N°2 | Oktober 2025

s:fi KNOWLEDGE

Swiss Finance Institute Roundups

Grundlagen der Cybersicherheit

Editorial

Cyberbedrohungen werden im Jahr 2025 voraussichtlich Kosten in Höhe von über 10 Billionen US-Dollar verursachen und zählen damit zu den grössten Herausforderungen dieses Jahrzehnts. In diesem SFI Roundup beleuchten Experten aus Wissenschaft und Industrie die kritischsten Schwachstellen und die Handlungsprioritäten. Der Finanzsektor erweist sich dabei aufgrund jahrzehntealter Legacy-Systeme und der Kaskadeneffekte in eng verflochtenen Zahlungsnetzwerken als besonders verwundbar. Anstatt Cybersicherheit an die IT-Abteilungen zu delegieren, müssen Vorstände und Verwaltungsräte sie als strategische Kernaufgabe begreifen, die kontinuierliche Investitionen und einen Kulturwandel erfordert, bei dem alle Mitarbeitenden ihre Mitverantwortung für die Sicherheit verstehen. Da sich die Grenzen zwischen Ransomware-Gruppierungen und staatlich gesteuerten Akteuren zunehmend verwischen und zentralisierte Cloud-Anbieter gefährliche Single Points of Failure, also zentrale Schwachstellen, schaffen, erfordert der Weg nach vorn nicht nur bessere Technologien, sondern ein grundsätzliches Neudenken, wie wir in unserer hypervernetzten Welt Effizienz und Widerstandsfähigkeitin Einklang bringen.

Wir wünschen Ihnen eine informative und zum Nachdenken anregende Lektüre.

Prof. François Degeorge
Managing Director

Mitwirkende

Alain Beuchat
Alain Beuchat war bis zu seiner Pensionierung im Juni 2025 Chief Information Security Officer bei Lombard Odier und dort für die Cyber-Resilienz, die Informationssicherheitsstrategie und die Einhaltung regulatorischer Vorschriften im gesamten Unternehmen verantwortlich. Er ist ausserdem Mitglied des Advisory Board Cybersecurity der Schweizerischen Akademie der Technischen Wissenschaften (SATW). Er hat einen Master of Science in Elektrotechnik der EPFL, der Eidgenössischen Technischen Hochschule in Lausanne.

Marc Henauer
Marc Henauer ist Senior Political and International Affairs Officer beim Bundesamt für Cybersicherheit (BACS). Zuvor leitete er die Melde- und Analysestelle Informationssicherung (MELANI), wo er die Überwachung von Cyberbedrohungen koordinierte, und zur Verbesserung des Cyberlagebildes der Schweiz beitrug. Beim BACS konzentriert er sich auf die Entwicklung nationaler und internationaler Cybersicherheitspolitik. Er hat einen Master of Arts in Foreign Service and National Security Studies der Georgetown University.

Anastasia Kartasheva
Anastasia Kartasheva ist SFI-Fakultätsmitglied und Associate Professor an der School of Finance sowie Direktorin am Schweizerischen Institut für Aussenwirtschaft und Angewandte Wirtschaftsforschung an der Universität St. Gallen. Zuvor arbeitete sie als Ökonomin bei der Bank für Internationalen Zahlungsausgleich (BIZ). Sie promovierte in Volkswirtschaftslehre an der Université Toulouse Capitole.

Olivier Scaillet
Olivier Scaillet ist SFI-Senior Chair und Professor für Finanzierung und Statistik an der Universität Genf. Seine Forschungsschwerpunkte liegen im Bereich der ökonometrischen Theorie und deren Anwendungen in der Finanz- und Versicherungswirtschaft. Neben seiner akademischen Tätigkeit bringt er seine Expertise in den Bereichen Risikomanagement und Modellierung bei mehreren in der Schweiz ansässigen Banken ein. Er promovierte in Angewandter Mathematik an der Université Paris Dauphine.

Beat Schär
Beat Schär ist Leiter der Facheinheit IT-Security und Architektur bei der Schweizerischen Nationalbank (SNB), wo er die Konzeption und Umsetzung sicherer IT-Architekturen überwacht, die Cybersicherheitsstrategie der Institution auf nationale und internationale Regulierungsstandards abstimmt und zu abteilungsübergreifenden Initiativen zum Schutz kritischer Systeme beiträgt. Er hat einen Master of Applied Science in Informationstechnologie und Elektrotechnik der ETH Zürich, der Eidgenössischen Technischen Hochschule Zürich.

Fabian Schär
Fabian Schär ist SFI-Fakultätsmitglied und Assistenzprofessor für Distributed-Ledger-Technologie und Fintech an der Universität Basel. Er ist Visiting Researcher beim Internationalen Währungsfonds (IWF), technischer Berater des Ausschusses für Zahlungsverkehrs- und Marktinfrastrukturen und geladener Experte für zahlreiche Zentralbanken, die Bank für Internationalen Zahlungsausgleich (BIZ), den Finanzstabilitätsrat und die G20. Er promovierte in Volkswirtschaftslehre an der Universität Basel.

Oktober 2025 (Interviews September 2025)

Diese Version ist die Übersetzung der Originalversion in englischer Sprache. Die Originalversion ist unter https://www.sfi.ch/rndp-cs25 abrufbar.

Das Wesentliche

Was ist Cybersicherheit und wie ist sie strukturiert?

Beat Schär: Cybersicherheit bezeichnet den Schutz von IT-Systemen, Netzwerken und Daten vor unbefugtem Zugriff, Beschädigung oder Störung. Die technischen Grundlagen – wie der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit – sind in den meisten Organisationen ähnlich. Die konkreten Prioritäten und Risiken hängen jedoch stark von der Art des Unternehmens ab. Ein Vermögensverwalter ist beispielsweise auf sichere Daten der Kundinnen und Kunden angewiesen, eine Zentralbank auf die Sicherheit, Verfügbarkeit und Unabhängigkeit ihrer Systeme, ein Industrieunternehmen auf die Integrität automatisierter Produktionsabläufe und ein Online-Shop auf eine sichere Zahlungsabwicklung und eine hohe Verfügbarkeit bei Spitzenlasten. In der heutigen Wirtschaft sind fast alle Branchen auf vernetzte IT-Systeme angewiesen, so dass Cybersicherheit zu einem zentralen strategischen Anliegen geworden ist – wenn auch in unterschiedlicher Ausprägung von Unternehmen zu Unternehmen.

Alain Beuchat: Vertraulichkeit, Integrität und Verfügbarkeit bilden die Grundlage der Cybersicherheit. Diese drei Prinzipien sind eng miteinander verknüpft: Es kommt häufig zu Zielkonflikten, Spannungsfeldern sowie zu komplementären oder kaskadierenden Ausfällen zwischen ihnen. Vertraulichkeit schützt die Identität von Nutzerinnen und Nutzern und stellt sicher, dass sie auf die richtigen Daten zugreifen können. Integrität schützt Daten und Systeme vor unbefugten Änderungen. Verfügbarkeit gewährleistet, dass Daten und Infrastrukturen bei Bedarf zugänglich sind. Cyberangriffe können auf alle drei Komponenten abzielen: Phishing-Angriffe versuchen, Zugangsdaten zu erlangen, um Hackerinnen und Hackern unbefugten Zugriff auf Daten zu verschaffen. Ransomware-Attacken zielen auf die Integrität und Vertraulichkeit von Daten. Distributed-Denial-of-Service-Angriffe (DDoS) überlasten Server und machen Websites für legitime Nutzerinnen und Nutzer unzugänglich. Um diese drei Kernaspekte der Cybersicherheit in der Praxis umzusetzen, setzen Organisationen auf gestaffelte Sicherheitskontrollen – darunter Verschlüsselung, Zugriffskontrollen, Schutz vor DDoS und Schadsoftware, Systemüberwachung sowie Notfall- und Reaktionspläne, die gezielt auf Risiken für Vertraulichkeit, Integrität und Verfügbarkeit ausgerichtet sind.

Wie fügt sich Cybersicherheit in das Gesamtbild der Sicherheit ein?

Fabian Schär: Sobald zwei Hardware- oder Softwarekomponenten miteinander interagieren, sind sie anfällig für Angriffe, und Cybersicherheit wird notwendig. Sicherheit im weitesten Sinne bedeutet Schutz vor Bedrohungen. Diese Bedrohungen können viele Formen annehmen – physische, digitale, emotionale oder institutionelle. Cybersicherheit konzentriert sich auf den Schutz von IT-Systemen und Daten vor digitalen Angriffen, hat aber auch Auswirkungen auf andere Bereiche der Sicherheit, darunter die nationale Sicherheit, die wirtschaftliche Stabilität und die persönliche Sicherheit.

Marc Henauer: Im Kern geht es bei Cybersicherheit um das Management unterschiedlicher Risikotypen in Wirtschaft und Gesellschaft. Es ist wichtig zu verstehen, dass Cybersicherheit keine zusätzliche Prozessebene ist, die man optional einführen kann. Vielmehr verändert sie die Art und Weise, wie bestehende Prozesse umgesetzt werden. In der Vergangenheit wurden beispielsweise wichtige Informationen meist per versiegelten Briefen oder Telegrammen verschickt. Heute werden sie über Instant-Messaging-Systeme versendet. Cybersicherheit hat die Nachrichtenübermittlung nicht erfunden, sondern lediglich angepasst, wie sie heute durchgeführt wird, um ihre Sicherheit zu gewährleisten.

Olivier Scaillet: Im Bankensektor bietet der Basler Ausschuss für Bankenaufsicht eine hilfreiche Orientierung, indem er Risiken in drei Hauptkategorien einteilt: Kreditrisiken, Marktrisiken und operationelle Risiken. Cyberrisiken fallen unter die operationellen Risiken. Sie nehmen jedoch eine besondere Stellung ein – aufgrund ihrer böswilligen Absicht, der erhöhten Eintrittswahrscheinlichkeit, ihres oft verdeckten und langanhaltenden Störungspotenzials sowie ihrer schnellen Ausbreitung durch digitale Vernetzung. Diese Eigenschaften zeigen deutlich, dass herkömmliche Rahmenwerke für operationelle Risiken nicht ausreichen. Der Umgang mit Cyberrisiken erfordert gezielte, vorausschauende Strategien – sowohl in der Unternehmensführung als auch in der Ausgestaltung von Regulierung und Risikoversicherung.

Anastasia Kartasheva: Aus Versicherungssicht wird das Cyberrisiko auch als operationelles Risiko betrachtet – aufgrund seiner Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie auf die IT-Infrastruktur. Diese Risiken können unautorisierten Zugriff beinhalten, was zu Datenpannen, Malware-Angriffen und internen Systemfehlern führen kann, die die Datensicherheit gefährden. Im Gegensatz zu anderen Risiken, wie Gesundheitsrisiken oder Naturkatastrophen, gibt es nur wenige Methoden zur Übertragung von Cybersicherheitsrisiken. Infolgedessen verfügen Unternehmen nur über einen minimalen Versicherungsschutz gegen Cyberrisiken und sind bei der Bewältigung der Folgen eines Angriffs weitgehend auf sich allein gestellt.

Wie unterscheiden sich gezielte und opportunistische Cyberangriffe?

Alain Beuchat: Die meisten Cyberangriffe sind opportunistisch und nicht gezielt. Angreifer scannen das Internet nach bekannten Schwachstellen, nutzen diese aus und finden erst danach heraus, wer das Opfer ist. Sobald sie Zugang erlangt haben, legen die oft in mehreren Ebenen arbeitenden Angreifer die Höhe des Lösegeldes anhand der Grösse und Sensibilität des Opfers fest. Es muss wehtun, aber nicht so sehr, dass das Opfer nicht zahlen kann. Gezielte Angriffe verlaufen anders. Sie beinhalten langfristige Überwachung, strategische Absicht und oft geopolitische Motive. Solche Operationen, die oft mit staatlichen Akteuren in Verbindung stehen, können Monate oder sogar Jahre der Vorbereitung erfordern und richten sich in der Regel gegen Regierungsbehörden oder kritische Infrastrukturen. Beide Arten von Bedrohungen existieren nebeneinander, und es ist entscheidend, ihre Logik zu verstehen, um Risiken einzuordnen und Gegenmassnahmen zu planen. Eine wirksame Verteidigung beginnt damit, nicht nur zu wissen, wie Angreifer vorgehen, sondern auch warum.

Welche aktuellen Zahlen verdeutlichen am besten das Ausmass heutiger Cyberbedrohungen?

Olivier Scaillet: Fachleute prognostizieren, dass die weltweiten Kosten der Cyberkriminalität im Jahr 2025 über 10 Billionen US-Dollar betragen werden – ein enormer Anstieg gegenüber 3 Billionen US-Dollar im Jahr 2015. Diese erschreckenden Zahlen sind zwar schwer zu verifizieren, unterstreichen jedoch das enorme Ausmass des Problems und seine alarmierende Wachstumsrate. Angesichts zunehmender Cyberangriffe und wachsender Verwundbarkeit gehen einige Prognosen davon aus, dass die Kosten bis 2027 sogar 25 Billionen US-Dollar erreichen könnten. Daher sind Cybersicherheit und Cyberrisiken zu einem wichtigen Thema für Regierungen, Unternehmen und Privatpersonen geworden.

Welche Cyberangriffe veranschaulichen den aktuellen Stand der Cybersicherheit am besten?

Olivier Scaillet: Einer der folgenschwersten Angriffe war wahrscheinlich der NotPetya-Angriff im Jahr 2017. Aus Sicht des operationellen Risikos zwang er die betroffenen Unternehmen, ihren Betrieb wochenlang einzustellen, mit massiven Auswirkungen auf ihre Fähigkeit, Waren und Dienstleistungen zu produzieren. Diese Störungen hatten eine Kettenreaktion zur Folge. Die Kunden der betroffenen Unternehmen erlitten erhebliche Verluste, die viermal so hoch waren wie die direkten Schäden der angegriffenen Firmen. Besonders schwer traf es Kunden, die nur wenige alternative Lieferanten hatten oder auf hochspezialisierte Güter angewiesen waren. Aus Sicht des Reputationsrisikos führte der Vorfall dazu, dass Kunden im Laufe der Zeit ihre Geschäftsbeziehungen zu den direkt betroffenen Unternehmen beendeten. Noch ein Jahr nach dem Angriff war die Wahrscheinlichkeit deutlich erhöht, dass Kunden sich von diesen Unternehmen trennten, was ein Anzeichen für einen langfristigen Vertrauens- und Reputationsverlust ist. Viele Kunden passten ihre Lieferketten an, um künftig mit Unternehmen mit einem besseren Cybersicherheitsprofil zusammenzuarbeiten. Der Angriff schadete somit dem Ruf der betroffenen Unternehmen als verlässliche Geschäftspartner. Der NotPetya-Angriff zählt zu den bisher technisch ausgefeiltesten Cyberangriffen und zeigt eindrucksvoll, welche weitreichenden und langfristigen Folgen solche Angriffe haben können.

Anastasia Kartasheva: Die Stilllegung der Colonial Pipeline im Jahr 2021 ist ein Paradebeispiel. Das Unternehmen, das fast die Hälfte des Kraftstoffs für die Ostküste der Vereinigten Staaten liefert, wurde Ziel eines Ransomware-Angriffs. Als Vorsichtsmassnahme schaltete es seine Systeme ab. Obwohl das Unternehmen bereits einen Tag nach dem Angriff ein Lösegeld in Höhe von rund 4.4 Millionen US-Dollar in Bitcoins zahlte, dauerte es fast eine Woche, bis der Betrieb wieder vollständig aufgenommen werden konnte. Dies führte zu Kraftstoffengpässen in mehreren Bundesstaaten, Panikkäufen und Preisanstiegen an Tankstellen um bis zu 10 Cent pro Gallone. Die Auswirkungen eines solchen Angriffs auf eine kritische Infrastruktur, ausgelöst durch nur ein einziges kompromittiertes Passwort, können erheblich sein und das Leben von Millionen Menschen beeinträchtigen. Es ist ausserdem wichtig, die vermeintlich geringe Lösegeldforderung ins Verhältnis zu den gesamten wirtschaftlichen und gesellschaftlichen Kosten der Stilllegung zu setzen.

Marc Henauer: Der Angriff auf Viasat, der am selben Tag wie der russische Einmarsch in die Ukraine im Jahr 2022 stattfand, zielte darauf ab, die Satellitenkommunikation von Tausenden von Ukrainern, darunter Militär- und Regierungsbehörden, zu stören. Dieser Angriff, der sich gezielt gegen die Ukraine richtete, hatte weitreichende Auswirkungen, die jede Erwartung übertrafen. Der Umfang der Kollateralschäden war enorm: In Deutschland fielen etwa 6'000 Windkraftanlagen aus, Festnetz-Breitbandnutzer in ganz Europa hatten mit Ausfällen zu kämpfen und mussten ihre Hardware ersetzen, und Satellitentelefonbenutzer in Marokko und Grossbritannien hatten Verbindungsprobleme.

Alain Beuchat: Der CrowdStrike-Vorfall im Jahr 2024, ausgelöst durch ein routinemässiges Software-Update, führte zur Annullierung von über 5'000 Flügen, zur Verschiebung nicht dringender medizinischer Eingriffe in Krankenhäusern und zu Online-Banking-Ausfällen bei Banken weltweit. Auch wenn es keine Hinweise auf eine böswillige Ursache gibt, übertraf das Ausmass der Störung alle bisherigen Cyberangriffe und verdeutlicht die Anfälligkeit zentralisierter IT-Systeme. Solche Vorfälle unterstreichen die gegenseitige Abhängigkeit unserer Cybersysteme: Eine Störung, sei sie absichtlich oder versehentlich verursacht, kann nicht nur einen einzelnen Computer beeinträchtigen, sondern auch die Funktion eines Geräts, das über viele Zeitzonen hinweg mit einem IT-Netzwerk verbunden ist. Zusätzlich zu den oben genannten Vorfällen beobachten wir weiterhin eine hohe Zahl von Cyberangriffen auf Unternehmen und deren Drittanbieter. Viele dieser Sicherheitsverletzungen sind auf das Fehlen grundlegender Cybersicherheitsmassnahmen zurückzuführen, wie beispielsweise eine inkonsistente Patch-Verwaltung oder das Fehlen einer Multi-Faktor-Authentifizierung.

Grundlegende Begriffe

Wie sind Cybersicherheitsfunktionen strukturiert und umgesetzt?

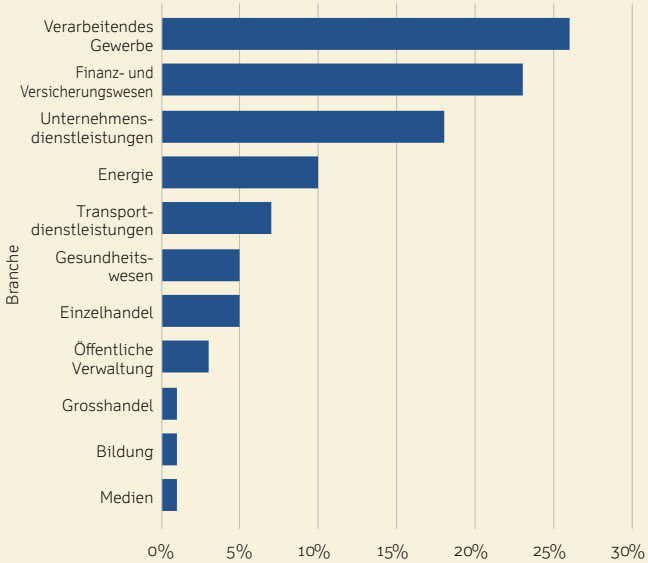
Beat Schär: Das Management von Cyberrisiken ist häufig entlang von drei Verteidigungslinien organisiert: Risikoverantwortung, Risikoüberwachung und unabhängige Prüfung. Die erste Linie, die Risikoverantwortung, umfasst die Identifizierung, Bewertung und Minderung von Cyberrisiken im spezifischen Kontext des Unternehmens. Diese Aktivitäten werden in der Regel von internen Cybersicherheitsspezialisten unterstützt. Die zweite Linie, die Risikoüberwachung, stellt sicher, dass Risiken wirksam erkannt und gesteuert werden. Diese Verantwortung liegt in der Regel bei der internen Risikomanagementabteilung des Unternehmens. Die dritte Linie, die unabhängige Prüfung, bietet eine externe Bewertung der Cybersicherheitskontrollen, -richtlinien und Risikomanagementpraktiken. Dieser dreistufige Ansatz minimiert blinde Flecken, schafft gegenseitige Kontrolle zwischen verschiedenen Organisationseinheiten und sorgt dafür, dass das Cyberrisikomanagement mit übergeordneten Governance- und Compliance-Standards in Einklang steht.

Wer sind die Hauptangreifer und die bevorzugten Opfer von Cyberangriffen?

Marc Henauer: Angreifer handeln sehr rational und opportunistisch und suchen sich Opfer aus, die sich keine erstklassige Sicherheit leisten können, aber über genügend finanzielle Mittel verfügen, um das Lösegeld zu zahlen. Zu ihren Opfern gehören fast alle, die mit einem Netzwerk verbunden sind, von Grossunternehmen und Regierungsbehörden bis hin zu kleinen Unternehmen, Bildungseinrichtungen, Forschungsinstituten, gemeinnützigen Organisationen, NGOs und Privatpersonen. Jeder, der über wertvolle Infrastruktur und Daten sowie finanzielle Ressourcen verfügt, kann zum Ziel werden. Ein bemerkenswertes Beispiel ist der Hackerangriff auf das Netzwerk eines Casinos im Jahr 2017, bei dem Hacker ein schlecht gesichertes, mit dem Internet verbundenes Aquarium-Thermometer ausnutzten, um 10 GB Daten aus der High-Roller-Datenbank des Casinos zu extrahieren. Dieser Vorfall gilt seither als klassisches Beispiel dafür, wie selbst das trivialste internetfähige Gerät zu einem Einfallstor für sensible Informationen werden kann, wenn es nicht ordnungsgemäss gesichert ist.

Anastasia Kartasheva: Es gibt ein komplexes Geflecht von Angreifern und Opfern, die nicht alle auf dem gleichen Schlachtfeld operieren. Auf der Seite der Angreifer sehen wir auf staatlicher Ebene typischerweise China, Nordkorea und Russland als wichtige Akteure, mit ausgeklügelten Angriffsmustern, die von strategischen, politischen oder finanziellen Motiven getrieben sind. Auf individueller Ebene handelt es sich bei den Hackern oft um Teenager, insbesondere aus den USA, die fliessend Englisch sprechen und sich mit Social Engineering auskennen. Ihr Vorgehen ist meist aggressiv und richtet sich über Wochen hinweg gezielt gegen bestimmte Wirtschaftssektoren. Ihre Motive reichen von Prestige über Aktivismus bis hin zu finanziellen Interessen. Wir dürfen ausserdem nicht vergessen, dass auch Mitarbeitende eine erhebliche Bedrohung für die Cybersicherheit darstellen und vorsätzlich oder fahrlässig erheblichen Schaden anrichten können. Auf der Opferseite geraten staatliche Stellen und Betreiber kritischer Infrastrukturen besonders ins Visier staatlich gesteuerter Angreifer. Finanzinstitute und Privatpersonen hingegen sind typischerweise das Ziel von finanziell motivierten Cyberkriminellen. Unternehmen, Medien und Regierungsinstitutionen werden hingegen von ideologisch motivierten Hackern, sogenannten Hacktivisten, angegriffen.

Verteilung von Cyberangriffen nach Branchen



Anmerkung: Diese Abbildung zeigt die Verteilung von Cyberangriffen auf verschiedene Branchen im Jahr 2024.

Quelle: IBM X-Force

Welche Cyberangriffsvektoren sind derzeit am weitesten verbreitet und wie haben sie sich entwickelt?

Fabian Schär: Mit dem Aufkommen künstlicher Intelligenz wird Social Engineering immer raffinierter. Hacker nutzen mehr Daten und fortschrittlichere Modelle, um gezielte und ausgeklügelte Angriffe durchzuführen. Vorbei sind die Zeiten offensichtlicher Fehler wie Tipp- und Grammatikfehler. Auch Lieferkettenangriffe haben sich weiterentwickelt: Angreifer infiltrieren viele Unternehmen, indem sie deren Softwareanbieter ins Visier nehmen. Der Angriff auf SolarWinds, der mit der russischen Regierung in Verbindung gebracht wird, ist ein Paradebeispiel dafür. In diesem Fall schleusten Hacker schädlichen Code in ein vertrauenswürdiges Software-Update ein und verschafften sich so Zugang zu Tausenden hochkarätiger Ziele, darunter US-Regierungsbehörden und Fortune-500-Unternehmen. Das Risiko von Cyberangriffen wächst täglich, da Software und Unternehmen immer stärker vernetzt sind und wir zunehmend auf Cloud-Lösungen und Dienste von Drittanbietern setzen.

Was motiviert unterschiedliche Gruppen von Bedrohungsakteuren – von Staaten bis zu Hacktivisten – zu Cyberangriffen?

Anastasia Kartasheva: Die Motive sind vielfältig. Die derzeitige instabile Weltlage hat deutlich gemacht, dass Propaganda, Desinformation vor Wahlen und Angriffe auf kritische Infrastrukturen gezielt eingesetzt werden, um politische oder militärische Vorteile zu erlangen. Industriesabotage ist ebenfalls ein grosses Problem, insbesondere für Unternehmen mit einer starken internationalen Präsenz, die weniger direkte Kontrolle über ihre Mitarbeitenden haben, stärker von globalen Abläufen und Lieferketten abhängig sind und sich in unterschiedlichen komplexen regulatorischen Systemen bewegen müssen. Die Bekämpfung dieser verschiedenen Bedrohungen bleibt eine ständige Herausforderung, die zahlreiche Schwierigkeiten mit sich bringt, darunter die Zusammenarbeit mit geeigneten Drittanbietern, den Aufbau von technischem Fachwissen, die Schulung der Mitarbeitenden und die Abwehr interner Bedrohungen.

Fabian Schär: Dabei spielt auch der Zeithorizont eine wichtige Rolle. Angriffe mit kurzfristigem Zeithorizont sind meist finanziell motiviert, während Angriffe mit langfristigem Zeithorizont in der Regel strategische oder politische Ziele verfolgen. Der Hackerangriff und die Explosion von Tausenden von Pagern und Walkie-Talkies der Hisbollah im letzten Jahr, bei denen über 40 Menschen getötet und mehr als 3'500 verletzt wurden, zeigen, wie ausgeklügelt und gut geplant solche Angriffe sein können. Heute kann nahezu jedes elektronische Gerät Ziel eines Cybervorfalls werden.

Welche Grundprinzipien leiten heute eine wirksame Cybersicherheits-Governance?

Beat Schär: Cybersicherheit ist eine fortlaufende tägliche Aufgabe. Mit einem risikobasierten Ansatz können Unternehmen eine effektive Cybersicherheits-Governance umsetzen. Am Anfang steht eine gründliche Risikoanalyse, um ein umfassendes Verständnis der eigenen Schwachstellen, Vermögenswerte und der Gefährdung durch Cyberbedrohungen zu gewinnen. Nach der Risikobewertung muss die Geschäftsleitung Sicherheitsmassnahmen priorisieren, die erforderlichen Massnahmen ergreifen und die Gesamtverantwortung für ihre Entscheidungen übernehmen. Eine offene interne Kommunikation ist entscheidend, um regelkonformes Verhalten bei allen Mitarbeitenden zu fördern und das Bewusstsein für Bedrohungen und erwartetes Verhalten zu schärfen. Die Risikobewertungen sollten regelmässig aktualisiert werden, auf Basis neuer Erkenntnisse über Bedrohungslagen und im Hinblick auf das Unternehmenswachstum.

Marc Henauer: Nach schweizerischem Zivilrecht tragen der Verwaltungsrat und die Geschäftsleitung die Verantwortung für das Risikomanagement. Auch wenn noch Verbesserungspotenzial besteht, wächst das Bewusstsein für Cyberrisiken in den Unternehmen. Es ist jedoch schwer zu beurteilen, welche Unternehmen hier Vorreiter sind und welche hinterherhinken. Einerseits verfügen einige kleine und mittlere Unternehmen, insbesondere solche mit einem hohen Automatisierungs- oder Digitalisierungsgrad, über viel Expertise in diesem Bereich. Andererseits haben auch grosse Unternehmen teils erhebliche Verluste erlitten und waren von massiven Störungen betroffen. So hatte beispielsweise die dänische Reederei Maersk 2017 aufgrund des NotPetya Angriffes weltweit mit erheblichen Kapazitätsproblemen zu kämpfen, während der Pharmariese Merck Schätzungen zufolge rund 900 Millionen US-Dollar durch Umsatzausfälle, Betriebsstörungen und Wiederherstellungskosten verloren hat. In der Cybersicherheit gilt: Grösse ist nicht alles. Ob auf Angreifer- oder Verteidigerseite – oft entscheiden Agilität und Einfallsreichtum über den Ausgang. Grösse allein garantiert keinen Erfolg.

Welche Folgen können schwerwiegende Cybersicherheitsverletzungen haben?

Olivier Scaillet: Grössere Cybersicherheitsverletzungen können weitreichende Folgen haben. Eine Studie über grosse börsennotierte US-amerikanische Unternehmen ergab, dass Cyberangriffe kurzfristig zu niedrigeren Renditen, höheren Handelsvolumina, geringerer Liquidität und grösseren Geld-/Brief-Spannen führen. Mit der Zeit erhöhen diese Unternehmen jedoch in der Regel ihre Investitionen in Cybersicherheit, während ihr Marktwert und ihr Gesamtergebnis relativ stabil bleiben. Untersuchungen zu Finanzinstituten zeigen, dass Cyberangriffe aufgrund direkter finanzieller Schäden, Betriebsstörungen und Reputationsschäden zu Verlusten von bis zu 50% des Jahresnettogewinns führen können. Darüber hinaus können einzelne Sicherheitsverletzungen auch systemische Risiken erhöhen und sich auf die Finanzmärkte auswirken.

Anastasia Kartasheva: Reputationsschäden sind ein zentrales Problem, insbesondere wenn sensible Daten kompromittiert werden. Der Umfang der offengelegten Informationen kann enorm sein und von Steuerunterlagen und Gewinn- und Verlustrechnungen bis hin zu Krankengeschichten, biometrischen Merkmalen, Standortdaten und geistigem Eigentum reichen. Die Auswirkungen variieren zwar, aber die Kosten für Reputationsschäden und Rechtsstreitigkeiten gehören oft zu den höchsten. Es ist entscheidend, sich der starken Vernetzung zwischen Unternehmen bewusst zu sein – Cybervorfälle bleiben selten isoliert und können weitreichende, schwer kontrollierbare Konsequenzen nach sich ziehen. Letztendlich muss jedes Unternehmen nicht nur seine eigene Cybersicherheit verwalten, sondern auch entscheiden, ob es sich lohnt, im Falle eines Angriffs Lösegeld zu zahlen, und dabei die möglichen Folgen einer Nichtzahlung berücksichtigen.

Fabian Schär: Eine oft übersehene Auswirkung eines Cyberangriffs ist psychologischer Natur: Angst. So wie jemand nach einem Wohnungseinbruch lange Zeit ein ungutes Gefühl hat, selbst wenn die Schlösser ausgetauscht wurden, kann auch nach einem Cybervorfall ein ähnliches Unbehagen zurückbleiben. Wenn ein Hacker in die IT-Systeme eines Unternehmens eindringt, kann auch nach der Einführung stärkerer Schutzmassnahmen ein Gefühl der Verletzung bestehen bleiben. Diese anhaltende Unsicherheit, ob es zu einem weiteren Angriff kommen wird, kann das Verhalten, das Vertrauen und die Entscheidungsfindung innerhalb des Unternehmens subtil beeinflussen.

Beat Schär: Schwere Cybersicherheitsvorfälle können erhebliche operative, finanzielle und rufschädigende Folgen haben. Im Finanzsektor kann ein schwerwiegender Vorfall die aufsichtsrechtliche Stellung gefährden und das öffentliche Vertrauen untergraben. In der Schweiz beispielsweise ist die Eidgenössische Finanzmarktaufsicht (FINMA) befugt, Banken die Lizenz zu entziehen, wenn sie die Anforderungen an das Risikomanagement, einschliesslich derjenigen im Zusammenhang mit der Cybersicherheit, nicht erfüllen. In den Vereinigten Staaten entwickeln sich die regulatorischen Ansätze weiter; dabei wird unter anderem diskutiert, wie sich verpflichtende Offenlegungspflichten mit wirksamen Cybersicherheitspraktiken vereinbaren lassen. Einige Branchenverbände haben Bedenken geäussert, dass bestimmte Vorschriften unbeabsichtigt die Reaktion auf Vorfälle erschweren könnten. Trotz unterschiedlicher Ansichten zielen die regulatorischen Initiativen im Allgemeinen darauf ab, die Widerstandsfähigkeit und Verantwortlichkeit im Gesamtsystem zu verbessern.

Was sind die Herausforderungen und Anreize für den Austausch von Bedrohungsinformationen zwischen Organisationen?

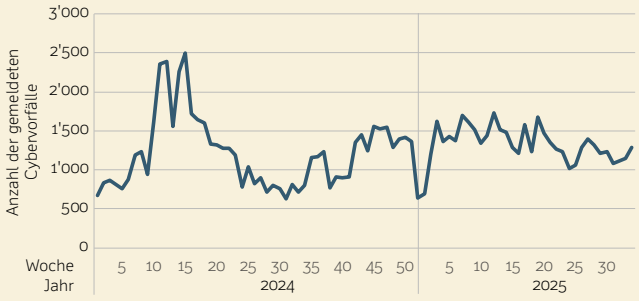
Fabian Schär: Einfach gesagt lautet die Antwort "Vertrauen". Es ist logisch, dass Unternehmen im Bereich Cybersicherheit zusammenarbeiten und ihre Best Practices austauschen, aber das bedeutet auch, dass sie in einem Wettbewerbsumfeld, in dem Verbündete und Konkurrenten oft ein und dieselben sind, viel über ihre internen Abläufe preisgeben müssen. Eine staatlich koordinierte Initiative, bei der Informationen anonymisiert und gebündelt ausgetauscht werden, könnte effektiver sein als ein direkter, bilateraler Austausch zwischen einzelnen Unternehmen.

Alain Beuchat: Die richtigen Informationen sind entscheidend, da sie das Bewusstsein schärfen und Unternehmen dabei helfen, ihr Risiko, potenzielles Ziel eines Angriffs zu werden, besser einzuschätzen und sich auf verschiedene Bedrohungen vorzubereiten. Es gibt zwei Hauptkanäle, um diese Informationen zu erhalten: Man kann sie von einem Drittanbieter kaufe, was eine passgenaue Informationssuche für das eigene Unternehmen ermöglicht, oder man tauscht Informationen mit Marktpartnern über Open-Source-Intelligence (OSINT) aus. Am effektivsten ist eine Kombination beider Kanäle. Ein weiterer wichtiger Aspekt ist der Aufbau vertrauensvoller Beziehungen durch diesen Austausch. Solche Beziehungen ermöglichen den schnellen und effektiven Austausch relevanter Informationen im Falle eines Cyberangriffs.

Anastasia Kartasheva: Ein wichtiger Schritt zur Verbesserung des internationalen Austauschs von Informationen über Cyberrisiken war die Erstellung eines Lexikons mit Cyberbegriffen durch den Finanzstabilitätsrat (Englisch: Financial Stability Board oder FSB) im Jahr 2018. Durch ein gemeinsames Verständnis der Unterschiede zwischen Warnmeldungen, Angriffen, Ereignissen, Vorfällen, Risiken und Bedrohungen wurde es möglich, Daten zu sammeln und zu vergleichen. Allerdings können solche Informationen auch Angreifern einen Vorteil verschaffen. Cyberangreifer sind hochintelligent und nutzen verschiedene Taktiken, um Informationen über ihre potenziellen Ziele zu sammeln. Unsere Kommunalverwaltung speichert beispielsweise grosse Mengen sensibler Daten, darunter auch Angaben zum Haushaltsvermögen. Ein gezielter Angriff auf der Grundlage gestohlener Steuerdaten eines bestimmten Haushalts ist zwangsläufig profitabler als ein zufälliger Angriff. Die Gesamtsicherheit hängt von der Stärke des schwächsten Glieds ab.

Marc Henauer: Auf nationaler Ebene in der Schweiz verpflichtet die kürzlich eingeführte Cybersicherheitsverordnung Betreiber kritischer Infrastrukturen, Cyberangriffe innerhalb von 24 Stunden nach ihrer Entdeckung an das Bundesamt für Cybersicherheit (BACS) zu melden und innerhalb von 14 Tagen einen vollständigen Bericht vorzulegen. Diese Regelung ist ein wichtiger Schritt zur Verbesserung der Sichtbarkeit solcher Vorfälle. Die Verordnung gilt derzeit für öffentliche Verkehrsunternehmen, Energieversorger, Behörden auf Bundes-, Kantons- und Gemeindeebene, Spitäler und Trinkwasserversorger sowie für weitere Sektoren wie den Finanzsektor. Meldepflichtig sind alle Vorfälle, welche die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Informationen beeinträchtigen, darunter erfolgreich installierte Schadsoftware, Verschlüsselungstrojaner, DDoS-Angriffe oder unautorisierter Zugriff über Sicherheitslücken. Das BACS analysiert diese Meldungen und leistet bei Bedarf Unterstützung. Durch die Auswertung dieser Daten werden wir ein besseres Verständnis der globalen Bedrohungslage gewinnen. Wir werden in der Lage sein, Angriffsmodelle auf kritische Infrastrukturen frühzeitig zu erkennen und andere potenzielle Opfer rechtzeitig zu warnen, damit sie geeignete Präventions- und Abwehrmassnahmen ergreifen können. Auch wenn es noch zu früh ist, um den Nutzen dieses Prozesses abzuschätzen, bin ich überzeugt, dass diese regulatorische Veränderung hin zu einem besseren Informationsaustausch zu vielen Erfolgsgeschichten führen wird.

Dem Bundesamt für Cybersicherheit gemeldete Cybervorfälle



Anmerkung: Diese Abbildung zeigt die wöchentliche Anzahl der Cybervorfälle, die dem Bundesamt für Cybersicherheit (BACS) von Januar 2024 bis September 2025 gemeldet wurden.

Quelle: Bundesamt für Cybersicherheit (BACS)

Digitale Exponierung

Wie sollten Kosten und Verantwortung für Cybersicherheit zwischen dem öffentlichen und dem privaten Sektor aufgeteilt werden?

Anastasia Kartasheva: Wie bei der klassischen Sicherheit gibt es auch im Bereich der Cybersicherheit deutlich spürbare externe Effekte, die oft die Gesamtwirtschaft betreffen. Dennoch wäre ich vorsichtig damit, zu fordern, dass der öffentliche Sektor Cybersicherheit finanzieren sollte – schon wegen des potenziellen moralischen Risikos. Es ist ein grosser Unterschied, ob der Staat etwa den Bau in katastrophengefährdeten Gebieten reguliert oder ob er Cybersicherheit überwacht. Jedes Unternehmen muss selbst eine Strategie festlegen und entscheiden, wie viel es bereit ist zu investieren, um seine Risiken zu senken.

Marc Henauer: Die digitale Welt ist im Grunde eine Erweiterung der physischen Welt mit all ihren guten und schlechten Seiten. Wie im echten Leben hat auch hier der Staat die Verantwortung, sich um die Schaffung eines besseren und sichereren Umfelds zu bemühen. Allerdings kann man von ihm weder verlangen, dass er dieses ehrgeizige Ziel vollständig erreicht, noch kann man ihm vorwerfen, wenn er dies nicht schafft. Genauso wie von Menschen erwartet wird, dass sie in der realen Welt ihre Türen abschliessen und ihre Häuser versichern, ist es Aufgabe von Privatpersonen und Unternehmen, ihre digitale Umgebung mit geeigneten Cybersicherheitsmassnahmen zu schützen.

Fabian Schär: Für bestmögliche Ergebnisse sollte sich jede Partei auf ihren jeweiligen Kompetenzbereich konzentrieren. Der öffentliche Sektor sollte unabhängig von der Eigentumsstruktur vorrangig die Sicherheit der kritischen Infrastruktur gewährleisten, während der private Sektor für einen reibungslosen Betrieb sowohl auf Unternehmens- als auch auf Branchenebene sorgen muss. Die Aufgabe der Regulierungsbehörde besteht darin, klare Richtlinien für Mindestanforderungen und die allgemeine wirtschaftliche Ausrichtung vorzugeben. Ausserdem ist es wichtig, die Zusammenarbeit und den Austausch zwischen verschiedenen Akteuren, darunter Wissenschaftlerinnen und Wissenschaftler, Unternehmen und Behörden, in der jeweils passenden Form zu fördern.

Was sagen Markttrends wie Fusionen, Übernahmen und der Aufstieg von One-Stop-Cloud-Lösungen über die Reaktion der Branche auf Cyber-Bedrohungen aus?

Beat Schär: Der Trend zur Konsolidierung, sei es durch Fusionen oder die Abhängigkeit von wenigen dominanten Cloud-Anbietern, spiegelt den Versuch wider, Organisationen und IT-Systeme effizienter zu gestalten. Weniger Systeme vereinfachen das Management, konzentrieren aber auch Risiken – was nicht nur den Nutzerinnen und Nutzern, sondern auch den Angreifern das Leben erleichtert. Cloud-Lösungen sind zwar effizient und skalierbar, aufgrund ihrer komplexen Konfigurationen jedoch mit täglich neuen Sicherheitsherausforderungen verbunden. Sie stehen im Fokus sich ständig weiterentwickelnder Bedrohungen. Eine Diversifizierung über verschiedene Systeme hinweg oder der Betrieb paralleler Clouds verbessert die Widerstandsfähigkeit, aber diese Massnahmen sind kostspielig und schwer zu verwalten. Da eine Handvoll Anbieter den Markt zunehmend dominieren, entsteht eine gefährliche Abhängigkeit: Wenn ein Anbieter ausfällt oder angegriffen wird, kann dies weitreichende Folgen haben. Letztlich bringt sowohl Integration als auch Diversifikation spezifische sicherheitsrelevante Zielkonflikte mit sich.

Wie unterscheiden sich die Cybersicherheitsrisiken im Finanzsektor und in anderen Branchen?

Marc Henauer: Banken waren bereits in den 1950er Jahren Vorreiter bei der Integration von IT in ihre zentralen Geschäftsprozesse. Anfangs unterstützten Computer vor allem die Buchhaltung und Rechnungswesen, aber im Laufe der Zeit kamen wichtige Funktionen wie Batch-Verarbeitung, sichere Finanznachrichten, Geldautomaten, Online-Banking und elektronischer Handel hinzu. Diese frühe Einführung hat zu fragmentierten und stark von Altsystemen geprägten IT-Infrastrukturen geführt. Allerdings neigt der Finanzsektor dazu, strukturierte Erneuerungszyklen konsequenter einzuhalten als viele Nicht-Finanzbranchen. IT-Systeme im Finanz- und Nicht-Finanzsektor wachsen in der Regel organisch – oft ohne langfristige Planung oder regulatorischen Rahmen, der festlegt, welche Infrastruktur in den nächsten zehn Jahren integriert werden soll.

Wie haben Organisationen ihre Vorbereitung auf Cyberangriffe verbessert und welche Herausforderungen bleiben bestehen?

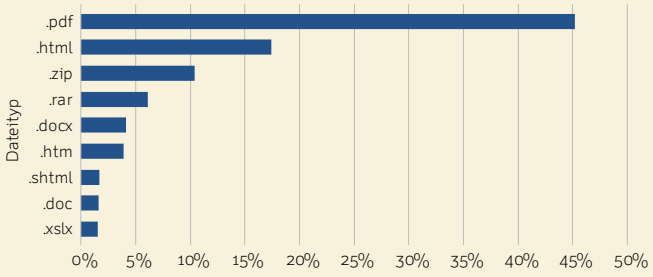
Alain Beuchat: Unternehmen haben erhebliche Fortschritte bei der Einrichtung grundlegender Cybersicherheitsprotokolle und der Auswahl geeigneter Sicherheitslösungen erzielt. Theoretisch sind die Grundlagen klar: Bekannte Schwachstellen müssen umgehend gepatcht, Malware-Schutz und -Überwachung implementiert, Multi-Faktor-Authentifizierung durchgesetzt und Backups sicher gespeichert werden. In der Praxis erweisen sich diese scheinbar einfachen Schritte jedoch als schwer in grossem Massstab umsetzbar. Die eigentliche Herausforderung besteht darin, sie konsequent und systemübergreifend umzusetzen. Was die Cyberabwehr in der Praxis so schwierig macht, ist nicht so sehr ein Mangel an Wissen, sondern die enorme Komplexität der Implementierung von Abwehrmassnahmen in grossen Netzwerken. Menschliches Versagen, fragmentierte Prozesse und verzögerte Patches schaffen weiterhin Schwachstellen, selbst wenn Abwehrmassnahmen vorhanden sind. Bei einer echten Vorbereitung geht es weniger darum, die richtige Checkliste zu haben, als vielmehr darum, diese konsequent und schnell anzuwenden.

Olivier Scaillet: Da Cybersicherheitsmassnahmen immer komplexer und teurer werden, stehen IT-Abteilungen unter zunehmendem Druck, einen geschäftlichen Mehrwert zu liefern. Unternehmen müssen sorgfältig abwägen, was sie schützen wollen, wie sie es schützen wollen und was sie sich leisten können, nicht zu schützen. Diese Entscheidungen sind naturgemäss mit Risiken und Unsicherheiten behaftet. Gleichzeitig müssen Management und Verwaltungsrat wachsam bleiben, da Cybervorfälle erhebliche Governance-Folgen mit sich bringen. Studien zeigen, dass erfolgreiche Angriffe die Wahrscheinlichkeit von personellen Veränderungen im Top-Management erhöhen, insbesondere bei Chief Investment Officers und Chief Information Security Officers, und in manchen Fällen auch auf Vorstands- und Verwaltungsratsebene, wenn Schwächen in der Aufsicht oder Vorbereitung sichtbar werden. Diese Herausforderungen unterstreichen, dass nicht nur Aufsichtsbehörden, sondern auch Aktionäre die Unternehmensleitung für Cybersicherheitsversäumnisse zur Rechenschaft ziehen.

Beat Schär: Staatlich gesteuerte Angriffe werden immer ausgefeilter. Hacker schleusen schädlichen Code in Software-Updates vertrauenswürdiger Drittanbietern ein und erreichen so auf diskrete Weise eine Vielzahl von Opfern. Diese Angriffe zeigen, wie vertrauenswürdige Partner zu einer Bedrohung werden können, und unterstreichen die Bedeutung von Zero-Trust-Architekturprinzipien und einem strengen Risikomanagement für Drittparteien. Da diese Angriffe sehr komplex sind, sind die Chancen, sie frühzeitig zu erkennen oder zu vermeiden, sehr gering. Gerade diese Komplexität macht deutlich, wie wichtig kontinuierliche Wachsamkeit, proaktives Bedrohungsmodellieren und Szenario-basierte Simulationen sind, um die Widerstandsfähigkeit von Organisationen zu testen und zu verbessern.

Marc Henauer: Das Management muss verstehen, dass Cybersicherheitskompetenz hochspezialisiert ist und Zeit sowie Aufmerksamkeit erfordert, um die Auswirkungen zu verstehen und Szenarien richtig einzuordnen. Jede Mitarbeiterin und jeder Mitarbeiter hat eine Rolle in der Cybersicherheit, daher ist ihre Schulung von entscheidender Bedeutung. In der Kommunikation reicht es nicht, nur nach aussen oder top-down intern zu kommunizieren. Es braucht auch funktionierende Kanäle, über die Endnutzer verdächtige IT-Vorgänge bottom-up melden können. Letztendlich muss die Cybersicherheitsbereitschaft in der gesamten Unternehmenskultur verankert sein und darf nicht auf die IT-Abteilung beschränkt bleiben.

Malware-Verbreitungskanäle nach Dateityp



Anmerkung: Diese Abbildung zeigt die Verteilung der Malware-Verbreitungsmethoden nach Dateityp im Jahr 2024.
Quelle: IBM X-Force

Welche aktuellen Trends bei Investitionen in Cybersicherheit prägen die Praxis der Branche besonders stark?

Marc Henauer: Es setzt sich zunehmend die Erkenntnis durch, dass kontinuierliches Testen von entscheidender Bedeutung ist. Dieses Testen muss sowohl technische als auch prozessuale Aspekte abdecken, einschliesslich Angriffssimulationen. Wenn das Testumfeld über den Kreis der Cybersicherheitsexperten hinaus erweitert wird, kann auch die Kommunikation verbessert werden. Dies ist ein zentraler Aspekt, um gegenüber Dritten, Investoren und Aufsichtsbehörden Vertrauen zu schaffen. Künstliche Intelligenz wird zunehmend eingesetzt, um Sicherheitsfunktionen zu stärken und Angriffe zu simulieren. Die Investitionen in Cybersicherheit und die Kosten von Sicherheitsvorfällen schlagen sich inzwischen zunehmend in den Finanzberichten nieder – etwa in Form steigender Betriebsausgaben oder finanzieller Folgen konkreter Vorfälle.

Fabian Schär: Neben Testen bilden Snapshots und mehrere Backups eine solide Verteidigung gegen Kontaminationsprobleme und Ransomware-Angriffe, die ganze Systeme lahmlegen können. Allerdings scheinen viele kleine und mittlere Unternehmen, die diesen Risiken besonders ausgesetzt sind, noch kein vollständiges Backup-System eingerichtet zu haben. Zwar bieten Snapshots und Backups keine umfassende Lösung für alle Cyberrisiken, aber sie sind ein vergleichsweise einfacher und kosteneffizienter Weg, um die IT-Infrastruktur gegen einen grossen Teil heutiger Bedrohungen abzusichern. Sie schützen jedoch nicht vor Angriffen wie Datenerpressung oder doppelter Erpressung, bei denen Daten zunächst verschlüsselt werden und der Angreifer dann ein Lösegeld verlangt, um sie geheim zu halten.

Wie entscheiden Finanzinstitute, wie viel sie in Cybersicherheit investieren, und welche Faktoren beeinflussen diese Entscheidungen?

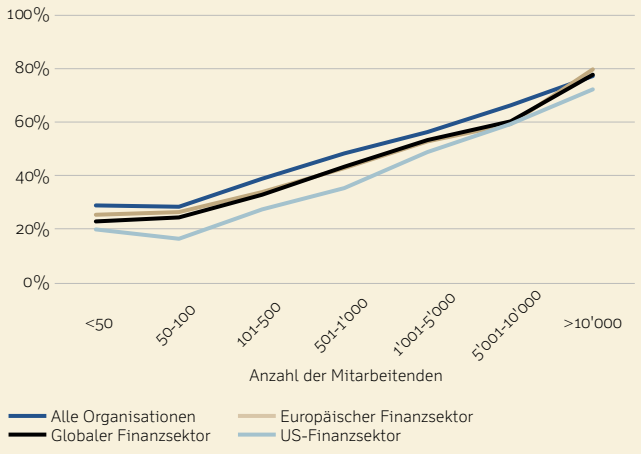
Olivier Scaillet: Einfach ausgedrückt: Entscheidungen über Investitionen in Cybersicherheit hängen davon ab, wie hoch Finanzinstitute ihr Cybersicherheitsrisiko einschätzen. Eine Analyse von in den USA börsennotierten Unternehmen zeigt, dass diese Einschätzung von mehreren Faktoren beeinflusst wird, darunter frühere Cyberangriffe, Unternehmens- und Branchenspezifika, die Qualität der Unternehmensführung sowie regulatorischer oder marktwirtschaftlicher Druck. Interessanterweise schneiden Unternehmen mit höherem Cybersicherheitsrisiko im Schnitt um etwa 10% pro Jahr besser ab als ihre Mitbewerber – solange das Risiko nicht eintritt. Wenn es jedoch zu einem Vorfall kommt, fallen ihre Verluste überdurchschnittlich hoch aus. Diese Differenz legt nahe, dass ein eigenständiger Cyberrisikofaktor existiert, der vom Markt eingepreist wird. Finanzinstitute müssen sich angesichts ihrer kritischen Rolle und ihrer erhöhten Gefährdung dieser dynamischen Bedrohung bewusst sein und sicherstellen, dass ihre Investitionen in Cybersicherheit sowohl vorausschauend als auch ihrem Risikoprofil angemessen sind.

Marc Henauer: Es ist wahrscheinlich, dass frühere Erfahrungen, Management und die Interessen des Verwaltungsrats bei diesen Entscheidungen eine wichtige Rolle spielen. Auch die Finanzaufsichtsbehörden haben einen grossen Einfluss, indem sie die grundlegenden zu erfüllenden Anforderungen festlegen. Ein wichtiger Faktor für die Verbesserung der Cybersicherheit ist ein langfristiger Plan, der die im Laufe der Zeit getätigten finanziellen Investitionen umreisst und es dem Management ermöglicht, Fortschritte und wichtige Meilensteine nachzuverfolgen.

Was sind die möglichen Folgen eines Cyberangriffs auf Kernbankensysteme oder Finanznachrichtensysteme?

Fabian Schär: Geschäftsbanken müssen sicherstellen, dass sie ihren Kundinnen und Kunden rund um die Uhr Finanzdienstleistungen wie Zahlungen anbieten können. Führende internationale Banken wickeln täglich bis zu 100 Millionen Transaktionen ab, darunter Überweisungen, Kreditkartenzahlungen und mobile Transaktionen. Wird das Kernbankensystem einer grossen Bank gezielt angegriffen, hat das sofortige Auswirkungen auf die Märkte: Geldströme geraten ins Stocken oder verlaufen unkontrolliert – sowohl im Finanzsystem als auch in der Realwirtschaft – bis andere Banken einspringen. Das zentrale Verrechnungs- und Abwicklungssystem ist das Rückgrat jedes Finanzsystems. Kommt es zu Problemen in einem Finanznachrichtennetz oder einem Abwicklungssystem – etwa bei SWIFT, TARGET2, Fedwire oder dem SIX Interbank Clearing – können die Folgen weitreichend sein und Panik sowohl im Finanzsektor als auch in der realen Welt auslösen – unabhängig von nationalen Grenzen.

Bekannte ausgenutzte Schwachstellen nach Unternehmensgrösse: Gesamtwirtschaft und Finanzsektor



Anmerkung: Diese Abbildung zeigt den Anteil der Organisationen, bei denen im Jahr 2023 mindestens eine bekannte ausgenutzte Schwachstelle (Englisch: Known-Exploited Vulnerability oder KEV) in ihrer IT-Infrastruktur entdeckt wurde, aufgeschlüsselt nach Unternehmensgrösse. Sie enthält einen gesamtwirtschaftlichen Referenzwert über alle Sektoren hinweg sowie aggregierte Zahlen für den globalen Finanzsektor und seine europäischen und US-amerikanischen Komponenten. Die Unternehmensgrössenkategorien sind nach der Anzahl der Mitarbeitenden definiert.

Quelle: Bitsight

Wie quantifizieren Finanzinstitute Cyberrisiken, um sie wirksam zu steuern?

Beat Schär: Angesichts der Vielzahl an Einflussfaktoren und Unwägbarkeiten erfordert eine präzise Quantifizierung dieser Risiken erheblichen zusätzlichen Aufwand, bei möglicherweise begrenztem Nutzen. Ein breit angelegter, Szenario-basierter Ansatz ist wahrscheinlich der effektivste Weg zur Situationsbewertung, und hat sich offenbar als Standard durchgesetzt. Da die Kommunikation über Cybersicherheit ohnehin komplex ist und das quantitative Cyber-Risikomanagement noch in den Kinderschuhen steckt, ist es am besten, die Informationen für die Unternehmensleitung klar und prägnant zu halten.

Welche Cybersicherheitsrisiken entstehen durch Drittanbieter?

Alain Beuchat: Der Einsatz von Drittanbietern, seien es Cloud-Anbieter, ausgelagerte IT-Dienstleister oder Softwareanbieter, ist heute unverzichtbar geworden. Damit entsteht jedoch eine neue Risikodimension, die immer schwieriger zu beherrschen ist. Aufsichtsbehörden erwarten von uns, dass wir an unsere Dienstleister dieselben Sicherheitsanforderungen stellen wie innerhalb der Bank selbst. In der Praxis bedeutet dies fortlaufende Audits, umfangreiche Fragebögen für Anbieter und regelmässige Nachkontrollen, um Standards auch ausserhalb unseres direkten Einflussbereichs durchzusetzen. Mit zunehmender Auslagerung wächst auch die Angriffsfläche. Für Finanzinstitute stellt dies eine doppelte Herausforderung dar: Sicherheitsvorgaben gegenüber externen Partnern durchzusetzen und gleichzeitig die Verantwortung für etwaige Vorfälle intern zu tragen.

Was sind die Grenzen und voraussichtlichen Entwicklungen auf dem Markt für Cyberversicherungen?

Beat Schär: Die Auswirkungen eines Cyberangriffs zu bewerten ist relativ einfach, aber die Wahrscheinlichkeit, angegriffen zu werden, zu bestimmen, ist äusserst komplex. Diese Komplexität macht es schwierig, das Gesamtrisiko genau einzuschätzen. Ein pragmatischer Ansatz besteht darin, das eigene Cybersicherheitsniveau mit dem der Branchenkollegen zu vergleichen und diese zu übertreffen. Wie in vielen Bereichen des Risikomanagements geht es darum, der Entwicklung stets einen Schritt voraus zu sein. Allerdings muss man realistisch bleiben: Jede Versicherungspolice hat ihre Lücken, und Cyberversicherungen bilden hier keine Ausnahme. Ein weiteres Problem für Versicherer ist das Konzentrationsrisiko – einzelne Cloud-Anbieter stellen heute einen erheblichen Anteil an der weltweiten Rechenkapazität bereit. Diese Konzentration wirft ernsthafte Fragen auf, wie Versicherer ihr systemisches Risiko in einem so stark vernetzten digitalen Ökosystem überhaupt noch steuern können.

Alain Beuchat: Der Markt für Cyberversicherungen entwickelt sich rasant, ebenso wie unser Bewusstsein für seine Grenzen und Haftungsrisiken. Früher waren Cyberpolicen günstig und wurden unter wenig strengen Zeichnungsbedingungen abgeschlossen. Heute führen Versicherer gründliche Due-Diligence-Prüfungen durch, stellen detaillierte technische Fragen und fechten im Schadenfall Ansprüche schnell an. Dabei geht es nicht nur um Kosten, sondern auch um Verlässlichkeit. Wenn ein Angriff auf ein Unternehmen auf eine falsch konfigurierte Maschine oder veraltete Anti-Malware-Software zurückzuführen ist, können Versicherer Ausschlüsse geltend machen und die Leistungen kürzen – unabhängig davon, wie solide das übrige Sicherheitskonzept ist. In vielen Fällen sind die Reputations- und Kundenverluste, die wirklich weh tun, überhaupt nicht durch die Versicherung gedeckt. Angesichts steigender Prämien und strengerer Ausschlüsse beginnen einige Unternehmen, Cyberversicherungen eher als letztes Mittel denn als Eckpfeiler ihrer Risikostrategie zu betrachten.

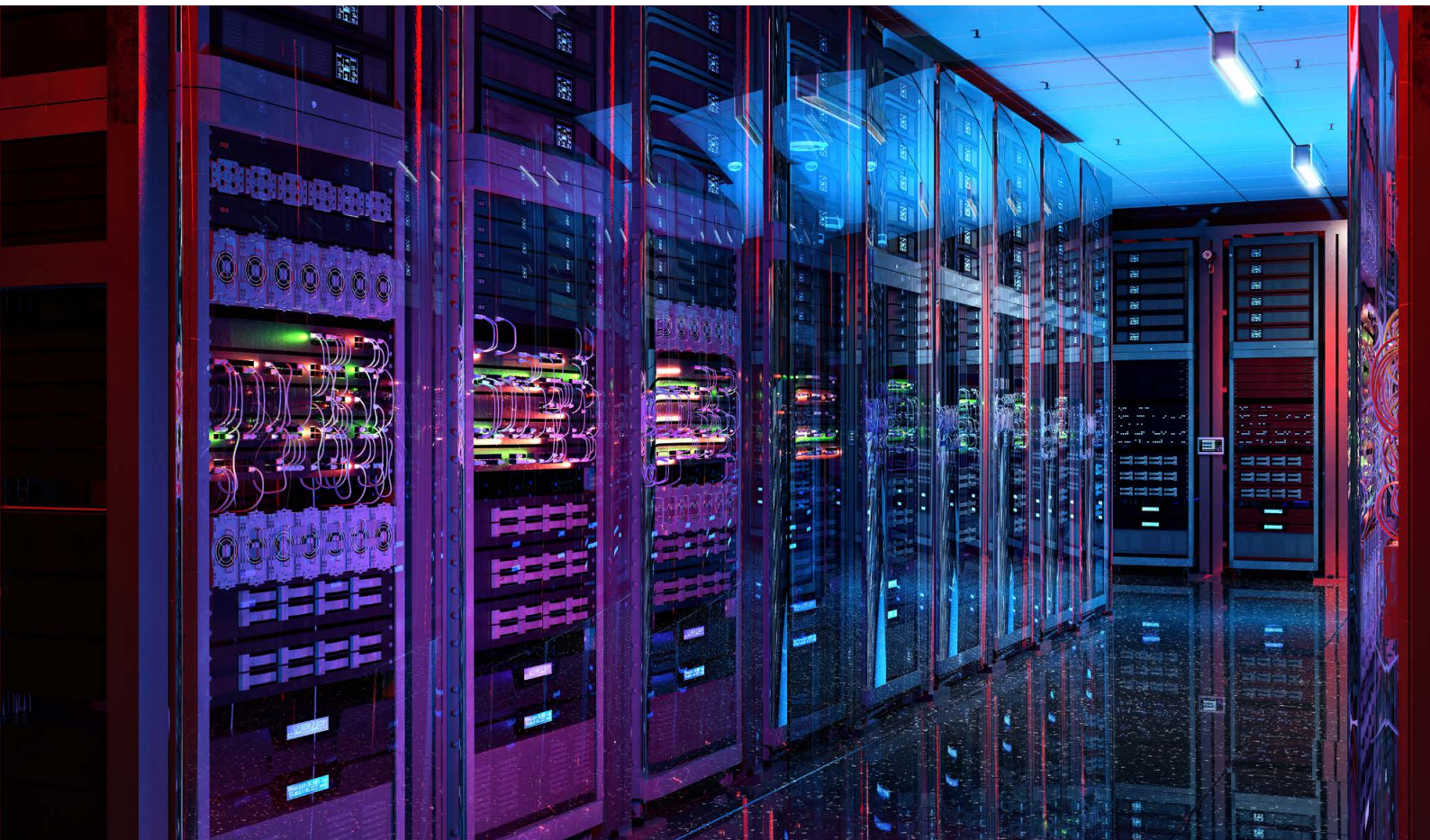
Anastasia Kartasheva: Cyberrisiken sind geprägt von Verlustverteilungen, bei denen seltene, aber sehr gravierende Schäden überproportional ins Gewicht fallen, unsicheren Modellen und asymmetrischer Informationslage. Im Gegensatz zu klassischen versicherbaren Risiken sind Cybereregnisse oft global, schnelllebig und bewusst anpassungsfähig, was ihre Prognose und Modellierung besonders schwierig macht. Ihre hohen Kosten und ihre sich verändernde Natur tragen zusätzlich zur Komplexität bei. Diese Eigenschaften stellen Versicherer vor grosse Herausforderungen, bedeuten aber auch, dass der Markt ein gewisses Potenzial birgt. Zu den neuen Lösungen gehört die Schaffung von Informationsvermittlern, die die Cyber-Resilienz eines Unternehmens bewerten, ähnlich wie Kreditratingagenturen in Anleihemärkten.

Olivier Scaillet: Der Markt für Cyberversicherungen entwickelt sich zunehmend zu einem eigenständigen Sektor. Eine Möglichkeit, diesen Wandel zu verstehen, ist der Blick auf das Verhältnis zwischen Investitionen in die eigene Cybersicherheit und der Risikotransfer über Versicherungen. Versicherer bieten mittlerweile nicht nur Versicherungsschutz an, sondern unterstützen Unternehmen auch direkt oder über Drittanbieter beim aktiven Management ihrer Cyberrisiken. Mit der Weiterentwicklung dieser Modelle dürfte auch der Druck auf die Rückversicherung steigen, da Kosten und Komplexität von Cyber-Exponierungen zunehmen. Langfristig könnte sich daraus eine globale Risikoteilung entwickeln – etwa in Form von Versicherungssyndikaten oder Sekundärmärkten für Cyberrisiken, ähnlich wie bei Katastrophenanleihen. Solche Instrumente würden es Investoren ermöglichen, cyberbezogene Wertpapiere zu handeln, und könnten die Kapazitäten über den traditionellen Versicherungsrahmen hinaus erweitern.

Welche fortschrittlichen Strategien brauchen Finanzinstitute in Zukunft, um Cyberangriffe wirksam abzuwehren?

Marc Henauer: Finanzinstitute verfügen über ein tiefgreifendes Verständnis der Cybersicherheitslandschaft und der Funktionsweise des vernetzten Finanzsystems sowie seiner potenziellen Schwachstellen. Ganz gleich, ob gross oder klein, jede Bank kann eine Kettenreaktion auslösen, die sich auf die gesamte Finanzinfrastruktur auswirkt. Zudem ist bekannt, wie stark Reputationsschäden auf die gesamte Branche abstrahlen. Wird eine Bank schwer getroffen, spürt das der gesamte Sektor. Ein individueller Vorteil ist in diesem Zusammenhang nicht zu erzielen. Diese Tatsache motiviert Finanzinstitute zu proaktiver Zusammenarbeit und zu offener und effizienter Kommunikation.

Olivier Scaillet: Mit Blick nach vorn müssen Finanzinstitute auf fortschrittliche, mehrschichtige Verteidigungsstrategien setzen – etwa KI-gestützte Bedrohungserkennung, Zero-Trust-Architekturen und kontinuierliche Schulung der Mitarbeitenden –, um einem zunehmend komplexen Bedrohungsumfeld einen Schritt voraus zu sein. Über den eigenen Schutz hinaus sind Banken jedoch in einer einzigartigen Position, um neue Geschäftsmöglichkeiten im Bereich der Cybersicherheit zu nutzen. Da Cyberrisiken zunehmend als messbare und bepreiste Vermögenswerte verstanden werden, können Finanzinstitute eine Vorreiterrolle bei der Entwicklung und dem Angebot innovativer Finanzprodukte übernehmen, beispielsweise Cyber-Risiko-Tranchen nach dem Vorbild von besicherten Schuldverschreibungen (Englisch: Collateralized Debt Obligations, oder CDOs). Durch die Aufteilung von Risiken in verlustabsorbierende Tranchen je nach Schweregrad ermöglichen Banken eine marktbasierte Diversifikation, bieten massgeschneiderte Cyberversicherungsprodukte an und helfen ihren Kunden, Cyberrisiken gezielt abzusichern. Auf diese Weise entwickeln sie sich von passiven Zielscheiben zu aktiven Marktgestaltern in der sich herausbildenden Cyberrisiko-Ökonomie.



Zukunftsbereiche

Machen Initiativen im Bereich der dezentralen Finanzdienstleistungen (DeFi) die Finanzwelt aus Cybersicherheitssicht sicherer oder anfälliger?

Fabian Schär: Dezentrale und zentralisierte Finanzsysteme weisen unterschiedliche Cybersicherheitsrisiken auf, wobei keines der beiden Systeme eindeutig überlegen ist. Einerseits bieten dezentrale Systeme gewisse Sicherheitsvorteile, insbesondere die Tatsache, dass kein einzelner Akteur das öffentliche Hauptbuch einseitig verändern kann. Dadurch entfallen viele Angriffspunkte, die in zentralisierten Architekturen typisch sind. Andererseits entstehen jedoch neuartige Verwundbarkeiten. Beispielsweise sind DeFi-Systeme stark von privaten Schlüsseln abhängig. Wenn ein Nutzer seinen Schlüssel verliert oder preisgibt, ist der Verlust endgültig – ohne rechtliche oder technische Rückabwicklung: Seine Vermögenswerte können unwiderruflich gestohlen werden, und Angreifer können sogar seine kompromittierte Identität nutzen, um neue Smart Contracts zu erstellen. Der grundlegende Reiz von DeFi liegt in seiner vertrauensfreien Struktur, der Prozessvereinfachung und den schnelleren Transaktionen – Eigenschaften, die aus geschäftlicher Sicht sehr vorteilhaft sein können. Doch durch das Fehlen klassischer Intermediäre verlagert sich das Risiko auf die Nutzer selbst. Nutzer müssen nicht nur ihre Schlüssel sichern, sondern sich auch in einem komplexen System zurechtfinden, in dem in der traditionellen Finanzwelt übliche Schutzmassnahmen wie Rückbuchungen oder Streitbeilegung weitgehend fehlen. In diesem Sinne erweitert DeFi zwar die Bandbreite der Möglichkeiten, bringt aber auch eine neue Klasse von Cybersicherheits- und Betriebsrisiken mit sich, die verstanden und aktiv gemanagt werden müssen.

Olivier Scaillet: Wie jede technologische Innovation hat auch diese Vor- und Nachteile. Untersuchungen haben ergeben, dass Ransomware-Angriffe die häufigste Art von Cyberangriffen sind, wobei eine kleine Anzahl hochentwickelter Ransomware-Banden die Szene dominiert. Diese Gruppen funktionieren inzwischen wie professionelle Unternehmen: mit klangvollen Namen, Büros, Callcentern und Franchise-Strukturen. Sie erhalten Lösegeldzahlungen in der Regel in Kryptowährungen und müssen die Erlöse über komplexe Konstrukte waschen. Da Bitcoin rückverfolgbar ist, bevorzugen Angreifer weniger transparente Kryptowährungen wie Monero oder Zcash. Es gibt vereinzelte Berichte, dass Banden einen Aufschlag von 20% verlangen, wenn Opfer auf einer Zahlung in Bitcoin bestehen. Eine Lösung, die den Missbrauch von Kryptowährungen im Cyberkriminalitätskontext vollständig unterbindet, ist kaum realistisch, da ein vollständiges Verbot aller Kryptowährungen in einem Staat deren Vorteile zunichtemachen und den Staat technologisch benachteiligen würde.

Was unterscheidet Zentralbankgeld, Geschäftsbankgeld und Krypto-Assets im Hinblick auf Cybersicherheitsrisiken?

Anastasia Kartasheva: Der Diebstahl von elektronischem Geld oder Vermögenswerten ist nur die halbe Miete. Die andere Hälfte besteht darin, es einzulösen. Der Angriff auf die Bangladesh Bank im Jahr 2016 ist ein anschauliches Beispiel. Hacker drangen in das IT-System der Zentralbank ein und verschafften sich Zugang zu ihrem SWIFT-Netzwerk, um fingierte Überweisungsaufträge in Höhe von insgesamt 951 Millionen US-Dollar zu versenden. Etwa 81 Millionen US-Dollar wurden auf Konten auf den Philippinen überwiesen und dann über ein komplexes und kostspieliges Netzwerk aus Briefkastenfirmen und Casinos gewaschen. Interessanterweise wurden die restlichen Überweisungen im Wert von über 850 Millionen US-Dollar gestoppt, weil ein Tippfehler im Überweisungsauftrag Verdacht erregte. Zwar ist es in Ländern mit schwacher Regulierung relativ einfach, unregulierte Vermögenswerte wie Bitcoins umzuwandeln, doch ist dies ein riskanter und undurchsichtiger Prozess, und am Ende hält der Empfänger womöglich nur "Spielgeld" in der Hand.

Wie verschärft künstliche Intelligenz Cybersicherheitsbedrohungen?

Anastasia Kartasheva: Künstliche Intelligenz ist ein zweischneidiges Schwert. Angreifer sind heute wesentlich raffinierter. Die Zeiten, in denen massenhaft E-Mails mit zufälligen Adressen, Tippfehlern und schlecht gestalteten Logos verschickt wurden, sind vorbei. Gleichzeitig können Verteidiger künstliche Intelligenz nutzen, um ihr Team zu stärken und ihre Abwehrmassnahmen zu automatisieren. Die Branche strebt den Einsatz von KI-Tools im gesamten IT-System an. Es ist von entscheidender Bedeutung, das Bewusstsein für die Bedrohungen von heute und morgen zu schärfen und Nutzer auf breiter Basis aufzuklären.

Fabian Schär: Besonders besorgniserregend finde ich die rasante Entwicklung von Deepfakes, die durch Deep-Learning-Modelle angetrieben wird. Der einzige Abwehrmechanismus, der mir derzeit einfällt, sind kryptografische Signaturen. Heutzutage sind Tausende von Stunden Videomaterial mit führenden Politikern im Netz verfügbar. Es ist vergleichsweise einfach, ein KI-Modell zu trainieren, das diese Personen glaubhaft imitiert und ihnen beliebige Aussagen in den Mund legt. Ich glaube, dass wir uns bald in einer Welt wiederfinden werden, in der Reden nicht mehr persönlich gehalten werden, sondern von einem künstlichen Intelligenzsystem geschrieben und präsentiert werden, wobei die Rede kryptografisch signiert ist, um ihre Authentizität zu gewährleisten.

Wie gehen Finanzinstitute heute mit Cybersicherheits-bedrohungen durch künstliche Intelligenz um?

Fabian Schär: Für Finanzunternehmen ist es aus zwei Gründen schwierig, in diesem Bereich die Nase vorn zu behalten. Erstens ist der Wettbewerb sehr schnelllebig. Zweitens existieren Banken häufig über sehr lange Zeiträume hinweg, was bedeutet, dass sie mit komplexen Altsystemen arbeiten, die schwer effektiv abzusichern sind. Künstliche Intelligenz wird ihnen künftig dabei helfen, verdächtige Aktivitäten frühzeitig zu erkennen und schneller zu reagieren. Allerdings scheinen die Angreifer hier die Oberhand zu gewinnen.

Olivier Scaillet: Es gibt eine Reihe vielversprechender Entwicklungen. Künstliche Intelligenz bietet zahlreiche Vorteile, wie Effizienz, Skalierbarkeit und Anpassungsfähigkeit in der Cybersicherheit. Diese Vorteile erleichtern die Identifizierung potenzieller betrügerischer Aktivitäten anhand von Kundenverhaltensmustern, das Antizipieren von Bedrohungen durch Lernen aus historischen Daten und die Schaffung automatisierter Abwehrsysteme, die Probleme isolieren und Reaktionszeiten verkürzen. Allerdings wird vieles von dem, was wir heute als Stand der Technik betrachten, grundlegend überdacht werden müssen, sobald Quantencomputing zum Standard wird.

Was ist ein realistischer Zeithorizont für Bedrohungen durch Quantencomputer?

Anastasia Kartasheva: Rechenleistung und -geschwindigkeit sind in der Cyberwelt von entscheidender Bedeutung. Einige Experten sagen voraus, dass komplexere Angriffe durch Quantencomputer innerhalb des nächsten Jahrzehnts zum Standard werden könnten. Doch obwohl Cyberangriffe per Definition mit Computern ausgeführt werden, ist immer auch ein menschlicher Faktor im Spiel. Rechenleistung ist nicht der einzige Faktor, sowohl Angreifer als auch Verteidiger müssen ihre Fähigkeiten im Laufe der Zeit verbessern.

Welche konkreten Schritte sollten Finanzinstitute unternehmen, um sich auf eine quantenresistente Cybersicherheit vorzubereiten?

Fabian Schär: Banken müssen sich immer auf zukünftige Herausforderungen vorbereiten. Meiner Meinung nach müssen sie ihr Verständnis sowohl des aktuellen Systems als auch des sich entwickelnden Systems verbessern. Das heutige IT-Framework im Bankwesen ist ein konsolidiertes Modell, das in den 1950er Jahren etabliert wurde und seitdem zahlreiche Fusionen und Übernahmen durchlaufen hat. Im Gegensatz zu vielen anderen Branchen ist die Bedeutung eines zentralisierten Systems im Bankensektor von entscheidender Bedeutung, und das Problem der Altsysteme ist erheblich. J.P. Morgan Chase beispielsweise ist das Ergebnis von über 1'200 Vorgängerinstituten.

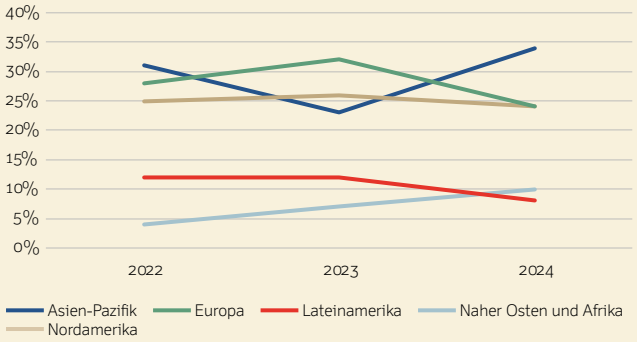
Olivier Scaillet: Die Vorbereitung auf das Quantenzeitalter umfasst mehrere Schritte. Zunächst müssen Banken eine klare Bestandsaufnahme ihrer aktuellen kryptografischen Bausteine erstellen, um deren Konfiguration und Schwachstellen zu verstehen. Anschliessend folgt die Entwicklungsphase, in der sie in Zusammenarbeit mit Systemanbietern und internen Systemverantwortlichen die neue Quantentechnologie gründlich testen. Anschliessend steht der Austausch der alten Technologie durch die neue an. Der derzeitige Ansatz zur Bewältigung der Risiken der Post-Quanten-Kryptografie (Englisch: Post-quantum cryptography oder PQC) und den möglichen Schwächen der neuen quantenresistenten Algorithmen besteht darin, alte und neue Methoden zu kombinieren – durch hybride Protokolle, die beide Technologien gleichzeitig anwenden.

Wie stark unterscheiden sich Länder und Branchen in ihren Möglichkeiten zur Gewährleistung der Cybersicherheit?

Fabian Schär: Die Unterschiede zwischen Ländern und Branchen sind erheblich, und oft historisch, geografisch und institutionell bedingt. Im Finanzsektor beispielsweise geniessen neuere Finanzzentren oft einen strukturellen Vorteil. Ihre Systeme wurden in einer Ära globaler Märkte und elektronischer Handelsgeschäfte aufgebaut und verfügen daher über modernere IT-Grundlagen. Im Gegensatz dazu sind traditionsreiche Banken häufig auf Altsysteme angewiesen, die teilweise mehrere Jahrzehnte alt sind und sich nur schwer und kostspielig modernisieren lassen. Das führt zu komplexen Systemlandschaften, die schwerer abzusichern und zu warten sind. Auf Länderebene verfügt die westliche Welt zwar generell über stärkere Cybersicherheitskapazitäten, doch gibt es weiterhin Unterschiede. Einige Länder stehen stärker im geopolitischen Fokus und sind daher häufiger Ziel von Cyberangriffen – insbesondere die Vereinigten Staaten. Andere Länder wie die Schweiz profitieren von einer neutraleren geopolitischen Position, gut ausgestatteten Institutionen und einer starken Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Diese Unterschiede prägen sowohl die Anfälligkeit als auch die Widerstandsfähigkeit gegenüber sich wandelnden Bedrohungen.

Anastasia Kartasheva: Die Cybersicherheitsbereitschaft variiert nicht nur von Land zu Land, sondern auch von Branche zu Branche, von Unternehmen zu Unternehmen und von Person zu Person, je nachdem, wie klar die Verantwortlichkeiten definiert sind und wie gut die Ressourcen aufeinander abgestimmt sind. In einigen Ländern hat der öffentliche Sektor eine Vorreiterrolle übernommen, indem er klare Standards festgelegt, Koordinationsstellen finanziert und den Austausch von Bedrohungsinformationen erleichtert hat. In anderen, insbesondere in Schwellenländern oder Transformationsökonomien, sind Unternehmen oft auf sich allein gestellt, mit wenig Orientierung oder regulatorischer Klarheit. Diese Situation führt zu einem uneinheitlichen Schutzniveau: Während einige grosse Unternehmen über erstklassige Abwehrmechanismen verfügen, sind andere – insbesondere kleinere Unternehmen und staatliche Institutionen – aufgrund begrenzter Budgets und fragmentierter Systeme nach wie vor sehr anfällig. Letztlich hängt die Wirksamkeit eines Cybersicherheitsrahmens ebenso stark von staatlicher Steuerung und institutioneller Reife ab wie von Technologie oder finanziellen Mitteln.

Verteilung von Cyberangriffen nach geografischen Regionen



Anmerkung: Diese Abbildung zeigt die Verteilung von Cyberangriffen nach geografischen Regionen in den Jahren 2022 bis 2024. Im Jahr 2024 waren die am stärksten betroffenen Länder innerhalb der jeweiligen Region die Vereinigten Staaten (86% von Nordamerika), Japan (66% von Asien-Pazifik), Saudi-Arabien (63% vom Nahen Osten und Afrika), Brasilien (53% von Lateinamerika) und das Vereinigte Königreich (25% von Europa).

Quelle: IBM X-Force

Wie würden Sie die Rolle internationaler Standards bei grenzüberschreitenden Cybersicherheitsbemühungen beschreiben?

Marc Henauer: Internationale Standards spielen eine entscheidende Rolle bei der Ermöglichung grenzüberschreitender Zusammenarbeit im Bereich Cybersicherheit. Sie bieten eine gemeinsame Sprache, einheitliche Erwartungen und technische Massstäbe für das Risikomanagement. Die Umsetzung variiert zwar je nach Region und Sektor, aber Standards wie ISO 27001 (von der Internationalen Organisation für Normung) und das Cybersecurity Framework des US-amerikanischen National Institute of Standards and Technology (NIST) tragen dazu bei, Fragmentierung zu verringern und die Zusammenarbeit zwischen Regierungen, Branchen und Lieferketten zu erleichtern. Ähnlich wie in der Klimapolitik braucht es auch in der Cybersicherheit eine globale Abstimmung, die praktische Umsetzung in koordiniertes Handeln bleibt jedoch eine komplexe Herausforderung. Echte Fortschritte hängen von Gegenseitigkeit und Vertrauen über Grenzen und Sektoren hinweg ab, nicht von der Auferlegung einheitlicher Modelle. Das Risiko, wichtige Einrichtungen wie MITRE zu verlieren, eine gemeinnützige Forschungsorganisation, die gemeinsame Infrastrukturen wie ein weltweit genutztes Verzeichnis öffentlich bekannter IT-Sicherheitslücken (English: Common Vulnerabilities and Exposures identifiers oder CVE) betreibt, zeigt die Fragilität zentralisierter Systeme. Es unterstreicht die Notwendigkeit widerstandsfähiger, verteilter und kooperativer Ansätze für eine globale Cybersicherheits-Governance.

Beat Schär: Internationale Standards sind als Referenzpunkte äusserst wertvoll. Sie helfen Organisationen einzuschätzen, wo sie stehen und wie sie sich verbessern können. Die Vielzahl an Initiativen in verschiedenen Ländern und Branchen liefert zudem wertvolle Einblicke in die Herausforderungen und Lösungsansätze anderer. Im Bereich der Cybersicherheit hat kein einzelner Akteur alle Antworten – kontinuierliches voneinander Lernen ist nicht nur hilfreich, sondern unerlässlich.

Fazit

Welche Rolle sollten Unternehmensführung, Verwaltungsratmitglieder und Regulierungsbehörden in der Cybersicherheits-Governance spielen?

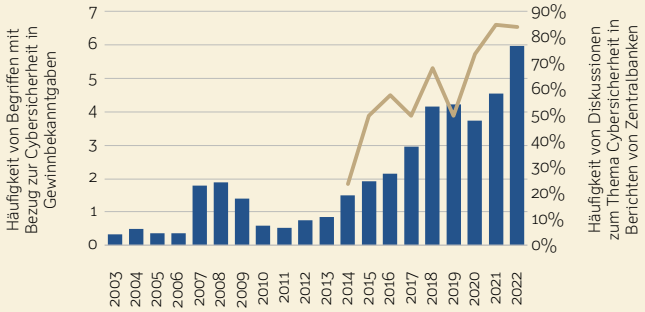
Alain Beuchat: Die jüngsten Schweizer Vorschriften verlangen, dass Cybersicherheitsstrategien vom Verwaltungsrat genehmigt werden müssen. Doch die Einbindung des Vorstands und Verwaltungsrats im Bereich Cybersicherheit ist mehr als nur eine Compliance-Anforderung – es ist zunehmend eine Frage des strategischen Überlebens. Mit anderen Worten: Formale Zuständigkeit bedeutet nicht automatisch wirksame Aufsicht. Viele Verwaltungsratsmitglieder unterschätzen, wie stark ihre Unternehmen von der IT-Infrastruktur abhängig sind – ganz zu schweigen vom Verständnis der Komplexität der Cyberabwehr. Zwar ist das Bewusstsein für die Folgen von Cyberangriffen durch die mediale Berichterstattung gewachsen, doch fällt es oft schwer, diese Risiken mit den konkreten Schwachstellen des eigenen Unternehmens zu verknüpfen. Um diese Lücke zu schliessen, sind mehr als nur gelegentliche Briefings erforderlich. Verwaltungsratsmitglieder müssen über ausreichende Grundkenntnisse verfügen, um relevante Fragen zu stellen, Kosten-Nutzen-Abwägungen zu bewerten und die eigene Risikolage richtig einzuschätzen. Solange dieses Cyberverständnis im Verwaltungsrat fehlt, hinkt die Governance dem Bedrohungsniveau hinterher.

Olivier Scaillet: Im Schweizer Kontext spielen Aufsichtsbehörden wie die FINMA eine entscheidende Rolle bei der Gestaltung der Cybersicherheits-Governance, insbesondere im Finanzsektor. Manche Institute sind weiter als andere, entweder durch bessere Ressourcen oder ein vertieftes Verständnis für Cyberrisiken. In Bereichen wie Cloud-Dienste und Lieferketten ist die Regulierung bislang allerdings noch relativ zurückhaltend. Ein wichtiger nächster Schritt wäre die Klärung der Rollen und Verantwortlichkeiten aller Führungsebenen im Falle eines Cybervorfalls, um eine grössere Verantwortlichkeit der Führungskräfte zu fördern. Gleichzeitig dürfen Verwaltungsrat und Vorstand Cybersicherheit nicht als rein technisches Problem betrachten, das an ihre IT-Teams delegiert werden kann. Sie sollten regelmässig über Vorfälle und wichtige Entwicklungen informiert werden und regelmässig Übungen durchführen, um sicherzustellen, dass sie auch unter Druck handlungsfähig bleiben. Cybersicherheit betrifft nahezu alle Geschäftsbereiche und alle Aspekte der Gesellschaft. Daher sind Verwaltungsräte verpflichtet, sich frühzeitig und proaktiv zu engagieren, anstatt zu warten, bis eine Krise sie zum Handeln zwingt.

Anastasia Kartasheva: Ein gut ausgearbeiteter Notfallplan ist unerlässlich. Dieser sollte wichtige Fragen klären, z. B. wie schnell Systeme wiederhergestellt werden können, ob der Angreifer weiterhin Zugriff hat, welche Schäden durch eine Cyberversicherung gedeckt sind und ob mit aufsichtsrechtlichen Sanktionen oder Geldstrafen zu rechnen ist. Es gibt keine Patentlösung, aber eine proaktive Aufklärung der Unternehmensführung über Cybersicherheitsrisiken ist von entscheidender Bedeutung.

Fabian Schär: Wie so oft gilt: Vernünftige Massnahmen sind hilfreich, aber übertriebene Vorgaben können kontraproduktiv sein. Wenn uns die obligatorischen Cookie-Banner auf Websites eines gelehrt haben, dann ist es, dass regulatorische Compliance häufig nur eine formale Anforderung erfüllt, ohne tatsächliche Sicherheit zu gewährleisten. Letztendlich können weder Unternehmen noch Einzelpersonen ihre Verantwortung an Dritte auslagern. Regulatorische Vorschriften legen die Mindestanforderungen für eine wirksame Cybersicherheit fest, nicht die Höchststandards.

Erwähnungen zum Thema Cybersicherheit durch Unternehmen und Zentralbanken



Schlüsselwörter zum Thema Cybersicherheit in Telefonkonferenzen zur Bekanntgabe der Quartalsergebnisse von Unternehmen (linke Achse)

Anteil der Finanzstabilitätsberichte von Zentralbanken, in denen Cybersicherheit erwähnt wird (rechte Achse)

Anmerkung: Diese Abbildung zeigt zwei Messgrössen institutioneller Aufmerksamkeit für Cybersicherheit zwischen 2003 und 2022. Die Balken zeigen die Häufigkeit von Begriffen mit Bezug zur Cybersicherheit (z. B. Cybersicherheit, Cyberangriff, Cyberbedrohung, Datenverlust, Malware, Ransomware) in Telefonkonferenzen zur Bekanntgabe der Quartalsergebnisse von Unternehmen, standardisiert pro 10'000 Sätze (linke Achse). Die Linie gibt den Anteil der Finanzstabilitätsberichte und Jahresberichte der G20-Zentralbanken an, die sich ausführlich mit Cybersicherheit befassen (rechte Achse).

Quellen: Advisen, NL Analytics und Internationaler Währungsfonds (IWF)

Wie beeinflusst Regulierung Ihrer Ansicht nach die Fähigkeit des Finanzsektors, Cyberrisiken zu bewältigen?

Marc Henauer: Das Bundesamt für Cybersicherheit (BACS) spielt eine entscheidende Rolle bei der Stärkung der Cyber-Resilienz in der Schweiz. Seine Arbeit konzentriert sich auf vier Hauptziele: ein besseres Verständnis der Bedrohungslage, die Ermöglichung von Prävention, die Minimierung von Auswirkungen bei Vorfällen sowie die Absicherung digitaler Produkte und Dienstleistungen. Ein wichtiger Meilenstein war kürzlich die Einführung einer 24-Stunden-Meldepflicht für Cyberangriffe auf kritische Infrastrukturen, die genauere Daten liefern und intelligentere Regulierungsansätze ermöglichen soll. Diese neue Meldepflicht wird zu klareren Bedrohungsanalysen, gezielterer Unterstützung und einer solideren Grundlage für das Management von Cyberrisiken in einem koordinierten nationalen Rahmen führen. Es wird sich zeigen, wie sich diese Vorgabe im Laufe der Zeit entwickelt.

Fabian Schär: Auch wenn sich keine eindeutigen Schlüsse ziehen lassen, deuten die Erfahrungen der Vergangenheit darauf hin, dass Cybersicherheitsvorschriften im Finanzsektor im Allgemeinen wirksam sind. Allerdings können selbst die robustesten regulatorischen Rahmenbedingungen und technischen Sicherheitsvorkehrungen das Risiko menschlicher Fehler nicht vollständig ausschliessen. Daher sind kontinuierliche Schulungen und Sensibilisierungsmassnahmen unerlässlich. Mit Blick auf die Zukunft werden Meldepflichten und eine erhöhte Datentransparenz wahrscheinlich weiterhin die regulatorischen Standards prägen und unser kollektives Verständnis von Cyberbedrohungen verbessern. Allerdings bleibt die Einhaltung kurzer Meldefristen – beispielsweise innerhalb von 24 Stunden – eine Herausforderung, da Unternehmen oft mehr Zeit benötigen, um das Ausmass eines Vorfalls vollständig zu erfassen, insbesondere bei einer Koordination mit externen Parteien.

Olivier Scaillet: In der Finanzbranche ist allen klar, dass es nicht darum geht, ob ein nächster Angriff stattfinden wird, sondern wann – und wie sich seine Auswirkungen möglichst gering halten lassen. Auch wenn diese Erkenntnis zunächst ernüchternd wirkt, schafft sie die notwendige Grundlage, damit sich Unternehmen und die gesamte Branche vorbereiten können. Innerhalb der Unternehmen braucht es eine ehrliche Auseinandersetzung mit der Frage, wie schnell man sich von einem Angriff erholen kann. Zwischen Unternehmen sollte die Diskussion darüber geführt werden, wie sich gemeinsame Risiken durch eine grössere Vielfalt an Hard- und Software begrenzen lassen. Viele dieser Massnahmen lassen sich regulatorisch vorgeben – aber Regulierung hat nur begrenzte Möglichkeiten, die Branche zur Einführung anderer Systeme zu bewegen. Ich sehe mit Sorge, dass die Zahl der Anbieter kontinuierlich sinkt und es bislang keinen gangbaren Weg gibt, diese Entwicklung umzukehren.

Welche neu aufkommenden Cybersicherheitsbedrohungen werden die Gesellschaft im nächsten Jahrzehnt am stärksten beeinflussen?

Fabian Schär: In den nächsten Jahren werden Fortschritte in den Bereichen künstliche Intelligenz, Big Data und Quantencomputing unsere Cybersicherheit auf ein neues Niveau heben.Ich bin fest davon überzeugt, dass wir das volle Potenzial von Bounty-Programmen ausschöpfen sollten, um aus den "Bösen" die "Guten" zu machen. Ransomware-Angriffe sind oft finanziell motiviert – daher ist es naheliegend, dass Unternehmen Personen belohnen, die ihnen helfen, ihre Sicherheit zu verbessern, anstatt Lösegeld zu zahlen, um zu überleben. Das Katz-und-Maus-Spiel gibt es schon seit Urzeiten, und es gibt keinen Grund anzunehmen, dass sich daran in Zukunft etwas ändern wird – lediglich die Werkzeuge werden sich weiterentwickeln.

Anastasia Kartasheva: Der Finanzsektor wird in den nächsten zehn Jahren aufgrund der wachsenden digitalen Abhängigkeiten und globalen Vernetzung mit immer komplexeren Cybersicherheitsbedrohungen konfrontiert sein. Eine zentrale Herausforderung wird die Überprüfung der Identität von Dritten – seien es Unternehmen oder Einzelpersonen – darstellen, insbesondere grenzüberschreitend, wo digitale Standards und Vorschriften unterschiedlich sind. Gleichzeitig wird sich die Angriffsfläche durch die zunehmende Verbreitung vernetzter Geräte, die Konsolidierung von IT-Systemen und die weitgehende Nutzung von Cloud-Diensten erweitern. Diese Entwicklungen werden in Verbindung mit Fortschritten in den Bereichen künstliche Intelligenz, maschinelles Lernen und Quantencomputing immer raffiniertere Angreifer hervorbringen. In der Folge wird ein grundlegendes Umdenken in Bezug auf Vertrauen, Verifizierung und Resilienz in der Cybersicherheit erforderlich sein.

Swiss Finance Institute

Mit Unterstützung seiner Gründer – der Schweizer Bankenbranche, der Schweizerischen Eidgenossenschaft sowie führender Schweizer Universitäten – fördert das Swiss Finance Institute (SFI) aktiv Forschung und Lehre auf Weltniveau im Bereich Banking und Finance in der Schweiz. Durch die Verbindung von akademischer Exzellenz mit Praxiserfahrung trägt das SFI zur Stärkung des Schweizer Finanzplatzes bei.

Herausgeber und Kontakt
Dr. Cyril Pasche
Senior Director Publications and Topic Development
+41 22 379 88 25
cyril.pasche@sfi.ch

swiss:finance:institute

Walchestr. 9, CH-8006 Zurich, T +41 44 254 30 80
c/o University of Geneva, 42, Bd du Pont d'Arve, CH-1211 Geneva 4, T +41 22 379 84 71
www.sfi.ch

Version 10/2025