PICTET GROUP

Cybersicherheit - Schutz, Erkennung und Reaktion auf Cyber-Bedrohungen

Florian Widmer

HEAD OF CYBERSECURITY & CRO TECH

10. JUNI 2026, MÜNCHEN

87% German companies affected by **data theft, espionage or sabotage** in 2025[1]

€289 bn in damages to the **German economy** in 2025[1] ($10tn globally)

57% employees use unapproved GenAI tools[2]

29 minutes average time between initial access and lateral movement[3]

1. *Wirtschaftsschutz 2025*, Bitkom
2. *Top 2026 Cybersecurity Trends*, Gartner
3. *Global Threat Report 2026*, Crowdstrike

1

What is at stake ?

5 Main Sources of Cyber Risk

External Actors

- **Nation-states**
- **Organized cybercrime**
- **Hacktivists**

Internal Factors

- **Third party dependencies**
- **Insider threat**

Snowflake data breach

External Actors

Organized cybercrime

Internal Factors

Third party dependencies

Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign

Ravie Lakshmanan Jun 11, 2024 Data Theft / Cloud

As many as 165 customers of Snowflake are said to have had their information potentially exposed as part of an ongoing campaign designed to facilitate data theft and extortion, indicating the operation has broader implications than previously thought.

Google-owned Mandiant, which is assisting the cloud data warehousing platform in its incident response efforts, is tracking the as-yet-unclassified activity cluster under the name **UNC5537**, describing it as a financially motivated threat actor.

"UNC5537 is systematically compromising Snowflake customer instances using stolen customer

Top Stories This Week

Ivanti, Fortinet, SAP, VMwar
RCE, SQL Injection, Privileg
Flaws

Microsoft Exchange (email system)

EXTERNAL ACTORS

ORGANIZED CYBERCRIME

Microsoft hack escalates as criminal groups rush to exploit flaws

Attack initially targeting 'specific' individuals turns to global free-for-all as criminal groups enter fray

Estimates of the number of victims of the cyber attack on Microsoft's email software have run as high as 250,000, with many believed to be small businesses © FT montage

Hannah Murphy in San Francisco

Published MAR 9 2021

172

Stay informed with free updates

Simply sign up to the Cyber Security myFT Digest -- delivered directly to your inbox.

Enter your email address

Sign up

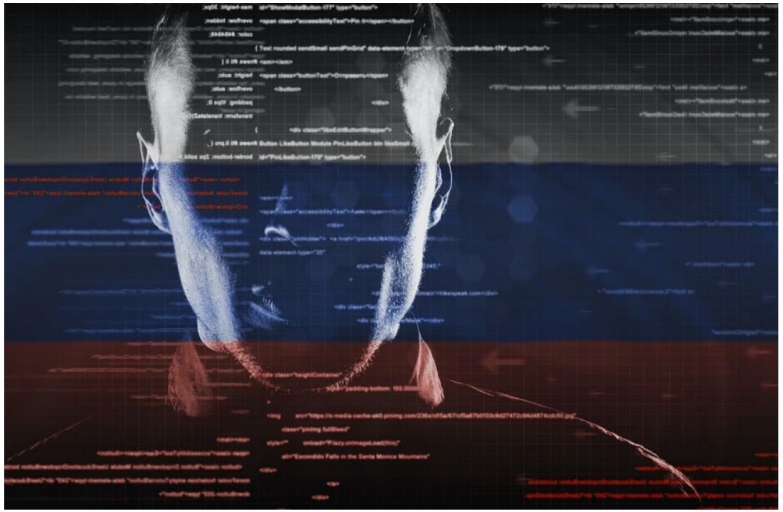
What began as a clandestine Chinese espionage campaign targeting "specific individuals" via flaws in Microsoft email software has escalated into a devastating global hacking free-for-all that is claiming tens of thousands of business and public-sector victims.

Distributed Denial of Service

External Actors

Hacktivists

Schweiz › Digital › Prorussische Gruppe NoName057(16) greift weiter Websites des Bundes an



NoName057(16) hat erneut für negative Schlagzeilen gesorgt.

bild: shutterstock

Prorussische Hacktivisten greifen weiter Websites des Bundes an

Ruag 2016

EXTERNAL ACTORS

NATION-STATES

Schweiz › Armee › Hacker greifen Ruag und VBS an: Steckt Russland dahinter?

Hacker greifen Ruag und VBS an: Steckt Russland dahinter?

10

Als bevorzugte Quelle hinzufügen

News folgen

04.05.2016, 06:12 04.05.2016, 06:29

Hacker haben im vergangenen Januar versucht, den Rüstungsbetrieb Ruag und das Verteidigungsdepartement VBS auszuspionieren. Bundesrat Guy Parmelin bestätigte entsprechende Medieninformationen. Unklar ist, welche Schäden die Angreifer anrichteten.

Salt Typhoon 2024

EXTERNAL ACTORS

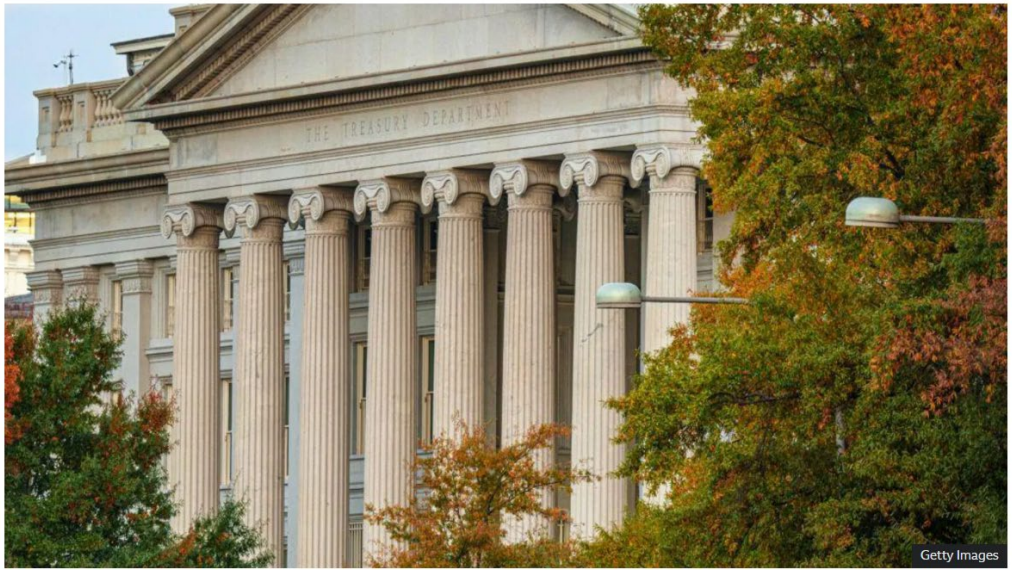
NATION-STATES

US Treasury says it was hacked by China in 'major incident'

31 December 2024

Share Save Add as preferred on Google

Nadine Yousif and Joe Tidy
BBC News



Chinese state-sponsored hackers broke into the US Treasury Department's systems earlier this month and were able to access employee workstations and some unclassified documents, American officials have said.

Salt Typhoon 2025

External Actors

Nation-states

China used three private companies to hack global telecoms, U.S. says

An FBI spokesperson told NBC News that Salt Typhoon has hacked more than 200 companies across 80 countries.

A Chinese flag is raised Wednesday in Tiananmen Square in Beijing. Kyodo via AP

SHARE | ADD NBC NEWS TO GOOGLE

Aug. 27, 2025, 11:03 PM GMT+2

By Kevin Collier

China OR Cloud 2023

External Actors

Nation-states

Internal Factors

Third party dependencies

Microsoft: China accused of hacking US government emails

13 July 2023

Share Save Add as preferred on Google

Annabelle Liang
Business reporter

China-based hackers have gained access to the email accounts of around 25 organisations, including government agencies, Microsoft says.

The software giant has not provided details of where the government agencies are based.

Drone Manufacturer 2026

EXTERNAL ACTORS

NATION-STATES

NZZ

Wollte Russland einen deutschen Drohnenfabrikanten töten lassen?

Ein Unternehmer aus Bayern wurde offenbar über Monate von mutmasslichen Spionen im Auftrag Moskaus beobachtet. Das Ziel könnte ein Anschlag auf den Mann gewesen sein. Der Fall ist nicht der erste dieser Art in Deutschland.

Anna Schiller, Berlin 25.03.2026, 11.58 Uhr 3 Leseminuten

Hören 4:56 Zusammenfassung Teilen Merken

Die Sabotagefälle in Deutschland häufen sich. Hinter vielen vermuten die deutschen Behörden Agenten im Auftrag des Kremls. Sergei Ilnitsky / EPA

Über Monate wurde ein deutscher Unternehmer aus dem Verborgenen beobachtet. Sein Umfeld wurde studiert, seine Wege aufgezeichnet. Alles hielten seine Verfolger mit Handykameras fest: wie es an seinem

Rheinmetall Ransomware 2025

External Actors

- **Nation-states**
- **Organized cybercrime**

tagesschau

tagesschau24 live

Startseite ▸ Wirtschaft ▸ Digitales ▸ Hackerangriff auf Rheinmetall: Nationale Sicherheit bedroht?

Sensible Daten von Rüstungsfirmen

Bedrohen Hackerangriffe die nationale Sicherheit?

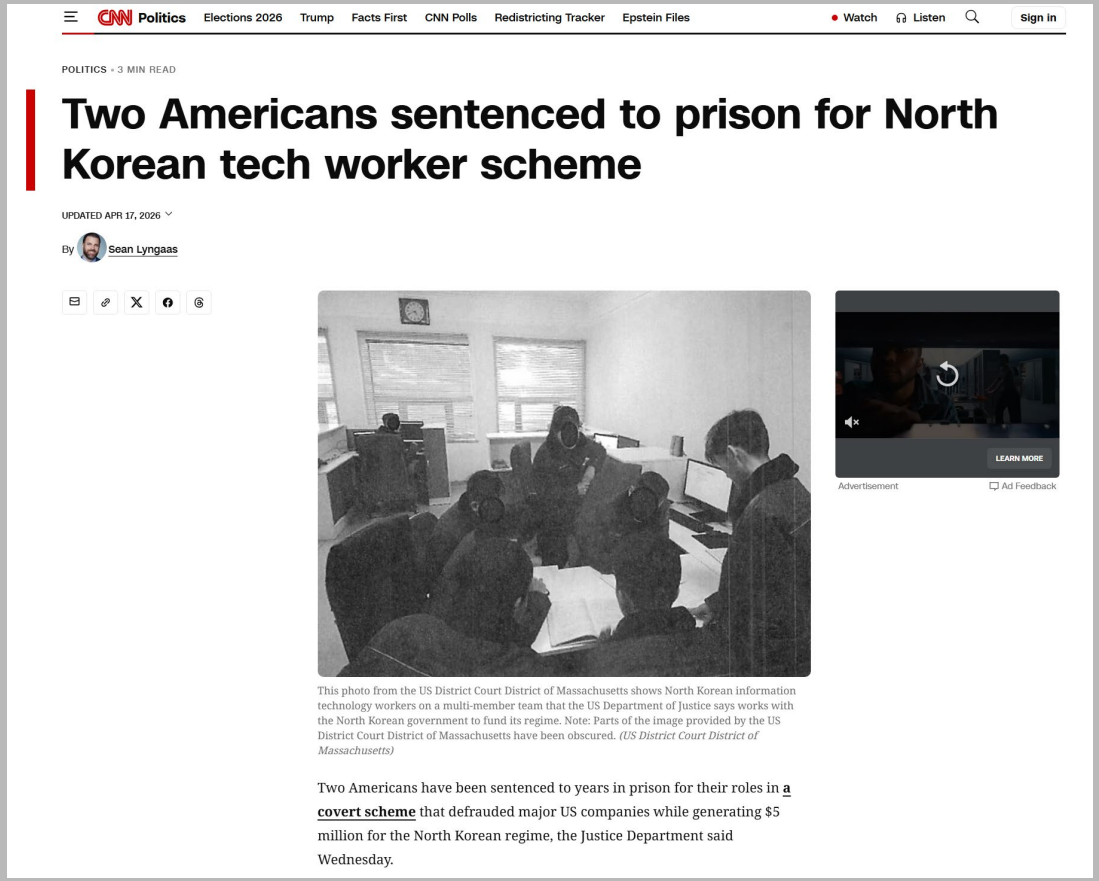
Stand: 01.06.2025 • 18:08 Uhr

Ein mutmaßlicher Hackerangriff auf Rheinmetall legt vertrauliche Informationen offen. Laut Verteidigungsexperten kann das Datenleck Sabotage und Spionage erleichtern.

Von Sabina Wolf und Katharina Brunner, br

Am 4. April dieses Jahres poppt eine Warnung auf den Dark-Web-Überwachungssystemen des IT-Sicherheitsexperten Benjamin Mejri auf: Eine mutmaßlich Russland nahestehende Hackergruppe gibt an, Zugriff auf insgesamt 750 Gigabyte interne Daten des deutschen Rüstungskonzerns Rheinmetall erlangt zu haben. Sie veröffentlicht dazu einen Link zum Download von 1.400 Dokumenten und versichert, im Besitz zahlreicher weiterer Dokumente zu sein.

North Korean Tech Workers



CNN Politics Elections 2026 Trump Facts First CNN Polls Redistricting Tracker Epstein Files Watch Listen Sign In

POLITICS • 3 MIN READ

Two Americans sentenced to prison for North Korean tech worker scheme

UPDATED APR 17, 2026

By Sean Lyngaas

This photo from the US District Court District of Massachusetts shows North Korean information technology workers on a multi-member team that the US Department of Justice says works with the North Korean government to fund its regime. Note: Parts of the image provided by the US District Court District of Massachusetts have been obscured. *(US District Court District of Massachusetts)*

Two Americans have been sentenced to years in prison for their roles in **a covert scheme** that defrauded major US companies while generating $5 million for the North Korean regime, the Justice Department said Wednesday.

INTERNAL FACTORS

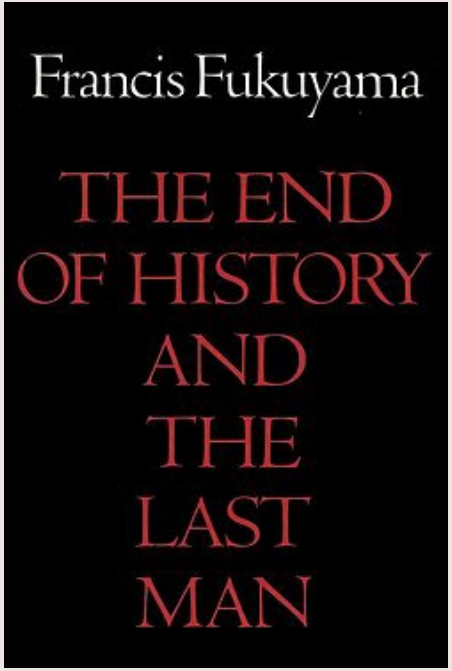
INSIDER THREAT

2

What lies ahead ?

Four main trends

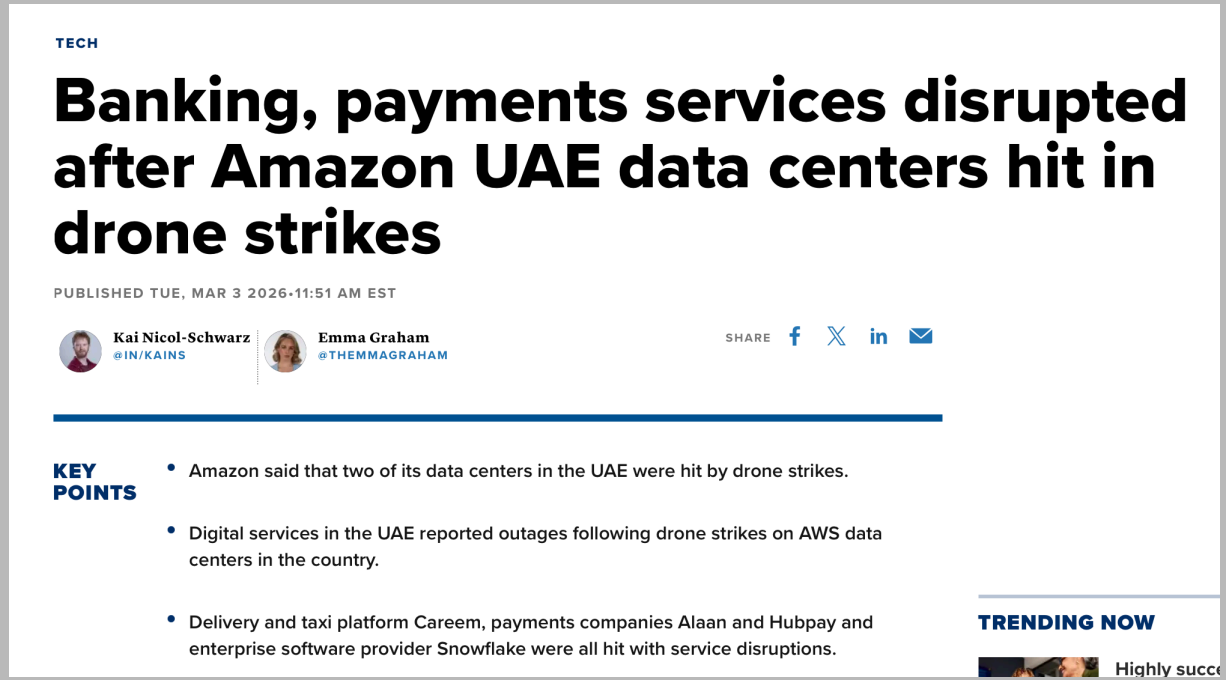
- Geopolitical tensions
- Generative AI
- Quantum Computing
- Regulatory pressure



Russia testing the limits of NATO

Middle-East instability

Convergence of cyber & physical security



TECH

Banking, payments services disrupted after Amazon UAE data centers hit in drone strikes

PUBLISHED TUE, MAR 3 2026•11:51 AM EST

Kai Nicol-Schwarz
@IN/KAINS

Emma Graham
@THEMMAGRAHAM

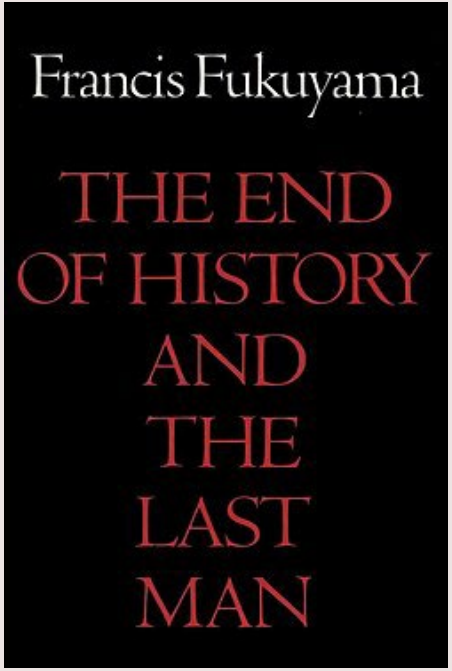
SHARE

KEY POINTS

- Amazon said that two of its data centers in the UAE were hit by drone strikes.
- Digital services in the UAE reported outages following drone strikes on AWS data centers in the country.
- Delivery and taxi platform Careem, payments companies Alaan and Hubpay and enterprise software provider Snowflake were all hit with service disruptions.

TRENDING NOW

Highly succ



Russia testing the limits of NATO

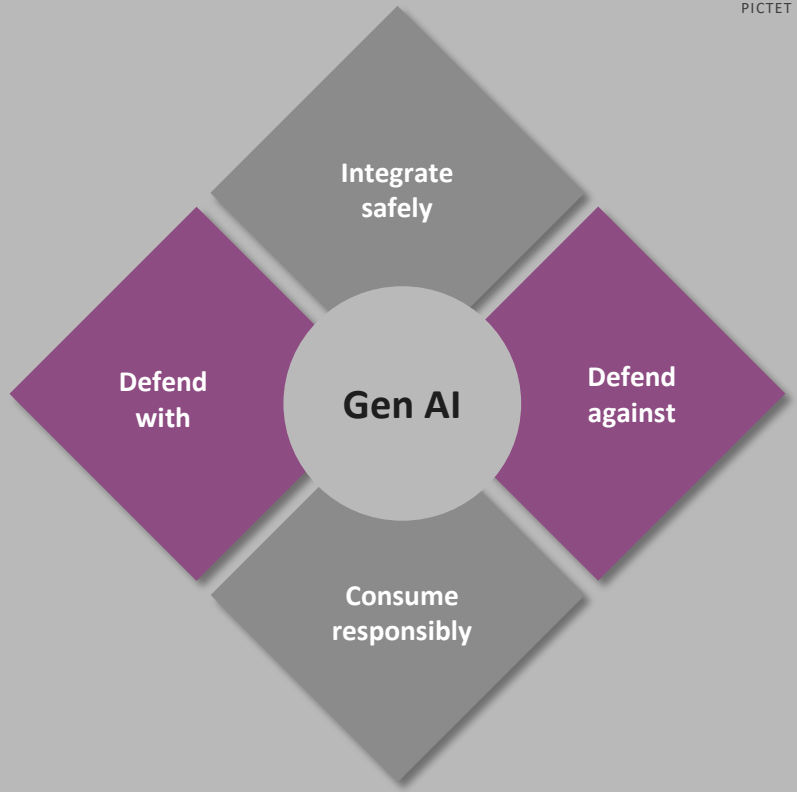
Middle-East instability

Rise in sanctions

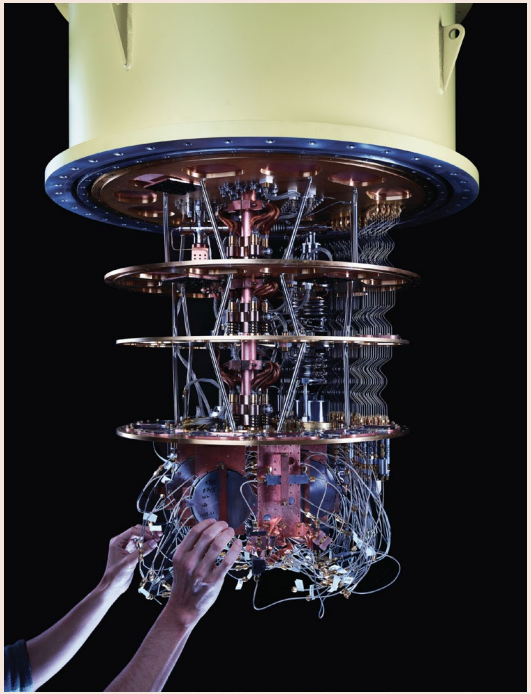
Unreliable EU-US relationship

Chinese expansionism

Generative AI disrupts cybersecurity across the board



Artificial Intelligence and cybersecurity, WEF, 2025



Quantum computing will break today's encryption foundations, putting digital trust at risk

The risk is already here: data stolen today can be decrypted tomorrow (**harvest-now, decrypt-later**)

Impact is **systemic** across banking, communications, identity and markets.

Response requires a multi-year transformation by **2030 to 2035**

Quantum-safe Migration, WEF

Cyberresilience a priority for regulators

Sector specific regulations, e.g.

- Banks and financial institutions (DORA, BAIT)
- Telecommunications Digital Services Data Protection Act (TDDDG)
- Digital Healthcare Act (DVG)
- Energy Industry Act (EnWG) – IT Sicherheits Katalog currently being updated

Broad regulations

- NIS2 Umsetzungsgesetz und German IT Security Act 2.0 for critical infrastructure
- EU Cyber Resilience Act (CRA) for products containing digital components

3

What to do about it ?

1

What are our **most critical systems** and applications?

… this might be more a discussion than a question. IT might not have the same sensitivity as the business when it comes to what's critical

- «Crown Jewels» or critical systems
- Knowledge of where confidential data resides
- Granular inventories

2

How do we **access** our systems and data?

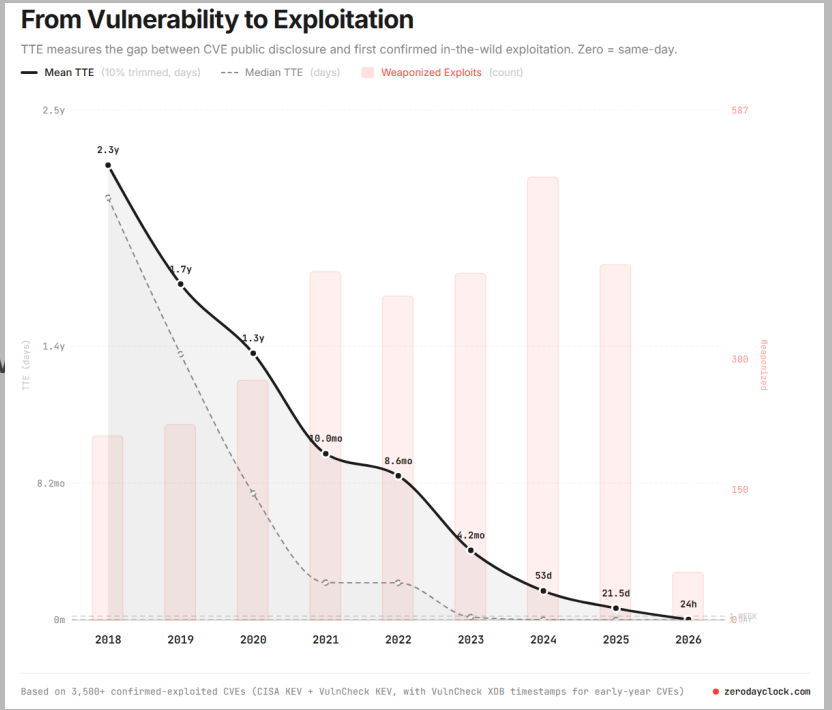
Especially crucial for remote access

- Company-owned devices with secure configurations
- Strong authentication mechanisms (MFA)
- Patching frequency of external perimeter

3

How often do we **patch** our systems? How fast can we do it?

- Automated or manual patching
- Frequency
- Elapsed time

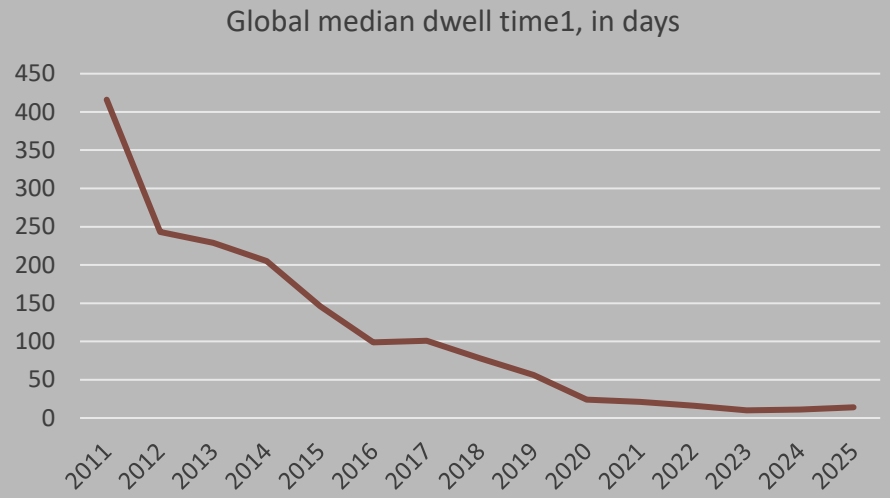


Zero-day clock - https://zerodayclock.com/

4

What do we do ourselves, what do we **outsource**?

- Cloud vs. on-premises
- Third parties handling sensitive data
- Third parties providing business critical services



1. Time an attacker is present in a compromised environment before they are detected
M-Trends 2026 Report, Google

5 What's our **response plan** ?

- «Assume breach» mindset – be ready to respond (retainer)
- Redundancy, backups and systems resilience

Five questions to ask your IT team

1. What are our **most critical systems** and applications?
2. How do we **access** our systems?
3. How often do we **patch** our systems ? How fast can we do it?
4. What do we do ourselves, what do we **outsource**?
5. What's our **response plan** ?

4

Closing remarks

Florian Widmer

CHIEF RISK OFFICER TECH – HEAD OF CYBERSECURITY

Florian Widmer is Pictet Group Head of Cybersecurity since 2019, as well as the Chief Risk Officer for the Tech division since 2025. In this capacity, Florian oversees the protection, detection, and response to cyber threats, while driving the safe adoption of innovative technologies. As a member of the Technology executive leadership team, he brings a strategic and cross-functional perspective to cybersecurity and emerging risks.

Before joining Pictet, Florian held various cyber-related roles at Lombard Odier, where he ultimately led the Cybersecurity function. He holds a Master's degree in Computer Science from the EPFL engineering school in Lausanne. Florian is committed to advancing cybersecurity practices and ensuring organizations remain resilient in an ever-evolving digital landscape. A strong advocate for information-sharing, Florian actively contributes to Swiss and European cybersecurity communities, serving in the Board of Directors of FS-ISAC Europe and in the Swiss FS-CSC Steering Board.

Glossare & Rechtlicher Hinweis

- **Glossar der Risiken:** Zugänglich über diesen Link oder QR-Code: pictet.com/macroeconomic-risks
- **Glossar der Termini**: Zugänglich über diesen Link oder QR-Code: pictet.com\glossary-of-terms
- **Haftungsausschlüsse der Index- und Datenanbieter:** Alle hier wiedergegebenen Indexdaten bleiben Eigentum des jeweiligen Datenanbieters. Die Haftungsausschlüsse der Datenanbieter sind über diesen Link oder QR-Code zugänglich (nur auf Englisch): pictet.com/3rd-party-data-providers
- **Rechtlicher Hinweis:** Verfügbar auf den folgenden Seiten

Rechtlicher Hinweis

Dieses Marketingdokument (nachstehend das „Dokument") darf nur von dessen Empfänger gelesen und/oder verwendet werden. Es ist nicht für natürliche oder juristische Personen bestimmt, welche die Staatsangehörigkeit von oder den Wohn- bzw. den Geschäftssitz in einem Staat oder Gerichtskreis haben, in dem seine Verteilung, Veröffentlichung, Bereitstellung oder Verwendung gegen Gesetze oder andere Bestimmungen verstösst. Es wird solchen Personen weder bereitgestellt noch darf es von ihnen verwendet werden. Es stellt in keinem Fall ein Angebot oder eine Aufforderung zum Kauf, Verkauf oder zur Zeichnung von Wertpapieren, Rohstoffen, Derivaten oder anderen Finanzinstrumenten (gemeinsam als „Anlage(n)" bezeichnet) noch zum Eingehen von Rechtsbeziehungen oder Vereinbarungen noch eine Beratung oder Empfehlung für irgendwelche Anlagen dar. Die in diesem Dokument erwähnten Instrumente wurden von der zuständigen Aufsichtsbehörde möglicherweise nicht zugelassen oder genehmigt. Ihr öffentlicher Vertrieb ist deshalb unter Umständen nicht erlaubt, und ihre private Platzierung kann auf bestimmte Arten von Anlegern beschränkt sein. Für die betreffende(n) Anlagen(n) gelten möglicherweise detaillierte Verkaufsrestriktionen, die berücksichtigt werden müssen. Dieses Dokument enthält keine persönliche, auf die Bedürfnisse, den Kenntnisstand, die Erfahrung, Nachhaltigkeitspräferenzen, Ziele und die finanzielle Situation einer Privatperson oder eines Empfänger. Das Dokument sollte nicht als Geeignetheitsbestätigung betrachtet werden, da der Bank nicht alle notwendigen Informationen über den Empfänger vorliegen, um eine Geeignetheitsprüfung durchzuführen, die Kenntnisse und Erfahrung, Risikotoleranz, eventuelle Nachhaltigkeitspräferenzen, Anlagebedürfnisse und Finanzrisikotragfähigkeit des Empfängers berücksichtigt. Weitere von der Bank veröffentlichte oder verteilte Berichte oder Dokumente können von den Informationen und/oder Meinungen in diesem Dokument abweichen und zu anderen Schlussfolgerungen führen, und die Bank kann im Widerspruch zu den in diesem Dokument vorgestellten Informationen und/oder Meinungen handeln und Interessen verfolgen, die den Interessen des Empfängers dieses Dokuments zuwiderlaufen. Anleger sollten eine unabhängige Finanzberatung über die Geeignetheit einer Anlage oder für die Übernahme von in diesem Dokument diskutierten Strategien einholen. Beschliesst der Anleger, eine Transaktion im Zusammenhang mit einer in diesem Dokument genannten Anlage zu tätigen, so ist er allein dafür verantwortlich, und die Geeignetheit/Angemessenheit der Transaktion sowie sonstige spezifische Finanzrisiken ebenso wie mögliche rechtliche, aufsichtsrechtliche, kreditspezifische, steuerliche und bilanzielle Aspekte sollten von ihm/ihr/einer Privatperson beurteilt werden. Zudem gibt die Bank keine Erklärung oder Beratung über die geeignete buchhalterische Materialien dienen reinen Informationszwecken, wurden in gutem Glauben übernommen und stammen aus Quellen, die als zuverlässig gelten. Diese Informationen können ohne vorherige Mitteilung geändert werden. Die Bank kann nicht für eventuelle Kursschwankungen der Wertpapiere haftbar gemacht werden. Die Preise, Wertangaben und Erträge der in diesem Dokument erwähnten Anlage(n) beruhen auf den üblichen Finanzinformationsquellen der Bank. Die Bank ist nicht verpflichtet, die in diesem Dokument wiedergegebenen Informationen zu aktualisieren, und ihre Genauigkeit und Vollständigkeit kann weder ausdrücklich noch implizit bestätigt oder garantiert werden. Die Bank übernimmt somit keine Haftung für Verluste, die sich aus der Verwendung dieses zu reinen Informationszwecken erstellten Dokuments oder der Bezugnahme darauf ergeben. Der Marktwert von Anlagen kann durch wirtschaftliche, finanzielle und politische Faktoren, die Restlaufzeit, Marktbedingungen und Volatilität sowie die Bonität des jeweiligen Emittenten oder des Benchmark-Emittenten steigen oder sinken, ohne dass dies mitgeteilt wird. Einige Anlagen sind möglicherweise nicht sofort realisierbar, weil der entsprechende Markt illiquide sein kann. Zudem können die Wechselkurse einen positiven oder negativen Einfluss auf Wert, Preis oder Rendite der in diesem Dokument erwähnten Anlage(n) haben. Die politische und wirtschaftliche Lage in Schwellenländern ist deutlich instabiler als in Industrieländern geben keinen verlässlichen Hinweis auf oder eine Garantie für die zukünftige Entwicklung. Die Bank übernimmt keinerlei Haftung – weder ausdrücklich noch stillschweigend – für die künftige Wertentwicklung. Dementsprechend muss der Anleger bereit und in der Lage sein, alle Risiken zu tragen, auch das Risiko, weniger zurückzuerhalten, als ursprünglich investiert wurde. Die angegebene Performance berücksichtigt weder Kommissionen noch Kosten (welche die Performance schmälern). Jede Anlageentscheidung setzt voraus, dass der Anleger die jeweilige(n) Anlage(n) und die damit verbundenen Risiken vollumfänglich versteht. Insbesondere sollte die Dokumentation der betreffenden Anlage(n) (wie Emissionsprogramm, endgültige Bedingungen, Prospekt, vereinfachter Prospekt, Private Placement Memorandum und wesentliche Anlegerinformationen) gelesen werden. Strukturierte Produkte sind komplexe Finanzprodukte und bergen ein hohes Risiko. Der Wert der strukturierten Produkte hängt nicht nur von der Performance des Basiswerts bzw. der Basiswerte ab, sondern auch von der Bonität des Emittenten. Ausserdem ist der Anleger dem Risiko ausgesetzt, dass der Emittent/Garantiegeber ausfällt. Falls dieses Dokument einen Link zu Dokumenten im Zusammenhang mit der/den Anlage(n) wie einem Schweizer Basisinformationsblatt oder einem Basisinformationsblatt für verpackte Anlageprodukte für Kleinanleger und Versicherungsanlageprodukte Bestätigung der Anlageentscheidung gegenüber der Bank muss der Anleger über den entsprechenden Link die jeweils neueste Version des betreffenden KID bzw. eines sonstigen Anlagedokuments abrufen. Sollte der Anleger keinen Link für den Zugriff auf die jeweiligen Dokumente erhalten haben oder unsicher sein, welches die jüngste Version des jeweiligen KID bzw. sonstiger Produktunterlagen ist oder wo diese zu finden ist, kann er sich an seinen Ansprechpartner bei der Bank wenden. Wenn die Bank nicht Hersteller der Anlage(n) ist, wird das KID/sonstige Dokument von einer Drittpartei bereitgestellt (das „Drittparteidokument"). Drittparteidokumente werden aus als zuverlässig erachteten Quellen bezogen. Die Bank gibt keinerlei Garantie für die Korrektheit bzw. Genauigkeit der im Drittparteidokument enthaltenen Daten. Die Bank haftet nicht für Anlageentscheidungen oder Transaktionen, die im Vertrauen oder gestützt auf im Drittparteidokument enthaltene Daten erfolgen. Sollte der Anleger die hier erwähnte(n) Anlage(n) zeichnen, erklärt er, (i) dass ihm die mit der/den Anlage(n) verbundene relevante Dokumentation – einschliesslich gegebenenfalls des jeweiligen KID/eines anderen Dokuments – rechtzeitig zur Verfügung gestellt wurde und dass er diese Dokumentation gelesen und verstanden hat; (ii) dass er die für die Anlage(n) bestehenden Beschränkungen zur Kenntnis genommen hat; und (iii) dass er die geltenden subjektiven und objektiven Voraussetzungen erfüllt, um die Anlage(n) zu tätigen Dienstleister zu übermitteln, sie gemäss den entsprechenden Klauseln des Mandats des Anlegers sowie den Allgemeinen Geschäftsbedingungen der Bank auszuführen und für die Zeichnung der Anlage(n) erforderliche Dokumente oder Bestätigungen im Namen des Anlegers zu unterzeichnen. Durch Zeichnung der Anlage(n) erklärt sich der Anleger ferner einverstanden, die Bank für jegliche Forderungen, Verluste und Schäden, die ihr in Verbindung mit der/den Anlage(n) entstehen könnten, zu entschädigen und schadlos zu halten. Jegliche Wiedergabe, Vervielfältigung, Offenlegung, Änderung und/oder Veröffentlichung dieses Dokuments ist nur mit vorheriger schriftlicher Erlaubnis der Bank gestattet und erfolgt unter Ausschluss jeglicher Haftung der Bank. Der Empfänger des Dokuments verpflichtet sich, die geltenden Gesetze und Bestimmungen in den Jurisdiktionen einzuhalten, in denen die in diesem Dokument bereitgestellten Informationen verwendet werden. Alle Rechte vorbehalten.

Vertrieb: Bank Pictet & Cie (Europe) AG ist ein von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zugelassenes und beaufsichtigtes Kreditinstitut nach deutschem Recht mit Sitz in Neue Mainzer Str. 2–4, 60311 Frankfurt am Main mit Niederlassungen in Luxemburg, Frankreich, Italien, Spanien, Monaco und dem Vereinigten Königreich, die jeweils der Aufsicht des entsprechenden