Deutsch

CYBER SECURITY

Report 2020

Grusswort

Liebe Leserin, lieber Leser,

es sind aussergewöhnliche Zeiten. Niemand von uns hat je etwas Vergleichbares wie die Corona-Pandemie erlebt und es bleibt ungewiss, wann wieder Normalität einkehren wird. Das Jahr 2020 bringt bisher wenige Lichtblicke. Doch die Krise hat zumindest eine positive Seite: Unternehmen, Verwaltungen und Bildungsstätten erleben derzeit einen enormen Digitalisierungsschub, wie man ihn noch im Januar kaum für möglich gehalten hätte.

Homeoffice, Videokonferenzlösungen und die Cloud bringen aber auch Herausforderungen mit sich, gerade für Finanzinstitutionen. Die Eidgenössische Finanzmarktaufsicht (FINMA) spricht von einer «stark gestiegenen» Anzahl von Phishing-Angriffen während der Pandemie und ergänzt: «Die Cyberkriminellen sind kreativ und rücksichtslos. Sie nutzen die aktuelle Krise, um ihre Attacken zu verfeinern.

Was ist zu tun, um dies zu verhindern? Darauf gibt es eine einfache Antwort: Wir brauchen in der Finanzbranche mehr Zusammenhalt und mehr Kooperation. Die Cyberabwehr funktioniert am besten im globalen Verbund von Banken, Versicherungen, FinTechs, InsurTechs, RegTechs sowie Politik und Wissenschaft – und wenn alle an einem Strang ziehen.

Der jährliche SIX Cyber Security Report soll den Wissensstand in der Community erhöhen. Für die vorliegende Ausgabe konnten wir einen breiten Kreis an Autoren und Interviewpartnern gewinnen. Vertreten sind die Geschäftsseite mit Alain Beuchat, einem der renommiertesten Sicherheitsspezialisten der Schweiz, die Politik mit Florian Schütz, dem Delegierten des Bundes für Cybersicherheit, und die Wissenschaft mit der ETH Zürich. Ein weiteres Novum dieser Ausgabe: Erstmals wagen wir einen Blick nach vorne und versuchen, die Bedrohungslage und die Abwehr von morgen zu antizipieren.

Zuletzt möchte ich auf unseren SIX Cyber Security Hub hinweisen. 2018 gründeten wir diesen Hub als Austauschplattform für Sicherheitsexperten. Innert kürzester Zeit hat er sich als zentraler Ort für den Informations- und Erfahrungsaustausch zum Thema Cyber Security im Finanzsektor etabliert. Für den vorliegenden Report haben wir eine Umfrage mit über 90 Mitgliedern durchgeführt, die Ergebnisse zusammengetragen und analysiert.

Ich wünsche Ihnen eine spannende Lektüre.

Jos Dijsselhof
CEO SIX

Inhaltsverzeichnis

6 **Zusammenfassung**
8 Warum dieser Report
10 Mitwirkende
11 Methodik
12 Interview

16 **Makroanalyse: Vergleich der Länder**
20 Grossbritannien
21 USA
23 Frankreich
25 Singapur
26 Spanien
27 Niederlande
28 Deutschland
30 Schweiz

32 **Mikroanalyse**
33 Zentrale Erkenntnisse
34 Zusammenfassung der Ergebnisse
36 Analyse möglicher Ursachen für die niedrige Beobachtungsrate von Cybervorfällen bei Schweizer Finanzinstitutionen
36 Beobachtete Vorfälle
38 COVID-19: Beschleunigung von Veränderungsprozessen und Intensivierung bestehender Herausforderungen
40 Künftige Herausforderungen identifizieren
41 Struktur von CISO-Tätigkeiten
43 Zusammenfassung

44 **Angewandte Forschung – SCION**
46 SCION und der Schweizer Finanzsektor
46 Entstehungsgeschichte und Motivation für SCION
47 Technischer Hintergrund von SCION
49 Fazit

50 **SIX Cyber Security Hub**

Zusammenfassung

Dieser Report bietet Einblicke in die im Schweizer Finanzsektor beobachteten Cyberbedrohungen.

Wie im Vorjahr untersucht der Bericht die Cyber-Security-Lage aus zwei verschiedenen Blickwinkeln. Zunächst vergleicht er, wie die Finanzsektoren ausgewählter Länder von Sicherheitsbedrohungen betroffen sind. Anschliessend bietet er eine Perspektive aus Sicht des Schweizer Finanzsektors auf die derzeit wichtigsten Cyber-Security-Themen. Darüber hinaus diskutiert der Bericht eine neue Technologie, die das Potenzial hat, Schweizer Finanzinstitutionen in Zukunft eine Nutzung der Internetkonnektivität mit mehr Sicherheit und verbesserter Widerstandsfähigkeit zu ermöglichen.

Der erste Teil des Berichts, die Makroanalyse, basiert in erster Linie auf der Auswertung von Open-Source-Quellen. Der zweite Teil, die Mikroanalyse, beruht weitgehend auf Informationen, die von Mitgliedern des SIX Cyber Security Hub bereitgestellt wurden. Der letzte Teil ist das Ergebnis einer Zusammenarbeit zwischen der ETH Zürich und SIX.

Betrachtet man die Cyberangriffe auf die Finanzsektoren in der Schweiz und anderen Ländern im vergangenen Jahr, so sind Finanzinstitutionen weiterhin häufigen Attacken ausgesetzt. Insgesamt ist die Zahl der beobachteten Vorfälle in jedem Land auf dem Niveau des Vorjahres geblieben. Ein wesentlicher Unterschied ergibt sich aber durch einen deutlichen Anstieg der Cyberangriffe um den Monat März, der mit dem Ausbruch der COVID-19-Pandemie zusammenhängt. Wie im Vorjahresbericht verzeichneten die USA mit Abstand die meisten Angriffe auf den Finanzsektor, gefolgt von Grossbritannien. Die global am häufigsten beobachtete Art der Bedrohung war Ransomware, gefolgt von Phishing-Angriffen.

Mit einem Fokus auf dem Schweizer Finanzsektor untersucht dieser Report zunächst die Struktur von Sicherheitsvorfällen anhand von Informationen, die von betroffenen Unternehmen beigetragen wurden. Dabei liegt ein besonderer Schwerpunkt auf den Auswirkungen der COVID-19-Pandemie. Phishing und an zweiter Stelle Ransomware waren die von Schweizer Institutionen am meisten wahrgenommenen Bedrohungen. Das deckt sich mit der Beobachtung, dass Akteure E-Mails als Hauptangriffsvektor auf Finanzinstitutionen nutzen. Daneben liess sich ein deutlicher Anstieg der Angriffsaktivität in Korrelation mit der COVID-19-Pandemie verzeichnen. Der Report analysiert, wie CISO-Tätigkeiten innerhalb des Sektors strukturiert sind, und gibt Einblicke in die verfügbaren Ressourcen sowie deren Verwendung. Es zeigt sich ein Zusammenhang zwischen der Transparenz und der Anzahl der beobachteten Vorfälle innerhalb eines Unternehmens: Eine höhere Transparenz korreliert mit einer grösseren Anzahl registrierter Vorfälle.

Anschliessend verlagert der Bericht seinen Fokus weg von Cyberangriffen und stellt eine neue Netzwerktechnologie vor, die aus Forschungsbemühungen hervorgegangen ist und einige Mängel des heutigen Internets beheben will. Diese neue Technologie befasst sich damit, wie Daten im Internet transportiert werden. Ihre Eigenschaften machen sie für den Einsatz im Finanzumfeld interessant. Sie stellt sicher, dass bestimmte übertragene Daten die Schweiz nicht verlassen. Derzeit evaluiert eine Gruppe von Finanzinstitutionen in Zusammenarbeit mit SIX diese Technologie weiter, um ihr Potenzial für den Transport von Finanzdaten wie Zahlungsinformationen zu ermitteln.

Dieser Bericht wurde von SIX verfasst und beinhaltet Forschungsergebnisse von QuoIntelligence sowie Daten von Recorded Future.

Die wichtigsten Ergebnisse

- Die Gesamtzahl der beobachteten Angriffe bleibt vergleichbar mit dem im Vorjahresbericht angegebenen Niveau.
- Zu Beginn der COVID-19-Pandemie im März kam es zu einer Zunahme an Cyberangriffen.
- Die häufigsten Angriffsmethoden unterscheiden sich kaum von Land zu Land.
- Der ITU Global Cybersecurity Index der einzelnen Länder korreliert nicht mit der gemeldeten Anzahl der beobachteten Angriffe.
- Der Schweizer Finanzsektor verzeichnet im Vergleich zu anderen Ländern weiterhin eine sehr geringe Anzahl von Cyberangriffen.
- Unabhängig von ihrer Grösse sehen Schweizer Unternehmen den durch die Digitalisierung verursachten raschen Wandel und die damit verbundene Notwendigkeit einer schnellen Anpassung der IT-Architektur als ihre bedeutendsten Cyber-Security-Herausforderungen.
- Schweizer CISOs zeigen sich besorgt darüber, diesen Wandel bewältigen zu können. Sie betonen die Notwendigkeit einer angemessenen Finanzierung ihres Verantwortungsbereichs sowie die Schwierigkeit, qualifizierte Fachkräfte zu halten, die für die Aufrechterhal-tung eines hohen Sicherheitslevels erforderlich sind.
- Nach Angaben verschiedener Schweizer Finanzinstitutionen sind Phishing, Malware und Ransomware die Cyberangriffe, denen Unternehmen am meisten ausgesetzt sind.
- Es besteht ein Zusammenhang zwischen der Anzahl der beobachteten Cybervorfälle und dem Reifegrad sowie der Transparenz der CISO-Tätigkeiten im Schweizer Finanzsektor. CISOs, die Transparenz und Reifegrad höher einstuften, beobachteten auch mehr Vorfälle.

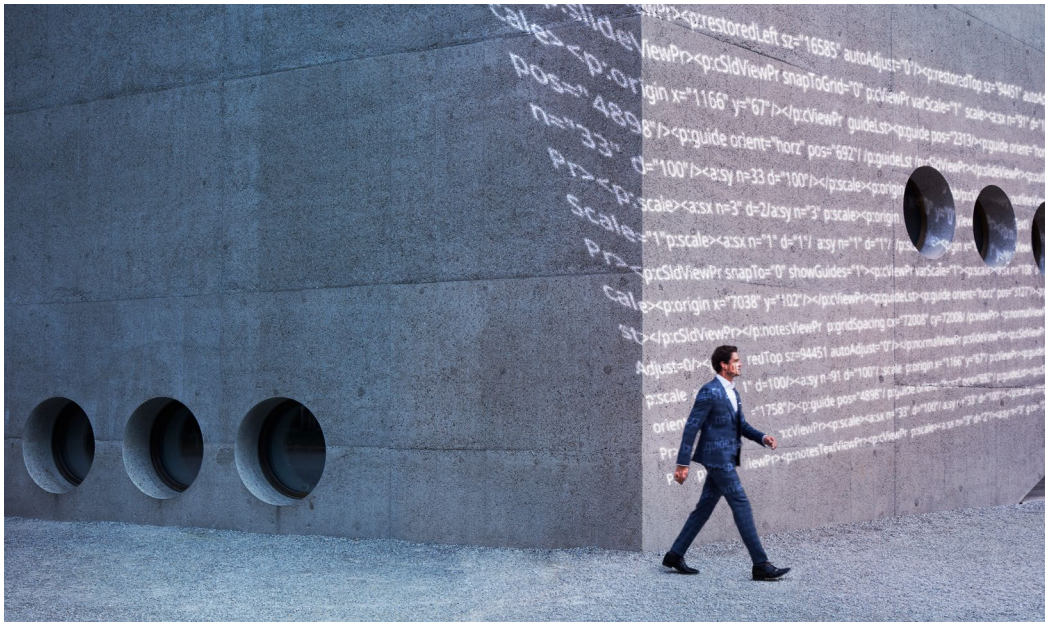
Warum dieser Report

Der vorliegende SIX Cyber Security Report gibt einen Überblick über die aktuelle Sicherheitslage der Schweizer Finanzindustrie und die Cyberbedrohungen, denen sie ausgesetzt ist. Um ein möglichst umfassendes Bild zu zeichnen, wurden Befragungen und Auswertungen durchgeführt sowie Stimmen aus Wirtschaft, Politik und Forschung mit aufgenommen.

In den letzten Jahren ist die Zahl veröffentlichter Reports, Studien und Analysen im Cyber-Security-Bereich deutlich gestiegen. Dementsprechend fällt es der Leserschaft immer schwerer, die Orientierung zu behalten. Der vorliegende Report stellt vor allem die Schweiz und insbesondere den Schweizer Finanzplatz in den Mittelpunkt. Dazu zählen alle hier ansässigen Banken und Versicherungen sowie FinTechs, InsurTechs und RegTechs in der Schweiz.

Der Cyber Security Report von SIX geht dabei einerseits ausführlich auf den Schweizer Finanzplatz ein und analysiert seine spezifische Bedrohungslage. Andererseits schlägt er den grossen Bogen und vergleicht den heimischen Finanzplatz mit anderen Ländern.

Wir glauben, dass eine starke Cyber Security Community die beste Antwort auf gegenwärtige Bedrohungen ist. Um diese zu stärken und weil die Vertreter des Finanzplatzes viel voneinander lernen können, erscheint der SIX Cyber Security Report in einem jährlichen Rhythmus. Besonders die anonymisierten Befragungen unter den über 90 Mitgliedern des SIX Cyber Security Hub geben umfassende und tiefe Einblicke in die Herausforderungen der hiesigen Cyber Security Community.



Einblicke von prominenten Unternehmen, Vertreter aus Politik und Forschung

Dieser Bericht konzentriert sich in erster Linie auf die Schweiz, insbesondere auf den Schweizer Finanzsektor

Die Cyber-Sicherheitsgemeinschaft stärken

Mitwirkende

Der SIX Cyber Security Report bietet eine umfassende und detaillierte Bestandsaufnahme der gegenwärtigen Bedrohungslage in der Schweiz. Er stützt sich auf die Fachkompetenz und die qualifizierte Meinung einer Vielzahl von Experten. SIX versteht sich als zentrales Organ der Branche, das für diesen Report die verschiedenen Akteure des Finanzsektors zusammenbringt und ihre Stimmen konsolidiert.

↪ Folgende Organisationen waren am diesjährigen SIX Cyber Security Report beteiligt:

- SIX betreibt die systemkritische Infrastruktur für den Zahlungsverkehr und für die Schweizer Börse und hat ein weltweit führendes SOC etabliert.
- Recorded Future sammelt globale Open Source Intelligence (OSINT)-Daten, die der Makroanalyse und einem Teil der Mikroanalyse dieses Reports zugrunde liegen.
- Mehr als 90 Mitglieder des SIX Cyber Security Hub nahmen an einer Feldbefragung zur Bedrohungslage in der Schweiz teil. Die Ergebnisse sind anonymisiert in diesem Report publiziert und bilden die Datengrundlage der Mikroanalyse. Zu den Mitgliedern des Hub zählen Banken, Versicherungen, FinTechs, InsurTechs und RegTechs.
- QuoIntelligence verantwortete einen wesentlichen Teil der Erhebung und Auswertung der Daten.
- Die ETH steuerte eine Einschätzung der Bedeutung neuer Technologien (hier SCION) für die bestehende Sicherheitslage bei (Departement Informationstechnologie und Elektrotechnik).

Der Cyber Security Hub von SIX ist eine nicht-kommerzielle Plattform, die den steten Informationsaustausch rund um das Thema Cyber Security sicherstellt. Die Community tauscht hier Erfahrungen, Learnings und Know-how sowie Informationen zu Schwachstellen und Attacken aus.

Wie werde ich Teil des Cyber Security Hub? Zur Teilnahme sind alle Schweizer Banken und Versicherungen eingeladen, die FINMA-reguliert sind. Bei Interesse melden Sie sich bitte bei securityhub@six-group.com.

Methodik

Die Mikro- und Makroanalyse basieren unter anderem auf einer Auswertung strukturiert gesammelter Daten in Zusammenarbeit mit QuoIntelligence. Mit dem Ziel, ein detailliertes Verständnis der aktuellen Bedrohungslage zu gewinnen, wurden die benötigten Rohdaten definiert, gesammelt und analysiert.

Die Makroanalyse untersucht Cyberbedrohungen im Finanzsektor verschiedener G20-Länder und der Schweiz. Die Länder wurden aufgrund ihrer geografischen Nähe zur Schweiz ausgesucht, weil Import/Export-Beziehungen bestehen oder weil ihr Finanzplatz dem hiesigen ähnlich ist. Die Makroanalyse verdeutlicht die Gesamtzahl der Vorkommnisse pro Land und erhebt eine Stimmungslage zu Cyberangriffen, die auf öffentlich geäusserten Meinungen, beispielsweise in Tweets, beruht. Besonderes Augenmerk wurde ausserdem auf die Vergleichbarkeit der Länder gelegt. Die Daten basieren auf OSINT-Informationen; erhoben wurden sie von Recorded Future.

Für die Mikroanalyse des Schweizer Finanzplatzes ordnet dieser Report die Finanzinstitute kleinen, mittleren und grossen Organisationen zu. Die Rohdaten stammen aus einer Befragung unter den über 90 Mitgliedern des SIX Cyber Security Hub. Sie wurden anonymisiert und aggregiert und – wo sinnvoll – durch OSINT-Daten ergänzt.

Angewandte Forschung: Hier geht es um die Fragestellung, welchen Einfluss neue Technologien auf die Bedrohungslandschaft des Schweizer Finanzplatzes haben könnten. Für diesen Report wurde das SCION-Projekt der ETH ausgewählt, das bereits von SIX, Swisscom und anderen Akteuren in der Schweiz genutzt wird. Die Abkürzung steht für «Scalability, Control, and Isolation On Next-Generation Networks» – gemeint ist eine Art neues, sehr sicheres Internet. Es gibt bereits ein erstes globales SCION-Netz, das den Vergleich mit anderen Ländern ermöglicht. Die SCION-Technologie will herkömmliche Internetverbindungen vollständig ersetzen. Dieser Report erörtert, welche Vorteile und Sicherheitsverbesserungen sich durch SCION ergeben – und welche nicht.

Über 90 Mitglieder des SIX-Hub für Cybersicherheit

«Scalability, Control, and Isolation on Next-Generation Networks»

Alain Beuchat,
CISO Lombard Odier

Florian Schütz,
Delegierter des Bundes
für Cybersicherheit

Interview mit Herrn Schütz & Herrn Beuchat

SIX: Herr Schütz, können Sie bitte Ihre Rolle und Ihre Aufgaben beschreiben?

Herr Schütz: Ich bin Delegierter der Schweiz für Cyber Security. Das bedeutet einerseits, dass ich dafür verantwortlich bin, departementsübergreifend alle Cyberaktivitäten der Schweizer Regierung zu koordinieren. In der Schweiz betrifft das Thema Cyber Security vor allem zwei Behörden: das Eidgenössische Departement für Verteidigung und das Bundesamt für Justiz. Für Cyberkriminalität ist vor allem das Bundesamt für Justiz zuständig. Das Eidgenössische Departement für Verteidigung befasst sich mit Cyberabwehr, militärischer Abwehr und nachrichtendienstlichen Aktivitäten. Darüber hinaus ist das Eidgenössische Finanzdepartement, wo ich angestellt bin, in erster Linie verantwortlich für Cyber Security. Andererseits bin ich auch verantwortlich für die Koordination und Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken, die NCS. Dort leite ich den Steuerungsausschuss, der sich aus Vertretern von Wirtschaft, Kantonen, Hochschulen und Regierung zusammensetzt.

SIX: Sie befassen sich also nicht nur mit dem öffentlichen, sondern auch mit dem privaten Sektor. Arbeiten Sie daran, Cyber Security auf nationaler Ebene zu verbessern?

Herr Schütz: Richtig. **Das ist das Mandat der NCS. Unser vorrangiges Ziel ist es, die Schweiz in einer digitalen Welt sicher zu positionieren und dafür zu sorgen, dass wir uns möglichst ungehindert darin bewegen können.**

SIX: Haben Sie in den letzten zwölf Monaten einen Anstieg oder Rückgang bei den Cybervorfällen oder eine Veränderung in deren Komplexität festgestellt?

Herr Beuchat: Über die vergangenen 12 bis 18 Monate hat die Anzahl der Cyberangriffe im Finanzsektor zugenommen. Kriminelle setzten Ransomware ein, um sich erhebliche finanzielle Vorteile zu verschaffen. Zudem sind Angriffe gezielter geworden, denn kriminelle Organisationen nutzen systematisch die neuen Schwachstellen aus, die von spezialisierten Anbietern und Sicherheitsfirmen aufgedeckt werden. Früher konnte es Monate dauern, bis die aktive Ausnutzung von Schwachstellen möglich wurde. Heute geschieht dies bereits innerhalb von wenigen Tagen. **Das Risiko für Unternehmen war im Jahr 2020 besonders hoch, da zahlreiche Schwachstellen von vernetzten Systemen aufgedeckt wurden,** wie etwa Konfigurationsprobleme bei Firewalls. Daher müssen wir sehr agil arbeiten und besser positioniert sein, um uns möglichst schnell verteidigen zu können. Wenn eine Schwachstelle nicht behoben werden kann, weil der erforderliche Patch fehlt, müssen wir in der Lage sein, potenzielle Angriffe zu erkennen, und im schlimmsten Fall den Zugang zu unseren Systemen blockieren, um sie zu schützen.

SIX: Sie würden Ihre Systeme blockieren?

Herr Beuchat: Ja, wenn es keinen anderen Ausweg gibt. Zum Beheben von Schwachstellen müssen wir den entsprechenden Sicherheits-Patch beschaffen, sämtliche Geschäftsfunktionen testen und die Korrekturen auf alle Instanzen anwenden. Das kann Tage dauern, und wenn wir in diesem Zeitraum Angriffe feststellen, müssen wir unter Umständen den Zugang zu den anfälligen Systemen blockieren, da ansonsten das Risiko zu gross wäre.

SIX: Ist Ihrem Vorstand bekannt, dass das Blockieren des externen Zugriffs auf Produktionssysteme eine Möglichkeit darstellt?

Herr Beuchat: Das ist eine gute Frage. **Wir informieren unsere Führungsetage, wenn eine kritische Schwachstelle unsere Systeme gefährdet.** Über unsere Threat-Intelligence-Funktionen überwachen wir die Situation sehr genau und erhalten Warnmeldungen im Fall eines Angriffs. **Wenn das Risiko steigt, entscheiden wir gemeinsam mit den betroffenen Stellen, ob wir den Zugang zu den Systemen blockieren oder nicht.**

Herr Schütz: Aus unserer Sicht steigt die Anzahl von Angriffen durchaus an. Dies gilt für den gesamten Zeitraum seit der Schaffung von MELANI (Melde- und Analysestelle Informationssicherung) vor 15 Jahren. **Eine der Hauptursachen liegt darin, dass die Welt immer stärker digitalisiert wird und kriminelle Aktivitäten sich ins Internet verlagert haben.** Dabei fällt auf, dass Angriffe vor allem bei hohem Gewinnpotenzial ausgereifter werden, also fast immer dort, wo Finanzinstitutionen das Ziel sind. Zugleich werden auch sehr einfache Angriffe häufiger, vor denen man sich mühelos schützen kann. Da aber so viele Unternehmen die Digitalisierung möglichst schnell vorantreiben wollen, ohne sich ausreichend über die potenziellen Gefahren zu informieren, sind sie ein leichtes Ziel für Kriminelle, die aus genau diesem Grund ihr Portfolio diversifizieren. Interessanterweise sehen wir Angreifer immer als Akteure in einem vollständig deregulierten Markt: Ihr Ziel ist ein grösstmöglicher Gewinn, sie müssen keine Regeln befolgen und entwickeln letztlich ihr eigenes Geschäftsmodell. Früher begann die Verschlüsselung bei Ransomware-Angriffen unmittelbar nach dem Eindringen in ein System. Dagegen haben es Cyberkriminelle heute auf das Kernsystem abgesehen, auf die wertvollsten Ressourcen einer Organisation. Zuerst stehlen sie Ihre Daten und erst dann wird die Verschlüsselung angewendet. Wenn eine Zahlung für die Entschlüsselung ausbleibt, werden die Daten veröffentlicht. Dabei wird der Betrag, der von Ihnen verlangt werden kann, sehr genau berechnet. Die Kriminellen investieren daher grosse Summen in immer ausgereiftere Prozesse und in die Weiterentwicklung ihres Geschäftsmodells.

Herr Beuchat: Ich habe vor Kurzem in einem Artikel gelesen, wie solche Geschäftsmodelle funktionieren. In der Regel gibt es Organisationen, die auf das Eindringen in Unternehmen spezialisiert sind, die sogenannten «Initial Access Broker», die Methoden entwickeln, um sich zu einem Unternehmen Zutritt zu verschaffen. Der Zutritt wird aber nicht von ihnen selbst genutzt, sondern an andere kriminelle Vereinigungen verkauft, die diesen dann, wie Herr Schütz schon erwähnt hat, mithilfe von Ransomware ausnutzen.

Herr Beuchat: Ich denke, das ist ein Grund dafür, dass diese Angriffe heute so häufig sind. Der Initial Access Broker identifiziert Schwachstellen, und sobald diese erfolgreich ausgenutzt werden können, verkauft er die Methode beispielsweise an einen Ransomware-Operator. Dieser schleust die Ransomware dann über diese Angriffsmethode in das Zielunternehmen ein.

«Über die vergangenen 12 bis 18 Monate hat die Anzahl der Cyberangriffe im Finanzsektor zugenommen.»

Herr Beuchat

SIX: Das ist ein ganzes Ökosystem.

Herr Beuchat: Genau, wir sprechen immer über Ökosysteme, sind ihnen ausserhalb des Finanzsektors bisher aber eher selten begegnet. Ein Beispiel dafür sind die Netzwerke von «Money Mules», die genutzt werden, um sich das gestohlene Geld aus betrügerischen Transaktionen auszahlen zu lassen. Heutzutage scheinen beispielsweise Ransomware-Angriffe immer ausgereifter zu werden. Das liegt vermutlich daran, dass Ransomware-Angriffe vor einigen Jahren auf Einzelpersonen abzielten und weniger lukrativ waren, vielleicht CHF 300 bis 500. Heute dagegen stehen globale Konzerne im Fokus, und es sind Gewinne in Millionenhöhe möglich.

Herr Schütz: Es ist interessant, wie sehr sich die Dynamik verändert hat. Aus Sicht der Regierung ist vor allem der wachsende Markt für Cyberversicherungen beunruhigend. In den USA beispielsweise haben einige Cyberversicherer entschieden, dass es günstiger ist, bei Ransomware- und Cyberangriffen zu zahlen, als später für die Wiederherstellung aufzukommen. Dieses Vorgehen signalisiert den Bedrohungsakteuren, dass ihr Geschäftsmodell funktioniert. Angesichts dieser Entwicklung fragen wir uns, wie wir deren Geschäftsmodell stören können. Deshalb konzentrieren wir uns nicht nur auf die eingesetzte Technologie. In Zusammenarbeit mit unserem Nachrichtendienst, der Bundespolizei und der Kantonspolizei versuchen wir auch zu ermitteln, wie und wo diese Organisationen arbeiten und wie sie Informationen austauschen. Dabei geht es wahrhaftig global zu und her. **Wir haben im Finanzsektor Angriffe analysiert, bei denen die Technologie von Akteuren in Nigeria stammte, während der eigentliche Angriff aus den Niederlanden erfolgte.** Diesen globalen Kontext haben wir im Blick, wenn wir versuchen, Übersicht über die Abläufe bereitzustellen. **Für die Zukunft planen wir, diese Art von Informationen einfacher zugänglich zu machen,** und zwar nicht nur für Finanzinstitutionen, sondern auch für Unternehmen in anderen Sektoren. Es gibt bereits entsprechende Pilotprojekte, in denen unsere Informationen Unternehmen helfen, sich effektiver zu schützen.

SIX: Herr Schütz, wenn Sie zu offen über Ihr Vorgehen sprechen, besteht das Risiko, dass Bedrohungsakteure ihre Methoden anhand dieser Informationen anpassen und sich der Erkennung entziehen?

Herr Schütz: Dieses Risiko besteht immer, vor allem, wenn wir über technische Gegenmassnahmen und unsere Ermittlungsmethoden sprechen. Daher vermeiden wir dies in der Regel. Da es sich aber um einen globalen Markt handelt, **verlagern diese Organisationen ihre geschäftlichen Tätigkeiten in sichere Bereiche, weshalb ich Unternehmen ausdrücklich dazu rate, über Cybervorfälle zu sprechen.**

Herr Beuchat: Ja, ich glaube, dass der Informationsaustausch entscheidend ist, denn schliesslich arbeiten die kriminellen Organisationen ebenso. Indem wir Informationen zu Angriffen miteinander teilen, verringern wir die Gefahr, dass auch andere Unternehmen solchen Angriffen zum Opfer fallen.

SIX: Herr Beuchat, was sind Ihre drei grössten Herausforderungen, und warum?

Herr Beuchat: Wir müssen agil bleiben, damit wir auch neue Angriffsmethoden schnell durchschauen und angemessen darauf reagieren können. Darüber hinaus ist die Abhängigkeit von Drittanbietern, wie etwa Managed Security Services Provider und ähnliche Anbieter, eine Herausforderung, denn bei ihnen müssen Cyber Security und Datenschutz auf dem gleichen Niveau gewährleistet sein wie im Finanzsektor.

SIX: Wie lassen sich also Managed Security Services wieder in das eigene Unternehmen integrieren?

Herr Beuchat: Ich glaube nicht, dass dies möglich ist. Einerseits wären interne Sicherheitsdienste für kleine und mittlere Unternehmen zu kostspielig, und andererseits wären wir ohnehin nicht in der Lage, ausreichend qualifizierte Mitarbeitende zu finden. Ich denke, es ist vor allem wichtig, besser mit den Anbietern von Managed Security Services zusammenzuarbeiten.

Herr Schütz: Bei den Cyberabläufen der Regierung sehe ich eine ähnliche Herausforderung. Aufgrund der zahlreichen Betriebsmodelle sind wir abhängig von externen Anbietern und SAPs. Auch die Cloud ist ein zentrales Thema. Meines Erachtens brauchen wir die Cloud, um wettbewerbsfähig bleiben zu können. Ich denke, die Lösung muss mit Data Governance beginnen. Was passiert, wenn die Systeme einer Bank wegen eines Cyberangriffs heruntergefahren werden müssen? Wer hat die Autorität für eine solche Entscheidung? Wie ist die Entscheidung überhaupt möglich? Welche Abhängigkeiten bestehen zwischen Banken? Lassen Sie mich anhand eines Beispiels erklären, warum dies relevant ist. Im ersten Golfkrieg in den 1990er-Jahren stellten sich die US-Amerikaner die Frage, welche Auswirkungen ein Angriff auf die Banken von Saddam Hussein auf andere globale Banken haben würde, weil es so viele gegenseitige Abhängigkeiten gab. Heutzutage ist dieses Thema noch viel wichtiger. Es geht darum, die Abhängigkeit mit zahlreichen unterschiedlichen Datentypen zu verwalten, und ich denke, hier bedarf es intelligenter Lösungen. Damit komme ich zur zweiten Herausforderung. Vor allem in der Schweiz bilden wir einige sehr kompetente Kräfte aus. Allerdings gibt es für sie auf nationaler Ebene kaum Chancen zum Aufstieg in Managementpositionen. Ich denke, in den Vorstandsetagen werden vor allem solche Führungskräfte gebraucht, die verstehen, dass unsere enorme Abhängigkeit von Technologie kein operatives Problem mehr ist, sondern ein strategisches. Zugleich müssen die derzeitigen Manager im Finanzsektor und in anderen Sektoren beginnen, die digitalen Aspekte ihres Geschäfts besser zu verstehen. ■

Makroanalyse

Vergleich der Länder

Methodik

Für diesen Bericht hat SIX in Zusammenarbeit mit QuoIntelligence und Recorded Future Daten über die Cyberbedrohungs-Landschaft in ausgewählten Ländern gesammelt, analysiert und bewertet. Die für diesen Bericht analysierten Daten stammen grösstenteils aus öffentlichen Quellen: Open Source Intelligence (OSINT). Der Grossteil der Daten wurde von Recorded Future zur Verfügung gestellt, zusätzliche Daten wurden von QuoIntelligence geliefert. In einigen Fällen haben wir die bereitgestellten Daten gefiltert und nur Datensätze mit entsprechendem Informationsgehalt berücksichtigt. Beispielsweise enthält nicht jeder Datensatz Informationen über eine spezifische Angriffsmethode, sodass wir bei der Analyse der Angriffsmethoden lediglich Datensätze mit dieser spezifischen Information berücksichtigt haben.

Folgende Länder wurden für den Makroteil dieses Berichts analysiert: Deutschland, Frankreich, Spanien, die Niederlande, Grossbritannien, die USA und Singapur. Die Makroanalyse zeigt in den ausgewählten Ländern, wo die Cyberbedrohungs-Landschaft im Finanzsektor Ähnlichkeiten zur Schweiz aufweist und wo die Unterschiede liegen.

Der Finanzsektor ist generell ein attraktives Ziel für Cyberakteure, da er potenziellen Zugang zu finanziellen Vermögenswerten und hochsensiblen Kundendaten bietet. Aufgrund dieser Faktoren nehmen Angreifer unterschiedlicher Art den Finanzsektor ins Visier: von Laienhackern mit geringen Fähigkeiten über opportunistische Angreifer, die in Untergrundforen gekaufte Malware einsetzen, bis hin zu professionellen, von Nationalstaaten geförderten Akteuren. Gleichzeitig nimmt die Angriffsfläche von Finanzinstitutionen aufgrund eines grösseren Digitalisierungsbedarfs und der steigenden Nachfrage nach Online-Diensten kontinuierlich zu. Diese Entwicklungen, die bereits in den vergangenen Jahren zu beobachten waren, haben sich mit dem Ausbruch der COVID-19-Pandemie weiter beschleunigt und verschärft. Innerhalb weniger Wochen verlagerten Unternehmen die Arbeit ins Homeoffice und die Kunden verliessen sich mehr denn je auf Online-Banking-Anwendungen. Das hat neue Ziele für böswillige Cyberakteure geschaffen.

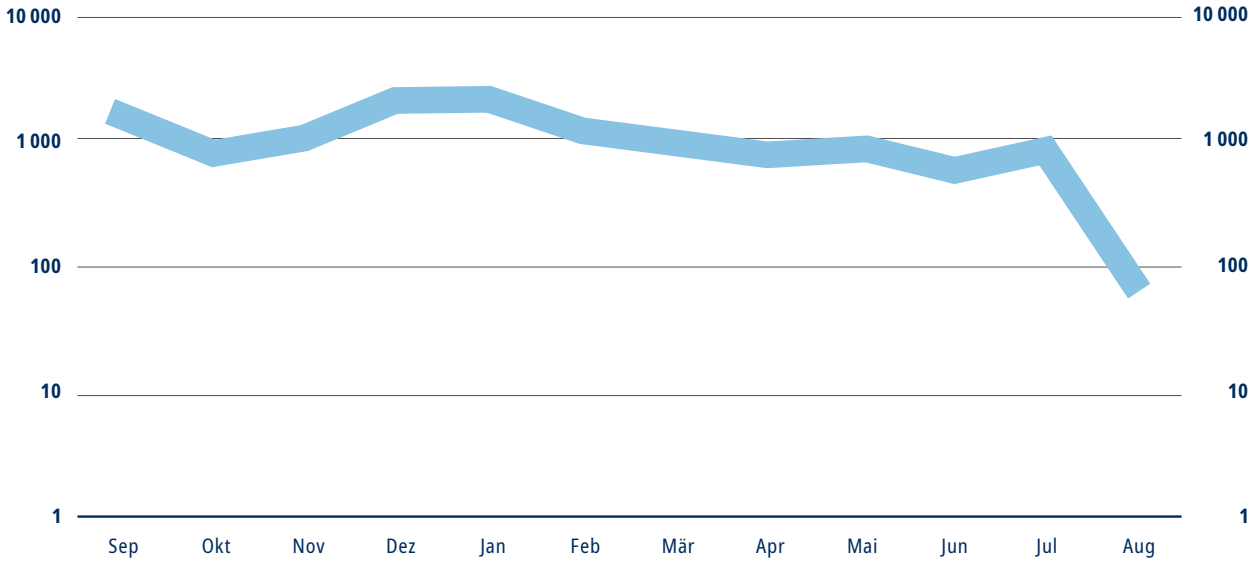


Abbildung 1 — Beobachtete Vorfälle insgesamt in ausgewählten Ländern (September 2019–August 2020)

Wie in Abbildung 1 zu sehen ist, ereigneten sich die zweitmeisten Cyberangriffe in den ausgewählten Ländern im März, zeitgleich mit der ersten Welle von COVID-19-bezogenen Beschränkungen in Europa. Im Allgemeinen blieb die Zahl der Vorfälle während des Berichtszeitraums jedoch konstant. Der Rückgang im August ist auf unseren Stichtag für den Dateneingang zurückzuführen und bedeutet nicht unbedingt einen Rückgang der Fälle.

Im Makroteil versuchen wir, die wichtigsten Gemeinsamkeiten der Cyberbedrohungs-Landschaften in der Schweiz und den ausgewählten Ländern zu skizzieren und die Unterschiede hervorzuheben. Dazu gehört ein kurzer Überblick über den regulatorischen Reifegrad jedes der untersuchten Länder sowie über die wichtigsten Entwicklungen und Cybervorfälle, die im vergangenen Jahr beobachtet wurden. Wir haben den Global Cybersecurity Index (GCI) der ITU[1] als Grundlage für die Beurteilung des Engagements und der Lage der Cyber Security in jedem unserer ausgewählten Länder verwendet.

Staat	Score	Globaler Rang	Regionaler Rang
Grossbritannien	0.931	1	1 (Europa)
USA	0.926	2	1 (Amerika)
Frankreich	0.918	3	2 (Europa)
Singapur	0.898	6	1 (Asien-Pazifik)
Spanien	0.896	7	5 (Europa)
Niederlande	0.885	12	8 (Europa)
Deutschland	0.849	22	13 (Europa)
Schweiz	0.788	37	22 (Europa)

Im nachfolgenden Bericht orientiert sich die Reihenfolge der Länder an der Höhe des GCI Scores. Die Analyse beginnt mit dem Land mit dem höchsten Score und endet mit der Schweiz, dem Land mit dem niedrigsten Score.

1 ITU, November 2019, Global Cybersecurity Index 2018

Grossbritannien

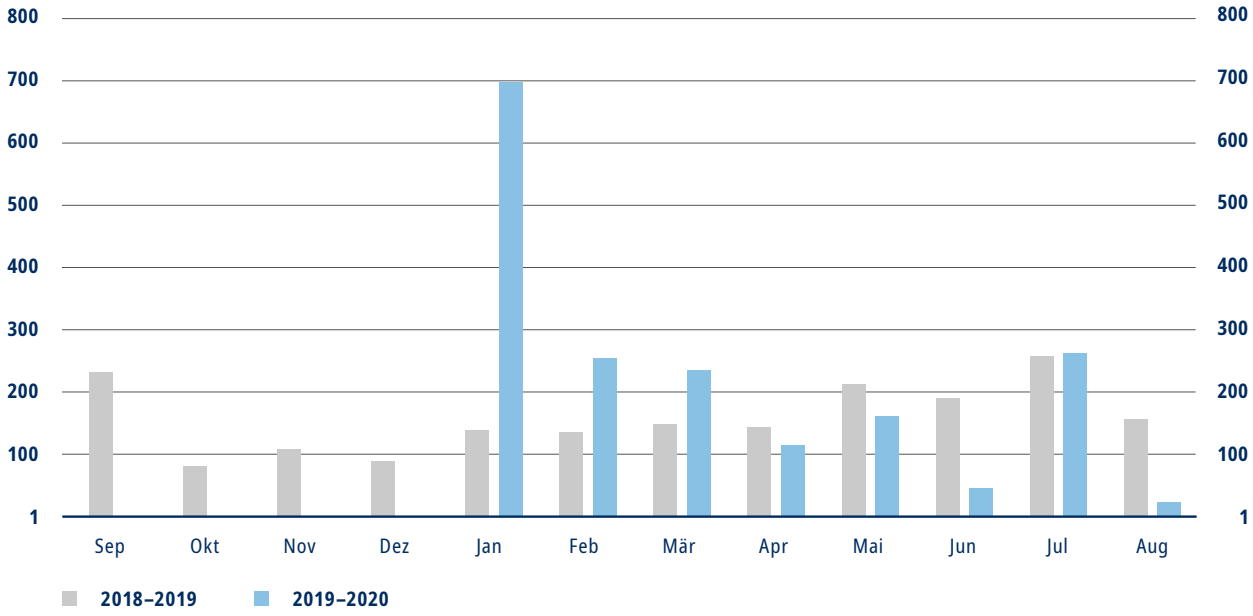


Abbildung 2 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in Grossbritannien (2018–2020)

London ist nach wie vor das grösste Finanzzentrum in Europa, mit der grössten europäischen Börse, der grössten Bank in Europa (HSBC Holdings) und drei britischen Banken aus den Top Ten der grössten Banken in Europa.[2] Der Finanzsektor Grossbritanniens wird von der Prudential Regulation Authority (PRA) reguliert. In Bezug auf Cyber Security steht Grossbritannien im internationalen Ranking der ITU an erster Stelle, insbesondere aufgrund der starken Leistung in den organisatorischen und regulatorischen Säulen des ITU-Index. Laut einer kürzlich von der britischen Regierung durchgeführten Umfrage hat der Finanzsektor Cyber Security eine sehr hohe Priorität eingeräumt.[3] Darüber hinaus wurde in Grossbritannien das geringste Verhältnis von Cybervorfällen zu Sicherheitsverletzungen verzeichnet, was möglicherweise auf eine hohe Fähigkeit zur Eindämmung von Angriffen hinweist.[4] Allerdings verzeichnete ein britisches Finanzdienstleistungsunternehmen mit EUR 94 Millionen den höchsten wirtschaftlichen Verlust durch einen Cyberangriff.

Auf der Grundlage unserer Daten zu beobachteten Cyberangriffen, gefiltert nach Datensätzen mit Informationen zur Angriffsmethode, war die häufigste Angriffsmethode Ransomware. Diese wurde in über 70 % der Vorfälle eingesetzt (→ Abbildung 3). Es folgten Phishing und SQL-Injektionen.

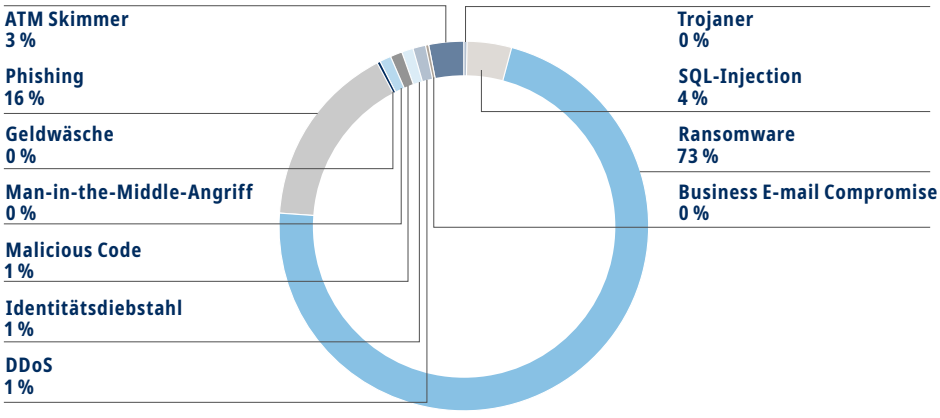


Abbildung 3 — Beobachtete Angriffsmethoden bei Finanzinstitutionen in Grossbritannien

2 S&P Global, April 2020, Europe's 50 largest banks by assets, 2020

3 Department for Digital, Culture, Media and Sport, March 2020, Cyber Security Breaches Survey 2020

4 Hiscox, June 2020, Cyber Readiness Report 2020

USA

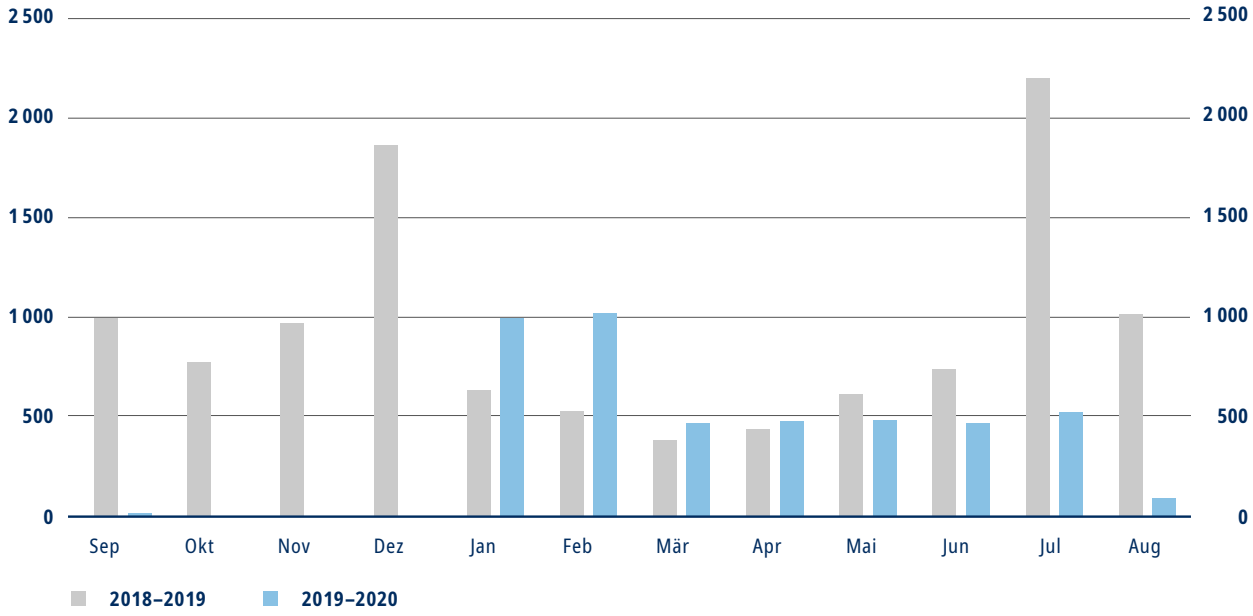


Abbildung 4 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in den USA (2018–2020)

Von allen in diesem Bericht untersuchten Ländern haben die USA bei Weitem die meisten Cybervorfälle zu verzeichnen, was zum grossen Teil darauf zurückzuführen ist, dass die USA ein äusserst attraktives Ziel für Angreifer sind. Allerdings dürfte es auch zu dieser grossen Menge an Informationen zu Cybervorfällen gekommen sein, weil es in den USA eine grosse Anzahl von Cyber-Security-Organisationen gibt. Diese zeichnen die Vorfälle in der gesamten Region akribisch auf und analysieren sie. Darüber hinaus verfügt der US-Finanzsektor weltweit über eine sehr hohe Bedeutung und die Cyber-Security-Massnahmen weisen einen hohen Reifegrad sowie eine hohe Transparenz auf. In Bezug auf Cyber Security rangieren die USA daher weltweit auf Platz zwei.

Laut einer kürzlich durchgeführten Umfrage berichteten 80% der Finanzinstitutionen von einer Zunahme der Cyberangriffe im Jahr 2020.[5] In Korrelation mit der COVID-19-Pandemie nahmen diese zwischen Februar und April angeblich um fast 240% zu.[6] Auf der Grundlage unserer Daten beobachteten wir im Januar und Februar 2020 Spitzenwerte und im März und April eine leicht höhere Zahl von Vorfällen als 2019 (⟶ Abbildung 4). Insbesondere wurden deutlich mehr Ransomware-Angriffe verzeichnet. Auf Grundlage unserer Daten (⟶ Abbildung 5) lässt sich ein solcher Anstieg im Februar und März 2020 ebenfalls feststellen, wobei die Anzahl der Ransomware-Angriffe Ende 2019 nachliess. Darüber hinaus ist die Zahl der DDoS-Angriffe im März gestiegen, obwohl sie im Allgemeinen niedrig ist. Die uns vorliegenden Daten haben wir im Hinblick auf die Aussagekraft so gefiltert, dass wir alle statistisch nicht relevanten Angriffsmethoden und alle Vorfälle ohne relevante Kennzeichnung ausgeschlossen haben.

5 VMWare Carbon Black, May 2020, Modern Bank Heists 3.0

6 VMWare Carbon Black, May 2020, Modern Bank Heists 3.0

Insgesamt wurden im Vergleich zu den anderen Ländern, die für diesen Bericht analysiert wurden, ähnliche Methoden bei Angriffen auf den Finanzsektor in den USA beobachtet, nämlich Ransomware-Angriffe und Angriffe auf Lieferketten.

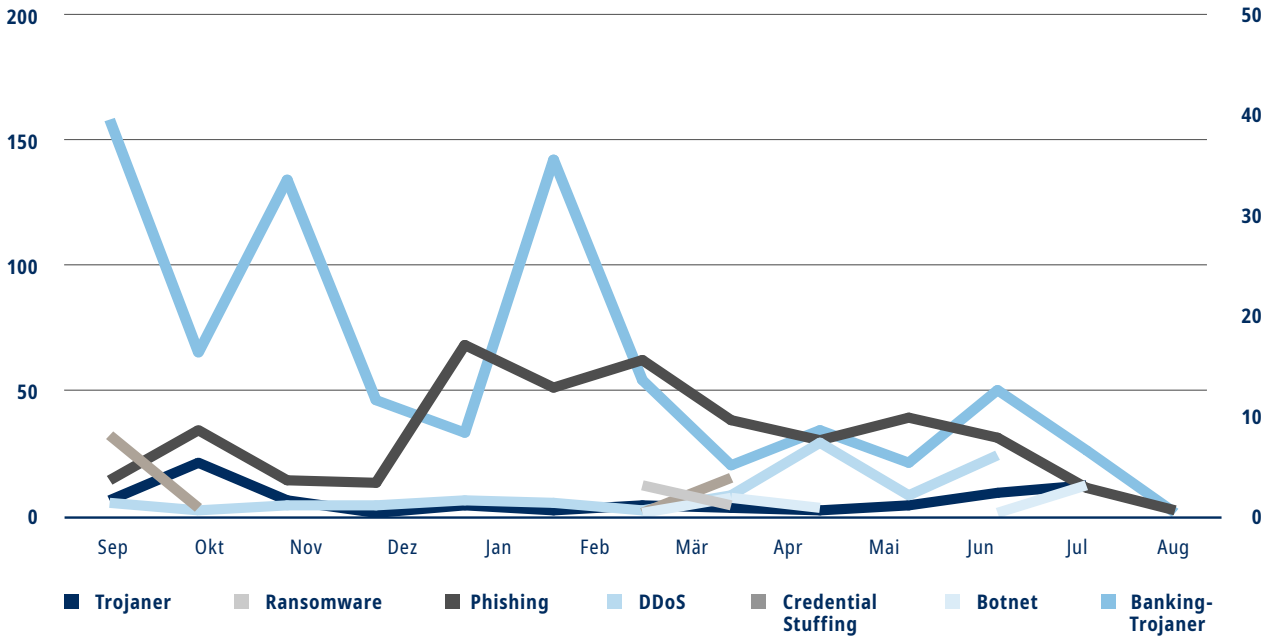


Abbildung 5 — Beobachtete Angriffsmethoden bei Finanzinstitutionen in den USA (2018–2020)

Frankreich

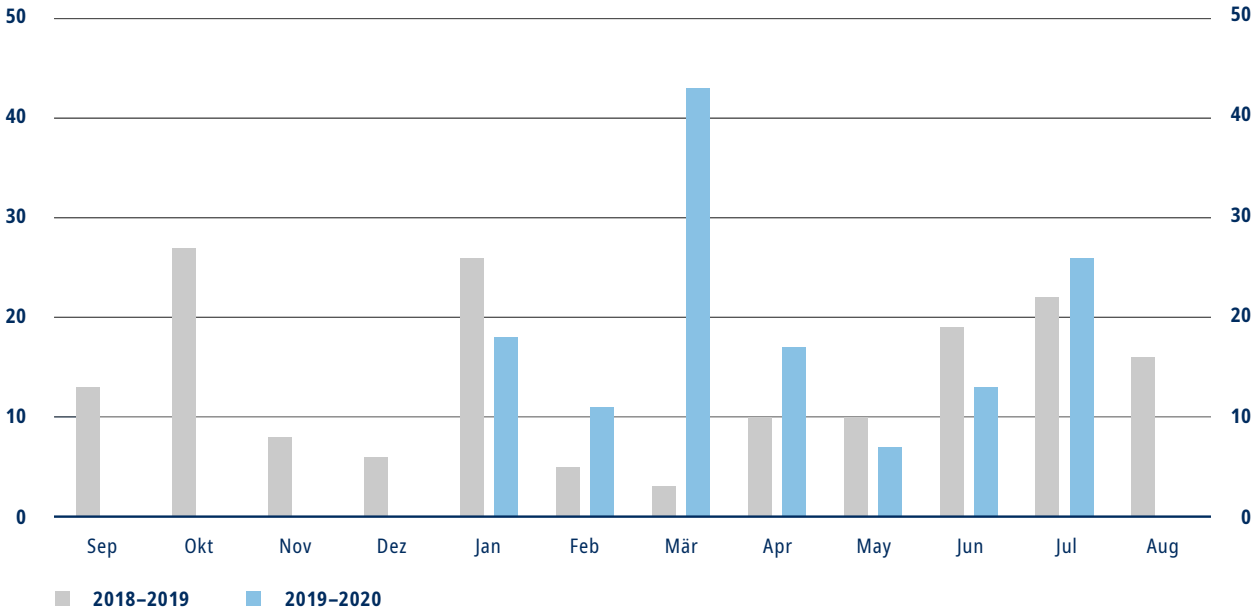


Abbildung 6 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in Frankreich (2018–2020)

Frankreich beheimatet vier der acht Global Systemically Important Banks (G-SIBs), die auch zu den zehn grössten Banken in Europa gehören.[7] Diese grossen, bekannten und international operierenden Banken – BNP Paribas, Crédit Agricole, Société Générale und Groupe BPCE – bringen den französischen Finanzsektor in den Fokus der Cyberakteure. Wahrscheinlich hat Frankreich aufgrund der Kenntnis dieser Exposition der Cyber Security in den letzten Jahren eine hohe Priorität eingeräumt. Laut ITU erreichte Frankreich in rechtlichen und organisatorischen Säulen 100% und rangierte damit weltweit an dritter Stelle bezüglich Cyber Security.[8] Frankreichs nationale Agentur für Cyber Security (Agence nationale de la sécurité des systèmes d'information – ANSSI) verzeichnete 2019 mehr als 370 Cybervorfälle, davon waren 9 grössere Vorfälle. Darüber hinaus war die Agentur 2019 an 16 Cyberabwehr-Operationen beteiligt.[9]

Wie in Abbildung 6 zu sehen ist, enthält unser Datensatz weniger Vorfälle, was auf die hohe Sichtbarkeit von ANSSI im gesamten Sektor hinweist. Interessanterweise wurde im März, April und erneut im Juli ein Anstieg der Cyberangriffe beobachtet, der mit dem Ausbruch der COVID-19-Pandemie zusammenfiel. Laut ANSSI sind die Haupttrends in Frankreichs Cyberbedrohungs-Landschaft Ransomware-Angriffe, Spionageversuche und Angriffe auf Lieferketten, ähnlich den in der Schweiz beobachteten Bedrohungen.

7 S&P Global, April 2020, Europe's 50 largest banks by assets, 2020

8 ITU, November 2019, Global Cybersecurity Index 2018

9 ANSSI, June 2020, ANSSI in action: Looking back on 2019

Auf Grundlage unserer Beobachtungen (⟶ Abbildung 7) und nachdem unser Datensatz so gefiltert wurde, dass nicht relevante Einträge ausgeschlossen wurden, lässt sich ableiten, dass Ransomware-Angriffe im beobachteten Zeitraum die häufigste Cyberangriffs-Methode auf französische Finanzinstitutionen waren. Der Anstieg im März, der in Abbildung 6 zu sehen ist, ist weitgehend auf eine Zunahme der Ransomware-Angriffe zurückzuführen. Die Phishing-Kampagnen blieben das ganze Jahr über relativ konstant, während sie im Mai und zu Beginn des dritten Quartals zurückgingen. Interessanterweise kam es zwischen März und Mai zu einer Welle von DDoS-Angriffen, die zeitlich mit dem Beginn der COVID-19-Beschränkungen und der plötzlichen Zunahme des Arbeitens im Homeoffice zusammenfiel. Die durch diese Zunahmen angespannten Bandbreiten sowie das Arbeiten im Homeoffice an sich erschweren die Nutzung von Patches für anfällige Geräte. Dies kann dazu führen, dass Geräte anfällig bleiben und somit für DDoS-Angriffe ausgenutzt werden können.

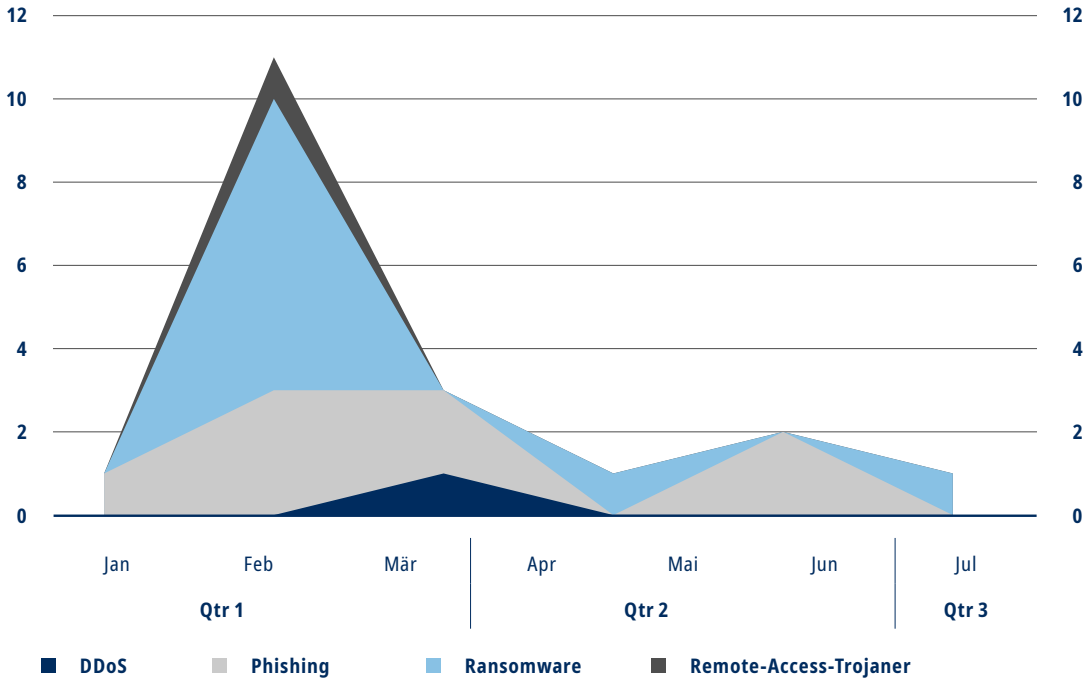


Abbildung 7 — Arten von Cyberangriffen in Frankreich

Singapur

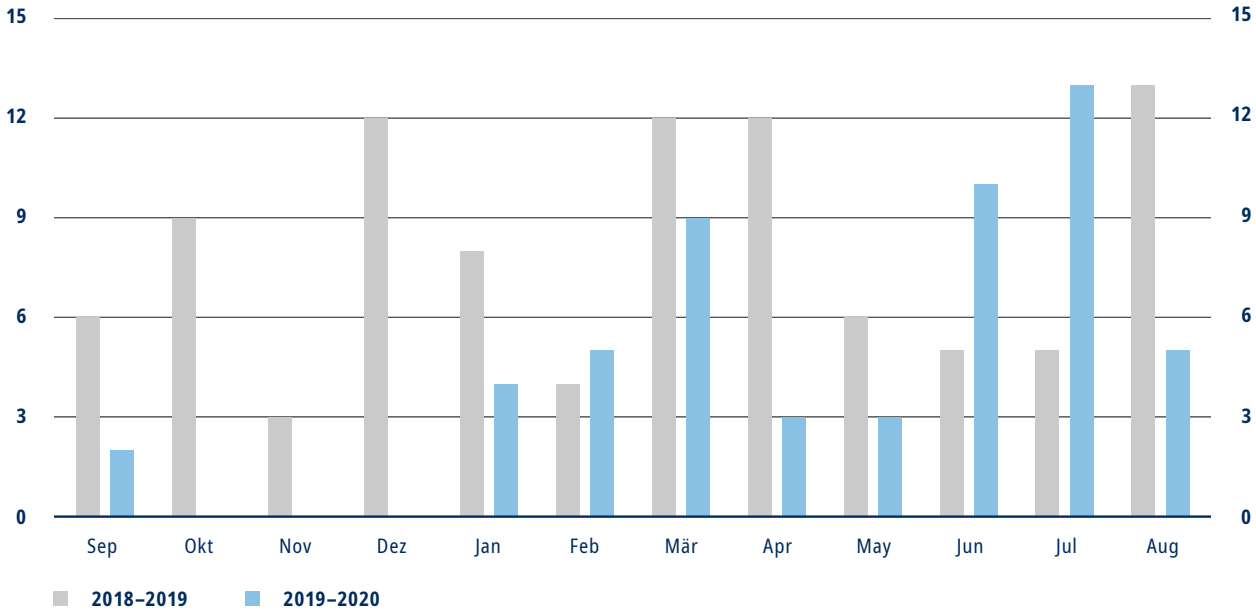


Abbildung 8 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in Singapur (2018–2020)

Dies hat möglicherweise Auswirkungen auf die Natur und Häufigkeit der Cybervorfälle, die das Land betreffen. Tatsächlich war laut einer kürzlich durchgeführten Umfrage[10] die häufigste Art von Cyberangriffen, die von Chief Information Security Officers (CISOs) in Singapur in den vergangenen zwölf Monaten beobachtet wurde, benutzerdefinierte Malware. 75% der Befragten aus dem Finanzsektor gaben an, dass dies die am häufigsten verwendete Angriffsmethode sei. Ransomware-Angriffe, die in den anderen ausgewählten Ländern im Allgemeinen zu den am häufigsten beobachteten Methoden gehörten, wurden nur auf Platz 10 eingestuft. Darüber hinaus wurden 80% der befragten Institutionen in den vergangenen Monaten Opfer einer Sicherheitsverletzung nach einem Cyberangriff. Als grösste Bedrohungen nannte Singapurs Cyber Security Agency (CSA) in ihrem Jahresbericht zusätzlich die Verunstaltung von Websites, Phishing und Malware-Infektionen.[11]

Unsere Daten enthielten für Singapur die zweitgeringste Anzahl von Vorfällen nach der Schweiz. Dies überrascht angesichts der oben genannten Zahlen, wonach 80% der befragten CISOs von Sicherheitsverletzungen durch Cyberangriffe berichteten. Aus den verfügbaren Daten geht jedoch hervor, dass im Jahr 2020 insgesamt weniger Vorfälle beobachtet wurden als 2019. Lediglich im Juni und Juli 2020 wurden im Vergleich zu 2019 deutlich mehr Vorfälle beobachtet (siehe Abbildung 8). Die Divergenz zwischen der niedrigen Beobachtungsrate einerseits und der Vielzahl von gemeldeten Vorfällen durch CISOs andererseits könnte mehrere Ursachen haben. Auf der einen Seite könnte – ähnlich wie in Grossbritannien – eine hohe Anzahl gemeldeter Cyberangriffe, aber eine geringe Anzahl gemeldeter Sicherheitsverletzungen auf eine ausgeprägte Fähigkeit zur Eindämmung von Cyberangriffen hindeuten. Die ITU stuft Singapur auf Platz sechs ihrer Cyber-Security-Rangliste ein und unterstreicht damit die ausgereiften Fähigkeiten Singapurs im Bereich der Cyber Security. Auf der anderen Seite könnte die niedrige Zahl der gemeldeten Cyberangriffe auf einen Mangel an Transparenz und Informationsaustausch hindeuten – in dem Sinne, dass Cyberangriffe nicht ausreichend öffentlich gemeldet werden.

10 VMWare Carbon Black, June 2020, Singapore Threat Report

11 CSA Singapore, 26 June 2020, Cyber Threats Grew in 2019 Amid Rapidly Evolving Global Cyber Landscape

Spanien

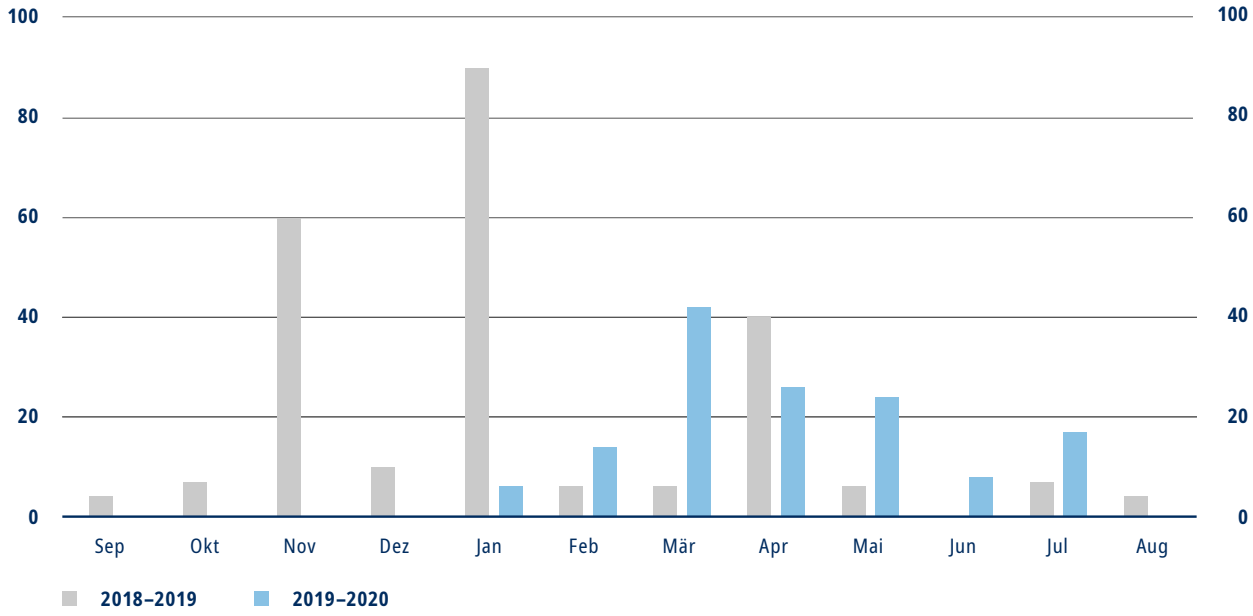


Abbildung 9 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in Spanien (2018–2020)

Der spanische Finanzsektor ist im Vergleich zu Frankreich, Deutschland und den Niederlanden kleiner. Nur eine einzige spanische Bank, Santander, gehört zu den grössten Banken Europas. Allerdings rangiert Spanien in Bezug auf Cyber Security weit oben, nämlich auf Platz sieben im ITU-Index. Auch die spanische Regierung hat der Cyber Security eindeutig Priorität eingeräumt. Die entsprechenden Investitionen haben sich bis 2020 mehr als verdoppelt.[12] Auf der Grundlage unserer Daten (→ Abbildung 9) haben Cybervorfälle im März stark zugenommen, möglicherweise zeitgleich mit COVID-19, und waren im Allgemeinen zahlreicher als 2019. Nur im Januar 2019 wurde eine hohe Anzahl an Phishing- und DDoS-Vorfällen beobachtet.

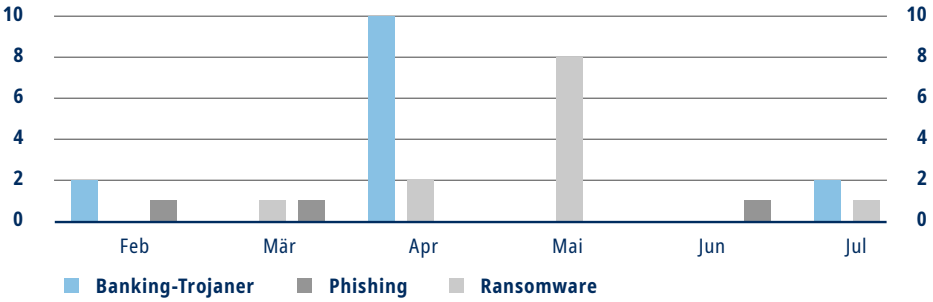


Abbildung 10 — Arten von beobachteten Cyberangriffen bei Finanzinstitutionen in Spanien

Abbildung 10 skizziert einige interessante regionale Unterschiede zwischen Spanien und anderen in diesem Bericht analysierten Ländern. Nachdem die Daten gefiltert wurden, um nicht statistisch relevante Einträge auszuschliessen, korrelierte eine Spitze der beobachteten Vorfälle im April mit dem brasilianischen Banktrojaner Grandoreiro, der spanische Banken ins Visier nahm. Ähnliche Vorfälle wurden in keinem der anderen ausgewählten Länder beobachtet. Ähnlich wie in den anderen Ländern und möglicherweise korrelierend mit dem Beginn der COVID-19-Beschränkungen nahmen Phishing-Kampagnen jedoch ab April zu und erreichten ihren Höhepunkt im Mai.

12 Hiscox, June 2020, Cyber Readiness Report 2020

13 ESET, April 2020, ESET investigates Grandoreiro, a trojan exploiting the coronavirus pandemic

Niederlande

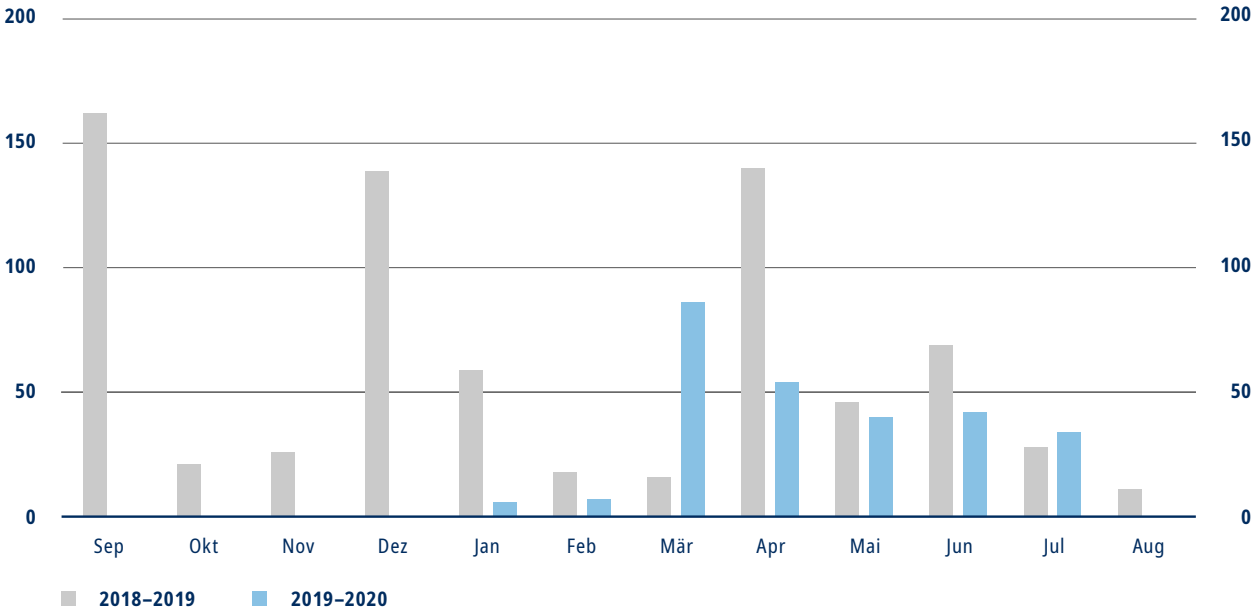


Abbildung 11 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in den Niederlanden (2018–2020)

Die niederländische Zentralbank stellte 2019 fest, dass Cyberbedrohungen nicht konsequent analysiert werden und die Datensicherheitsmassnahmen teilweise unzureichend sind.[14] Aus unseren Daten (→ Abbildung 11) geht hervor, dass ein deutlicher Anstieg der Cybervorfälle in den Monaten März, April und Mai mit dem Ausbruch der COVID-19-Pandemie korreliert sein könnte. Insgesamt wurden im Jahr 2020 wesentlich mehr Cybervorfälle beobachtet als im Jahr 2019. Für die Niederlande mangelte es an Informationen über die beobachteten Angriffsspezifikationen, was eine Analyse der Angriffsmuster und -trends erschwert. Insgesamt sind die Niederlande in Bezug auf ihre Cyber-Security-Kapazitäten sehr hoch eingestuft. Die ITU ordnet sie weltweit auf Rang 12 ein. Das niederländische nationale Zentrum für Cyber Security berichtete[15] in seiner Bewertung der Cyber Security, dass einfache Eindringtechniken wie Phishing, Ransomware und der Missbrauch von Lieferketten weiterhin wirksame Instrumente sind, um gegen Finanzinstitutionen vorzugehen. Darüber hinaus waren Finanzinstitutionen im Jahr 2020 auch Ziel von DDoS-Angriffen.

14 National Cyber Security Centre, September 2019, Cyber Security Assessment Netherlands 2019

15 National Cyber Security Centre, September 2019, Cyber Security Assessment Netherlands 2019

Deutschland

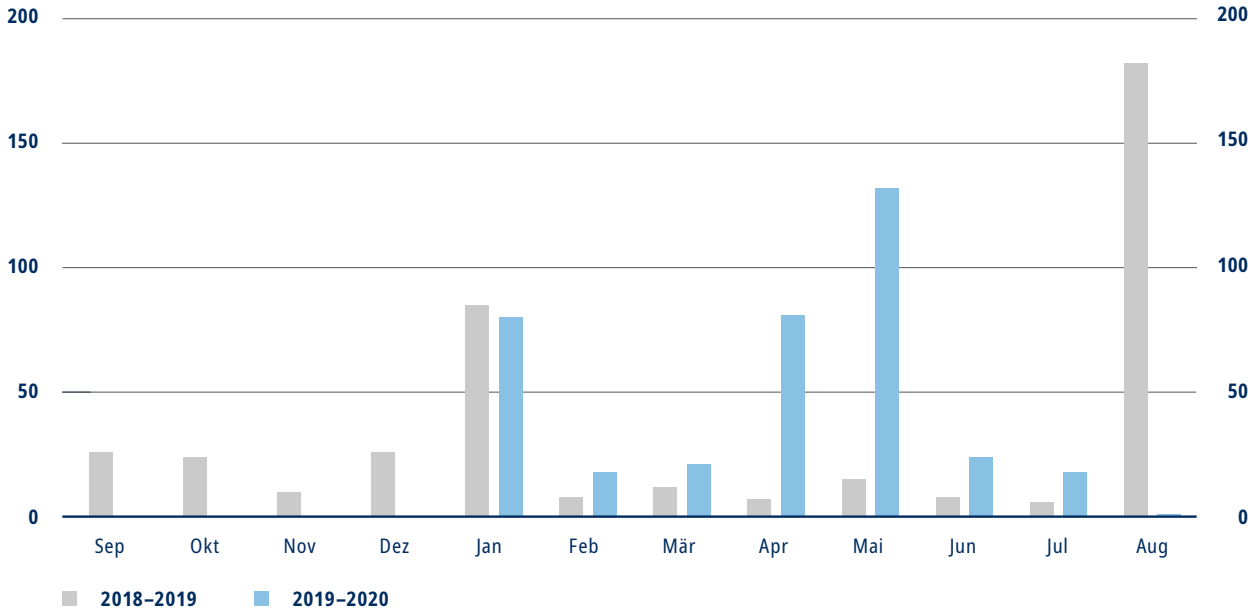


Abbildung 12 — Gesamtzahl der beobachteten Cybervorfälle bei Finanzinstitutionen in Deutschland (2018–2020)

In Deutschland befinden sich der grösste Finanzsektor der EU sowie die meisten europäischen Finanzaufsichtsbehörden, darunter die Europäische Zentralbank (EZB). Diese Konzentration von Finanzinstitutionen macht Deutschland zu einem attraktiven Ziel für Cyberakteure.

Die Verletzung des Schutzes persönlicher Daten deutscher Politiker in mehreren Fällen im Januar 2019[16] und ein Datenleck bei Mastercard im August 2019[17] haben Spitzenwerte verursacht. Davon abgesehen wurde die höchste Anzahl von Vorfällen im April und Mai 2020 beobachtet (⟶ Abbildung 12).

Auf der Grundlage der Beobachtungen von QuoIntelligence war die Mehrzahl der in Deutschland registrierten Cyberangriffe auf den Finanz- und Industriesektor gerichtet (⟶ Abbildung 13). Zudem nahmen die beobachteten Angriffe im Vergleich zum Vorjahr erheblich zu.

16 Süddeutsche Zeitung, Januar 2019, Seehofer verspricht volle Transparenz zu Daten-Hack

17 Verbraucherzentrale, August 2019, Datenleck bei Mastercard: Was Kreditkartenbesitzer jetzt tun sollten

Der deutsche Finanzsektor ist in hohem Masse reguliert und hat spezifische regulatorische Anforderungen an Cyber Security. Im Vergleich zu den anderen ausgewählten Ländern in diesem Bericht wird Deutschland von der ITU jedoch auf Rang 22 relativ niedrig eingestuft. Die bei Cyberangriffen auf Finanzinstitutionen beobachteten Angriffsvektoren ähneln den Beobachtungen in der Schweiz. So sind die am häufigsten verwendeten Angriffsvektoren bösartige E-Mails, die über (Spear-) Phishing-Kampagnen verbreitet werden, gefolgt von Angriffen auf die Lieferkette (→ Abbildung 14).

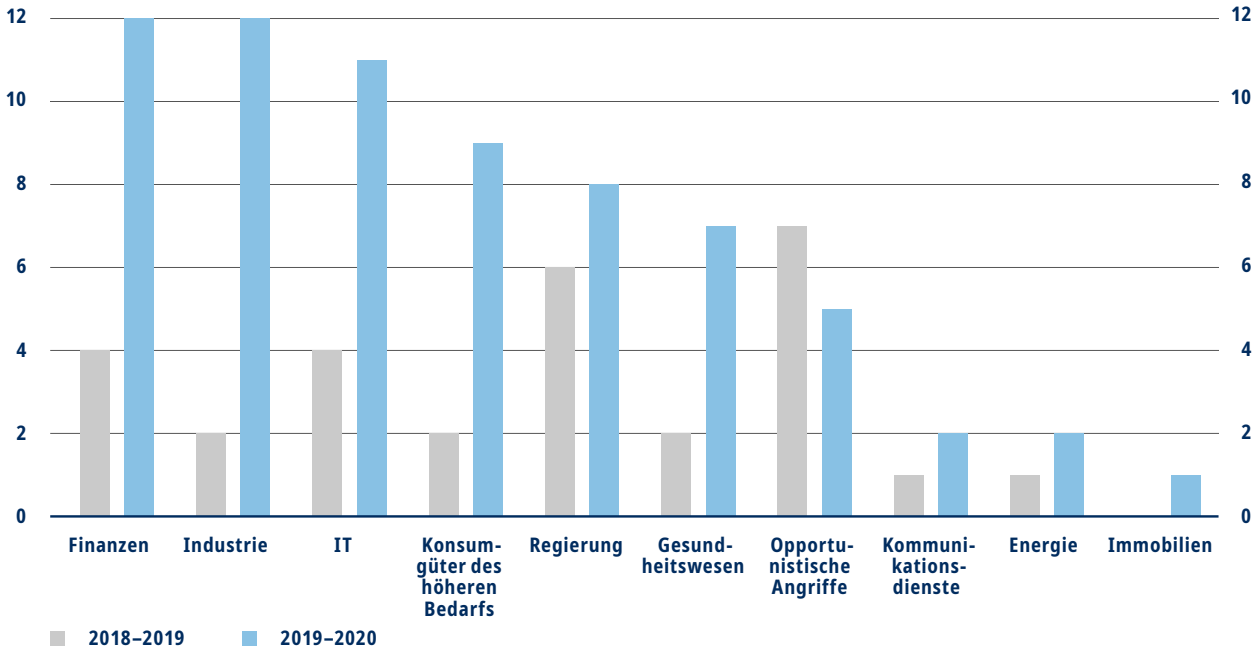


Abbildung 13 — Von Cyberangriffen betroffene Sektoren in Deutschland (2018–2020)

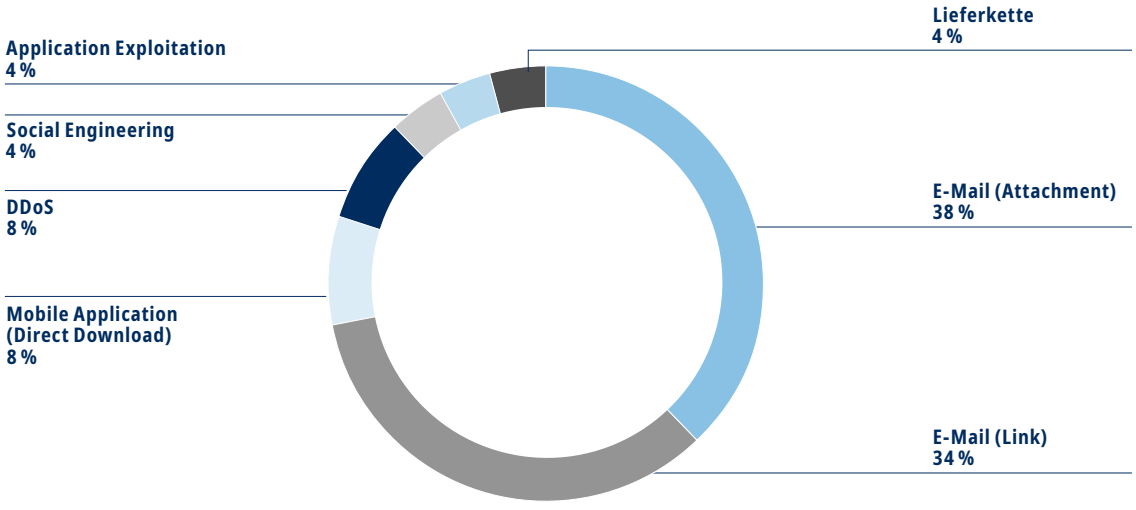


Abbildung 14 — Bei Cyberangriffen auf Finanzinstitutionen in Deutschland beobachtete Angriffsvektoren

Schweiz

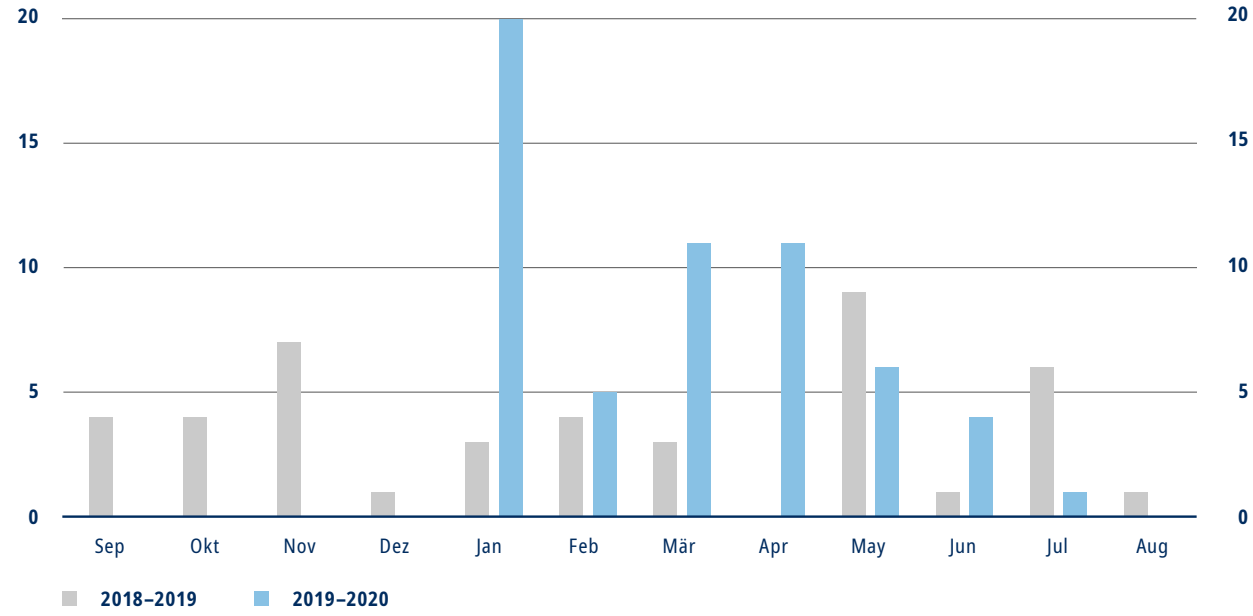


Abbildung 15 — Gesamtzahl der beobachteten Cybervorfälle bei Schweizer Finanzinstitutionen (2018–2020)

In den vergangenen Jahren war die Zahl der Cyberangriffe auf Schweizer Finanzinstitutionen durchweg gering[18] und im Vergleich zu allen anderen in diesem Bericht analysierten Ländern viel niedriger. Im Mikroteil dieses Berichts beschreiben wir, dass diese niedrige Beobachtungsrate nicht unbedingt darauf hindeutet, dass Schweizer Finanzinstitutionen weniger ins Visier genommen werden als Institutionen in anderen Ländern. Es ist anzunehmen, dass ein gewisser Prozentsatz der Fälle aufgrund des Fehlens einer robusten Infrastruktur für den Informationsaustausch nicht gemeldet wird. Darüber hinaus stellen wir im Mikroteil eine Hypothese über eine Korrelation zwischen der Potenz und Transparenz von CISO-Tätigkeiten und den beobachteten Cyberangriffen auf. Der Finanzsektor der Schweiz wird jedoch von der FINMA streng reguliert, und alle Institutionen müssen hohe Standards für Cyber Security einhalten.

Im Jahr 2020 ist die Zahl der Cybervorfälle im Vergleich zum Vorjahr gestiegen (→ Abbildung 15). Im Januar, März und April war die Zahl der beobachteten Vorfälle besonders hoch.

Im ITU Global Cybersecurity Index 2018 liegt die Schweiz weltweit auf Rang 37, niedriger als jedes andere in diesem Bericht analysierte Land. Die Schweizer Regierung hat dieses Manko offenbar erkannt und investiert in die Verbesserung ihrer Cyber Security. Im Jahr 2018 wurde die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) (2018–2022) veröffentlicht[19] und die zentrale Melde- und Analysestelle für Informationssicherung MELANI eingerichtet.

Angesichts der Tatsache, dass die Schweiz eine der attraktivsten und bekanntesten Bankendestinationen ist und es zugleich möglicherweise an Cyber-Security-Kapazitäten mangelt, überrascht die geringe Zahl der beobachteten Angriffe.

18 SIX Cyber Security Report 2019

19 Der Bundesrat, A1, September 2018, SN002 – Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Zusammenfassung

Der Zweck der Makroanalyse in diesem Bericht bestand darin, die wichtigsten Ähnlichkeiten der verschiedenen Cyberbedrohungs-Landschaften aufzuzeigen und die Unterschiede zwischen der Schweiz und den anderen ausgewählten Ländern zu verstehen.

Die erste wesentliche Feststellung besteht darin, dass die am häufigsten beobachteten Angriffsmethoden in allen untersuchten Ländern im Allgemeinen gleich sind. Ransomware, Phishing und bis zu einem gewissen Grad auch Angriffe auf die Lieferkette sind nach wie vor die grösste Cyberbedrohung für Finanzinstitutionen, unabhängig von ihrer Grösse oder ihrem Standort.

Zweitens kam es zu einer Zunahme der beobachteten Cyberangriffe während des Ausbruchs der COVID-19-Pandemie im März. Dies verdeutlicht, dass die Angriffsfläche aufgrund der zunehmenden Abhängigkeit von Online-Diensten sowie der Bereitschaft und Fähigkeit der Cyberakteure, ihre Methoden schnell anzupassen, um jede Situation auszunutzen, tatsächlich zunahm.

Diese Gemeinsamkeiten unterstreichen erneut die Notwendigkeit einer globalen Infrastruktur für den Informationsaustausch. Angesichts der Tatsache, dass die meisten von ähnlichen Angriffsmethoden betroffen sind, könnten Finanzinstitutionen stark profitieren. Dazu müssten sie in der Lage sein, nahezu in Echtzeit auf Informationen über Kampagnen zuzugreifen, die auf andere Finanzinstitutionen abzielen. Die Wahrscheinlichkeit, dass sie von den gleichen oder ähnlichen Kampagnen ins Visier genommen werden, ist hoch. Die Institutionen könnten spezifische Abwehrmassnahmen ergreifen.

Ein wesentlicher Unterschied zwischen den für diesen Bericht analysierten Ländern ist die unterschiedliche Anzahl der beobachteten Vorfälle. Während die Informationen über Vorfälle in den USA sehr umfangreich sind, stehen für die Schweiz oder Singapur wesentlich weniger Informationen zur Verfügung. Auch dieses Problem könnte eine internationale Gemeinschaft für den Informationsaustausch verringern. Allgemein anerkannte Definitionen darüber, was Cybervorfälle sind, wie sie gemeldet werden sollten und zu welchem Zeitpunkt, würden transparentere Daten über Vorfälle liefern.


<p:normalViewPr
Pr><p:slideView
cale><p:origin
pos="4898"
n="33" d="
Pr><p:sc
Scale=
Pr><
ft sz="16585" autoAdjust="0"/><p:restoredTop sz="9445
wPr snapToGrid="0" p:cViewPr varScale="1" scale><a:sx n
7"/></p:cViewPr guideLst><p:guide pos="2
nt="horz" pos="692"/ /p:guideLst /p:cSldView
33 d="100"/></p:scale><p:origin x="0" y="0"
d=2/a:sy n="3" p:scale><p:origin x="0" y="0"/
x n="1" d="1"/ a:sy n="1" d="1"/ /p:scale><p:ori
apTo="0" show uides="1"><p:cViewPr varScale=
038" y="102"
cViewPr><p:guideLst><p:guid
gridSpacing cx="72008" cy=
r></p:notesVie
autoAdjust="0"/></p:normalV
redTop sz=94
91 d="100"/ :scale p:origin x=
guide orient

Mikroanalyse

Zentrale Erkenntnisse

Die rapiden Veränderungen durch Digitalisierung und die damit verbundene Notwendigkeit, IT-Architekturen schnell und unmittelbar anzupassen, werden als die grössten Herausforderungen für die Aufrechterhaltung von Cyber Security im Schweizer Finanzsektor angesehen. Das konnten wir basierend auf unserer Analyse, unabhängig von der Grösse eines Unternehmens, feststellen.

Während diese Entwicklung bereits seit mehreren Jahren andauert, hat der Ausbruch der COVID-19-Pandemie diesen Prozess erheblich beschleunigt und die bereits bestehenden Herausforderungen hinsichtlich Cyber Security noch verschärft. Die plötzliche und massive Verlagerung auf die Arbeit im Homeoffice erfordert eine schnelle Anpassung der IT-Architekturen und schafft neue Angriffsflächen.

Chief Information Security Officers (CISOs) machen sich Gedanken darüber, wie sie diesen Veränderungen begegnen können. Sie betonen die Notwendigkeit einer angemessenen Finanzierung ihrer Aufgaben – insbesondere auch, um qualifizierte Arbeitskräfte zu binden, die für das Aufrechterhalten eines hohen Niveaus an Cyber Security unerlässlich sind. Laut diversen Schweizer Finanzinstitutionen werden Phishing, Malware und Ransomware als grösstes Risiko für Cyber Security eingestuft, gefolgt von mangelnden IT-Sicherheitsarchitekturen und mangelndem Risikomanagement.

Darüber hinaus konnte bei der Analyse eine deutliche Korrelation zwischen der Anzahl der beobachteten Vorfälle, dem Reifegrad und der Transparenz der CISO-Tätigkeiten festgestellt werden. CISOs, die Reifegrad und Transparenz als hoch bewerteten, beobachteten auch deutlich mehr Zwischenfälle.

CISOs sollten sowohl von innerhalb ihres Unternehmens als auch von Aufsichtsbehörden Unterstützung erhalten, um effektiv auf die sich verändernde Bedrohungslandschaft reagieren zu können. Einerseits ist eine ausreichende Finanzierung notwendig, um den Reifegrad und die Transparenz innerhalb des Unternehmens zu erhöhen, was für die Risikominderung von wesentlicher Bedeutung ist. Ausserdem ist eine angemessene Finanzierung erforderlich, um qualifizierte Arbeitskräfte zu halten, was von den Befragten als wichtiger Punkt genannt wurde. Zweitens sollte Cyber Security vom Management als Priorität anerkannt werden, damit CISOs unternehmensweit agieren können. Darüber hinaus haben CISOs Bedenken bezüglich der zunehmenden Digitalisierung, wie z. B. den Umstieg auf die Cloud sowie hinsichtlich des damit verbundenen Risikomanagements von Drittanbietern. Um diese Risiken zu mindern, sollten Regulierungs- und Aufsichtsbehörden angemessene Sicherheitsrichtlinien für Drittanbieter und Lieferketten implementieren.

Der nachfolgende Bericht untersucht die Cyberbedrohungs-Landschaft des Schweizer Finanzsektors in den vergangenen zwölf Monaten. Die Ergebnisse in diesem Bericht basieren auf vertraulichen Interviews mit 53 Cyber-Security-Führungskräften von Schweizer Finanzinstitutionen, die im Juli 2020 durchgeführt wurden, sowie auf Open- und Closed-Source-Analysen. Die Befragten verteilen sich gleichmässig auf kleine, mittlere und grosse Unternehmen. Daher gibt der Bericht Einblicke in verschiedene Segmente des Finanzsektors. Um Vertraulichkeit zu gewährleisten, wurden alle Informationen nach der Erhebung anonymisiert und nur in aggregierten Analysen verwendet.

Zusammenfassung der Ergebnisse

Die Befragten unserer Umfrage bewerteten die Bedrohungen, die in die Kategorie Cyberangriffe fallen, als die grössten Herausforderungen für Cyber Security im Schweizer Finanzsektor im vergangenen Jahr. Es folgten die Bedrohungen in den Kategorien Sicherheitsarchitektur und Risikomanagement (→ Abbildung 16).

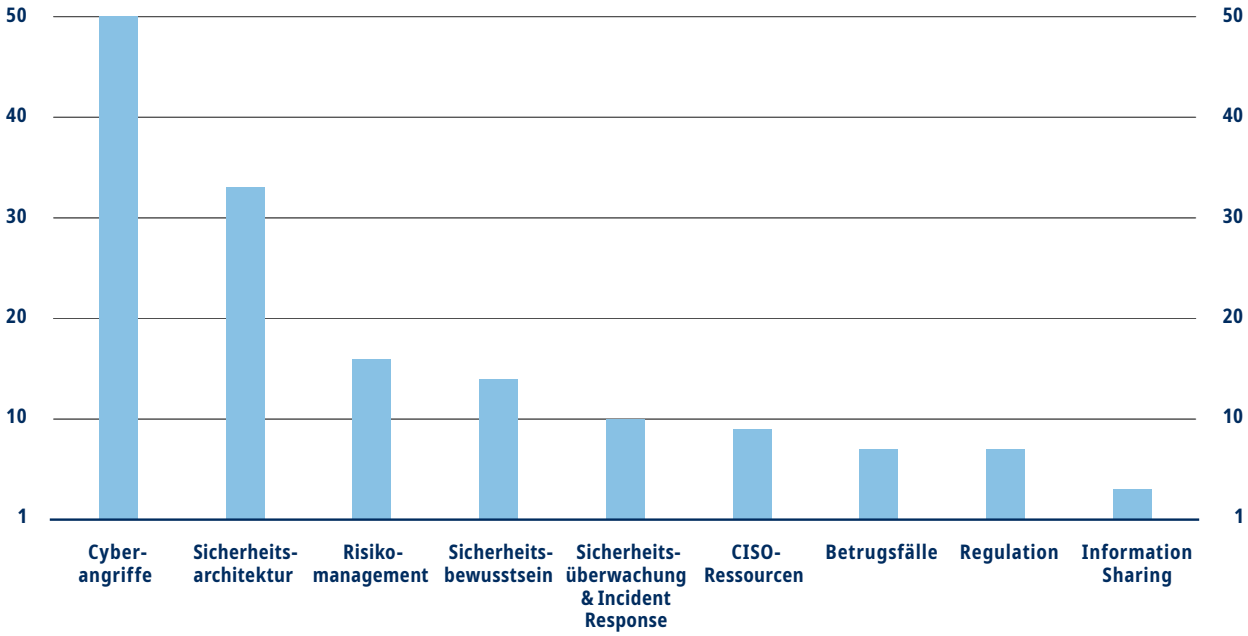


Abbildung 16 — Grösste Herausforderungen für Cyber Security im Schweizer Finanzsektor

In Abbildung 17 kann man sehen, dass Phishing, Malware und Ransomware am häufigsten als Arten von Cyberangriffen genannt wurden. In Bezug auf die Sicherheitsarchitektur rangierten Themen im Zusammenhang mit der Cloud und dem Risikomanagement von Drittanbietern auf den vorderen Plätzen.

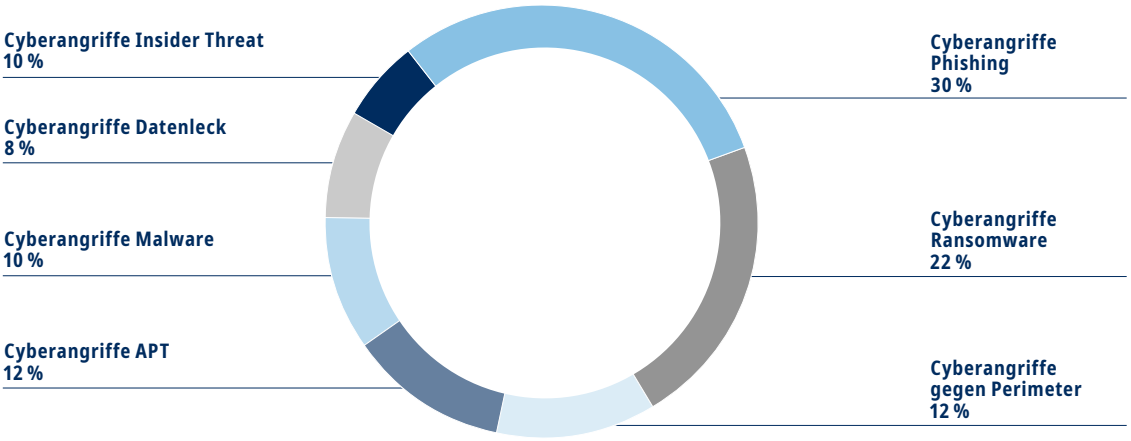


Abbildung 17 — Arten von Cyberangriffen als Hauptbedrohungen für den Schweizer Finanzsektor

Die von den Befragten identifizierten Bedrohungen decken sich mit den im vergangenen Jahr beobachteten Angriffsvektoren gegen Finanzinstitutionen. Wie aus Abbildung 18 hervorgeht, die auf Daten von QuoIntelligence basiert, wurden E-Mails mit bösartigen Anhängen oder Links zur Verbreitung von Malware bei mehr als der Hälfte der Vorfälle, die auf Finanzinstitutionen abzielten und in denen Angriffsvektoren aufgezeichnet wurden, als Angriffsvektor identifiziert. Darauf folgten Angriffe auf die Lieferkette. Dieser Trend entspricht dem letztjährigen Bericht, in dem Phishing-E-Mails als häufigster Angriffsvektor genannt wurden.

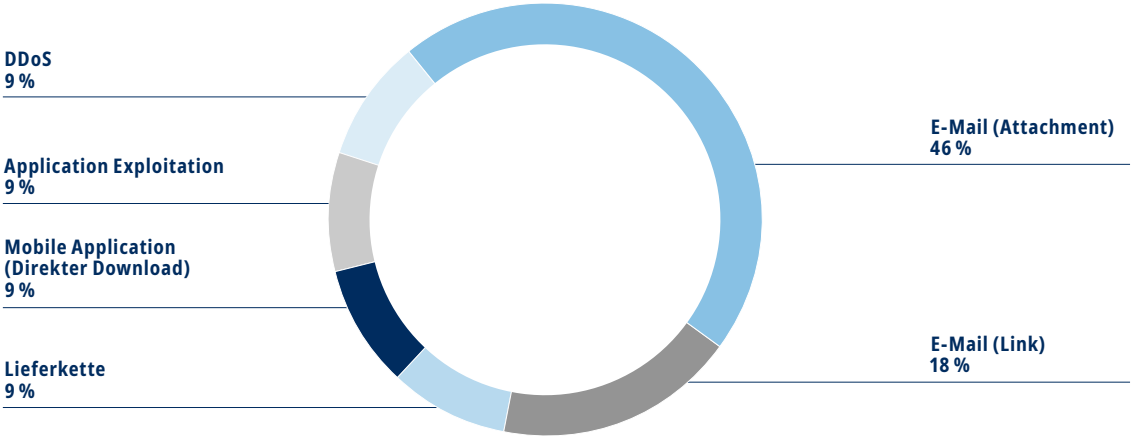


Abbildung 18 — Bei Angriffen auf Finanzinstitutionen beobachtete Angriffsvektoren

Bei der Frage nach Bedrohungen für das eigene Unternehmen war mehr als die Hälfte (rund 53%) «sehr besorgt» über Malware-Ausbrüche, was den identifizierten Top-Bedrohungen entspricht, die auf den Schweizer Finanzsektor insgesamt abzielen. Dicht gefolgt wurde dieser Wert von der Ausnutzung von Schwachstellen (49%). Während die Sorge bezüglich qualifizierter Arbeitskräfte bei den Gesamtbedrohungen als sehr hoch eingestuft wurde, war der Mangel an Sicherheitsexpertise und -erhalt im Unternehmen nur für 3% der Befragten «sehr besorgniserregend», wenn sie nach ihrem eigenen Unternehmen gefragt wurden.

Analyse möglicher Ursachen für die niedrige Beobachtungsrate von Cybervorfällen bei Schweizer Finanzinstitutionen

Im vergangenen Jahr beobachtete SIX, dass die Mehrzahl der Cyberangriffe im Finanzsektor gegen grosse Retailbanken gerichtet war. Angesichts der relativ geringen Anzahl grosser Retailbanken in der Schweiz im Vergleich zu anderen europäischen Ländern könnte dieser Faktor die Beobachtung von wenigen Cyberangriffen gegen Schweizer Finanzinstitutionen erklären. Hinzu kommt, dass die Cyber-Security-Regulierung in der Schweiz sehr ausgereift ist und von den Finanzinstitutionen ein hohes Sicherheitsniveau verlangt wird. Dies würde Angreifer zwar nicht unbedingt abschrecken, aber wahrscheinlich den Schaden der Angriffe minimieren.

Die Umfrage ergab aber auch, dass ein anderer Aspekt zu diesem niedrigen Niveau der beobachteten Cyberattacken beigetragen haben könnte – die eingeschränkte Transparenz der CISOs in ihren Unternehmen.

Beobachtete Vorfälle

Über 80% der Befragten beobachteten im vergangenen Jahr nur jeweils weniger als 50 Sicherheitsvorfälle, was mit der insgesamt niedrigen Zahl von Cyberangriffen auf Schweizer Finanzinstitutionen laut öffentlich zugänglichen Informationen korreliert. Die Mehrheit dieser Vorfälle waren Phishing-Angriffe.

Während die Befragten überwiegend der Meinung sind, dass die nationalen Finanzregulierungsstandards und das hohe Bewusstsein der Nutzer zu dieser niedrigen Beobachtungsrate beigetragen haben, könnten möglicherweise auch andere Faktoren verantwortlich sein. Insbesondere stellten wir fest, dass die Zahl der beobachteten Vorfälle in Unternehmen, in denen CISOs über eine hohe Transparenz im Unternehmen berichten, zunahm. In Unternehmen, in denen weniger als 50 Vorfälle gemeldet wurden, gaben umgekehrt fast 40% der Befragten an, dass sie die Transparenz als unzureichend einstufen. **Dies deutet darauf hin, dass die geringe Zahl der beobachteten Angriffe möglicherweise auf die geringe Transparenz im Unternehmen zurückzuführen ist.**

In der Umfrage baten wir die Befragten, die Transparenz der CISOs im gesamten Unternehmen von 1 (eingeschränkte Transparenz), 3 (teilweise Transparenz) bis 5 (hohe Transparenz) zu bewerten. Wie in Abbildung 19 zu sehen ist, hatten von den Befragten, die weniger als 50 Vorfälle beobachteten, mehr als 40% eine gute Transparenz in ihrem Unternehmen. Fast 30% hatten jedoch nur eine teilweise Transparenz und 9% eine geringe Transparenz. Rund 20% hatten eine hohe Transparenz.

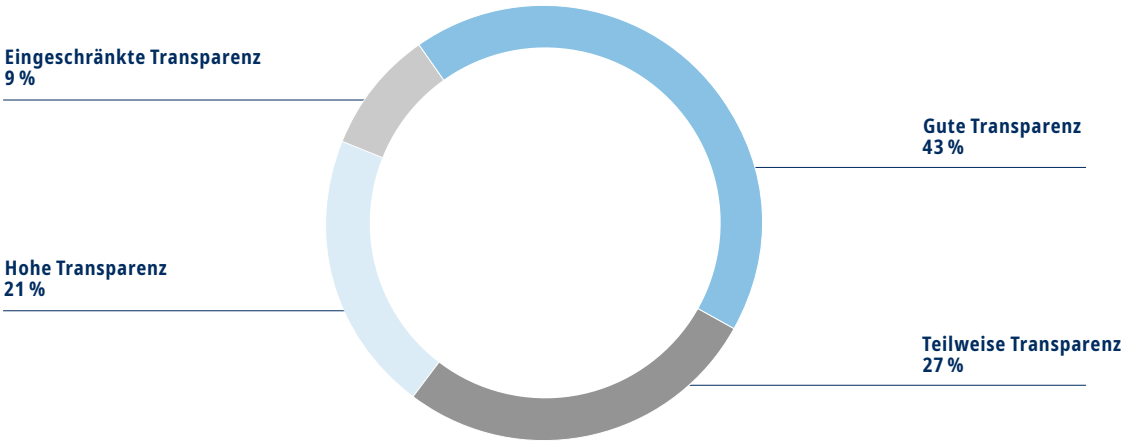


Abbildung 19 — CISO-Transparenz nach gemeldeten Vorfällen: 0 bis 50 Vorfälle gemeldet

Je höher die Zahl der beobachteten Vorfälle war, desto häufiger gaben die Befragten an, dass sie eine gute Transparenz hatten. Abbildung 20 zeigt, dass bei 51 bis 200 beobachteten Vorfällen 80% der Befragten eine gute Transparenz hatten und 20% sogar eine hohe Transparenz.

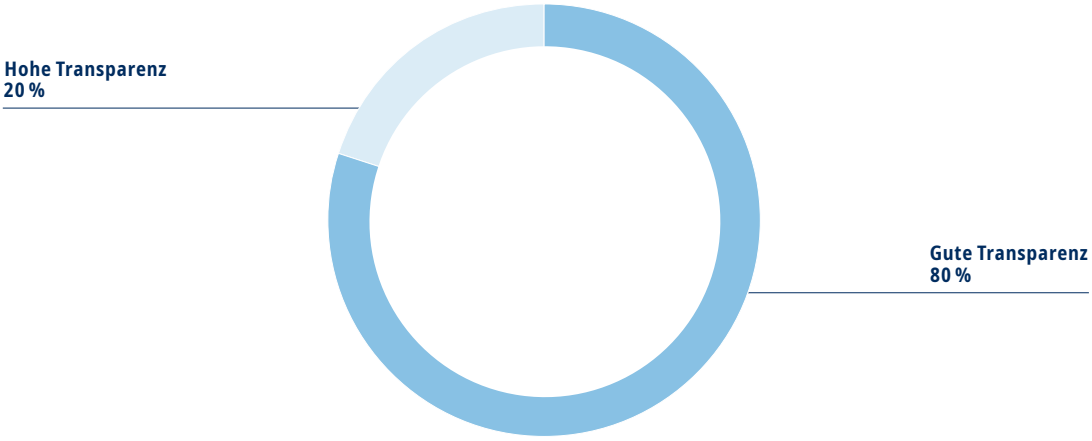


Abbildung 20 — CISO-Transparenz nach gemeldeten Vorfällen: 51 bis 200 Vorfälle gemeldet

Abschliessend ist festzustellen, dass 100% der Befragten, die mehr als 200 Vorfälle beobachteten, eine gute Transparenz aufwiesen.

Ähnliche Schlussfolgerungen können gezogen werden, wenn man die Anzahl der gemeldeten Vorfälle und den Reifegrad der CISO-Tätigkeiten analysiert. CISOs, die den Reifegrad ihrer Tätigkeiten als niedrig oder im Entstehen begriffen eingestuft haben, verzeichneten weniger Vorfälle als CISOs, die den Reifegrad als mittel oder hoch eingestuft haben. Wie in Abbildung 21 zu sehen ist, beobachteten alle Befragten, die den Reifegrad als im Entstehen begriffen einstuften, weniger als 50 Vorfälle. Befragte, die den Reifegrad als gering einstuften, sahen bis zu 200 Vorfälle. Alle Befragten, die mehr als 200 Vorfälle beobachteten, stuften den Reifegrad als mittel ein. Interessanterweise sah keiner der Befragten, die den Reifegrad als hoch einstuften, mehr als 200 Vorfälle, jedoch sahen etwa 20% jeweils weniger als 50 beziehungsweise zwischen 50 und 200 Vorfälle.

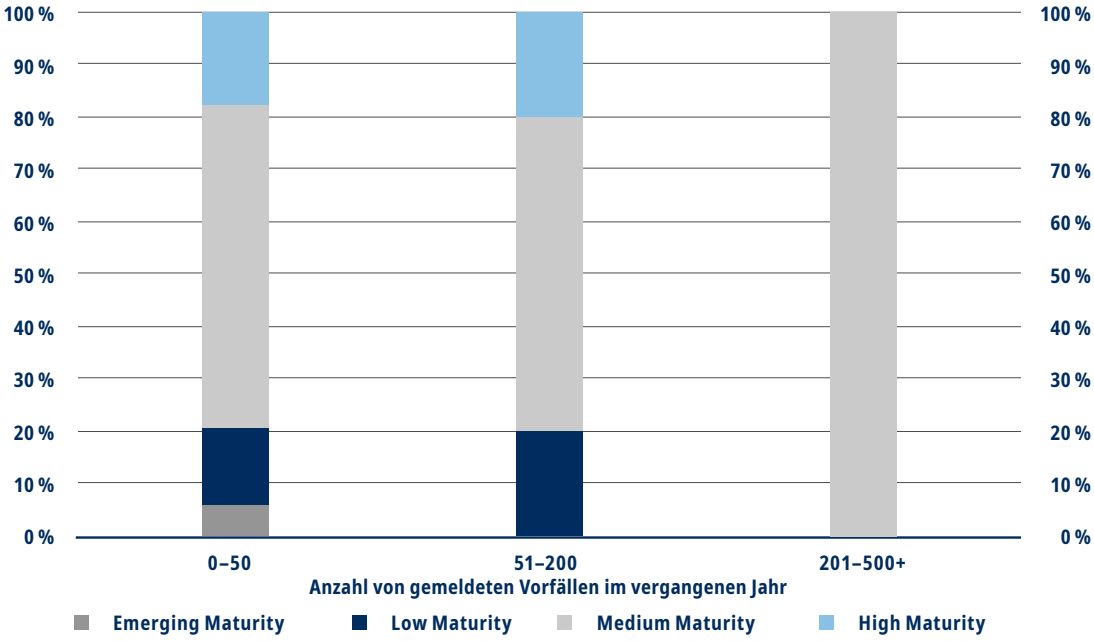


Abbildung 21 — Reifegrad nach gemeldeten Vorfällen

Die Befragten stuften die Mehrzahl der beobachteten Angriffe als weniger schwerwiegend ein als zum Beispiel Phishing-Angriffe, die Nutzung betrügerischer Websites, die den Namen der Finanzinstitution missbrauchen, oder Versuche, sich in betrügerischer Weise als Führungskräfte auszugeben. Die Befragten gaben an, dass von den beobachteten Angriffen **nur 15% bestimmten Bedrohungsakteuren zugeschrieben wurden. Dies könnte zum einen darauf hindeuten, dass die meisten Angriffe von opportunistischen Cyberakteuren ausgeführt wurden. Andererseits erfordert die Zuordnung von Angriffen zu bestimmten Akteuren Zeit und Fähigkeiten und ist nur selten eine einfache Entscheidung. Daher könnte diese Zuschreibungsrate auch aufgrund der Schwierigkeit der Zuschreibung niedrig sein.**

Nach Angaben der Befragten richteten sich 32% aller beobachteten Angriffe speziell gegen die Finanzinstitutionen, 23% gegen Kunden, etwa 15% gegen Drittanbieter und etwa 20% unterschiedslos gegen Kunden, die Finanzinstitutionen und Drittanbieter. Insgesamt gab eine Mehrheit der Befragten an, dass dieses Muster der gezielten Angriffe seit dem Vorjahr stabil geblieben sei. Etwa 30% der Befragten sahen jedoch auch eine Zunahme bei Angriffen gegen Kunden und bei willkürlichen Angriffen, die unterschiedslos auf alle abzielen.

COVID-19: Beschleunigung von Veränderungsprozessen und Intensivierung bestehender Herausforderungen

Die COVID-19-Pandemie hat sich weltweit auf alle Unternehmen ausgewirkt und unmittelbar zu neuen Angriffsflächen und zu Konsequenzen für Cyber Security geführt. Auf die Frage nach neuen Gefahren für Cyber Security gaben 75% der Befragten an, dass eine Zunahme der Arbeit im Homeoffice aufgrund von COVID-19 Anlass zur Sorge gebe(→ Abbildung 22).

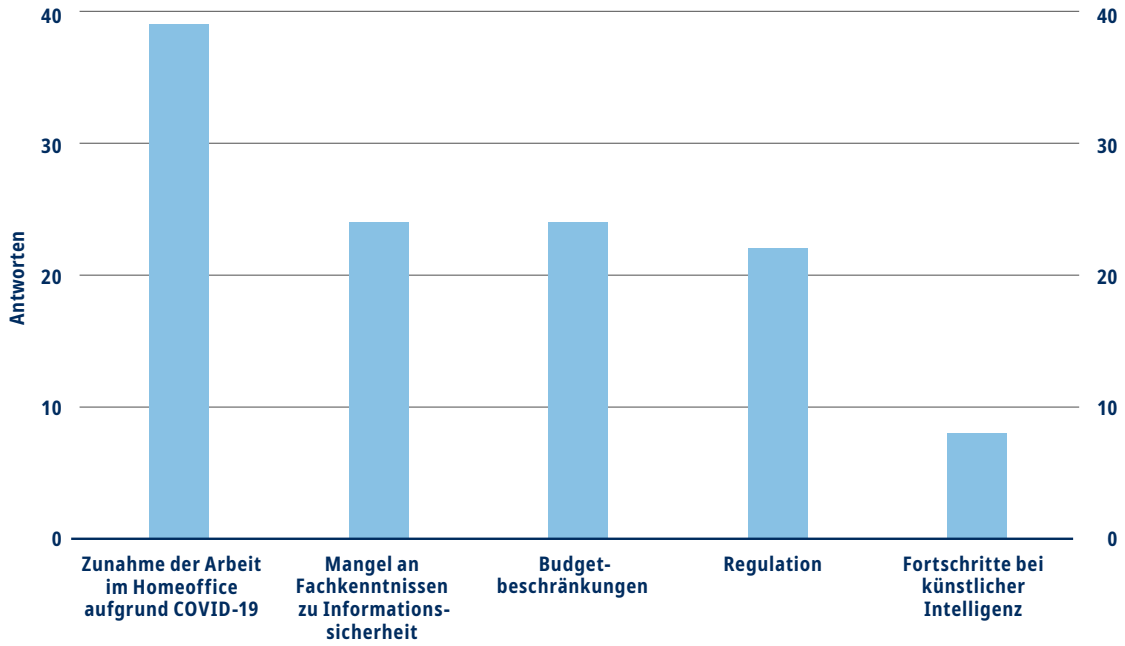


Abbildung 22 —Neue Bedrohungen im Vergleich zum Vorjahr

Dies korrelierte mit unserer Analyse der Cybervorfälle, die im letzten Jahr in Schweizer Finanzinstitutionen beobachtet wurden und die im März und April zunahmen (⟶ Abbildung 23 unten sowie den Makroteil des Berichts für weitere Informationen).

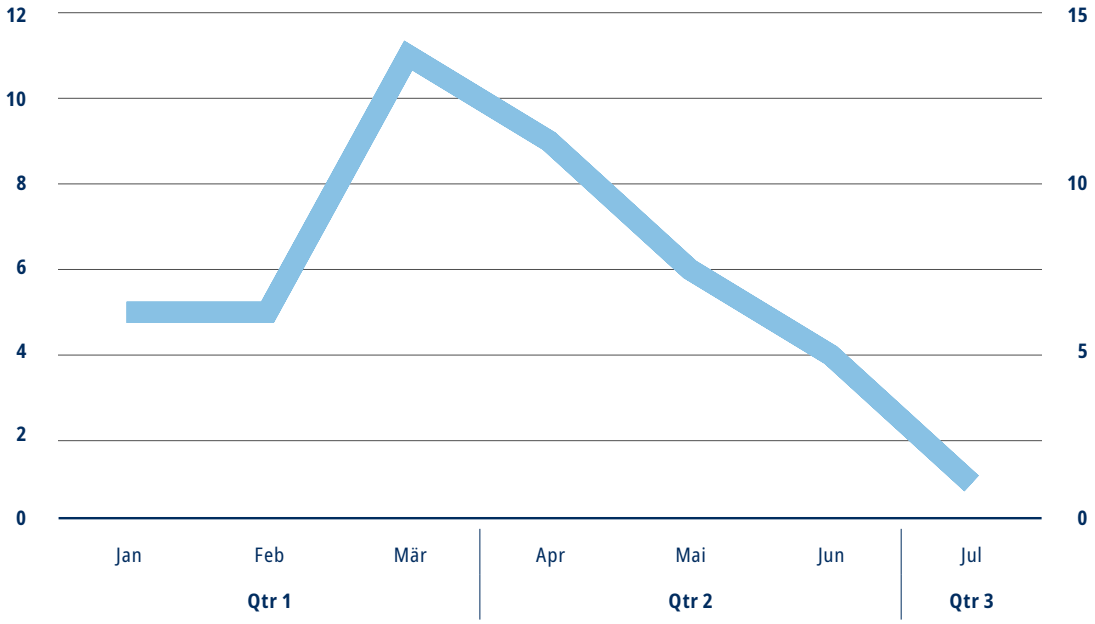


Abbildung 23 — Monatlich beobachtete Cyberangriffe

Diese Bedenken decken sich mit der seit Beginn der Pandemie beobachteten Cyberaktivität insgesamt. Die plötzliche Verlagerung auf die Arbeit im Homeoffice zwang Unternehmen, ihre Sicherheitsstrategien schnell anzupassen, um eine ununterbrochene Fortsetzung des Geschäftsbetriebs zu gewährleisten. Das schränkte wahrscheinlich die Durchführung von Sicherheitsüberwachungen durch IT-Sicherheitsteams ein. Dass schnell eine weitreichende Arbeit im Homeoffice ermöglicht wurde, führte darüber hinaus vielleicht zu einer Lockerung der Sicherheitsrichtlinien.

Cyberakteure haben versucht, diese neuen Schwachstellen auszunutzen, und haben zunehmend Mitarbeitende und die Öffentlichkeit attackiert, indem sie deren Unsicherheit und Angst missbrauchten.

DDoS:
Die Zunahme der Homeoffice-Tätigkeit beansprucht die verfügbare Bandbreite über das übliche Mass hinaus, was den Erfolg von DDoS-Angriffen wahrscheinlicher macht. Fast die Hälfte der Befragten gab an, dass die Verfügbarkeitsprobleme aufgrund einer Zunahme der Arbeit im Homeoffice ihre Bedenken bezüglich Cyber Security verstärkt haben. Darüber hinaus ist Remote-Software, wie zum Beispiel VPN, eine kritische Komponente für die Kontinuität des Geschäftsbetriebs in Heimarbeitsplätzen. Diese erhöhte Angriffsfläche aufgrund der Verwendung von Geräten wie Home-Routern oder ungesicherten Wi-Fi-Netzwerken ist für mehr als 40 % der Befragten besorgniserregend. Hinzu kommt, dass die Arbeit im Homeoffice die Installation von Sicherheitspatches an allen Endpunkten erschweren kann, wodurch Geräte anfällig für Angriffe werden. Weitere Bedenken wurden in Bezug auf die Verwendung nicht genehmigter Workaround-Lösungen von Mitarbeitenden und das Potenzial für ein erhöhtes Risiko der Datenexfiltration geäussert.

Spear Phishing:
Von den Befragten gaben mehr als 60 % an, dass COVID-19 das Risiko erhöht, dass Benutzer durch Phishing-Angriffe getäuscht werden. Seit Ausbruch der Pandemie haben Bedrohungsakteure, wie etwa Emotet[20], Hancitor[21], Trickbot[22], Netwalker[23] und Chinoxy[24], E-Mails mit dem COVID-19-Thema verwendet, um Malware zu verbreiten. Da die befragten CISOs Phishing-E-Mails und Malware bereits als die grösste Bedrohung für ihre Unternehmen betrachten, hat die COVID-19-Pandemie dieses Problem noch verschärft.

Künftige Herausforderungen identifizieren

Zusätzlich zu COVID-19 sieht fast die Hälfte der nach «neuen Bedenken» befragten CISOs den Mangel an Fachkenntnissen zu Informationssicherheit sowie Budgetbeschränkungen als Herausforderungen an. Fast 60 % der Befragten betonen auch den Bedarf an zusätzlichen Geldmitteln. Was die Entwicklung der Angriffe betrifft, so stellten die meisten Befragten fest, dass die Angriffe und Akteure immer fortgeschrittener und anspruchsvoller werden. **CISOs sind über die zunehmende Digitalisierung besorgt und, damit zusammenhängend, über den Druck, IT-Architekturen schnell anpassen zu müssen. Ebenfalls haben sie Bedenken, ob der Bedarf an qualifizierten Arbeitskräften und ausreichenden Finanzmitteln gedeckt werden kann, um diese Herausforderungen zu bewältigen.** Während diese Entwicklung bereits seit mehreren Jahren andauert, hat der Ausbruch der COVID-19-Pandemie diesen Prozess erheblich beschleunigt und die bereits bestehenden Herausforderungen hinsichtlich Cyber Security noch verschärft. Während mehr als die Hälfte der Befragten angibt, dass ihre Unternehmen bereit seien, mit Cyber-Security-Problemen umzugehen, ist mehr als ein Drittel nicht sicher, ob ihr Unternehmen in der Lage ist, sich solchen Bedrohungen zu stellen. Darüber hinaus führt die Mehrheit der Befragten jährlich unternehmensweite Sicherheitstests durch. Sicherheitstests sind wichtig, um die Angriffsfläche und potenzielle Sicherheitsschwächen zu verstehen und so Bedrohungen zu mindern. Ein Mangel an Tests könnte Einblicke in die Schwächen der Unternehmen und ihre Bereitschaft für aufkommende Bedrohungen einschränken.

20 Bleeping Computer, B2, 18 March, Trickbot, Emotet Malware Use Coronavirus News to Evade Detection

21 SANS, B2, 12 March, Hancitor distributed through coronavirus-themed malspam

22 Bleeping Computer, B2, 18 March, Trickbot, Emotet Malware Use Coronavirus News to Evade Detection

23 MalwareHunter-Team, C2, 19 March, @Malwrhunterteam

24 Sebdraven, F6, March 20, New version of chinoxy backdoor using COVID19 alerts document lure

Struktur von CISO-Tätigkeiten

Die Eidgenössische Finanzmarktaufsicht (FINMA) teilt die von ihr beaufsichtigten Finanzinstitutionen nach ihren Risikoauswirkungen in fünf Überwachungskategorien ein, wobei Kategorie 1 extrem grosse Marktteilnehmer mit sehr hohen Risiken und Kategorie 5 kleine Teilnehmer mit geringem Risiko sind. Die Befragten waren gleichmässig auf kleine, mittlere und grosse Unternehmen verteilt. Daher kann davon ausgegangen werden, dass CISOs aus allen FINMA-Kategorien an der Umfrage teilgenommen haben. Unabhängig von der Grösse ihres Unternehmens bewerteten die Befragten ihre Fähigkeiten im Bereich des CISO-Betriebs als durchschnittlich (56/100).

Bei allen Befragten bestehen die CISO-Abteilungen grösstenteils aus SOC-Teams mit mehr als 40 %, gefolgt von Incident-Response-Teams mit 30 %. Threat-Intelligence und Red-Teams machen 16 bzw. 10 % aus.

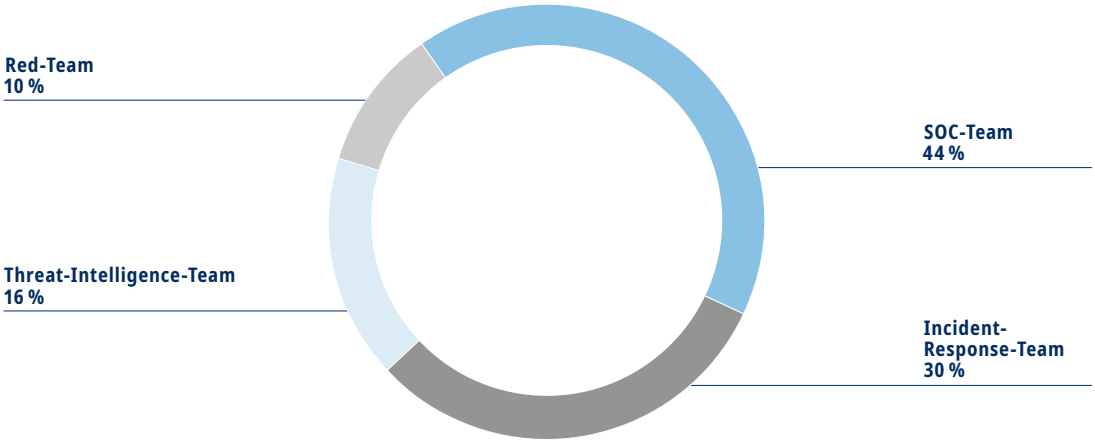


Abbildung 24 — CISO-Ressourcen nach Funktionen (Durchschnitt)

Zwar gibt es in allen Finanzinstitutionen SOC- und Incident-Response-Teams, doch die Tatsache, dass fast 90 % der Unternehmen auch über Threat-Intelligence-Teams verfügen, ist eine Anerkennung der wichtigen Rolle von Threat Intelligence im Rahmen der CISO-Tätigkeiten.

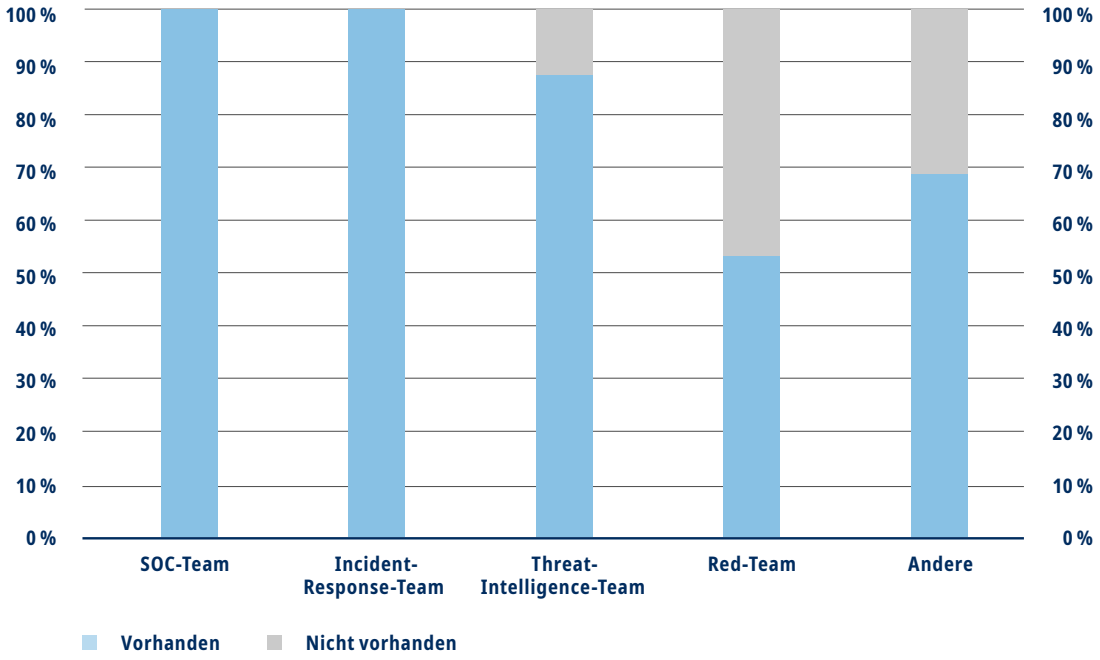


Abbildung 25 — Funktionen innerhalb der CISO-Tätigkeiten

Unabhängig von der Unternehmensgrösse blieb die Zahl der CISO-Mitarbeitenden konstant, was darauf hindeutet, dass auch kleinere Finanzinstitutionen die Informationssicherheit ernst nehmen. Wie in Abbildung 25 zu sehen ist, liegt die Zahl der CISO-Mitarbeitenden im Durchschnitt zwischen 26 und 75.

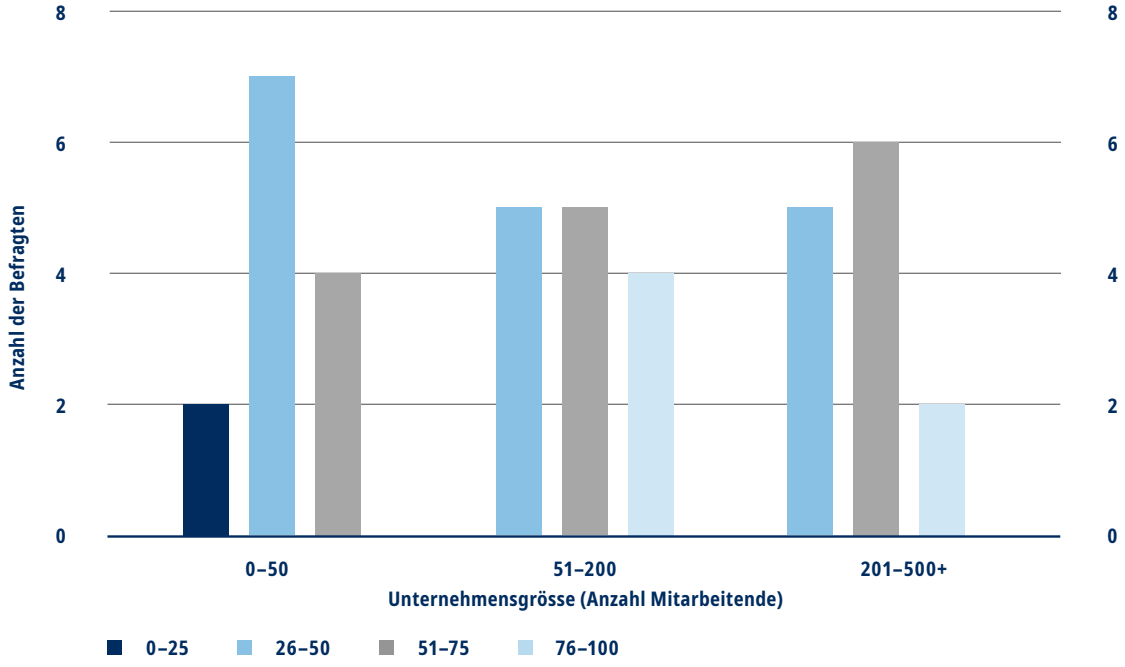


Abbildung 26 — CISO Headcount by Size of Organization Size

Die Mehrheit der Befragten bewerteten ihr Budget als angemessen (⟶ Abbildung 27).

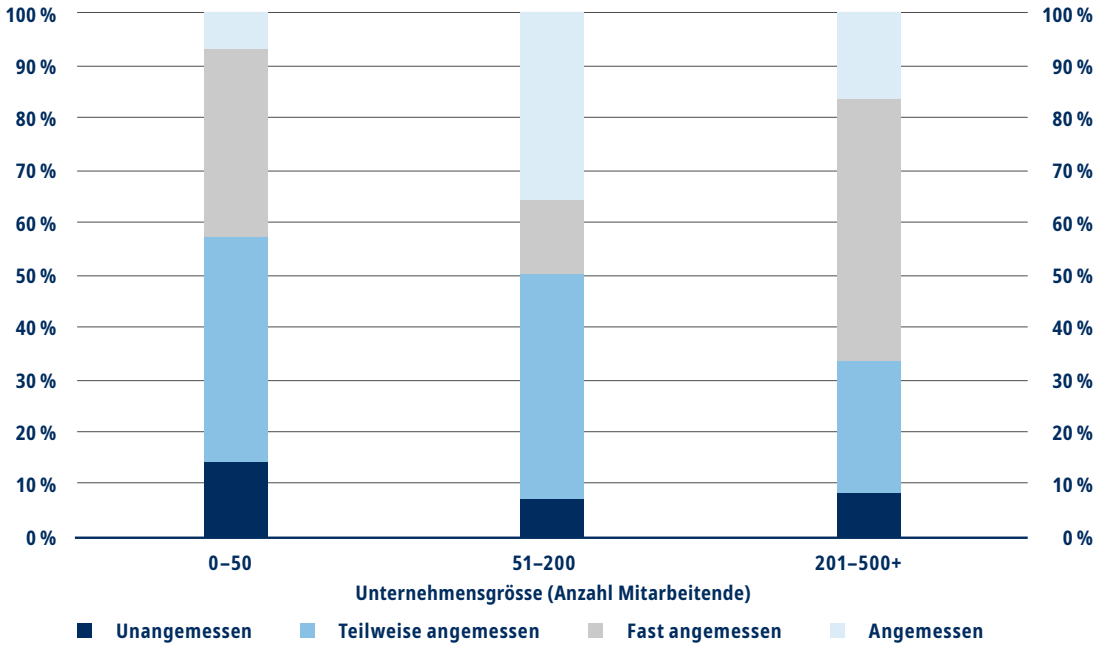


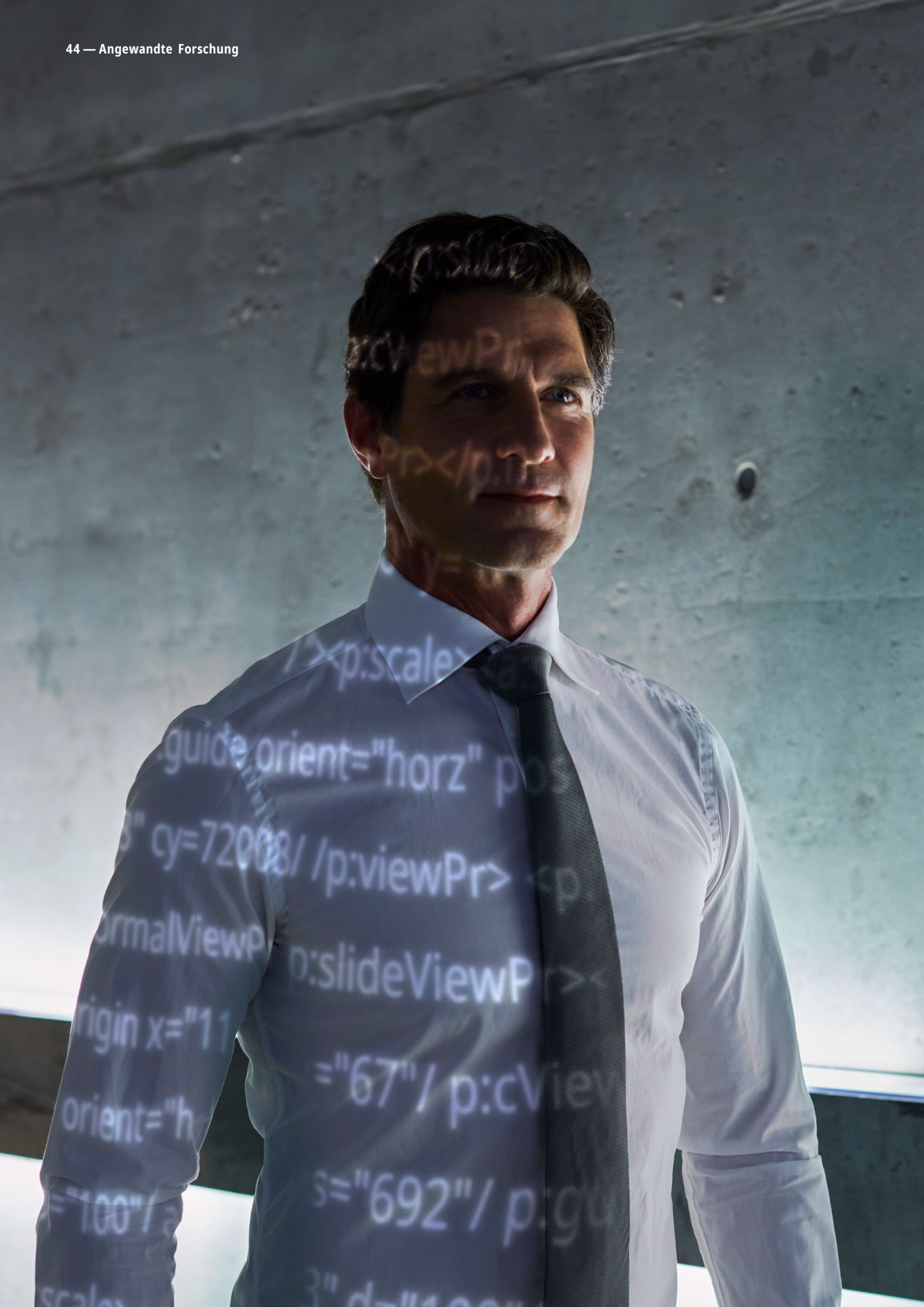
Abbildung 27 — Wahrnehmung der Budget-Angemessenheit nach Unternehmensgrösse

Während sich insgesamt jede Grösse von CISO-Team bereit fühlte, mit Bedrohungen der Cyber Security umzugehen, gaben in kleineren CISO-Teams (weniger als 10 Mitarbeitende) mehr Befragte an, sie seien nicht vorbereitet oder unsicher.

Zusammenfassung

Die Umfrage, die diesem Bericht zugrunde liegt, bot hochinteressante Einblicke in die Cyberbedrohungs-Landschaft des Schweizer Finanzsektors. Die von den Befragten identifizierten grössten Cyberbedrohungen sind Cyberangriffe wie Phishing und Ransomware sowie die Bedrohungen gegen die Cloud. Dies korreliert mit unserer Analyse der gemeldeten Vorfälle des vergangenen Jahres. Darüber hinaus hat die mit COVID-19 zusammenhängende Verlagerung auf Arbeit im Homeoffice zusätzliche Angriffsflächen geschaffen und wurde daher von den Befragten als neues Problem identifiziert. Tatsächlich beobachteten wir im März und April zeitgleich mit dem Ausbruch der Pandemie in Europa eine Zunahme der Cyberangriffe.

Ausserdem bot die Umfrage interessante Einblicke in die Zusammenhänge zwischen der Transparenz und dem Reifegrad bei CISOs sowie den beobachteten Vorfällen. Die Befragten, die die Transparenz und den Reifegrad bei CISOs höher einschätzten, beobachteten auch eine höhere Anzahl von Cybervorfällen.


orient="horz"
/p:viewPr>
p:slideViewP
="67"/ p:cV
="692"/ p:

Angewandte Forschung – SCION

In diesem Abschnitt präsentieren und erörtern wir SCION (Scalability, Control, and Isolation On Next-Generation Networks), die möglichen Auswirkungen dieser Technologie sowie ihre potenziellen Vorteile für Finanzinstitutionen. In diesem Zusammenhang bewegen wir unseren Fokus weg von Cyberangriffen und hin zur grundlegenden Kommunikationstechnologie, die der Finanzsektor tagtäglich einsetzt. SCION zielt darauf ab, die zugrunde liegenden Prozesse der Datensteuerung und -kontrolle im Internet zu verändern. Das bedeutet, dass jedes System und jede Anwendung, die auf SCION aufbaut, automatisch von den Verbesserungen dieser Technologie profitiert.

Wir geben zunächst einen kurzen Überblick über den aktuellen Umsetzungsstand von SCION, um die Relevanz dieser Technologie für den Finanzsektor zu unterstreichen. Anschliessend beleuchten wir ihre Entstehungsgeschichte, die wesentlichen Veränderungen, die sie im Vergleich zum derzeitigen Internet bewirkt, und wie eine solche neue Internetarchitektur dazu beitragen kann, die Cybersicherheitslage zu verbessern.

Scalability, Control, and Isolation On Next-Generation Networks

Den Fokus von Cyberangriffen wegbewegen, hin zur grundlegenden Kommunikationstechnologie

SCION und der Schweizer Finanzsektor

Das native SCION-Netzwerk erstreckt sich über zwei Kontinente. Verschiedene Internetanbieter (Internet Service Providers, ISPs) bieten ihren Kunden SCION-Verbindungen an. Mehrere Schweizer Banken, das Eidgenössische Departement für auswärtige Angelegenheiten und einige grosse Unternehmen nutzen SCION im Produktionsdatenverkehr.

Der Finanzsektor muss eine Vielzahl von Hürden überwinden, um das Internet im täglichen Geschäft einsetzen zu können, insbesondere in Bezug auf Verteilung, Flexibilität und Sicherheit. Das Internet ist verwundbar gegenüber Cyberangriffen, einschliesslich Distributed-Denial-of-Service-Attacken (DDoS-Attacken) und Datenverkehrsumleitungen (Stichwort BGP Hijacking). Das hat dazu geführt, dass die Schweizer Finanzinstitutionen für kritische Dienstleistungen wie das Schweizer Bezahlsystem dedizierte Kommunikationsdienste nutzen – beispielsweise das Finance IPNet. Die Einführung eines hochsicheren, flexiblen und effektiven Kommunikationssystems könnte eine Alternative zum Finance IPNet ergeben. Diese würde die Kontrolle über den Austausch von Finanzinformationen zwischen Marktteilnehmern verbessern und gleichzeitig den Implementationsaufwand reduzieren.

SIX arbeitet eng mit der Schweizer Nationalbank und anderen Partnern zusammen, um in einem Pilot-Projekt SCION-basierte Alternativen zum Finance IPNet zu implementieren. Die mögliche Alternative würde alle Vorzüge von SCION mitbringen, zum Beispiel die vollständige Kontrolle über die Pfade von Datenpaketen (die z. B. die Schweiz nicht verlassen sollen). Einige weitere Vorteile sind in den folgenden Abschnitten beschrieben. Seit August 2017 ist SCION zudem bei einer grossen Schweizer Bank im Einsatz, die eine Zweigstelle ausschliesslich über SCION an ihr Rechenzentrum angebunden hat.

Entstehungsgeschichte und Motivation für SCION

Ursprünglich wurde das Internet um 1970 als kleines Forschungsnetzwerk entwickelt; inzwischen ist es zu einer systemkritischen Infrastruktur geworden, die täglich Milliarden von Menschen benutzen. Trotzdem haben sich die grundlegenden Mechanismen seit Jahrzehnten kaum verändert. Dank der langen Historie des Internets sind seine Protokolle und ihr Einsatz optimiert und vielfach getestet worden. Allerdings gibt es auch einen grossen Nachteil. Zu der Zeit, als die Internetprotokolle entwickelt wurden, kannten sich die meisten Internetanwender und vertrauten sich gegenseitig; kaum jemand konnte sich vorstellen, dass das Internet seine heutigen Dimensionen erreichen würde. Dass während der letzten zwei Jahrzehnte die Zahl der Cyberangriffe dramatisch zugenommen hat, macht offensichtlich, dass nicht alle Internetanwender vertrauenswürdig sind. Als Reaktion darauf wurden dem Internet-Ökosystem Sicherheitsmechanismen hinzugefügt, die allerdings nur teilweise die immer ausgeklügelteren Angriffe abwehren konnten.

Mehrere Schweizer Banken, das Eidgenössische Departement für auswärtige Angelegenheiten und einige grosse Unternehmen nutzen SCION im Produktionsdatenverkehr

Seit August 2017 nutzt eine Zweigstelle einer grossen Schweizer Bank ausschliesslich SCION

Die dramatische Zunahme der Cyberangriffe während der letzten zwei Jahrzehnte zeigt, dass nicht alle Internetanwender vertrauenswürdig sind

Diese unbefriedigende Situation war Anlass für Forschungsarbeiten zu komplett neuen Internetarchitekturen. Im Jahr 2009 begann Adrian Perrig, damals Professor an der Carnegie Mellon University und mittlerweile Professor an der ETH Zürich, an einer solchen neuen Internetarchitektur zu arbeiten. Sie trägt mittlerweile den Namen SCION und verfolgt das klare Ziel, viele der Sicherheitsprobleme des heutigen Internets grundlegend zu lösen. Heute arbeiten über 60 Forscher auf der ganzen Welt aktiv an der Entwicklung, Implementierung, Validierung und dem Einsatz von SCION.

Technischer Hintergrund von SCION

Das Internet ist im Wesentlichen ein Netzwerk, das wiederum aus zahlreichen kleineren, unabhängigen Netzwerken, sogenannten autonomen Systemen (ASes) besteht. Beispiele für ASes sind ISPs, Universitäten und grosse Informationsanbieter. All diese ASes kontrollieren ihre eigenen Netzwerke unabhängig voneinander. An verschiedenen Verknüpfungsstellen verbinden sie sich mit anderen ASes und tauschen Daten aus, um eine globale Konnektivität zu erreichen.

SCION verändert diese grundlegende Struktur des Internets nicht, unter anderem, um die Einführung der neuen Architektur zu erleichtern. Die ASes können ihre interne Infrastruktur beibehalten. Allerdings fasst SCION als Ergänzung zu dieser Struktur mehrere ASes zu unabhängigen Gruppen mit gemeinsamen Vertrauensankern zusammen, sogenannte Isolationsdomänen (ISDs), beispielsweise innerhalb eines Landes.

Das Routing-Protokoll (der Prozess, durch den im Internet Pfade zwischen verschiedenen Teilnehmern gefunden werden) profitiert von dieser zusätzlichen Struktur, die im Vergleich zum heutigen Internet für bessere Skalierbarkeit und mehr Sicherheit sorgt. Einerseits ermöglichen ISDs eine Aufteilung des Routing-Protokolls in einen Teil innerhalb einer ISD und einen Teil zwischen den ISDs. Das verringert die Komplexität insgesamt. Andererseits garantiert die Isolation des Routing-Prozesses innerhalb einer ISD, dass die Auswirkungen von Fehlkonfigurationen und Routing-Angriffen lokal begrenzt bleiben. Zudem sind alle Routing-Nachrichten basierend auf einer sicheren, aber flexiblen Public-Key-Infrastruktur (PKI) authentifiziert. Darin kann jede ISD selbstständig ihre eigenen Vertrauensanker wählen. Das ermöglicht Netzwerk-Souveränität, da Netzwerk-Teilnehmer selbst festlegen können, welchem Anker sie bei der Verifizierung vertrauen wollen. Ausserdem vermeidet es globale «Kill Switches», die in einigen heutigen Sicherheitsmechanismen de facto existieren. Folglich bietet die SCION-Architektur allein durch ihren Aufbau sowohl eine hohe Belastbarkeit als auch Sicherheit.

Im Jahr 2009 begann Adrian Perrig an einer neuen Internetarchitektur zu arbeiten

Das Internet ist ein Netzwerk, das aus zahlreichen kleineren, unabhängigen Netzwerken, sogenannten autonomen Systemen (ASes), besteht

SCION fasst als Ergänzung zu dieser Internetstruktur mehrere ASes zu unabhängigen Gruppen mit gemeinsamen Vertrauensankern zusammen, sogenannte Isolationsdomänen (ISDs)

Alle Routing-Nachrichten basieren auf einer sicheren, aber flexiblen Public-Key-Infrastruktur (PKI)

Zusätzlich zum Routing-Protokoll und anderen Hintergrundprozessen verändert SCION auch die Art und Weise, wie Daten gesendet und weitergeleitet werden. Im heutigen IP-basierten Internet können die Anwender lediglich den Absender und Empfänger von Datenpaketen festlegen. Über den Weg, den ihre Daten nehmen, haben sie jedoch keine Kontrolle – dieser wird vom Netzwerk gewählt und bleibt den Anwendern verborgen. Mit SCION haben die Anwender dagegen die Möglichkeit, die Pfade der einzelnen Datenpakete auszuwählen; diese sind dann explizit in den Paketen aufgeführt, was wiederum eine vereinfachte Weiterleitung auf den dazwischenliegenden Routern ermöglicht. Durch den Einsatz integrierter kryptografischer Mechanismen in SCION behalten ASes die Kontrolle darüber, welche Pfade von den Anwendern benutzt werden können.

Es gibt darüber hinaus Erweiterungen zum grundlegenden SCION-Konzept, die unter anderem die Authentifizierung von Datenquellen oder die Reservierung von Bandbreite ermöglichen. Diese zusätzlichen Eigenschaften ermöglichen die Verteidigung gegen die meisten DDoS-Szenarien. Zum Beispiel können Verbindungen mit reservierter Bandbreite nicht durch nicht-reservierte volumetrische DDoS-Angriffe beeinträchtigt werden. Da diese Funktionen auf normalen SCION-Internetverbindungen verfügbar sein könnten, wären dedizierte Verbindungen (z. B. mit MPLS) in vielen Szenarien nicht weiter erforderlich. Das würde Kosten sparen, die Flexibilität erhöhen und die Redundanz bei Uplink-Verbindungen reduzieren.

Betrachten wir zunächst ein Unternehmen, das regulatorisch verpflichtet ist, sicherzustellen, dass gewisse Daten die Schweiz nicht verlassen können. Dieses Unternehmen kann das heutige Internet nicht nutzen, um diese Daten auszutauschen, da es keinerlei Kontrolle über den Transferpfad der Datenpakete hat. **Im Gegensatz dazu kann das Unternehmen mit SCION sein System einfach so konfigurieren, dass nur Pfade innerhalb der Schweizer ISD erlaubt sind. So stellt das Unternehmen sicher, dass die Daten das Land nicht verlassen.**

Als zweites Beispiel nehmen wir ein europäisches Unternehmen, das Finanzdaten aus Südkorea sammelt und verarbeitet. Im heutigen Internet wird Datenverkehr zwischen Europa und (Süd-) Ostasien meist über die USA geleitet. Das ist ein beträchtlicher Umweg und kann zu einer Latenz von etwa 300 Millisekunden führen. **SCION erlaubt es dagegen, die direkte Ostroute zu wählen, wo die Latenz mit etwa 200 Millisekunden um ein Drittel geringer ist.**

Fazit

Einige der meistgenannten Bedrohungen in diesem Report wie Phishing, Malware und Ransomware stellen Angriffe auf der Applikationsebene dar, wo die unmittelbaren Vorteile von SCION weniger offensichtlich sind. Bei anderen Bedrohungen wie Routing- und DDoS-Angriffen bringt SCION jedoch bedeutende und unmittelbare Verbesserungen. Die positiven Effekte von SCION beschränken sich nicht auf bestimmte Angriffsszenarien und sein Hauptzweck besteht darin, die Kontrolle des Datenverkehrs zu erweitern. Die Konzepte der Isolation Domains und der Pfadauswahl geben sowohl Absendern als auch Internetanbietern die Möglichkeit, sehr genau festzulegen, wie Daten durch das Netzwerk fliessen. Verschiedene Erweiterungen schützen zusätzlich vor sehr ausgeklügelten Cyberangriffen.

Seit 2009 ist SCION von einem rein akademischen Projekt zu einem System mit Implementierung in Produktionsqualität und weltweitem Einsatz gereift. Es löst schon lange bestehende Probleme wie die Erreichung von Verfügbarkeitsgarantien in einem öffentlichen Netzwerk. Solche waren bisher nur in geschlossenen, privaten Netzwerken erhältlich. Was als faszinierende Idee vor mehr als zehn Jahren begann, ist heute Realität und bereits jetzt für den praktischen Einsatz in vielen Unternehmen verfügbar.

SIX
Cyber Security Hub

Ausgerichtet auf den Schweizer Finanzsektor, informiert der SIX Cyber Security Hub Banken und Versicherungen zuverlässig und relevant über aktuelle Gefahren und gefährliche Entwicklungen im Bereich Cyber Security.

Die Zusammenarbeit der beteiligten Unternehmen verbessert den Schutz vor Cyberrisiken und Cyberangriffen – ein wichtiges Fundament für die Attraktivität und Stabilität des Schweizer Finanzsektors.

↪ Die zentralen Elemente des SIX Cyber Security Hub sind:

- Austausch von Informationen und Erfahrungen
- Erörterung und Umsetzung koordinierter Massnahmen im Fall von Angriffen und anschliessende Evaluation

Eine gemeinsame Plattform, entwickelt und verwaltet von einem unabhängigen Anbieter, ist dafür unabdingbar. SIX ist die zentrale Infrastruktur-Providerin des Schweizer Finanzsektors und Cyber Security eine unserer Kernaufgaben.

Um die systemkritische Infrastruktur des Schweizer Finanzsektors zu sichern, hat SIX ein Security Operations Center (SOC) aufgebaut. Es arbeitet rund um die Uhr (24x7x365) und nutzt eine einzigartige, branchenspezifische Threat-Intelligence-Technologie. Eine wichtige Aufgabe ist dabei die stetige Aktualisierung der Anwendungsfälle mit optimierten Erkennungsregeln, die mit den neuesten Erkenntnissen zur aktuellen Bedrohungslage speziell darauf ausgerichtet sind, Risiken für den Schweizer Finanzsektor zu identifizieren und zu minimieren.

Das gesamte Wissen aus dem SOC fliesst in den SIX Cyber Security Hub mit ein, sodass alle Mitglieder von den Erfahrungen der Community profitieren.

An wen richtet sich das Angebot?

Besonders kleine und mittlere Banken und Versicherungen haben davon einen deutlichen Nutzen. Ihre Ressourcen reichen für solche Tätigkeiten neben der Abarbeitung von Sicherheitsvorfällen oftmals nicht aus. Das SOC von SIX greift auf eine Vielzahl nationaler und internationaler Quellen zurück, selektiert und bewertet die Informationen und bereitet sie einfach verständlich für alle Teilnehmer des Schweizer Finanzsektors auf.

Aufgrund der sich laufend ändernden Angriffsmuster hat SIX ein eigenes Rechercheteam eingerichtet, das sich ausschliesslich dem Sammeln, Analysieren und Bereitstellen dieser Sicherheitsinformationen widmet.

Was bietet der Cyber Security Hub?

Der Hub stellt spezifisch für die Zielgruppen – Banken und Versicherungen – aufbereitete, relevante und detaillierte Informationen zum Thema Cyber Security bereit. Diese decken drei Bereiche ab:

- **Strategisch:**
  Threat Landscape Report zum strategischen Briefing von Entscheidungsträgern
- **Taktisch:**
  umfassende Bibliothek mit Best Practice Use Cases und Playbooks von SIX und weiteren Teilnehmern
- **Operativ:**
  Bedrohungsinformationen (Indicators of Compromise) von SIX und weiteren Teilnehmern, die die Systeme lesen können

Ihre Vorteile

«Als CEO/CIO stärke ich die Mitarbeitenden meines Sicherheitsteams, erleichtere die Vernetzung mit Kollegen und verbessere insgesamt die Cyber-Resilienz meiner Organisation.»

«Als CISO/CRO erhalte ich aufbereitete Informationen für die Führungsebene, sodass ich über die aktuellen Trends und Entwicklungen jederzeit im Bilde bin. Das erlaubt mir, die Risikoabwehr und die Abwehraktionen richtig zu priorisieren.»

«Als Leiter SOC erhalte ich Informationen, die für Banken und Versicherungen relevant sind. Das ermöglicht mir, im Risikomanagementprozess kurz- und mittelfristig die richtigen Fokuspunkte zu setzen.»

«Als Security Analyst erhalte ich Informationen über Cyberrisiken, Cybergefahren und Cyberangriffe, die ich für die Echtzeitabwehr nutzen kann. Ich muss mich nicht um die Qualität und die Aktualität der verschiedenen Quellen kümmern.»

SIX
Pfingstweidstrasse 110
Postfach
CH-8021 Zürich

T +41 58 399 2111
securityhub@six-group.com
www.six-group.com

#discoverSIX