorfälle ausgerichtete Arbeit, ohne Folgemassnahmen und proaktive Sicherheitsverbesserungen
- Konzentration auf punktuelle Lösungen und Vertrauen in das Marketing der Security-Hersteller.

«Es gibt noch sehr viele weitere mögliche Probleme», sagte Guggenheim, bevor er auf seinen Slides scherzhaft als Problem Nummer 999 aufführte: der Glaube, dass KI alle oben genannten Probleme lösen könne.

«Security ist ein 24/7-Betrieb; dafür braucht es mindestens acht bis neun Personen, um drei Schichten abdecken zu können», rechnete Guggenheim vor. Nur so könne man krankheits- oder ferienbedingte Ausfälle abfedern. Trotz grosser Marketingversprechen löse KI dieses Problem nicht. Guggenheim warnte daher vor überzogenen Erwartungen. Machine Learning helfe zwar bei der Effizienz, könne aber getäuscht werden und liefere nicht immer sinnvolle Empfehlungen. KI eigne sich vielmehr als Hilfsmittel für menschliche Analysten, nicht als deren Ersatz.

Cloud Act, Open Source und Economies of Scale

«Wie kann ich sehr viele dieser Probleme einfach umgehen?», fragte Guggenheim rhetorisch. «Man kann das Ganze etwa als Service beziehen. Denn all diese Probleme sind schon gelöst.» Unternehmen, die nicht bereit sind, die notwendigen Ressourcen aufzubringen, oder keine erfahrenen Fachkräfte finden, empfiehlt Guggenheim einen externen Service. Diese seien in der Regel sehr schnell bereit und «finanziell sehr, sehr attraktiv». Denn die Kunden profitieren hier von Skaleneffekten beim Hersteller: Einmal gebaut, wird so ein Service bei vielen Kunden ausgerollt, was den Kosten- und Ressourcenaufwand optimiert.

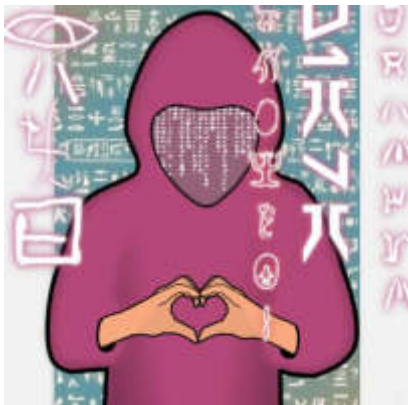
In der Frage-und-Antwort-Runde, die auf Guggenheims Präsentation folgte, fragte ein Webinar-Teilnehmer nach den Implikationen des US-Cloud-Acts. Als US-amerikanisches Unternehmen untersteht auch Arctic Wolf dem «Clarifying Lawful Overseas Use of Data Act», dem Gesetz, das es US-Behörden erlaubt, auf Daten zuzugreifen, die von US-Cloud-Anbietern im Ausland gespeichert werden. «Das heisst, man muss sich natürlich Gedanken machen, welche Daten über das SOC laufen und wie gross das Risiko ist, dass die amerikanischen Strafverfolgungsbehörden tatsächlich ein Interesse an diesen Daten haben», sagte Guggenheim. Log-Daten seien aber typischerweise «nichts wirklich Spannendes», sagte er. Benutzernamen, E-Mail-Adressen, IP-Adressen, Hostnamen. «Jede Firma, die sich etwa für Microsoft 365 entschlossen hat und Exchange Online oder Sharepoint Online betreibt, hat bereits weitaus sensiblere Daten an ein amerikanisches Unternehmen geschickt.»

Im Rahmen der Diskussion ging Guggenheim auch auf das Thema Open Source ein. So gibt es etwa Threat Intelligence, die man von Bundesbehörden beziehen kann. «Das Problem hier ist die Standardisierung», sagte Guggenheim. Es stellen sich Fragen wie: «Wie kriege ich das geordnet in ein Detektionssystem?» oder: «Was ist auch alles wesentlich für mich?». «Wenn man alles einfließen lässt, besteht die Gefahr, von so vielen Alerts überflutet zu werden, dass man sie gar nicht abarbeiten kann – obwohl sie gar nicht relevant sind», gibt Guggenheim zu bedenken. Der wahre Aufwand liegt hier also nicht in der Beschaffung der Informationen, sondern darin, diese Daten zu pflegen und aus der Fülle die richtigen herauszulesen.



Den vollständigen Artikel finden Sie online
swisscybersecurity.net

Was Sicherheitsexperten derzeit den Schlaf raubt



Malware-Entwickler liebäugeln mit ausgefallenen Programmiersprachen

Das Katz-und-Maus-Spiel zwischen der Cyberabwehr und der Cyberkriminalität ist ein konstantes Wettrüsten. Um der Detektion durch Antivirenprogramme und sonstige Abwehrmechanismen zu entgehen, setzen einige Malware-Entwicklerinnen und -Entwickler auf «ausgefallene Programmiersprachen». Zu diesem Schluss kommen Forschende der Universität von Piräus und des Athena Research Center in Griechenland sowie der Delft University of Technology in den Niederlanden. Dieser Ansatz wird als «Security through obscurity» bezeichnet, wie es in einem Bericht von «The Register» heisst. Wenn nur wenige Personen mit einer Sprache vertraut sind, gibt es wohl auch weniger manuelle Erkennungen von Malware in dieser Sprache. Zudem funktioniert auch eine signaturbasierte Erkennung nicht mehr. Als Beispiele nennen die Forschenden die Hive- und die Akira-Ransomware – diese wechselten zu Rust. Die Blackbyte-Ransomware gab derweil C# zugunsten von Go auf.



Mehr im Security-Blog:
[SwissCybersecurity.net/Blog](https://swisscybersecurity.net/Blog)



Ghost Calls – wenn Hacker im Hintergrund mittelefonieren

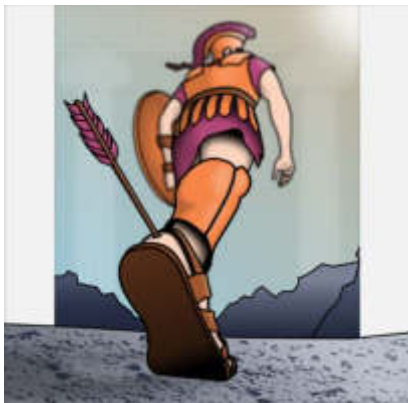
Damit Cyberattacken funktionieren, müssen Hacker eine verlässliche Kommunikation zu ihren Schadprogrammen auf infizierten Rechnern aufbauen. Während die Angreifer neue Methoden suchen, um ihre Kommunikation zu verstecken, tut die Cyberabwehr genau dasselbe, um neue Verschleierungstaktiken durchschauen zu können, noch ehe sie zum Problem werden. So auch die Security-Experten von Praetorian. Das Unternehmen beschreibt, wie Hacker Zoom und Microsoft Teams für ihren eigenen Datentransfer ausnutzen könnten, und nennt die Methode «Ghost Calls». Die Attacke läuft über legitime Anmeldedaten, WebRTC und eigens entwickelte Tools, um die meisten bestehenden Abwehrmechanismen zu umgehen. Ghost Calls kapert die TURN-Server, die Videokonferenz-Lösungen wie Zoom und Microsoft Teams nutzen. TURN ist ein Netzwerkprotokoll, das Geräten hinter NAT-Firewalls hilft, miteinander zu kommunizieren. Versucht ein Zoom- oder Teams-Client einem Meeting beizutreten, erhält er temporäre TURN-Anmeldedaten. Mit diesen kann ein Angreifer einen TURN-basierten WebRTC-Tunnel zu einem infizierten Rechner aufbauen.



Traue keiner Spinne, die sich angeblich vom Cybercrime verabschiedet

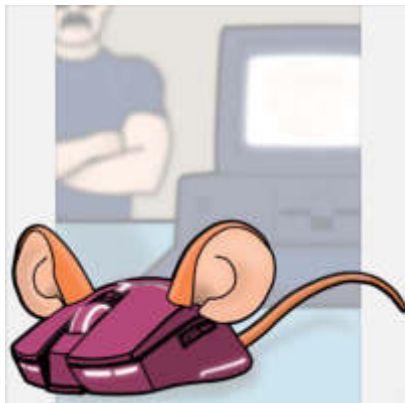
Da haben die Optimisten aufgehört: 15 Ransomware-Banden kündigten an, sich aus dem Cybercrime zurückzuziehen. Dies gaben die Kriminellen Mitte September 2025 auf Breachforums bekannt. Unter den erwähnten Gruppierungen sind auch einige Namen, die in jüngster Vergangenheit immer wieder für Negativschlagzeilen sorgten, wie etwa Scattered Spider und Lapsus\$. Gemäss dem Post geniessen die Cyberkriminellen nun ihre «goldenen Fallschirme mit den Millionen, die die Gruppe angehäuft hat». Die Ansage könnte auch mit der Verhaftung verschiedener Mitglieder der kriminellen Banden im Zusammenhang stehen. Doch aus Wölfen werden keine Lämmer – und aus Spinnen auch nicht. Die «Pensionierung» scheint nur eine Finte gewesen zu sein: Scattered Spider hat bereits wieder zugeschlagen, wie «The Register» berichtet. Die Security-Firma Reliaquest erappte die Bande dabei, wie sie in das Netzwerk einer US-amerikanischen Bank eindrang. Die Cyberattacke sei erfolgt, nachdem die Ransomware-Gruppen ihren angeblichen Austritt aus dem Cybercrime angekündigt hatten.

Komisch, spannend und beängstigend. Jeden Tag gibt es neue Meldungen zu Distributed-Denial-of-Service-Attacken, Ransomware, Cryptominern und Co. Die gefundenen Perlen erscheinen online im IT-Security-Blog. An dieser Stelle eine kleine Auswahl aus den Sammlungen des vergangenen Jahres. Texte und Illustrationen: Coen Kaat



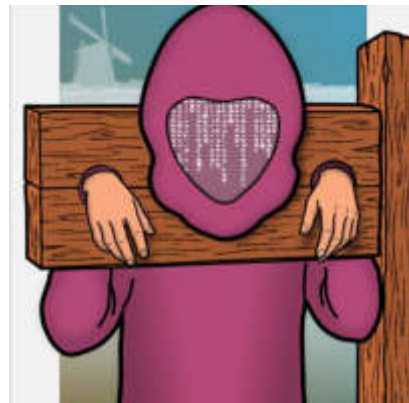
Clickjacking offenbart die Achillesferse von Passwortmanagern

Ein Passwortmanager kann helfen, die eigene Sicherheit zu erhöhen. User können damit für jedes Konto ein individuelles, starkes Passwort setzen, ohne dass sie sich alle merken müssen. Eine solche Lösung verursacht allerdings auch ein Klumpenrisiko: Nun schützt lediglich eine einzelne Schranke die Sicherheit aller Zugangsdaten. Genau das ist nun ein Problem. Der unabhängige Sicherheitsforscher Marek Tóth entdeckte eine Clickjacking-Schwachstelle in elf prominenten Passwortmanagern. Diese ermögliche es einem Hacker, Zugangsdaten, MFA-Codes und Kreditkartendaten zu stehlen. Die Schwachstelle wird zu einem Problem, wenn User eine manipulierte Website besuchen, die anfällig für Cross-Site-Scripting (XSS) oder Cache-Poisoning ist. Auf solchen Websites könnte ein Angreifer ein Skript ausführen, das mithilfe von Transparenzeinstellungen, Overlays oder Pointer-Event-Tricks das Autofill-Dropdown-Menü eines browserbasierten Passwortmanagers verbirgt. Tóth hatte die elf betroffenen Anbieter zuvor über die Schwachstelle informiert. Dennoch waren fünf Passwortmanager weiterhin angreifbar, als er seine Forschungsergebnisse präsentierte.



Auch die Computermaus kann lange Ohren machen

Die unscheinbaren Objekte im Alltag eignen sich oft hervorragend für Attacken. Schliesslich vergisst man schnell, etwas zu schützen, wenn man es gar nicht mehr bewusst wahrnimmt. Aber auch eine Computermaus kann bedrohlich werden: Forschende der University of California, Irvine zeigten, wie eine optische Maus zur Lausch-Maus wird. In ihrem Test nutzten die Forschenden eine Maus für 35 US-Dollar und eine eigens entwickelte Software, wie «The Register» berichtet. Die Software leitet aus den Sensorwerten der Maus Sprachmuster ab. «Und sie ist in der Lage, mehr als nur Sprache aufzunehmen», sagte Mohamad Fakih gegenüber «The Register». «Wenn jemand im Raum ist und dessen Schritte Vibrationen verursachen, kann man deren Bewegung verfolgen.» Da jeder Tastaturanschlag ein anderes Geräusch verursacht, könne eine Maus wohl auch entziffern, was man eintippt. Um diesen Angriffsvektor auszunutzen, muss ein Angreifer zunächst den Rechner seines Opfers infizieren. Die gewünschten Daten seien aber relativ einfach zu exfiltrieren. Erforderlich ist lediglich eine App, die Mausdaten verwendet, wie es im Bericht heisst.



Scammer treffen auf niederländische Direktheit und landen am Pranger

Die Niederlande sind bekannt für Windmühlen, Tulpen und Grachten – aber auch für die Direktheit ihrer Bevölkerung. In der Kommunikation machen Niederländer und Niederländerinnen für gewöhnlich keine Umwege: Effizienz und Transparenz stehen im Fokus. Auch die neue Strategie gegen Cyberbetrüger der niederländischen Polizei scheint geprägt von dieser Haltung. Sie will die Cyberkriminellen nämlich künftig öffentlich anprangern. Und zwar in ganz grossem Stil: Im Rahmen der «Game Over» genannten Kampagne zeigen seit dem 9. März Plakate im öffentlichen Raum, Werbespots im TV, Onlineanzeigen und die Website der Polizei 100 verdächtige Personen. Zunächst waren die Gesichter anonymisiert. Die Polizei gab den abgebildeten Personen die Chance, sich selbst bis zum 19. März zu melden. Bei ihnen verzichtete die Polizei darauf, das Foto unverpixelt zu publizieren. Die Fotos derjenigen Verdächtigen, deren Identität unbekannt blieb und die sich nicht stellten, gingen am 23. März online. Nur einen Tag darauf hatte die Polizei nach eigenen Angaben bereits 48 Verdächtige identifiziert. Die Kampagne soll zudem potenzielle Täter abschrecken.

Back on-prem: Die Renaissance hybrider Sicherheitsarchitekturen

Die Sicherheitslage der Schweiz verschärft sich kontinuierlich. In dieser Welt bieten Verträge kaum noch Schutz. Resiliente Unternehmen reagieren 2026 mit gezielter Repatriierung kritischer Daten in den lokalen Rechtsraum.



Die Schweiz befindet sich im Jahr 2026 nicht mehr in der Rolle des distanzierten Beobachters, sondern ist zum unmittelbaren Schauplatz und Ziel strategischer Auseinandersetzungen geworden. Der letztjährige Lagebericht des Nachrichtendienstes des Bundes (NDB) zeigt eine Welt im Umbruch, geprägt von einer globalen Konfrontation zwischen den USA, China und Russland. Christian Dussey, Direktor des NDB bis März 2026, beschreibt eine Ära der «strategischen Unsicherheit», in der technologische Abhängigkeiten als Machtmittel instrumentalisiert werden («Weaponization of Everything») – von Desinformation, Spionage bis zu Cyberoperationen. Die Eskalation im Nahen Osten verschärft derweil die geökonomischen Spannungen und macht die Energieversorgung zu einem weiteren Schauplatz strategischer Abhängigkeiten.

Die Schweiz gilt weiterhin als bevorzugter Operationsraum für Spionage, war während des Bürgerstock-Gipfels 2024 Ziel erhöhter Desinformationskampagnen und verzeichnete einen Anstieg der Meldungen von Cybervorfällen von 21 000 (2021) auf 65 000 (2025).

US CLOUD Act: Das Ende des blinden Vertrauens

In diesem volatilen Umfeld stossen kooperative Sicherheitsansätze an ihre Grenzen. Der NDB warnt, dass internationale Ordnungsmächte zunehmend unberechenbar agieren und die liberale Weltordnung unter Druck gerät. Dies macht blindes Vertrauen in grenzüberschreitende Abkommen und Verträge zu einem geschäftlichen Risiko.

Besonders kritisch ist die rechtliche Dimension: Je nach Anbieterjurisdiktion und Konstellation können extraterritoriale Regelungen (z. B. der US CLOUD Act) zu Herausgabepflichten führen, auch wenn Daten ausserhalb der USA gespeichert sind. Für Unternehmen wird damit entscheidend, wo Daten liegen, wer den Zugriff kontrolliert und wie Schlüssel- sowie Berechtigungskonzepte umgesetzt sind oder werden.

Die hybride Wende

Mangels einer rein souveränen europäischen Cloud-Lösung erleben wir 2026 eine Renaissance von On-Premise- und hybriden Sicherheitsarchitekturen. Ein hybrides Set-up erlaubt es, kritische

Geschäftsgeheimnisse sicher einzuschliessen und gleichzeitig agil auf wirtschaftliche, technologische und geopolitische Richtungsänderungen zu reagieren und somit die Wettbewerbsfähigkeit sicherzustellen.

Wer echte Resilienz erreichen will, muss zudem weg von fragmentierten Sicherheitsmassnahmen. Denn genau diese schwächen die Abwehrkraft – insbesondere heute, wo Angreifer Schwachstellen mithilfe von KI in Rekordgeschwindigkeit ausnutzen.

Die Partnerschaft von Symantec und e3 ermöglicht eine ganzheitliche, robuste Sicherheitsarchitektur: Symantec deckt als globaler Technologieführer die gesamte infrastrukturelle Breite ab – von SASE/SSE (Secure Web Gateway) über E-Mail- und Cloud-/SaaS-Schutz bis hin zum Endpoint-Schutz.

e3 verankert diese Breite operativ und setzt sie um: Hochpräzise Datenklassifizierung, individualisierte DLP-Policies und automatisierte Incident-Workflows sorgen dafür, dass sensible Daten im hybriden Alltag – auch bei der Nutzung von KI-Tools wie Copilot – unter Kontrolle bleiben.

Sichere Daten heute bedeuten ein starkes Business morgen. Erfahren Sie hier mehr über unsere ganzheitliche Sicherheitslandschaft:



e³

e3 AG

Binzstrasse 24 | 8045 Zürich
e3ag.ch

 Symantec
by Broadcom

 Carbon Black.
by Broadcom



Arrow ECS GmbH

Richtistrasse 11 | 8304 Wallisellen
arrow.com/globalecs/ch-de

KI-Angriffe setzen auf Masse statt Klasse

Ein neuer HP-Report zeigt, wie Cyberkriminelle KI für schnelle und skalierbare Angriffe nutzen. Dabei setzen sie statt auf Qualität auf Effizienz und umgehen dennoch die Abwehrmassnahmen von Unternehmen. Autorin: Dylan Windhaber, Netz-KI Bot

Cyberkriminelle setzen zunehmend künstliche Intelligenz ein, um ihre Kampagnen zu beschleunigen und zu skalieren. Dabei stellen sie jedoch Kosten und Aufwand über Qualität, wie aus dem aktuellen Threat Insights Report von HP hervorgeht. Obwohl KI-gestützte Angriffe oft einfach aufgebaut sind, erweisen sie sich als effektiv bei der Umgehung von Abwehrmassnahmen von Unternehmen, wie HP schreibt.

«Es geht um das klassische Projektmanagement-Dreieck: Geschwindigkeit, Qualität und Kosten. Oft muss man eines davon opfern», erklärt Alex Holland, Principal Threat Research im HP Security Lab. Die Betrüger nutzen KI dabei nicht, «um die Messlatte höher zu legen, sondern um schneller voranzukommen und den Aufwand zu reduzieren. Die Kampagnen selbst sind einfach aufgebaut, aber die unangenehme Realität ist: Sie funktionieren immer noch.»

Eine der identifizierten Techniken nennt sich «Vibe-Hacking». Dabei setzen Angreifer auf KI, um vorgefertigte Infektionsskripte zu generieren und so die Verbreitung von Malware zu automatisieren. Laut Report löste in einer Kampagne beispielsweise ein Link in einer gefälschten PDF-Rechnung das Laden einer kompromittierten Website aus. Mit dem Ziel, die Glaubwürdigkeit zu erhöhen und den Anwender zu täuschen, seien die Opfer im Anschluss auf vertrauenswürdige Plattformen wie Booking.com weitergeleitet worden.

Eine weitere Methode ist die sogenannte «Flat-Pack-Malware», wie HP schreibt. Laut Bericht stellen die Kriminellen hierbei Angriffe aus kostengünstigen, handelsüblichen Malware-Komponenten zusammen, die sie vermutlich in Hackerforen erwerben. Dazu legen die Bedrohungsakteure zwar jeweils andere Köder aus, verwenden aber wiederholt dieselben Zwischenskripte und Installationsprogramme. Dies ermöglicht es, Kampagnen mit mini-

malem Aufwand zu erstellen und zu skalieren. Dabei handle es sich nicht um das Werk einer einzelnen Gruppe, sondern um eine Taktik, die von mehreren unabhängigen Akteuren genutzt werde.

Des Weiteren habe HP Wolf Security sogenannte «Piggyback»-Angriffe beobachtet, bei denen Malware in gefälschten Installationsprogrammen versteckt wird. Angreifer nutzen bei dieser Taktik gemäss Bericht Suchmaschinenvergiftung und bösartige Anzeigen, um auf gefälschte Microsoft-Teams-Websites zu locken. Dort würden die Opfer ein Installationspaket herunterladen, das die «Oyster-Loader»-Malware enthalte. Diese werde unbemerkt während des Installationsprozesses der echten App eingeschleust und verschaffe den Cyberkriminellen eine Hintertür zum jeweiligen Gerät.

Detektionsbasierte Sicherheit stösst an Grenzen

Die Analyse, die Daten von Millionen von Endgeräten zwischen Oktober und Dezember 2025 untersuchte, zeigt, dass mindestens 14 Prozent der von HP Sure Click identifizierten E-Mail-Bedrohungen einen oder mehrere E-Mail-Gateway-Scanner umgingen. Die beliebteste Art der Übertragung von Malware waren laut Bericht mit 37 Prozent ausführbare Dateien, gefolgt von .zip-Dateien mit 11 Prozent und .docx-Dateien mit 10 Prozent.

«KI-gestützte Angriffe zeigen die Grenzen der detektionsbasierten Sicherheit auf. Angreifer generieren innerhalb von Minuten Malware und verpacken sie neu – detektionsbasierte Abwehrmassnahmen können da nicht mithalten», kommentiert Ian Pratt, Global Head of Security for Personal Systems bei HP. Er empfiehlt Unternehmen, stattdessen ihre Angriffsfläche zu reduzieren. «Indem sie risikoreiche Aktivitäten – beispielsweise das Öffnen nicht vertrauenswürdiger Anhänge oder das Anklicken unbekannter Links – in einer isolierten Umgebung eindämmen, sind Unternehmen in der Lage, Bedrohungen zu stoppen, bevor sie Schaden anrichten, und eine Risikoklasse komplett zu beseitigen.»



LLMs durchbrechen Anonymität im Netz

Eine Studie zeigt, dass LLMs Personen anhand von ansonsten anonymen Onlinebeiträgen identifizieren können. Durch die Kombination aus der Analyse von Sprachmustern und automatisierter Recherche gelingt es den KI-Modellen, Konten zu verknüpfen und Identitäten in grossem Umfang abzuleiten. Ein Befund, der neue Fragen zum Datenschutz aufwirft. Autorin: Alexia Muanza, Übersetzung: Dylan Windhaber, Netz-KI Bot

Unter dem Titel «Large-Scale Online Deanonimization with LLMs» zeigt eine aktuelle Studie, veröffentlicht auf dem Onlinearchiv Arxiv, dass Large Language Models (LLMs) bereits anhand weniger Veröffentlichungen persönliche Attribute wie Wohnort, berufliche Tätigkeit oder Interessen ableiten können. Diese Informationen könnten anschliessend genutzt werden, um plausible Übereinstimmungen im Internet zu suchen. Dabei handle es sich nicht um eine garantierte automatische Identifizierung, sondern um einen probabilistischen Schlussfolgerungsprozess, der auf der Aggregation öffentlich verfügbarer Daten basiert.

Die Autoren der Studie weisen darauf hin, dass die Identifizierung von Personen anhand einer begrenzten Anzahl von Attributen bereits seit Langem bekannt ist, jedoch bislang wegen des unstrukturierten Charakters der Daten und des Aufwands der dafür notwendigen menschlichen Ermittlungen nur schwer in grossem Umfang umsetzbar war. LLMs würden dies ändern, indem sie eine automatisierte Strukturierung dieser Informationen ermöglichen und zugleich über eine hohe Fähigkeit zur Mustererkennung und zur Recherche verfügen.

Kontrollierte Experimente auf mehreren Plattformen

Um diese Fähigkeiten zu bewerten, ohne dabei direkt Personen zu deanonymisieren, die keinerlei öffentliche Informationen preisgegeben haben, wurden laut den Studienautoren mehrere experimentelle Protokolle entwickelt.

Das erste Protokoll beinhaltete die Verknüpfung von Konten derselben Person über verschiedene Plattformen. Öffentliche Hacker-News-Konten, die absichtlich mit LinkedIn-Profilen verknüpft waren, habe man im Nachhinein anonymisiert und anschliessend den Modellen vorgelegt. Die Modelle sollten die korrekte Übereinstimmung aus einer grossen Menge von Kandidaten ermitteln.

Ein zweites Protokoll basierte auf der künstlichen Aufteilung bestehender Reddit-Konten nach zeitlichen oder communitybezogenen Merkmalen. Wie es heisst, übertrafen in diesen Szenarien die LLMs, die Einbettungen (Embeddings) und logische Schlussfolgerungen kombinieren, deutlich die herkömmlichen Methoden, die ausschliesslich auf Metadaten oder Aktivitätsmustern basierten.

Hohe Leistungsfähigkeit trotz Skalierung

Die Analyse zeigt, dass die Leistung mit zunehmender Grösse der Kandidatenmenge allmählich abnimmt, die Genauigkeit



Bild: SnowElf - stock.adobe.com

selbst bei mehreren zehntausend Profilen jedoch hoch bleibt. Die Autoren schätzen, dass diese Methoden mit zusätzlichen Rechenressourcen und der kontinuierlichen Weiterentwicklung der Modelle bereits auf ganze Plattformen angewendet werden könnten.

Abschliessend habe man den Ansatz auf einem echten Datensatz anonymisierter Interviews aus einem Forschungsprogramm von Anthropic getestet. Laut Studie konnten dabei von 125 Interviews neun Personen anhand einer manuellen Verifizierung identifiziert werden, obwohl keine offiziellen Referenzdaten vorlagen.

Mögliche Gegenmassnahmen

Die Studie untersucht zudem mehrere Strategien zur Minderung des Risikos. Plattformen könnten den Datenzugriff einschränken und Massensexporte begrenzen. Auf Anbieterseite stiessen Opt-out- und Nutzungsüberwachungsmechanismen an ihre Grenzen, da diese Angriffe in scheinbar harmlose Teilaufgaben unterteilt werden können. Generell betonten die Autoren die Notwendigkeit, die kumulative Verbreitung personenbezogener Informationen im öffentlichen Raum oder unter Pseudonymen zu reduzieren.



Den vollständigen Artikel finden Sie online

[swisscybersecurity.net](https://www.swisscybersecurity.net)

Wir brauchen einen Gesellschaftsvertrag für die digitale Welt

Die digitale Transformation ist längst Realität. Doch wir leben noch immer nach Regeln, die für eine vordigitale Gesellschaft gemacht wurden. Es ist höchste Zeit, einen neuen Gesellschaftsvertrag auszuhandeln, bevor andere die Bedingungen für uns festlegen.

Auf der Bühne der Swiss Cyber Security Days in Bern haben wir kürzlich über die Abhängigkeit Europas von fremder Technologie diskutiert. Zwei Drittel bis drei Viertel unserer digitalen Infrastruktur stammen nicht aus der Schweiz oder Europa, sondern meist aus den USA oder China. Doch das eigentliche Problem liegt tiefer: Wir haben die Wichtigkeit des digitalen Raumes nie wirklich erkannt. Wir haben uns bei Dritten in ihre Clouds eingemietet, ohne über die Konsequenzen, die Kontrolle oder die Verantwortung nachzudenken.

Früher kaufte man Software, installierte sie lokal und bestimmte selbst, was damit passiert. Heute mieten wir Plattformen. Unsere Daten, unsere Prozesse, unsere Kommunikation laufen über Server, die wir nicht kontrollieren, in Jurisdiktionen, die nicht unsere sind, nach Regeln, die wir nicht mitbestimmt haben. Jede Zeile Code ist ein Regelwerk. Und dieses Regelwerk schreiben andere.

Ehrlich gesagt haben wir die Digitalisierung nur zur Hälfte gemacht. Wir haben uns von Features blenden lassen, aber vergessen, das Fundament zu bauen. Der Cyberspace ist zur fünften Dimension geworden, zum Fundament unserer Gesellschaft. Ohne ihn funktioniert nichts mehr. Und trotzdem leben wir dort zur Miete. Wir verbauen Betriebssysteme in kritischen Infrastrukturen wie einem Kraftwerk, deren Lizenzvereinbarungen jede Haftung ausschliessen. Niemand würde ein Kraftwerk von einem fremden Staat betreiben lassen. Aber genau das tun wir jeden Tag im digitalen Raum.



Der Autor

Nick Mayencourt,
Founder, Dreamlab Technologies

Wohin das führen kann, zeigt China. Wechat begann als Messenger und ist heute Identitätskarte, Bankkonto, Jobportal und Transportticket in einem. Jede Interaktion wird erfasst, bewertet, kontrolliert. Totale gesellschaftliche Steuerung über eine einzige App. Das ist keine ferne Dystopie. Wenn Elon Musk erklärt, er wolle X zur westlichen Version von Wechat machen, sollte uns das hellhörig machen.

Was wir erleben, ist im Grunde eine digitale Kolonialisierung. Wir sind die Kolonisierten und bezahlen freiwillig dafür. Dazu kommt ein Aspekt, der fast noch schwerer wiegt: der kulturelle. Wer ausschliesslich fremde Software konsumiert, übernimmt unweigerlich einen kulturellen Imprint. Software ist normativ, sie gibt vor, wie wir arbeiten, kommunizieren und denken. Unsere Identität wird schleichend verwässert. Wir werden kulturell assimiliert, ohne es zu merken.

Deshalb brauchen wir jetzt einen neuen Gesellschaftsvertrag für die digitale Welt. Einen Vertrag, der klärt, welche Rolle der Staat hat, welche Verantwortung Unternehmen tragen und welche Rechte und Pflichten Bürgerinnen und Bürger im digitalen Raum haben. Einen Vertrag, der den gesamten Digitalraum als das behandelt, was er ist: kritische Infrastruktur. Und einen Vertrag, der auch die Frage beantwortet, was mit den Menschen passiert, deren Arbeit künftig von Maschinen erledigt wird.

Bern als Bundesstadt mit dem Bundesamt für Cybersicherheit, dem Kommando Cyber und dem diplomatischen Corps ist der richtige Ort, um diesen Dialog zu führen. Mit den Swiss Cyber Security Days und den geplanten Konferenzen entstehen hier die Formate dafür.

Was es dafür braucht, ist mehr als politischer Wille. Es braucht einen Ruck durch die gesamte Gesellschaft und einen Bewusstseinswandel: IT ist kein Spielzeug, sondern kritische Infrastruktur und muss als solche behandelt werden. Die Technologie ist da, um uns zu dienen. Nicht umgekehrt. Aber das passiert nicht von allein.



Den Beitrag finden
Sie auch online

swisscybersecurity.net

Bild: ikhsan - stock.adobe.com

Digitale Transformation umsetzen und steuern

Netrics begleitet Unternehmen End-to-End auf dem Weg der digitalen Transformation – mit Fokus auf Multi-Cloud, Data & AI sowie Security by Design. Ziel ist es, digitale Initiativen nicht nur umzusetzen, sondern nachhaltig zu betreiben und wirtschaftlich zu steuern.

Der Schweizer ICT-Markt entwickelt sich zunehmend in Richtung service- und beratungsgetriebener Modelle. Cloud, KI und Cybersecurity stehen im Fokus, während die Anforderungen an Effizienz, Sicherheit und Integration steigen. Viele Unternehmen stehen vor der Herausforderung, digitale Initiativen in stabile, skalierbare und wirtschaftlich tragfähige Lösungen zu überführen.

Netrics setzt genau hier an und begleitet als IT-Dienstleister im Schweizer Mid-Market Unternehmen über den gesamten Lebenszyklus der digitalen Transformation – von der Strategie bis zum Betrieb. Dabei verbinden wir Beratung und Umsetzung und übernehmen Verantwortung für das Zusammenspiel von Technologie, Prozessen und Organisation. Im Zentrum steht nicht die Technologie, sondern der konkrete Nutzen für Kunden und ihr Business. Ziel sind praxisnahe Lösungen, die sich nachhaltig integrieren lassen und langfristig funktionieren.

Zusammenarbeit und Produktivität verbessern

Netrics unterstützt Unternehmen, ihre Workplace-Strategie ganzheitlich zu entwickeln und umzusetzen. Im Fokus steht die Abstimmung von Tools, Prozessen und Mitarbeitenden, um die Zusammenarbeit zu vereinfachen, Medienbrüche zu reduzieren und die Effizienz zu steigern. Gleichzeitig schaffen wir moderne Workplace-Lösungen mit standardisierten Security Base Layer – die Grundlage für flexible Arbeitsmodelle und den sicheren Umgang mit Daten.

Da die grösste Herausforderung in der nachhaltigen Integration in bestehende Prozesse liegt, unterstützt Netrics Unternehmen dabei, konkrete Use Cases zu identifizieren und in den operativen Betrieb zu überführen.

Die Cloud als Betriebsmodell – mit klarer Steuerung

Wir helfen Unternehmen dabei, ihre Cloud-Architektur ganzheitlich zu entwickeln und zu betreiben – inklusive klarer Zuordnung von Workloads, Aufbau geeigneter Plattformstrukturen und der Steuerung über verschiedene Umgebungen hinweg. Ein zentraler Bestandteil ist dabei FinOps, das als verbindendes Steuerungsmodell zwischen IT, Finance und Business Transparenz über die Cloud-Kosten schafft, Verantwortlichkeiten klärt und

fundierte Entscheidungen ermöglicht. So wird Cloud nicht nur technisch betrieben, sondern gezielt als wirtschaftlicher Hebel genutzt.



Das Company Profile finden Sie auch online
[swisscybersecurity.net](https://www.swisscybersecurity.net)



Security-by-design

Steigende Bedrohungen, regulatorische Anforderungen und komplexe IT-Landschaften erhöhen den Handlungsbedarf für Unternehmen deutlich. Entscheidend ist dabei die Fähigkeit, Security im Alltag wirksam zu betreiben. Netrics verfolgt einen ganzheitlichen Ansatz – von der Analyse über die Umsetzung bis hin zum laufenden Betrieb von Security-Lösungen. Dabei stehen nebst Systemen vor allem Menschen im Fokus, die diese betreiben und weiterentwickeln.

Digitale Transformation durchgängig umsetzen

Unternehmen arbeiten mit unterschiedlichen Partnern für Beratung, Umsetzung und Betrieb zusammen, was zu einem erhöhten Abstimmungsaufwand und unklaren Zuständigkeiten führt. Besonders bei Cloud-, Security- oder Data- und KI-Lösungen zeigt sich, dass Systeme im Alltag nicht immer reibungslos zusammenspielen. Wir verfolgen daher einen durchgängigen Ansatz mit Planung, Umsetzung und Betrieb aus einer Hand. Für unsere Kunden bedeutet das: weniger Komplexität und eine IT, die mit den Anforderungen mitwächst.

netrics

Netrics AG

Tennisweg 6 | 2504 Biel | 058 531 31 31
info@netrics.ch | netrics.ch

Schweizer und Schweizerinnen verschwitzen Datenschutz bei KI

Der VPN-Anbieter NordVPN hat sich mit dem Datenschutz bei der Nutzung von KI in der Schweiz auseinandergesetzt. Demnach zeigen sich erhebliche Wissenslücken im Umgang mit solchen Tools im Arbeitsalltag. Autor: Coen Kaat

Anlässlich des Data Privacy Day am 28. Januar 2026 hat der VPN-Anbieter NordVPN über Datenschutzrisiken im Umgang mit künstlicher Intelligenz im Geschäftsalltag informiert. Demnach fehlt in Schweizer Unternehmen ein Verständnis dafür, welche Datenschutzaspekte sie bei KI-Anwendungen im beruflichen Kontext berücksichtigen müssen. Gemäss einer Umfrage dazu wissen 94 Prozent der Schweizer Teilnehmenden nichts darüber.

Die Daten stammen aus NordVPNs «National Privacy Test», einer weltweit durchgeführten Umfrage des VPN-Anbieters. Im Jahr 2025 beantworteten 36 667 Teilnehmende aus 192 Län-

dern 22 Fragen zu ihren Kenntnissen und Fähigkeiten rund um den Online-Datenschutz, wie NordVPN mitteilt. Wie viele Personen aus der Schweiz teilgenommen haben, ist nicht ersichtlich.

Die Studie offenbart laut Mitteilung weitere Sicherheitslücken: 38 Prozent der Schweizer Teilnehmenden seien nicht in der Lage, KI-gestützte Betrugsmaschen wie Deepfakes oder Voice-Cloning-Angriffe zuverlässig zu erkennen.

Die KI liest mit

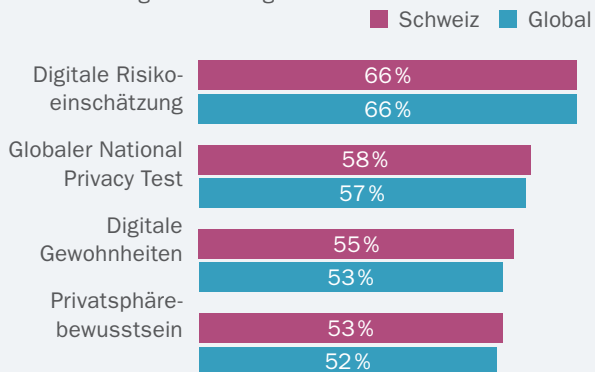
«Die rasante Verbreitung von KI am Arbeitsplatz hat unser Verständnis für die damit verbundenen Risiken überholt», sagt Marijus Briedis, Chief Technology Officer von NordVPN. «Viele Menschen geben vertrauliche Informationen in KI-Tools ein, ohne zu wissen, wohin diese Daten fliessen, wie sie gespeichert werden oder wer darauf Zugriff hat.»

Der entscheidende Unterschied zu klassischer Kommunikation liegt laut Briedis in der Persistenz der Daten: Interaktionen mit KI-Tools lassen sich speichern, analysieren und zum Training zukünftiger Modelle nutzen. Wenn Mitarbeitende Kundendaten oder interne Strategien mit KI-Assistenten teilen, könnten unbeabsichtigt potenzielle Datenschutzlücken entstehen.

Das Unternehmen empfiehlt, niemals vertrauliche Unternehmensdaten, Kundeninformationen oder persönliche Daten in KI-Assistenten einzugeben. Man solle sich bewusst sein, dass Gespräche mit KI-Tools möglicherweise protokolliert, gespeichert und ausgewertet werden.

DATENSCHUTZ-KENNTNISSE

Einschätzung der Kenntnisse und Fähigkeiten rund um den Online-Datenschutz der Schweizerinnen und Schweizer im globalen Vergleich



Quelle: NordVPN



Den vollständigen Artikel finden Sie online

swisscybersecurity.net

Asymmetrie in der Cybersicherheit – «schön» ist nicht immer «sicher»

In vielen Strategien wird Cybersecurity noch immer als ein «lösbares IT-Problem» im Sinne des Gleichgewichts der Kräfte behandelt, während es in der Realität ein dynamisches, asymmetrisches Wettrüsten ist, bei dem die Gegenseite erhebliche strukturelle Vorteile nutzen kann.

Lange galt Symmetrie als Schönheitsideal – sei es in der Architektur, der Kunst oder der Natur. Erst spät wurde die Asymmetrie zum Mittel des Ausdrucks von Individualität und gestalterischer Freiheit. Sätze wie «Symmetrie ist die Ästhetik der Dummheit» des Architekten Mies van der Rohe dokumentieren dieses veränderte Weltbild. In der Cybersicherheit gilt dies leider nicht – die Verteidigung digitaler Umgebungen gleicht heute einem Spiel, bei dem Regeln, Spielfeld und Zeit zugunsten der Angreifer manipuliert sind. Diese Asymmetrie verschärft sich zusehends. Dies hat folgende Gründe:

1. Strukturelle Ungleichgewichte: Während Verteidiger alle potenziellen Einfallstore (Hardware, Software, Identitäten, Lieferketten, Menschen etc.) rund um die Uhr lückenlos schützen müssen, führt den Angreifer eine einzige Schwachstelle oder ein unachtsamer Klick zum Erfolg. Die Angreiferseite hat sich professionalisiert. Von staatlich alimentierten Akteuren bis hin zu «Ransomware-as-a-Service»-Anbietern ist das Ökosystem hochgradig arbeitsteilig. Die Motivation ist oft finanziell oder geopolitisch getrieben und kennt weder Feierabend noch Mitleid.

2. Ressourcen und Technologie: Angreifer agieren oft mit minimalem Budget bei maximalem Schadenspotenzial durch geeignete Werkzeuge. Verteidiger hingegen müssen enorme Summen in Personal, Lizenzen und Infrastruktur investieren, oft ohne einen direkten «Return on Investment» nachweisen zu können – bis es zu spät ist. Angreifer nutzen neue Technologien wie KI und Automatisierung (und demnächst Quantencomputer), um Angriffe zu skalieren, gewonnene Daten auszuwerten usw. Die Verteidiger sind hingegen oft durch komplexe Legacy-Systeme, proprietäre Schnittstellen, langsame Change-Prozesse und akuten Fachkräftemangel gelähmt.

3. Regulierung als zweiseitiges Schwert: Während Regulierungen wie NIS-2, DORA etc. die Resilienz von IT-Umgebungen langfristig stärken sollen, binden sie kurzfristig massiv Ressourcen in der Compliance-Arbeit. Angreifer operieren hingegen losgelöst von

rechtlicher Verfolgung oder ethischen Rahmenbedingungen, was ihnen eine Agilität verleiht, die Unternehmen oder Behörden kaum kontern können.



Den Beitrag finden
Sie auch online
swisscybersecurity.net



Der Autor

Hannes P. Lubich, Professor für
Informatik, Fachhochschule
Nordwestschweiz



Bild: Jibber - stock.adobe.com

STRATEGISCHE HANDLUNGSOPTIONEN

Strategien müssen von der reinen Prävention hin zur Resilienz umschwenken. Hierfür sind die folgenden Punkte besonders zu berücksichtigen:

- Man muss akzeptieren und antizipieren, dass Kompromittierungen stattfinden werden. Hier liegt der Fokus auf Detektion und schneller, eingeübter Wiederherstellung von Not- und Regelbetrieb statt nur auf Schutzmauern. Dies darf jedoch nicht als «Kapitulation» verstanden werden – Awareness und Krisenresistenz der eigenen Organisation bleiben relevante Sicherheitsbausteine.
- KI-gestützte Systeme sind kein Luxus mehr, sondern die einzige Möglichkeit, der schier Masse an automatisierten Angriffen zu begegnen – jedoch weiterhin in den Grenzen der rechtlichen und regulatorischen Machbarkeit, Zuverlässigkeit und Nachvollziehbarkeit.
- Da der Fachkräftemangel ein systemisches Risiko ist, müssen Unternehmen verstärkt auf spezialisierte «Managed Security Service»-Partner mit nachgewiesenen Fähigkeiten (7/24, Incident Response etc.) setzen, um Skaleneffekte der Verteidigung zu nutzen. Die finale Verantwortung und Governance bleibt jedoch undelegierbar.
- Je weniger Angriffsfläche vorhanden ist (z. B. durch die Migration und Abschaltung von Altsystemen oder die Umsetzung von «Security by Design»- und «Privacy by Default»-Konzepten in Projekten und Beschaffungen), desto geringer ist die asymmetrische Last.

