WHITEPAPER

# Cybersicherheitslage im Schweizer Finanzsektor

JULI 2023

# Inhalt

# 1. Vorwort

«Wir bei Mastercard haben uns verpflichtet, unser Netzwerk zukunftsfähig aufzustellen und Cybersicherheit mithilfe von KI und unseren fundierten Erfahrungen ganzheitlich anzugehen. Dieses Angebot aus einer Hand hilft unseren Kund:innen, sich gegen Cyberrisiken zu schützen – und ermöglicht ihnen ihrerseits, geschäftliches Vertrauen aufzubauen.»

Ajay Bhalla, President, Cyber and Intelligence Solutions bei Mastercard

Nie war Cybersicherheit wichtiger und wurde breiter diskutiert als heute. Die Digitalisierung aller Branchen – Privatwirtschaft wie staatliche Verwaltungen – schreitet immer schneller voran, macht sie in diesem Bereich angreifbarer und erfordert deshalb stärkeren Schutz. Zwei Ereignisse haben das in den vergangenen Jahren noch weiter in den Blickpunkt gerückt.

**Die Covid-19-Pandemie hat eine beispiellose digitale Transformation von Regierungen, Institutionen und Unternehmen vorangetrieben.** Videoanrufe, elektronische Identifikationen und Signaturen, mobile Zahlungen und andere Technologien wurden als neue Standards breit implementiert und angenommen. Damit erhöhen sich auch die möglichen Zugangswege und Anreize für Datendiebstahl und betrügerische Manipulationen.

**Die aktuelle geopolitische Lage hat Auswirkungen, die weltweit ebenso den digitalen Raum betreffen.** Daten von Cyber Quant, einer Cybersecurity-Lösung von Mastercard, zeigen, dass sich rund zwei Drittel der politisch motivierten Cyberangriffe auf europäische Unternehmen mit ausländischen Akteuren in Verbindung bringen lassen – mit klar steigender Tendenz.

**Die Entwicklung noch stärker hin zum Digitalen hat enorme Vorteile, schafft aber auch eine noch einmal attraktivere Umgebung für Cyberkriminelle.** Sie sind organisierter als je zuvor und nutzen selbst komplexe Technologien, um ihre finanziellen oder politischen Ziele zu erreichen. Gleichzeitig versuchen Nationalstaaten, ihren Einfluss im Cyberspace zu vergrössern, ebenso ideologisch, politisch oder sozial motivierte Aktivist:innen.

Die Finanzbranche ist dabei ein besonders attraktives Ziel. So liegt es in ihrem Interesse, auf bestehende und kommende Cyberbedrohungen vorbereitet zu sein. Das gilt insbesondere für die Schweiz als einen der weltweit wichtigsten Finanzplätze.

Die nachfolgend ausgeführte Studie benennt die wichtigsten Risiken sowie organisatorische und technische Lösungen für Unternehmen und Verwaltungen. Mastercard, der weltweite Pionier in Sachen Zahlungsinnovation und -technologie, bringt dafür die Erfahrung aus mehr als 50 Jahren und der Sicherung von zwei Milliarden Karten ein.

**Dr. Daniela Massaro**
Country Manager
Mastercard Schweiz

# 2. Höhere Risiken durch globale Umbrüche

Schon in den vergangenen Jahrzehnten haben Cyberkriminelle jede technologische Weiterentwicklung durch neue und komplexere Angriffsmethoden nachvollzogen. **Mit der Erweiterung digitaler Netzwerke steigt das Risiko, dass Bedrohungsakteur:innen neue Einstiegspunkte für ihre Angriffe nutzen.** Ein hoher Grad an Cybersicherheit und aktives Risikomanagement sind deshalb entscheidend zu deren Abwehr. Bisher unbekannte Arten von Cyberangriffen und eine vergrösserte Angriffsfläche erfordern, dass Organisationen widerstandsfähiger werden und beginnen, Erfolgsmethoden für Cybersicherheit vollständig zu integrieren.

Malware- oder Ransomware-Angriffe nehmen alarmierend zu. Das Nationale Zentrum für Cybersicherheit der Schweiz (NCSC) meldete 2022 rund 34 000 Cybervorfälle, mehr als 90 pro Tag. Das entspricht einer Zunahme von rund 50 Prozent gegenüber dem Vorjahr. Da die Meldung auf freiwilliger Basis erfolgt, dürfte die tatsächliche Zahl noch deutlich höher liegen.

Ein IT-Systemausfall kostet Unternehmen durchschnittlich 5200 Franken pro Minute.[1] Doch mehr verrät der Blick auf die Schadenssummen nach einer Datenschutzverletzung. Sie liegen nach einer Studie von IBM **bei durchschnittlich 4,1 Millionen Franken pro Fall, für Finanzinstitute sogar bei 5,8 Millionen Franken** – noch bevor Reputationsschäden berücksichtigt sind. Für die kommenden fünf Jahre prognostiziert diese Erhebung **einen Anstieg von jährlich 15 Prozent.[2] Rund 40 Prozent der angegriffenen Firmen zahlen Hacker:innen ein Lösegeld,** um wieder Zugriff auf kompromittierte oder blockierte Systeme zu erhalten. Gezahlt werden von betroffenen Unternehmen in der Schweiz im Schnitt aktuell rund 80 000 Franken (weltweit 167 000 Franken). Die anschliessende Behebung des technischen, organisatorischen und reputativen Schadens kostet typischerweise mehr als 1,5 Millionen Franken.[3]

Börsennotierte Unternehmen **verloren bei einem Datenleck durchschnittlich 1,1 Prozent ihres Marktwertes und mussten einen Rückgang ihres Umsatzwachstums um 3,2 Prozent gegenüber dem Vorjahr hinnehmen,** stellte die amerikanische NGO National Bureau of Economic Research (NBER) fest.[4] Viele Schweizer Kader benennen die Cybersicherheit bereits als einen der grössten Risikofaktoren für ihre Unternehmen.[5]

[1] Everbridge, *The Impact of Cybersecurity Risks on Financial Services*, https://www.everbridge.com/blog/the-impact-of-cybersecurity-risks-on-financial-services/
[2] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach
[3] Sophos, *The State of Ransomware, 2022*, https://assets.sophos.com/X24WTUEQ/at/ 4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf
[4] National Bureau of Economic Research, *Economic and Financial Consequences of Corporate Cyberattacks*, 2. Juni 2018, https://www.nber.org/digest/jun18/economic-and-financial-consequences-corporate-cyberattacks
[5] Allianz, *Risikobarometer 2022*, 18. Januar 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Die Auswirkungen der geopolitisch veränderten Bedrohungslandschaft spiegeln sich ebenso in der Schweiz wider: Der Nachrichtendienst des Bundes (NDB) berichtete, dass Hacker:innen aus dem Ausland wahrscheinlich Schweizer Server für die Orchestrierung von Cyberangriffen verwendet haben, um Wahlen in anderen westlichen Ländern zu beeinflussen.[6] Auch hier sind Rufschäden zu befürchten, ebenso der Verlust eigener strategischer Einflussmöglichkeiten.

Gleichwohl sind viele Schweizer Unternehmen noch immer nicht ausreichend ausgerüstet, um Schwachstellen in ihren Systemen und Abläufen zu adressieren und damit verbundene Risiken zu beseitigen. Das NCSC berichtete im November 2022[7] von knapp 3000 Unternehmen, die seit zwei Monaten bekannte Sicherheitslücken in ihren IT-Systemen immer noch nicht geschlossen hatten. Die FINMA weist daneben darauf hin, dass rund ein Viertel der angegriffenen Institute indirekt über einen Dienstleister attackiert wurde.

Für die nachfolgend dargestellte Studie wurden **5935 Meldungen zu Cybervorfällen, die Schweizer Unternehmen und Behörden zwischen dem ersten Quartal 2021 und dem zweiten Quartal 2022 betrafen,** ausgewertet. Die Daten wurden von Mastercard mit der Cyber Quant Lösung generiert. Ihr Hauptziel ist ein datengestützter Einblick insbesondere in die Sicherheitslage der Schweizer Finanzdienstleister inmitten der aktuellen Bedrohungslandschaft.

Neben ausgewählten Ergebnissen und Bewertungen enthält sie auch eine Typologie der wichtigsten Bedrohungsakteur:innen, ihrer Motive, Ziele und Angriffsmethoden. Den Abschluss bilden das Ergebnis einer Mastercard-Umfrage unter Schweizer Kartenherausgebern sowie Empfehlungen zur Risikominderung.

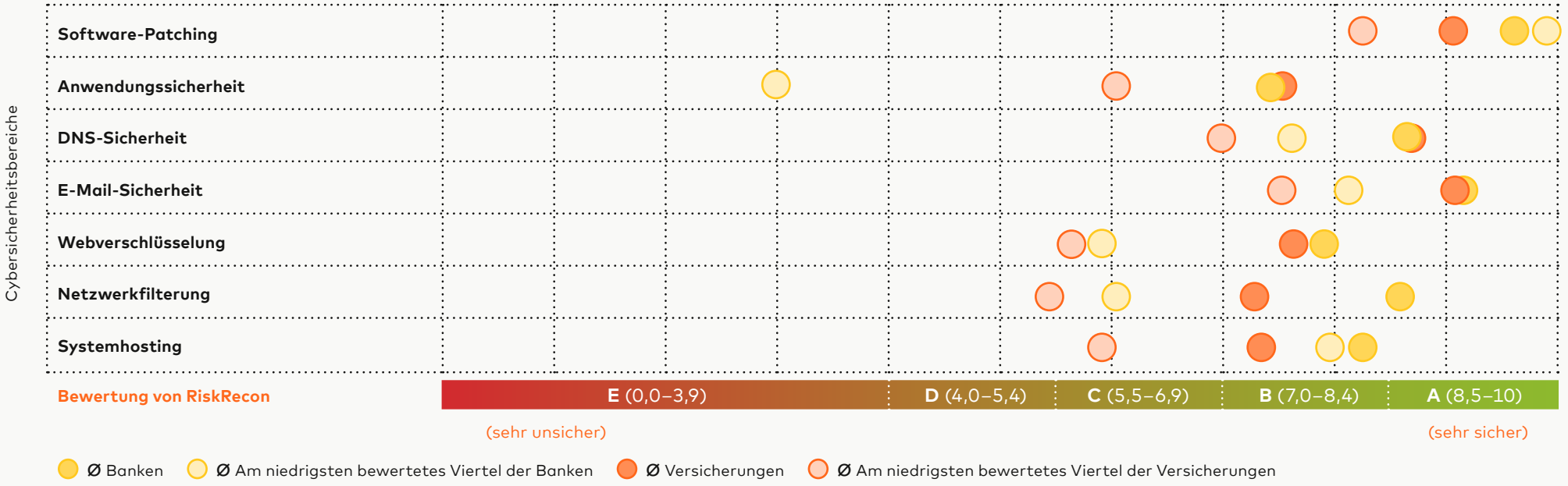
[6] NZZ, 28. August 2022, https://www.nzz.ch/schweiz/wie-aktiv-agitiert-der-kreml-von-der-schweiz-aus-ld.1700064
[7] Nationales Zentrum für Cybersicherheit, *Erneut über 2'800 verwundbare Microsoft Exchange Server in der Schweiz («ProxyNotShell»)*, 18. November 2022, https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/schwachstelle-proxynotshell.html

# 3. Cyberrisiken im Schweizer Finanzsektor

**Mit RiskRecon bietet Mastercard eine Lösung an, um automatisiert den Reifegrad von Domains (Ausprägung von Sicherheitsmerkmalen) zu bewerten.** Sie scannt öffentlich zugängliche Inhalte unter der Domain einer Organisation und bewertet sie nach Sicherheitsaspekten. Diese Lösung wurde eingesetzt, um die Sicherheitslage im Schweizer Finanzsektor zu bewerten und häufige Schwachstellen zu identifizieren.

Die Ergebnisse zeigen, dass der Grad der Cybersicherheit zwischen den analysierten Unternehmen erheblich variiert (Abb. 1, unten). **Im Durchschnitt erhielten sie 8,5 Punkte auf einer Skala von 0 bis maximal 10, was der Höchstnote A entspricht.** Etwa 54 Prozent der Unternehmen erhielten die höchste Bewertung A (8,5 bis 10 Punkte). Sieben Prozent erreichten dagegen nur die Bewertung C (5,5 bis 6,9 Punkte) wegen wesentlichen Sicherheitslücken in mehreren untersuchten Bereichen.

**Abbildung 1: Ausprägung von Sicherheitsmerkmalen nach Bereich und Finanzsektor**



Wie die vorstehende Grafik (Abb. 1, S. 6) zeigt, erzielten die Schweizer Finanzdienstleister **die niedrigsten Bewertungen in den Bereichen Anwendungssicherheit (7,4 Punkte), Webverschlüsselung (7,8 Punkte), Systemhosting (7,9 Punkte) und Netzwerkfilterung (8,0 Punkte).** Entsprechend stellen diese Bereiche ihre grössten sicherheitsbezogenen Herausforderungen dar. Versicherungen erreichten dabei ähnliche Bewertungen wie Banken. Die grössten Unterschiede zeigten sich bei Netzwerkfilterung, Software-Patching und Webverschlüsselung.

**20 %**

der analysierten Schweizer Unternehmen haben mindestens ein System mit ungepatchten Webanwendungen, die eine grosse oder kritische Schwachstelle darstellen.

Im Bereich Software-Patching (siehe entsprechende Kategorie in Abbildung 1) zeigte sich, dass **20 Prozent der analysierten Unternehmen auf mindestens einem System ungepatchte Versionen von Anwendungsservern ausführten,** die als grosse oder sogar kritische Schwachstellen eingestuft wurden. Häufig liefen Webanwendungen zum Beispiel auf älteren Versionen von PHP 5 oder niedriger, die keine Updates zur Behebung von Schwachstellen mehr erhalten. Damit bieten sie Bedrohungsakteur:innen einen leicht zugänglichen Einstiegspunkt.

In den meisten Fällen bezogen sich die ungepatchten Anwendungen auf Subdomains mit Inhalten von vergleichsweise geringerer Bedeutung. Die Analyse hat jedoch auch Fälle identifiziert, in denen primäre Domains betroffen waren. Schweizer Finanzdienstleister sollten ihre Webserver daher aktiv nach nicht gepatchten Schwachstellen durchsuchen, um die potenzielle Verbreitung von Schadsoftware und Reputationsrisiken zu reduzieren.

**30 %**

der analysierten Schweizer Unternehmen verwenden Content-Management-System (CMS)-Schnittstellen, die eine grosse oder kritische Schwachstelle aufweisen.

**30 Prozent der untersuchten Unternehmen zeigten im Bereich Anwendungssicherheit** (siehe entsprechende Kategorie in der Abbildung 1) grosse oder kritische Probleme, die sich auf Schnittstellen des **Content-Management-Systems (CMS)** zurückführen liessen. Meist waren sie von jedem Gerät aus zugänglich und erforderten nur einen Benutzernamen und ein Passwort zur Authentifizierung ohne weitere Schutzmassnahmen.

Cyberkriminelle können hier potenziell mit einfachen Methoden wie Brute-Force-Angriffen (Ausprobieren von Kombinationen aus möglichen Nutzernamen und Passwörtern) zugreifen. Während die betroffenen Webanwendungen oftmals Inhalte von relativ geringer Bedeutung umfassten, hätte in einem Fall die offizielle Webseite mit den Geschäftsberichten des Unternehmens unbefugt geöffnet und bearbeitet werden können. CMS sind besonders bei kleineren Banken beliebt, die daher im Bereich Anwendungssicherheit im niedrigen unteren Quartil bewertet wurden.

**46 %**

der analysierten Unternehmen nutzen unsichere Netzwerkdienste wie zum Beispiel MySQL, die eine hohe oder kritische Schwachstelle darstellen.

Schliesslich zeigten **46 Prozent der analysierten Finanzdienstleister** grosse oder kritische Schwachstellen im **Netzwerkfilterbereich** (siehe entsprechende Kategorie in der Abbildung 1), vor allem **unsichere Netzwerkdienste.** Dabei handelte es sich meist um Datenbankserver und Fernzugriffsprotokolle, die als unsicher und unnötig angesehen werden. Sie können Systeme durch Methoden wie das Erraten von Anmeldeinformationen, das Abfangen von Kommunikation und das Ausnutzen von Schwachstellen kompromittieren.

Für alle Finanzdienstleister, die mit kritischen Problemen bei der Netzwerkfilterung konfrontiert waren, wurden unsichere Datenspeicher wie MySQL, PostgreSQL und Samba identifiziert. Sie erhöhen die Angriffsfläche der Organisation, da sie als Webnetzwerk-Ports fungieren, über die mögliche Angreifer zugreifen können. Diese Schwachstelle kann ausgenutzt werden, um sensible Daten abzufangen, etwa über ein Kontaktformular übermittelte Informationen oder Daten von Teilnehmer:innen eines Gewinnspiels.

In Bezug auf die **Webverschlüsselungsdomäne** verwendeten 65 % der untersuchten Unternehmen Zertifikate, die abgelaufen waren oder ungültige Subjekte hatten, was jeweils als mittelschweres Risiko eingestuft wurde. Ungültige Zertifikatssubjekte führen dazu, dass der Browser den Benutzer:innen Sicherheitswarnungen anzeigt, die einen unsicheren Eindruck vermitteln und dem Nutzererlebnis schaden. Abgelaufene Zertifikate hindern Benutzer:innen hingegen daran, die Authentizität der Website einfach zu überprüfen. Die Zertifikate zur Verschlüsselung sollten daher fortlaufend aktuell gehalten bzw. bei Bedarf ersetzt werden.

Im Bereich **Systemhosting-Domain** nutzten 49 Prozent der analysierten Finanzdienstleister zumindest für einen Teil ihrer Domains gemeinsame IP-Adressen. Das stellt ein mittleres Sicherheitsproblem dar. Gemeinsam genutzte IP-Adressen sind schwieriger zu verteidigen, da die Kontrolloptionen auf Netzwerkebene begrenzt sind, etwa zur IP-Adressfilterung und Angriffserkennung. Darüber hinaus besteht nach einem Cybervorfall das Risiko, dass wegen der geteilten IP-Adresse auch eigentlich nicht betroffene Domains mitgeblockt werden. Durch die Verwendung dedizierter IP-Adressen kann ein Unternehmen die Reputation seines Systems besser kontrollieren und Sicherheitskontrollen auf Netzwerkebene effektiver betreiben.

Schliesslich wurde im Bereich **DNS-Sicherheit** bei 41 Prozent der Unternehmen mindestens eine Domain identifiziert, die nicht über grundlegende Konfigurationen verfügt, um Domain-Hijacking zu verhindern. Ohne geeignete Konfigurationen können Cyberkriminelle unberechtigt die Kontrolle über diese Domain erlangen. Vorbeugend können Unternehmen die Option «clientTransferProhibited» aktivieren. Sie weist den Domain-Registrar an, eine starke Authentifizierung aller Protagonist:innen durchzuführen, die versuchen, die Domain zu verändern, und hilft, nicht autorisierte Änderungen der Konfiguration zu verhindern.

# 4. Die Schweiz und ihr Bedrohungsraum

Die Datenauswertungen von Mastercard Cyber Quant für diese Studie zeigen, dass sich **93 Prozent der Cyberangriffe in der Schweiz auf drei Hauptbedrohungsakteur:innen** zurückführen lassen: Finanzhacker:innen, politisch motivierte Cyberkriminelle und politische Aktivist:innen. Sie lassen sich nach ihren Hauptmotiven, Methoden und Zielen unterscheiden, wie unten dargestellt (Abb. 2).

So nutzen Finanzhacker:innen vor allem Ransomware, Malware und Phishing, um Regierungseinrichtungen, Software- und Finanzdienstleister anzugreifen und monetarisierbare Informationen zu erbeuten.

Politisch motivierte Cyberkriminelle setzen dagegen auf Malware, Command-and-Control Server (C&C, Infizieren und Nutzen fremder Rechner für Angriffe) sowie Lieferketten-Angriffe. Ihre bevorzugten Ziele sind Regierungseinrichtungen, Software-Unternehmen und Infrastrukturbetreiber, um geistiges Eigentum und Geschäftsinformationen zu erlangen. Mastercard Cyber Quant analysiert automatisch **tausende relevanter Quellen einschliesslich Medienberichten, Deep Web (Firmendatenbanken, Streaming-Server und Online-Speicher) sowie das Darknet (anonyme, verschlüsselte und oft kriminelle Foren und Marktplätze).** Die resultierenden Daten spiegeln die Anzahl der Berichte über Cyberereignisse wider, nicht die Anzahl der zugrunde liegenden Versuche. Dennoch können sie als verlässliche Annäherung an die Angriffshäufigkeit angesehen werden.

Auch wenn für die Studie explizit Schweizer Finanzdienstleister untersucht wurden, ist Cybersicherheit eine globale Herausforderung, denn der grösste Teil der Cyberangriffe hat seinen Ursprung im Ausland.

**Abbildung 2: Charakterisierung der wichtigsten Bedrohungsakteur:innen**

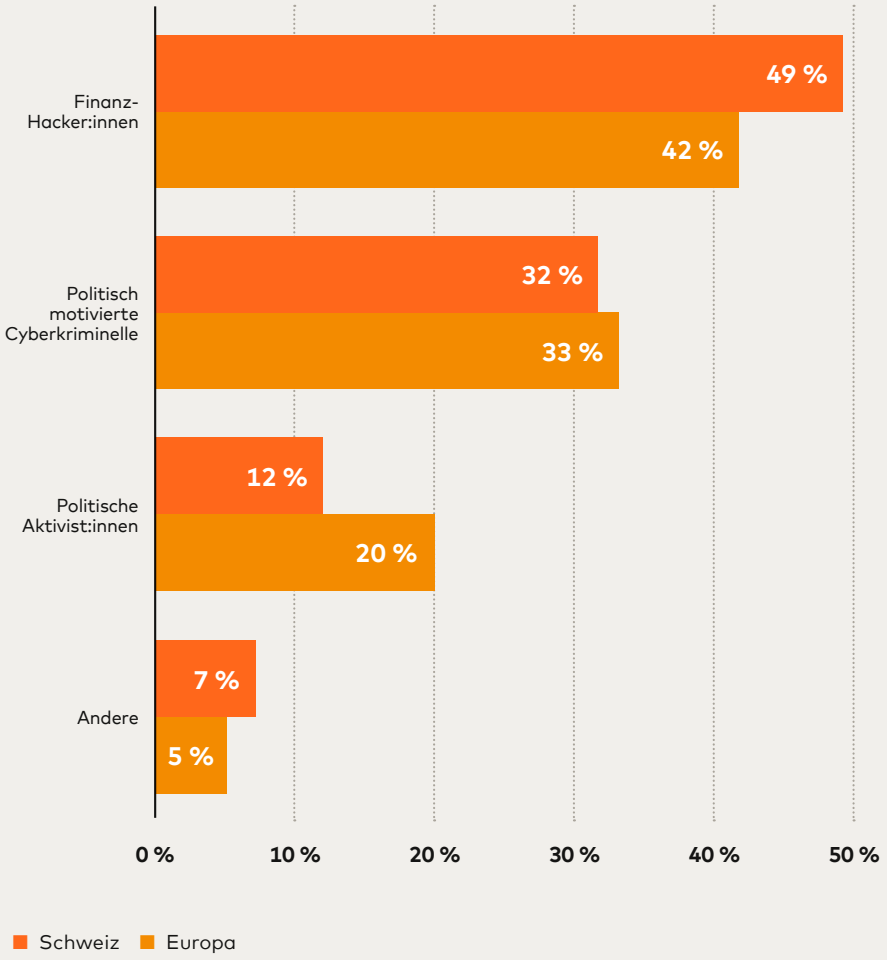
| | Bedrohungsakteur:innen | Zugrunde liegendes Motiv | Charakteristische Angriffstypen | Betroffene Branchen | Betroffene Informationen |
|---|---|---|---|---|---|
|  | **Finanzhacker:innen** | Finanziell | Ransomware, Malware, Phishing | Regierung, Software, Finanzdienstleistungen | Monetarisierbare Informationen (z. B. Zugangsdaten) |
|  | **Politisch motivierte Cyberkriminelle** | Politisch | Malware, C&C, Lieferketten-Angriff | Regierung, Software, Infrastruktur | Geistiges Eigentum, Geschäftsinformationen |
|  | **Politische Aktivist:innen** | Ideologisch | (D)DoS | Regierung, Medien, Finanzdienstleistungen | Erbrachte Dienstleistungen, vertrauliche Informationen |

**Finanzhacker:innen haben in der Schweiz mit 49 Prozent den grössten Anteil an Cybervorfällen** (siehe Abb. 3), was der besonderen Rolle des Finanzplatzes zuzuschreiben ist. In Gesamteuropa liegt er bei 42 Prozent. Politisch motivierte Cyberkriminelle stellen in der Schweiz mit 32 Prozent den zweitgrössten Anteil, der europaweit mit 33 Prozent ähnlich hoch liegt. An dritter Stelle stehen mit 12 Prozent politische Aktivist:innen.

7 Prozent der Bedrohungsakteur:innen (Europa: 5 Prozent) lassen sich keiner dieser drei Gruppen zuordnen. Hierbei handelt es sich vor allem um klassische Betrüger:innen (Schweiz: 5 Prozent, Europa: 3 Prozent). Sie sind finanziell motiviert, nutzen aber deutlich einfachere Methoden als Finanzhacker:innen, etwa das Abgreifen von Kreditkartendaten durch Phishing mit anschliessender Nutzung für eigene Käufe.

Ein Prozent der Cybervorfälle in der Schweiz und Europa lassen sich Mitarbeiter:innen zuordnen, die ihren rechtmässigen Zugang zu internen Systemen ausnutzen, was besonders schwer zu erkennen ist. Jeweils unter 0,5 Prozent liegen in der Schweiz und Europa Täter:innen, die aus Sensationslust und Nervenkitzel angreifen, sowie Industriespion:innen, die Wettbewerber ausforschen.

**Abbildung 3: Arten von Bedrohungsakteur:innen**

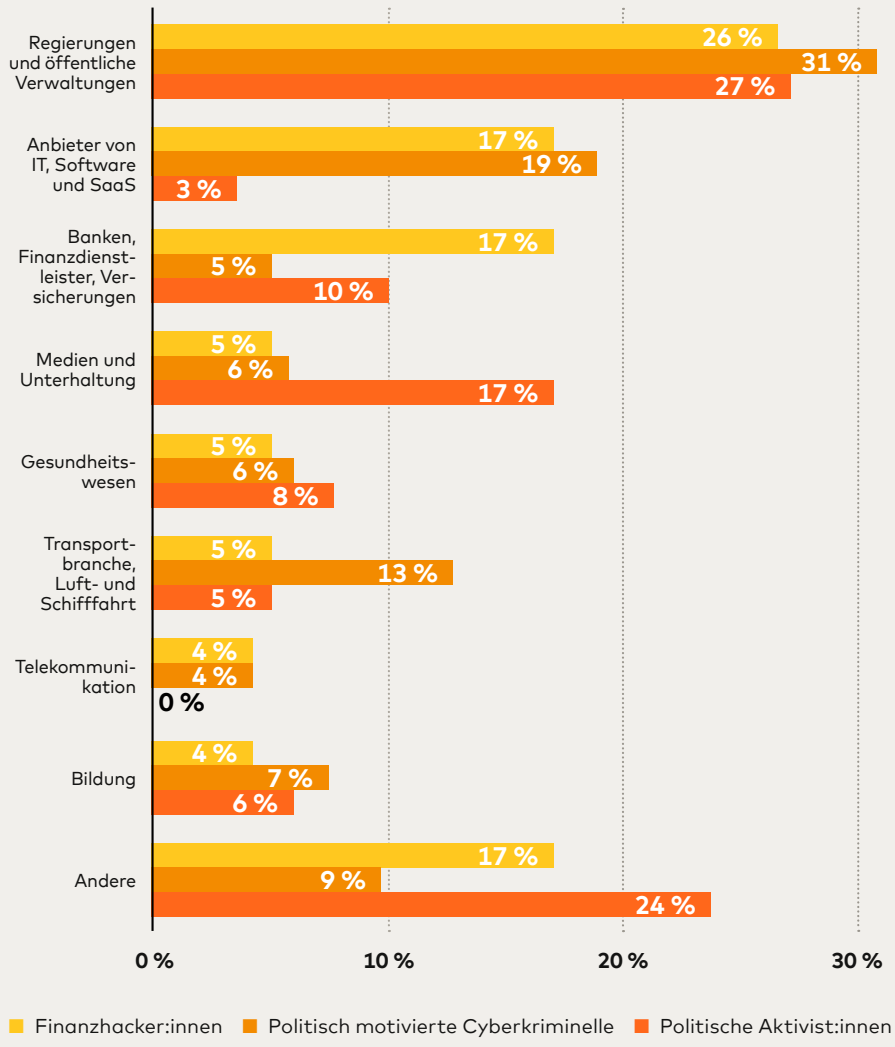


Aufgrund der relativ geringen Angriffshäufigkeit – und weil entsprechend nur wenige Daten über sie vorliegen – geht diese Studie nicht auf diese kleinsten Gruppen von Bedrohungsakteur:innen ein. Unternehmen und Verwaltungen sind jedoch dazu angehalten, sie bei ihrer Risikoabschätzung und -vorsorge gleichwohl zu berücksichtigen, da sie potenziell ebenso grosse Schäden anrichten können.

### Finanzhacker:innen

**Knapp die Hälfte der Cybereregnisse in der Schweiz werden von Finanzhacker:innen** verursacht, die vor allem finanziell motiviert sind. Entsprechend sind **Finanzdienstleister,** insbesondere **Banken** aber auch Kartenherausgeber und Versicherungen, mit 17 Prozent der Angriffe (siehe Abb. 4) ihr bevorzugtes Ziel. Üblicherweise versuchen sie, sensible Informationen zu stehlen und zu monetarisieren. In jüngerer Zeit wurden ihre Methoden immer ausgefeilter und bewegten sich in Richtung Ransomware-Angriffe (40 Prozent der Angriffe; siehe Abb. 5, Seite 12). Bei dieser Methode werden wichtige Daten von Dritten unbefugt verschlüsselt und die Eigentümer:innen dazu erpresst, für die Wiederherstellung ihres Zugriff zu bezahlen. Cyberangriffe durch Finanzhacker:innen sind eine Bedrohung für **alle Branchen und gefährden betriebliche Prozesse in höchstem Grad.**

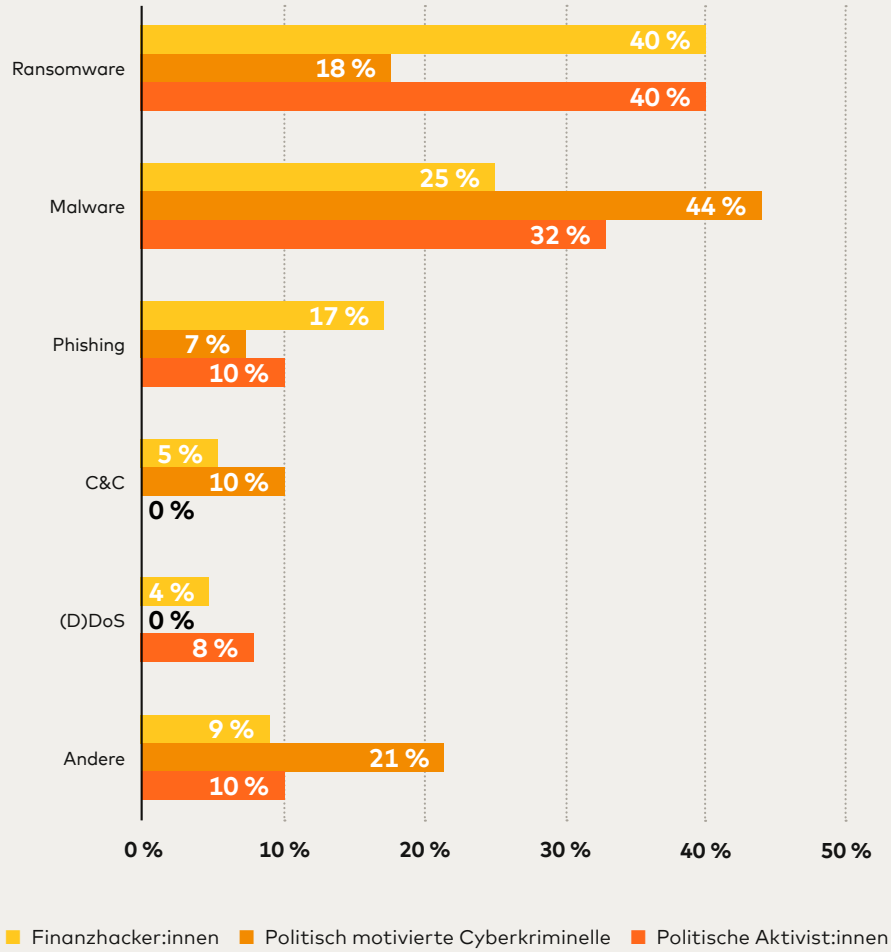
**Abbildung 4: Hauptangriffsziele nach Akteur:innen**



### Politisch motivierte Cyberkriminelle

Die zweitaktivsten Bedrohungsakteur:innen in der Schweiz sind **politisch motivierte Cyberkriminelle,** die rund ein Drittel aller Vorfälle ausmachen. Ihre Motive sind **politischer Natur,** hängen aber im Konkreten von ihrer **staatlichen Zugehörigkeit oder Förderung ab.** Sie sind meist Industrie- oder Nationalstaatspion:innen, die auf staatliche Institutionen und strategisch wichtige Branchen abzielen, etwa Unternehmen in den Bereichen **Transport, Luft- und Schifffahrt, Bildung, Medien und Unterhaltung** sowie **Gesundheitswesen** (siehe Abb. 4, Seite 11). Die bevorzugten Angriffsmethoden dieser Gruppen – Malware, Command & Control (C&C) und Lieferketten-Angriffe (siehe Abb. 5) – sind **deutlich komplexer als bei Finanzhacker:innen** und entsprechend schwieriger zu erkennen.

**Abbildung 5: Bevorzugte Angriffsmethoden nach Akteur:innen**




### Politische Aktivist:innen

Die drittaktivste Gruppe von Bedrohungsakteur:innen in der Schweiz stellen **politische Aktivist:innen (oft als Hacktivist:innen** bezeichnet). Sie sind durch ihre ausgeprägt **ideologischen, politischen oder sozialen Motive** gekennzeichnet. Politische Aktivist:innen sind Einzelpersonen oder dezentrale Gruppen, die ihre Botschaften häufig durch blockierte Zugänge zu wichtigen Websites wie Nachrichtenseiten öffentlich verbreiten wollen. Entsprechend wählen sie ihre Ziele aufgrund ihrer politischen Ansichten, Ideologie oder ihres Geschäftsmodells und handeln eher opportunistisch nach aktueller Lage.

## Angriffsmethoden

Die dargestellten drei Gruppen von Bedrohungsakteur:innen verwenden **eine Vielzahl von Angriffsmethoden,** ausgewählt nach Gelegenheit, Motiv und Ziel. Ransomware (Erpressungstrojaner) und Malware (Schadenssoftware) gehören dabei insgesamt zu den bevorzugten Methoden. Doch auch hier zeigen sich typische Unterschiede innerhalb der Bedrohungsakteur:innen.

**Ransomware**

**Ransomware** wird hauptsächlich von Finanzhacker:innen verwendet, um wichtige Systeme oder Daten zu attackieren und so den Eigentümer:innen den Zugriff zu verwehren. Von den auf diese Art erpressten Unternehmen fordern sie ein meist beträchtliches Lösegeld für die Entschlüsselung. Zunehmend wenden sie eine **Strategie der doppelten Erpressung** an, indem sie zusätzlich damit drohen, vertrauliche Daten zu veröffentlichen, falls das Unternehmen nicht zur Zahlung bereit ist. Ciphertrace, ein Unternehmen von Mastercard, stellte fest, dass Ransomware-Angriffe mit doppelter Erpressung von 2020 bis 2021 um fast das Fünffache zugenommen haben.[8]

Ransomware kann jede Organisation treffen, da Angreifer sie **unabhängig von Grösse oder Branche anwenden können, sobald sie sich** einen Zugang zu deren Netzwerken verschafft haben und davon ausgehen, dass die Organisation ausreichend finanzstark für ein Lösegeld ist.

Gemäss einer Analyse des Financial Crimes Enforcement Network (FinCEN) des amerikanischen Finanzministeriums wurde in den USA allein im ersten Halbjahr 2021 **Lösegeld in Höhe von insgesamt 590 Millionen US-Dollar** im Zusammenhang mit Ransomware gezahlt.[9] Nach der Rückverfolgung von Kryptowährungstransfers kam Chainanalysis zum Schluss, dass mehr als 70 Prozent der Lösegeldzahlungen ausländischen Bedrohungsakteur:innen zugeschrieben werden können. Diese Einnahmen werden Berichten zufolge von den beteiligten Finanzhacker:innen genutzt, um komplexere und professioneller organisierte «Geschäftsmodelle» wie **Ransomware as a Service** (analog zu SaaS) zu betreiben, die es auch weniger spezialisierten Angreifer:innen ermöglichen, Ransomware zu verbreiten.[10] Darüber hinaus führen sie geschäftsähnliche Operationen durch, einschliesslich «Kundenservice»-Teams, die professionell mit Opfern interagieren, um Verhandlungen zu beschleunigen und die Glaubwürdigkeit ihrer Absicht zu erhöhen, betroffene Systeme wiederherzustellen.

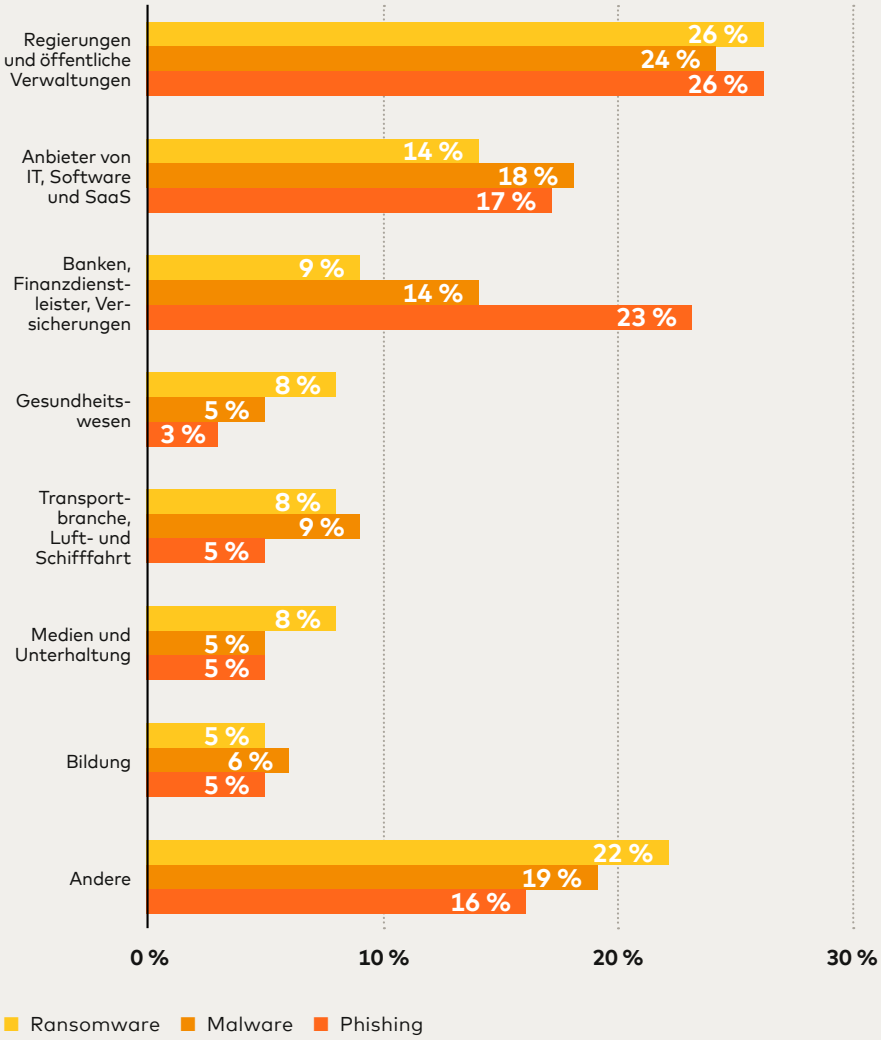
[8] Ciphertrace, *Double extortion ransomware jumped by nearly 500% last year,* 18. April 2022, https://ciphertrace.com/ciphertrace-report-double-extortion-ransomware-jumped-by-nearly-500-last-year/
[9] Financial Crimes Enforcement Network, *FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021,* 1. November 2021, https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly
[10] Microsoft, *Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself,* 9. Mai 2022, https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

**Malware**

Besonders in der Bankenbranche ist **Malware** verbreitet und macht 14 Prozent der gemeldeten Cybervorfälle (siehe Abb. 6) aus. Dies zeigen verschiedene Trojaner, die auf Kund:innen im Finanzsektor angesetzt wurden. Eines der relevantesten Beispiele, das den Schweizer Bankensektor stark beeinflusst hat, ist die Android-Malware **FluBot**. Die Finanzhacker:innen verleiteten die Verbraucher:innen dazu, auf einen betrügerischen Link zu klicken, der per SMS verbreitet wurde und scheinbar Informationen zur Paketverfolgung oder Sprachnachrichten enthielt.

Stattdessen wurden sie dazu verleitet, die betrügerische Anwendung zu installieren. Sie ist in der Lage, die Bankdaten der Benutzer:innen einschliesslich Zwei-Faktor-SMS-Nachrichten abzufangen, was den Cyberkriminellen den Zugriff auf das Online-Banking der Kund:in und Transaktionen zum eigenen Vorteil erlaubt. In ähnlicher Weise wurde im Fall von **TeaBot** der Banking-Trojaner hauptsächlich als legitim erscheinende QR-Code-Scanning-App über die offiziellen App-Stores verbreitet.

**Abbildung 6: Hauptangriffsziele nach Angriffsmethode**



# 5. Sicherheitsbewusste Kartenherausgeber

Die Schweizer Kartenherausgeber räumen organisatorischen und technischen Massnahmen für mehr Cybersicherheit schon jetzt hohe Priorität ein. **Mehrheitlich bewerten sie ihre Kontrollen und Sicherheitsprotokolle jährlich und mit eigenen Ressourcen.** Nur wenige lagern dies an externe Anbieter:innen aus. Auch Sicherheitsübungen führen sie meist jährlich durch. Fast alle überwachen **die Cybersicherheitsrisiken ihrer Lieferant:innen** durch **manuelle Bewertungen.** Das ergab eine Mastercard-Umfrage im Juli 2022 unter den Unternehmen.

**Phishing –** der Diebstahl von Benutzerdaten über gefälschte Webseiten, E-Mails oder Kurznachrichten – wurde dabei **als häufigste Angriffsmethode angesehen.** Daher konzentrierten sich die Schulungen von Mitarbeiter:innen darauf und wurden meist quartalsweise durchgeführt. Dies galt bevorzugt für Mitarbeiter:innen mit Kundenkontakt, da Phishing meist auf Kundendaten abzielt. Einige Kartenherausgeber **weiteten diese Schulungen auch auf ausgewählte Lieferant:innen aus,** um indirekte Risiken zu reduzieren.

**Perimetersicherheit,** also die Risikominderung im Bereich zwischen Unternehmensnetz und öffentlichem Netz, **sowie das Identitäts- und Zugriffsmanagement** stellten bei den befragten Unternehmen **die wichtigsten IT-Investitionsbereiche** dar. Bei weitgehend unveränderten IT-Gesamtbudgets im Vergleich zum Vorjahr betrug der **Ausgabenanteil für Cybersicherheit allerdings weniger als zehn Prozent** und blieb mehrheitlich ebenso konstant. Nur eine Minderheit erhöhte die Ausgaben dafür.

Vielerorts wurde die spezialisierte Position eines **Chief Information Security Officers (CISO)** geschaffen, welche allerdings häufig nicht direkt an den CEO berichtet. Die **möglichen finanziellen Auswirkungen von Cybersecurity-Risiken berechneten die meisten Unternehmen,** die sich an der Umfrage beteiligt hatten, und liessen diese regelmässig in Geschäftsentscheide einfliessen.

# 6. Empfehlungen für die Praxis

Das insgesamt ermutigende Sicherheitsbewusstsein berechtigt zu der Hoffnung, dass Schweizer Finanzdienstleister auch zukünftig der Cybersicherheit hohe Relevanz beimessen, um ihre Risiken fortlaufend weiter zu reduzieren. Die **Kombination aus schnell umsetzbaren und langfristigen, komplexen Massnahmen** ermöglicht den konstant notwendigen Fokus auf Cybersicherheit in einem Umfeld, in dem Bedrohungsakteur:innen stetig neue Angriffsmethoden entwickeln.

Dazu gehört, die **Schulung von Mitarbeiter:innen und Lieferant:innen inhaltlich auf die inzwischen häufigsten Sicherheitsrisiken auszurichten,** wie sie diese Studie aufgeführt hat. Bei der Budgetierung empfiehlt es sich, für die Aufwendungen **für Cybersicherheit eine eigene Kostenstelle** einzurichten, damit sie nicht mit anderen IT-Investitionen konkurrieren, die einen leichter greifbaren ROI haben und damit unbewusst bevorzugt werden könnten.

Cyberrisiken in der Lieferkette lassen sich durch **routinemässige Sicherheitskontrollen und Schulungen von Lieferant:innen und Dienstleister:innen** weiter reduzieren. Bei einer grösseren Anzahl von Partner:innen bietet es sich an, die manuelle Sicherheitsbewertung um **zeitsparende automatisierte Bewertungen** zu ergänzen. Nicht zuletzt empfiehlt es sich, Cybersicherheit grundsätzlich als potenzielles Geschäftsrisiko neben den anderen Messgrössen, KPIs und Erfolgsfaktoren in unternehmerische Entscheidungen einzubeziehen.

**Höchste strategische Priorität**

- Cybersicherheit als Stabsstelle dem CEO zuordnen
- Als Investition statt Kostenfaktor bewerten

**Vorbeugen und verteidigen**

- Cybersicherheit fortlaufend weiterentwickeln
- Regelmässige Angriffssimulationen

**Zusammenarbeit**

- Transparenz zur aktuellen Bedrohungslage
- Erfahrungsaustausch innerhalb des Finanzsektors

Organisatorische Massnahmen dafür können sein, den **Chief Information Security Officer als Stabsstelle dem CEO zuzuordnen** und sich gegen eine komplette Auslagerung dieses Bereiches zu entscheiden.

Viele Schwachstellen resultieren aus unzureichend gesicherten Domains und IT-Systemen erworbener Tochtergesellschaften. Es empfiehlt sich daher, dass Unternehmen **vor einer Übernahme eine Cyber-Due-Diligence durchführen und Richtlinien für übernommene Unternehmen einführen** und durchsetzen, die sicherstellen, dass sie dieselben Sicherheitsstandards erfüllen.

Auch wenn die Wahrscheinlichkeit eines Angriffs zunächst gering erscheint, ist es angesichts der hohen Schadensrisiken und -kosten ratsam, es nicht allein bei Sicherheitskontrollen zu belassen. Stattdessen sollten Unternehmen und Verwaltungen erwägen, **zusätzlich gängige Angriffe selbst zu simulieren,** um vorhandene Schwachstellen in den eigenen Systemen und bei Dritten früh erkennen und beseitigen zu können.

Mit dem Verständnis **von Cybersicherheit als Investition –** nicht allein als Kostenfaktor – stellen sich Unternehmen zukunftssicher auf. Verstärkte Zusammenarbeit unter den Schweizer Finanzdienstleistern könnte die Effektivität der individuellen Massnahmen noch einmal erhöhen.

# 7. Lösungen von Mastercard

Mastercard unterstützt Unternehmen dabei, potenzielle Sicherheitsrisiken frühzeitig zu erkennen und fortlaufend zu reduzieren. Dabei hat sich ein zweigleisiger Lösungsansatz entwickelt und in der Praxis bewährt.

**«Outside-in» bewerten die Mastercard-Lösungen die digitalen Netzwerke aktiv auf Schwachstellen, überprüfen alle Transaktionen und schränken Betrug ein. «Inside-out» bewerten und stärken sie die internen Prozesse, Technologien und Praktiken des Unternehmens in Bezug auf dessen Risikoexposition.** Folgende drei Lösungen verhelfen Unternehmen besonders effektiv zu mehr Cybersicherheit und Vertrauenswürdigkeit innerhalb einer digital vernetzten Wirtschaft:

### Cyber Quant («Inside-out»)

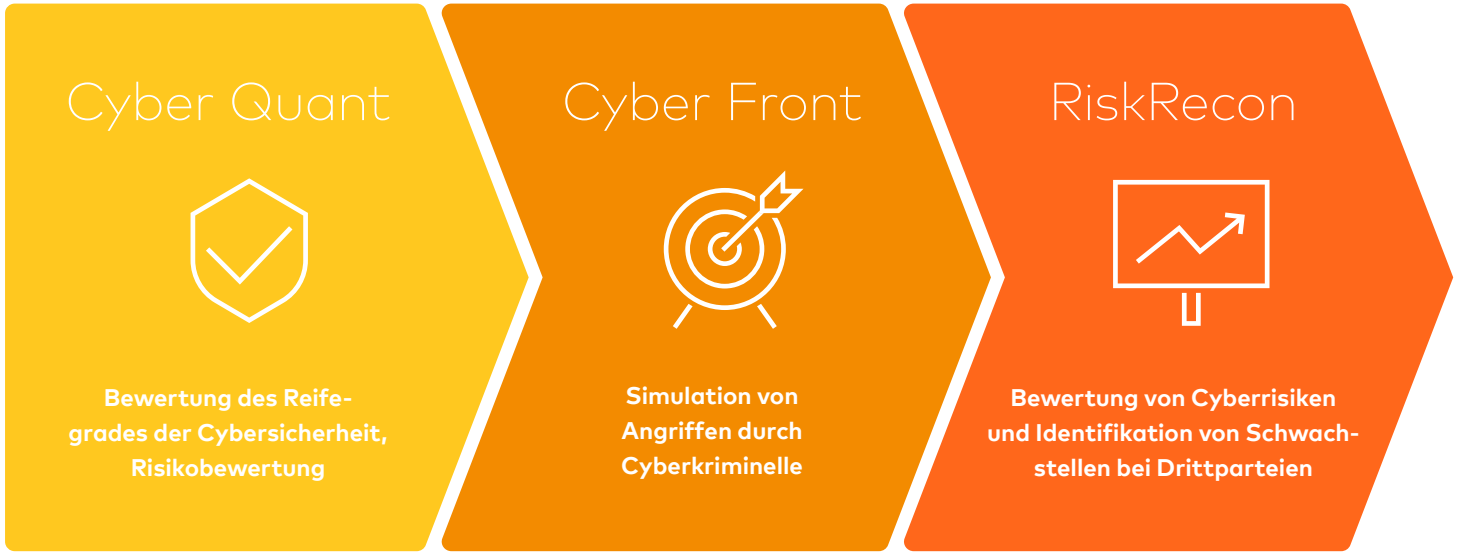
Bei Cyber Quant handelt es sich um eine Lösung zur **Risikobewertung der Sicherheitsprozesse und -praktiken sowie der technologischen Infrastruktur im Unternehmen.** Cyber Quant bewertet die Reifegrade von 50 Arten von Sicherheitsmassnahmen in den Bereichen Infrastruktur, Vorbeugung und Aufdeckung. Diese Lösung hilft Unternehmen dabei, ihre Massnahmen entsprechend ihrer jeweiligen Bedrohungslage auszuwählen und zu priorisieren.

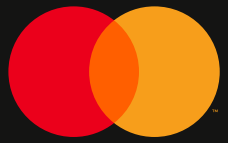
### Cyber Front («Outside-in»)

Cyber Front bewertet, wie widerstandsfähig die Sicherheitsmechanismen einer Organisation sind. Cyber Front **ahmt dafür das Verhalten von organisierten Cyberkriminellen nach,** die auf mehreren Wegen gleichzeitig angreifen. Das Programm bewertet die Wirksamkeit jeder Sicherheitskontrolle, etwa von Firewalls und Angriffserkennungssystemen, und gibt Empfehlungen, um die bestehende Konfiguration noch weiter zu verstärken.

### RiskRecon («Outside-in»)

RiskRecon überwacht automatisiert und dadurch personal- und zeitsparend die Cyberumgebung jedes Unternehmens mit einer Online-Präsenz, um Cyberrisiken und Schwachstellen zu identifizieren, bevor sie ausgenutzt werden können. Durch die **fortlaufende, effektive Bewertung von Risiken durch Dritte** minimieren Unternehmen ihr Risiko, das Opfer von indirekten Cyberangriffen über externe Geschäftspartner zu werden, noch einmal.





Mastercard | Löwenstrasse 25 | 8001 Zürich
media-zuerich@mastercard.com | www.mastercard.ch