Cyber Security Report 2019

Grusswort

Liebe Leserin, lieber Leser

Das Schweizer Banking gibt es bereits seit dem ausgehenden 14. Jahrhundert. Mit der Entstehung des modernen Bankensystems ab 1850 kristallisierten sich unsere Stärken immer mehr heraus: Stabilität und Sicherheit. Heute, im 21. Jahrhundert, sind diese Stärken wichtiger als je zuvor. Denn Cyberkriminalität gilt als eines der wichtigsten operationellen Risiken unserer Branche. Um dieses Risiko in den Griff zu bekommen, müssen wir als Finanzplatz Schweiz unsere Kräfte bündeln. Zusammenarbeit ist das Stichwort. Beim Thema Cyber Security dürfen wir keinen Unterschied zwischen gross und klein, zwischen Banken und Versicherungen machen. Wir müssen gemeinsam handeln. Und das darf keine Floskel bleiben. Wir als SIX sind bereit, die Finanzplatzakteure in ihren Anstrengungen zu unterstützen.

Der vorliegende SIX Cyber Security Report zeigt das Potenzial einer solchen Zusammenarbeit deutlich auf: Die Fixkosten in der Cyber-Abwehr sind sehr hoch, es gibt einen akuten Fachkräftemangel und tendenziell zu wenig Austausch zwischen den Banken. SIX investiert kontinuierlich in die Sicherheit, um Cyber-Risiken für unsere systemkritischen Infrastrukturen zu minimieren. So können Banken und Versicherungen ihr Sicherheitsversprechen gegenüber ihrer Kundschaft schon heute wahren. Mit dem vorliegenden Cyber Security Report von SIX wollen wir einen Impuls zum besseren Austausch innerhalb der Branche geben. Ähnlich wie mit unserem SIX Cyber Security Hub, dem Treffpunkt der hiesigen Cyber Security Community, über den Sie auf Seite 8 mehr erfahren. Treten Sie mit uns in Kontakt – wir reden gerne über Cyber Security.

Ich wünsche Ihnen eine spannende Lektüre.

Jos Dijsselhof
CEO SIX

Inhaltsverzeichnis

Einleitung **6**
Warum dieser Report 7
Mitwirkende 8
Methodik 9

Makroanalyse: Ländervergleich **10**
Schweiz 12
Singapur 13
Vereinigtes Königreich 14
Vereinigte Staaten 15
Deutschland 16
Niederlande 17
Frankreich 18

Mikroanalyse: der Schweizer Finanzsektor **20**
Wesentliche Ermessungsentscheide 20
Vergleich der Schweiz mit ihren Nachbarn 21
Vermögensverwaltung und Private Banking in der Schweiz: gegen gezielte Angriffe gefeit? 21
Über die Organisationsgrenzen hinaus: Kunden und Partner schützen 22
Ausgewählte Erkenntnisse 22
Tier-3-Organisationen 23
Tier-2-Organisationen 24
Tier-1-Organisationen 25

Fazit **26**

Zusammenfassung

Dieser Bericht beleuchtet, in welchem Ausmass die Schweizer Finanzdienstleistungsbranche verschiedenen Cyber-Risiken ausgesetzt ist.

Er konzentriert sich dabei auf zwei Aspekte: Zum einen vergleicht er die Schweiz mit internationalen Nachbarn, die gleichwertige oder bedeutendere Finanzdienstleistungssektoren haben. Zum anderen kategorisiert er die Schweizer Finanzdienstleistungsbranche nach Sektoren und Geschäftstypen und untersucht, wo sich die Cyber-Bedrohungen konzentrieren und wo die Risiken am ausgeprägtesten sind.

Der erste Teil – die Makroanalyse – stützt sich hauptsächlich auf Daten, die aus Open-Source-Quellen stammen. Für den zweiten Teil – die Mikroanalyse – trug der Bericht Informationen aus erster Hand von Mitgliedern des SIX Cyber Security Hub zusammen.

Der Report zeigt, dass die untersuchten Länder in den letzten zwölf Monaten immer wieder Cyber-Angriffe registrierten, die ausdrücklich auf ihr Finanzdienstleistungs-Ökosystem ausgerichtet waren. Darüber hinaus gibt es Hinweise darauf, dass hoch entwickelte Gruppen von Cyber-Kriminellen ihre Angriffe auf ganz bestimmte Unternehmen in der Finanzdienstleistungsbranche konzentrieren; von diesen Gruppen gingen hauptsächlich gezielte Angriffe aus. Die nennenswertesten Beispiele stammten dabei von Gruppen, von denen wir wissen, dass sie in Nordkorea oder Russland ansässig sind.

Unseren Analysen zeigten, dass die Gesamtheit der Cyber-Angriffe entweder exponierte Netzwerke und nicht gepatchte Sicherheitslücken ausnutzten oder als weit gestreute Angriffe im Finanzsektor ausgelegt waren. Banking-Trojaner, Crypto-Miner und mobile Malware waren dabei weiterhin die von den Bedrohungsakteuren bevorzugten Malware-Gattungen.

Unter Berücksichtigung der Besonderheiten des Schweizer Finanzsektors zeigt die Analyse, dass wir jedes Unternehmen einer von drei Kategorien (Tiers) zuordnen können, welche die Bedrohungen charakterisieren, denen die Unternehmung ausgesetzt ist.

Ausgehend von der Kategorie mit der geringsten Vielfalt an Bedrohungen erweitert jede Kategorie diese Menge durch zusätzliche Bedrohungen in direktem Zusammenhang mit ihrem Tätigkeitsprofil auf dem Finanzmarkt. Insgesamt verursachen Phishing-Bedrohungen die höchste Anzahl von Vorfällen, wobei auch zu beobachten ist, dass die Menge an zielgerichtetem Phishing im Vergleich zu nicht zielgerichtetem Phishing je nach Kategorie variiert.

Dieser Bericht wurde von SIX unter Mitwirkung von Sicherheitsforschern des Threat-Intelligence-Spezialisten Recorded Future verfasst.

Die Ergebnisse im Überblick

- Die Finanzdienstleistungsbranche ist nach wie vor ein attraktives Ziel für Cyber-Kriminelle.
- Die wichtigsten Bedrohungsakteure sind Cyber-Kriminelle, die auf Profit aus sind, und staatlich unterstützte Akteure, die sich Wettbewerbsvorteile verschaffen wollen.
- Von allen Malware-Familien hatten Banking-Trojaner, Crypto-Miner und mobile Malware im vergangenen Jahr die grössten Auswirkungen auf die Finanzdienstleistungsbranche.
- Ein Grossteil der Konversationen im Darkweb, die sich auf Angriffe auf Finanzdienstleistungsunternehmen bezogen, beschränkte sich auf die folgenden vier Foren: Offensive Community, Raid Forums, Gaza Hacker Team Forum und Bits Hacking Forum. Die Bedrohungsakteure, die auf solchen Plattformen agieren, unterscheiden sich im Grad ihrer Ausgereiftheit.
- Im Jahr 2018 verursachte der Datendiebstahl per PoS-Malware (Point of Sale) E-Commerce-Organisationen und Online-Zahlungssystemen neben Reputationsschäden auch finanzielle Verluste in Millionenhöhe.
- Das aktuelle Wachstum in den Bereichen Internet der Dinge (IoT), Mobiltechnologie und Cloud Computing wird die Angriffsfläche von Finanzdienstleistern – also die Zahl der potenziellen Angriffspunkte – in den kommenden Jahren deutlich vergrössern.
- Hinweise auf Cyber-Vorfälle in der Finanzdienstleistungsbranche haben sich im Lauf des vergangenen Jahres verdoppelt, wahrscheinlich als Folge der schwerwiegenderen Bedrohung durch mobile Malware. Cyber-Kriminelle können mobile Malware in Untergrundforen inzwischen leichter und billiger erstehen.

Warum dieser Report

Ginni Rometty, CEO und Präsidentin von IBM, formulierte bereits im Jahr 2015: «Cyberkriminalität ist die global grösste Gefahr für alle Unternehmen». Bei der Abwehr dieser Gefahr sind der langjährigen Erfahrung von SIX nach zwei Elemente absolut zentral: Der Schutz gegen Cyber-Angriffe muss sowohl umfassend als auch kontinuierlich sein. Nur so lässt sich die Bedrohungslage in den Griff bekommen. Unter umfassend verstehen wir dabei nebst der technischen Betrachtung vor allem auch die Nähe zum Geschäftsfeld: Die Bankeninfrastruktur ist besonders systemkritisch und muss dementsprechend sorgfältig geschützt werden. Kontinuierlich bedeutet, dass Schutz und Abwehr rund um die Uhr an jedem Tag des Jahres präsent und innert kürzester Zeit verfügbar sind.

Auf diese beiden Grundprinzipien stützen sich die vier Pfeiler der Cyber Security Services von SIX:

1. **Von Banken für Banken.** Die systemrelevante Infrastruktur von SIX unterliegt staatlicher Aufsicht und Überwachung. Darum verstehen wir die Bedürfnisse unserer Kunden aus dem Banken- und Versicherungsbereich im Detail und kennen auch die hohen Anforderungen seitens des Regulators.

2. **1+1=3.** Der Skaleneffekt ist im Bereich Cyber Security enorm: Ob für eine Bank oder 20 Banken, der Schutz erfordert fast die gleiche Infrastruktur. Deshalb macht es für Finanzinstitute Sinn, diese Tätigkeit, die nicht zu ihrem Kerngeschäft gehört, an einen Experten auszulagern. Dank des grösseren Volumens kann SIX ein breiteres Angebot zur Verfügung stellen, das die Schutzmassnahmen, die eine Bank für sich selbst umsetzen könnte, weit übertrifft.

3. **Sharing is caring.** Ein geschützter, moderierter und maximal transparenter Austausch unter Sicherheitsexperten ist im Kampf gegen die Cyberkriminalität immens wichtig. Mit dem SIX Cyber Security Hub unterstützen wir den Informations- und Erfahrungsaustausch. Auf dieser nicht-kommerziellen Kommunikationsplattform teilen und diskutieren Experten ihre Learnings, ihr Know-how sowie Informationen zu Schwachstellen und Attacken. Die Teilnehmer unterzeichnen einen Code of Conduct; so garantiert SIX die hohe Qualität der Diskussion.

4. **Die besten Arbeitskräfte.** Dem Fachkräftemangel im Bereich Cyber Security tritt SIX entgegen, indem wir Mitarbeitende bewusst und umfangreich ausbilden und schulen. Weil digitale Sicherheit zu unserem Kerngeschäft gehört und wir damit ein grosses Volumen abdecken, sind wir ein interessanter und attraktiver Arbeitgeber für Cyber Security Experten.

Mitwirkende

Der Cyber Security Report bildet das Wissen und die Expertise von SIX ab. Er analysiert und interpretiert Daten von SIX und externe Vorfälle wie Hackerangriffe, Störungen und Sicherheitsschwachstellen. Da sich Cyber Security nur beschränkt an nationale Grenzen hält, haben wir dem Vergleich der Schweiz mit dem Rest der Welt entsprechend viel Platz eingeräumt.

Am SIX Cyber Security Report 2019 haben mitgearbeitet:

- Recorded Future. Recorded Future ist ein Internet-Technologieunternehmen, das sich auf Echtzeit-Bedrohungsdaten spezialisiert hat. Recorded Future erfasst und analysiert Daten aus einer breiten Palette von technischen, offenen und Darkweb-Quellen. Diese Informationen helfen Sicherheitsteams, Cyber-Angreifern immer einen Schritt voraus zu sein.
- Mitglieder des Cyber Security Hub von SIX

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 besuchen Sie
www.six-group.com/cybersecurityhub

Methodik

SIX erfasste und analysierte für diesen Bericht in Zusammenarbeit mit Recorded Future gezielt Informationen rund um das Thema Cyber Security.

Als wichtigste Datenquellen dienten dabei die Auswertung von Open Source Intelligence (OSINT) sowie Informationen, die von Mitgliedern des SIX Cyber Security Hub zur Verfügung gestellt wurden.

Die Makroanalyse untersucht Cyber-Bedrohungen im Finanzsektor für eine Stichprobe der G20-Staaten und die Schweiz. Die Grafiken im Makrobereich zeigen die Gesamtzahl der Vorkommnisse sowie eine Stimmungslage zu Cyber-Angriffen, die auf einer Interpretation öffentlich geäusserter Meinungen – beispielsweise in Tweets – basiert.

Für die Mikroanalyse des Schweizer Finanzsektors ordnet dieser Bericht die Schweizer Finanzinstitute einer von drei Ebenen zu, basierend auf dem Haupttätigkeitsfeld der Institute (wie etwa Vermögensverwaltung).

Makroanalyse: Ländervergleich

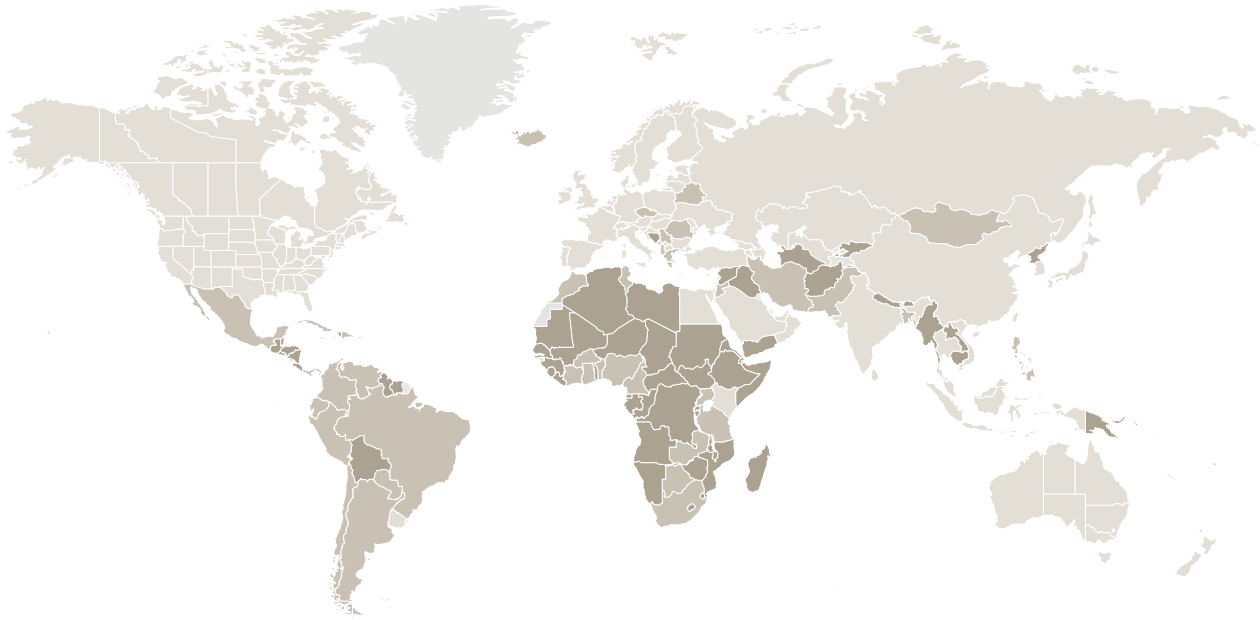
Angesichts der zunehmenden Anzahl von Cyber-Angriffen auf Unternehmen in der Finanzdienstleistungsbranche wurde im Lauf des vergangenen Jahres eine wachsende Besorgnis in der Presse, in der allgemeinen Öffentlichkeit wie auch im Finanzsektor selbst deutlich. Ein Faktor, der diese Angriffe wohl begünstigt, ist die Vielzahl von Systemen, die in der Finanzbranche tagtäglich zum Einsatz kommen und von denen viele entweder veraltet oder ungesichert sind. Darüber hinaus ist die Branche schon aufgrund der in diesen Systemen enthaltenen Zahlungsinformationen ein attraktives Ziel für finanziell motivierte Bedrohungsgruppen und Cyber-Kriminelle.

Parallel zum Anstieg krimineller Cyber-Aktivitäten war in den letzten Jahren ein weiterer Trend zu beobachten: Cyber-Angriffe in den G20-Staaten werden oft nicht in ihrem ganzen Ausmass gemeldet. So verständigten die Opfer solcher Angriffe in G20-Ländern wie Grossbritannien Schätzungen zufolge im Jahr 2017 nur in 49 % der Fälle die Finanzbehörden. Ein zentraler Mitgrund dafür ist die Tatsache, dass es keinen universellen Standard für die Meldung solcher Angriffe gibt. Hinzu kommt, dass eine zunehmende Zahl von Organisationen grenzübergreifende Geschäftsaktivitäten in mehreren G20-Ländern betreibt. Sofern strengere gesetzliche Vorschriften in einem Land dies nicht erfordern, haben Organisationen kaum einen Anreiz, Vorfälle zu melden.

Darüber hinaus zeigen sich zwischen den einzelnen G20-Ländern in Bezug auf nationale Cyber-Sicherheitsstrategien und Rechtsvorschriften im weiteren Sinne zahlreiche weitere Unterschiede, die auch Lücken offen lassen.

Die Internationale Fernmeldeunion (ITU), eine Agentur der Vereinten Nationen (UN), erstellt jährlich einen globalen Cyber Security Index, der das Engagement einzelner Länder für die Cyber Security anhand von fünf Säulen misst. Diese sind:

- der rechtliche Rahmen (bestehende Gesetze und Vorschriften)
- technische Gegebenheiten (Verteidigungstechnologien, Rahmen für die Implementierung von Standards, Einsatz von CERT- oder Incident-Response-Teams)
- organisatorische Bedingungen (nationale Strategien, Aufsichtsbehörden, Kennzahlen zur Cyber Security)
- der Aufbau von Sicherheitskapazitäten (professionelle Schulungen, öffentliche Akkreditierung, Sensibilisierungskampagnen)
- das Niveau der Zusammenarbeit im Kampf gegen Cyber-Bedrohungen (Partnerschaften zwischen öffentlichem und privatem Sektor, Teilnahme an internationalen Foren)



Länder werden nach ihrem Engagement klassifiziert: hoch, mittel, niedrig
- Länder, die in allen fünf Bereichen des Index hohes Engagement zeigen
- Länder, die komplexe Verpflichtungen eingegangen sind und sich an Cyber-Sicherheitsprogrammen und Initiativen beteiligen
- Länder, die begonnen haben, Verpflichtungen im Bereich Cyber Security einzugehen

Klassifizierung nach dem Global Cyber Security Index 2018, Quelle: ITU

Derzeit gibt es keine allgemein anerkannte Methode, um das Cyber-Risiko innerhalb des Finanzdienstleistungsbereichs einzelner Länder zu messen. Alle in der vorliegenden Makroanalyse untersuchten G20-Länder weisen jedoch ein hohes Mass an Engagement für die Sicherheit auf und erreichen offiziell das höchste Ranking innerhalb dieses Standards.

Ende 2017 versuchte die ITU einen Index zu erstellen, der die Cyber-Bedrohungsterminologie im Zusammenhang mit internationalen Bankinstituten akkurat beobachtet. Im Lauf dieses Vorhabens stellte sich heraus, dass vollständige Datensätze zu Cyber-Angriffen so gut wie nicht vorhanden sind. Zwar existieren durchaus ausgewählte öffentliche und kommerzielle Datensätze. Diese sind jedoch häufig unvollständig, haben unterschiedliche Abdeckungsgrade und verwenden unterschiedliche Definitionen für Cyber-Angriffe. Dies erschwert es letztendlich, die Schäden und Verluste zu analysieren, die durch Cyber-Vorfälle entstanden sind.

Die folgenden Abschnitte über verschiedene Länder enthalten Grafiken die wie folgt aufgebaut sind. Die Grafiken zeigen zwei Aspekte von Cyber-Angriffsaktivitäten die sich auf den Finanzsektor des jeweiligen Landes beziehen und über open source Berichte erfasst wurden. Der Balken zeigt die Gesamtzahl der erfassten Ereignisse pro Monat. Zusätzlich gibt die Markierung die am stärksten negative Stimmung an, die sich auf eines der erfassten Ereignisse bezieht (für mehr Informationen zur negativen Stimmung finden sich im Abschnitt Methodik).

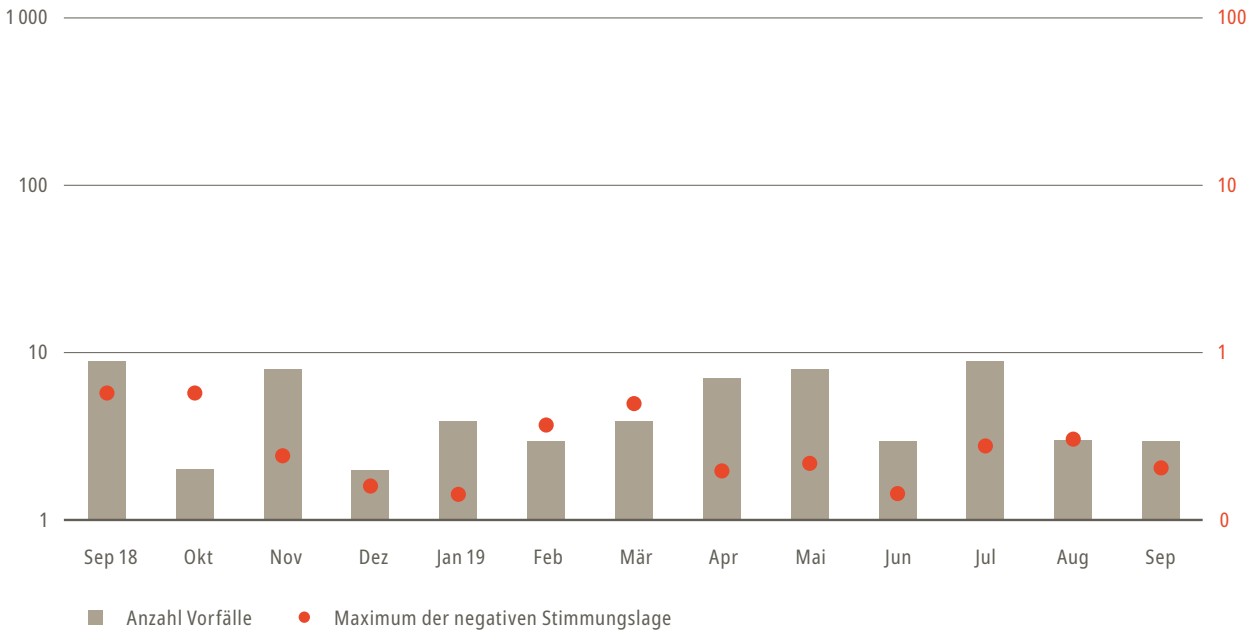
Die X-Achse unterteilt den untersuchten Zeitraum in einzelne Monate. Die Y-Achse auf der linken Seite bezieht sich auf die Balken und gibt die Gesamtanzahl der beobachteten Ereignisse an. Die Y-Achse auf der rechten Seite gibt die stärkste negative Stimmung an, die in diesem Monat erfasst wurde und ist in der gleichen Farbe gehalten wie die entsprechenden Markierungen. Wenn für einen Monat keine Markierung eingezeichnet ist, dann wurde in diesem Monat kein negative Stimmung erfasst.

Weil sich die Werte der einzelnen Länder sehr stark unterscheiden, sind beide Y-Achsen mit «komprimierten» (logarithmischen) Skalen versehen. Das bedeutet, dass der erste Abschnitt z.B. Werte zwischen 1 und 10 angibt, während der nächste gleich grosse Abschnitt Werte von 10 bis 100 zeigt. Der angezeigte Bereich beider Achsen ist ebenfalls unterschiedlich, für die Anzahl der Ereignisse liegt er von 1 bis 1000 und für die negative Stimmung von 0 bis 100.

Schweiz

Die schweizerische Finanzdienstleistungsbranche leidet auf Makroebene unter ähnlichen Cyber-Schwachstellen wie andere in diesem Bericht beschriebene Staaten. Gängige Angriffsmethoden wie gezielte Phishing-Angriffe auf Mitarbeiter mit Zugang zu kritischen Finanzsystemen geben Anlass zur Sorge. Im vergangenen Jahr haben sich Cyber-Kriminelle zudem bereit gezeigt, Malware-Varianten wie Trickbot zu aktualisieren, um Unternehmen in der Schweiz anzugreifen.

Die Grafik unterhalb zeigt die auf den Schweizer Finanzplatz bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



Cyber-Event-Chronik Schweiz (Finanzen / Banken / Versicherungen)

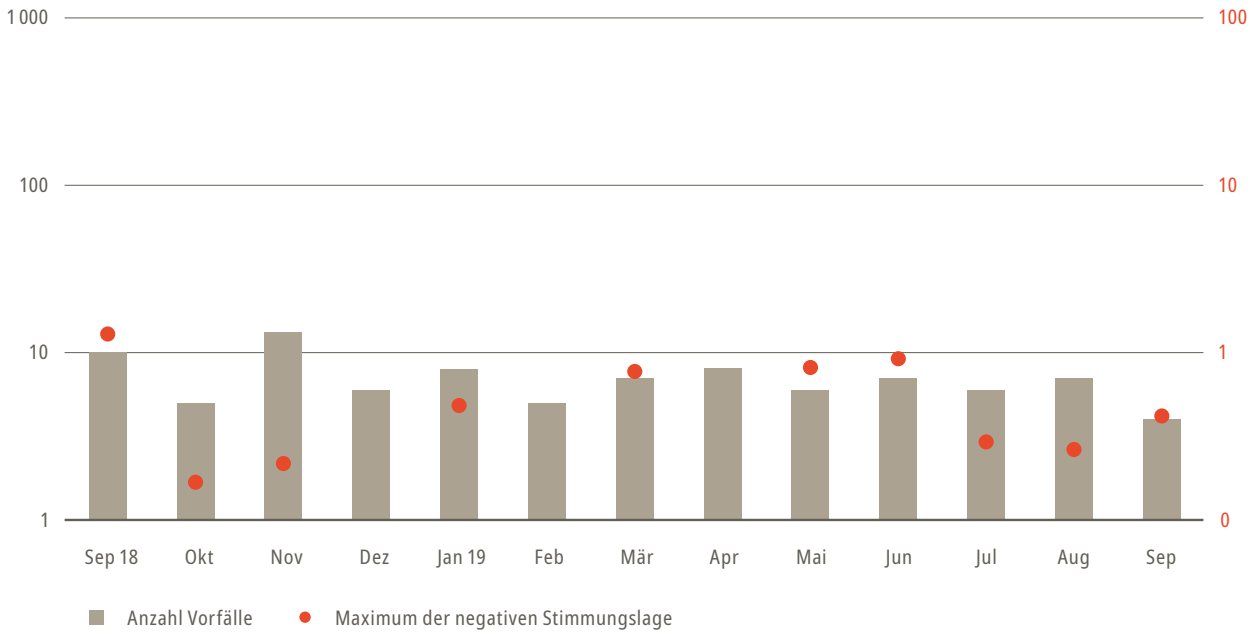
Singapur

Die Recherche im Rahmen dieses Berichts identifizierte drei Advanced Persistent Threat-Gruppen (APT-Gruppen), die im vergangenen Jahr gezielt Organisationen in Singapur angegriffen haben. Unsere Analyse zeigt, dass dabei am ehesten die Sektoren Gesundheitswesen, Medien, Telekommunikation und Maschinenbau betroffen waren, nicht aber der Finanzdienstleistungsbereich. Die APT-Gruppen zielten wahrscheinlich auf diese Branchen ab, weil entsprechende in Singapur ansässige Organisationen (wie SingHealth) Unmengen an vertraulichen Informationen beherbergen. Finanziell motivierte Cyber-Kriminelle könnten solche Daten zum Zweck der Unternehmensspionage verwenden oder durch den Verkauf von Patientendaten Gewinne erzielen.

In der Finanzdienstleistungsbranche hat die nationale Aufsichtsbehörde (Monetary Authority of Singapore) aufgrund der Besonderheiten dieser Region besonders gründlich und wirksam dafür gesorgt, dass die von ihr regulierten Organisationen eine solide Cyber-Sicherheitsgrundlage haben. Dieser Tatsache hat die Finanzdienstleistungsbranche in Singapur im Branchenvergleich eine verhältnismässig stärkere Infrastruktur zu verdanken.

Die Grafik unterhalb zeigt die auf den Finanzplatz von Singapur bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.

Wie die Grafik zeigt, gab es im vergangenen Jahr dennoch Beispiele für Angriffe auf Banken in Singapur. Diese Angriffe wurden russischen Cyber-Kriminellen zugeschrieben, die jedoch keiner in Russland ansässigen APT-Gruppe angehören.



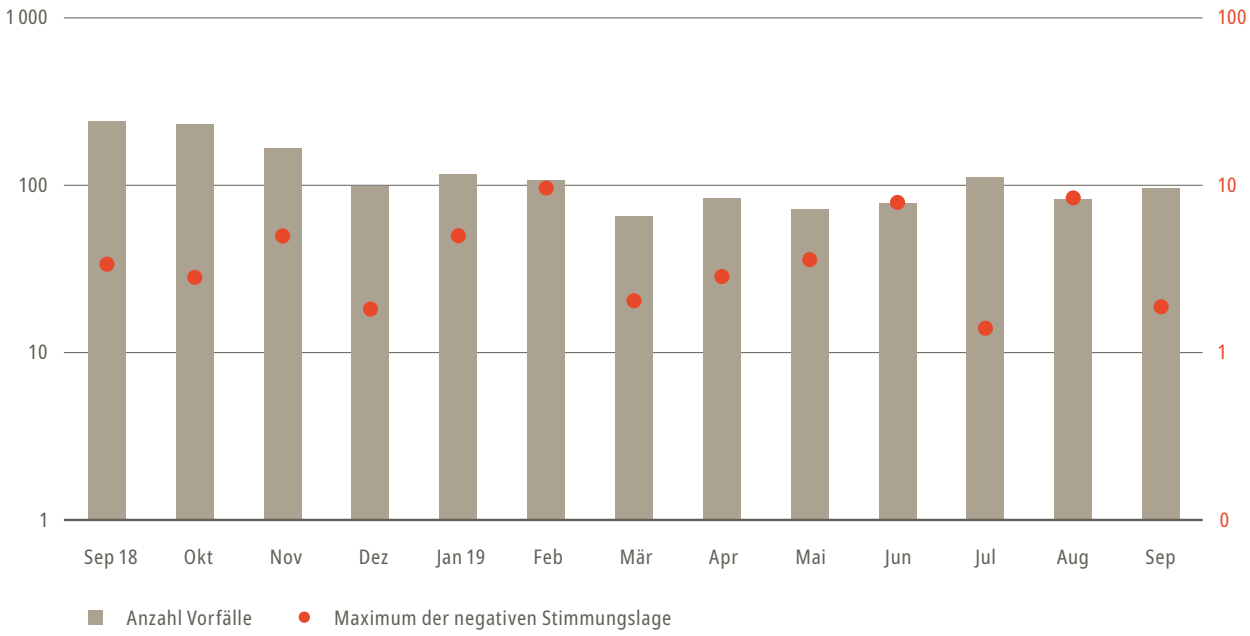
Cyber-Event-Chronik Singapur (Finanzen / Banken / Versicherungen)

Vereinigtes Königreich

Vor Kurzem warnten die britischen Sicherheitsdienste Finanzorganisationen vor einer wachsenden Gefahr von Cyber-Angriffen durch nationalstaatliche Akteure, insbesondere mit Ursprung in Russland. Die Warnung enthielt einen Hinweis auf das Risiko, dem sich britische Unternehmen durch ihre Abhängigkeit von einer Handvoll von Cloud-Anbietern aussetzen: Für viele Organisationen stellt diese Abhängigkeit einen Single Point of Failure dar. Ein wirksamer Angriff – selbst wenn dieser nur einen der zentralen Cloud-Anbieter träfe – könnte theoretisch die gesamte Finanzdienstleistungsbranche in Grossbritannien lahm legen und potenzielle Konsequenzen auch für das Ausland haben.

Insgesamt verzeichnete dieser Bericht einen Rückgang der bedrohlichen Cyber-Aktivitäten in der britischen Finanzdienstleistungsbranche im vergangenen Jahr, wie die nachstehende Zeitleiste illustriert. Dabei ist jedoch – wie von den Sicherheitsdiensten hervorgehoben – zu beachten, dass mögliche Angriffe durch Nationalstaaten voraussichtlich auf einem technischen Niveau stattfinden, das eine Zuordnung und Schadensminderung erheblich erschwert.

Die Grafik unterhalb zeigt die auf den Britischen Finanzplatz bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



Cyber-Event-Chronik Vereinigtes Königreich (Finanzen / Banken / Versicherungen)

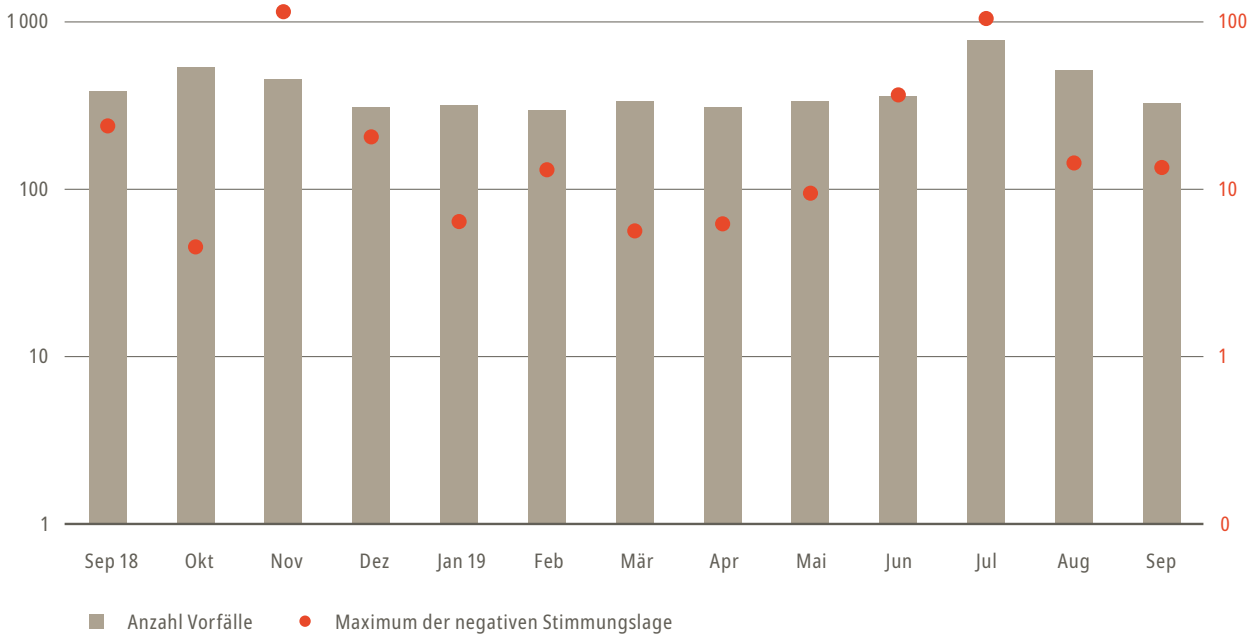
Vereinigte Staaten

Der Finanzdienstleistungssektor in den USA war schon in der Vergangenheit ein beliebtes Ziel für Cyber-Angriffe – ein Trend, der sich auch 2019 fortsetzte. Das hat einen ziemlich einfachen Grund: Der Rest der Wirtschaft ist sehr von der starken internationalen Geschäftspräsenz der USA wie auch vom Zugang zu Finanzinformationen abhängig.

Allerdings sind US-amerikanische Finanzorganisationen keineswegs das einzige oder sogar das bevorzugte Angriffsziel. Kunden, Dritte und Anbieter nachgelagerter Dienste bieten für Angreifer offenbar bequemere Möglichkeiten zum Zugriff auf Finanzinformationen, die sich zu Geld machen lassen – denn die Finanzinstitute selbst haben massiv in ihre Cyber-Abwehr investiert. Gerissene Cyber-Kriminelle konzentrieren sich deshalb gerne auf weniger gut geschützte Glieder in der Wertschöpfungskette. Das belegen dokumentierte Angriffe auf physische Peripheriegeräte wie etwa Geldautomaten und POS-Geräte (Point of Sale).

Technologische Neuerungen im Bereich Blockchain- und Kryptowährungen haben zusätzlich dazu beigetragen, sowohl die verfügbare Angriffsfläche als auch die Menge von Organisationen, die an Finanztransaktionen beteiligt sind, zu erweitern. Darüber hinaus ist es nach gross angelegten US-amerikanischen Datenschutzverletzungen und Datenlecks im vergangenen Jahr sehr viel wahrscheinlicher, dass gestohlene Anmeldeinformationen in Brute-Force-Angriffen und Credential Stuffing zum Einsatz kommen. In beiden Fällen ist das Hauptmotiv des Angreifers, Zugang zu Kundendaten zu erlangen, um damit finanzielle Vorteile zu erzielen.

Die Grafik unterhalb zeigt die auf den Finanzplatz der Vereinigten Staaten bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Die stärkste negative Stimmungslage wurde rund um Ereignisse bezogen auf HSBC um November 2018 und Capital One im Juli 2019 erfasst. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



Cyber-Event-Chronik Vereinigte Staaten (Finanzen / Banken / Versicherungen)

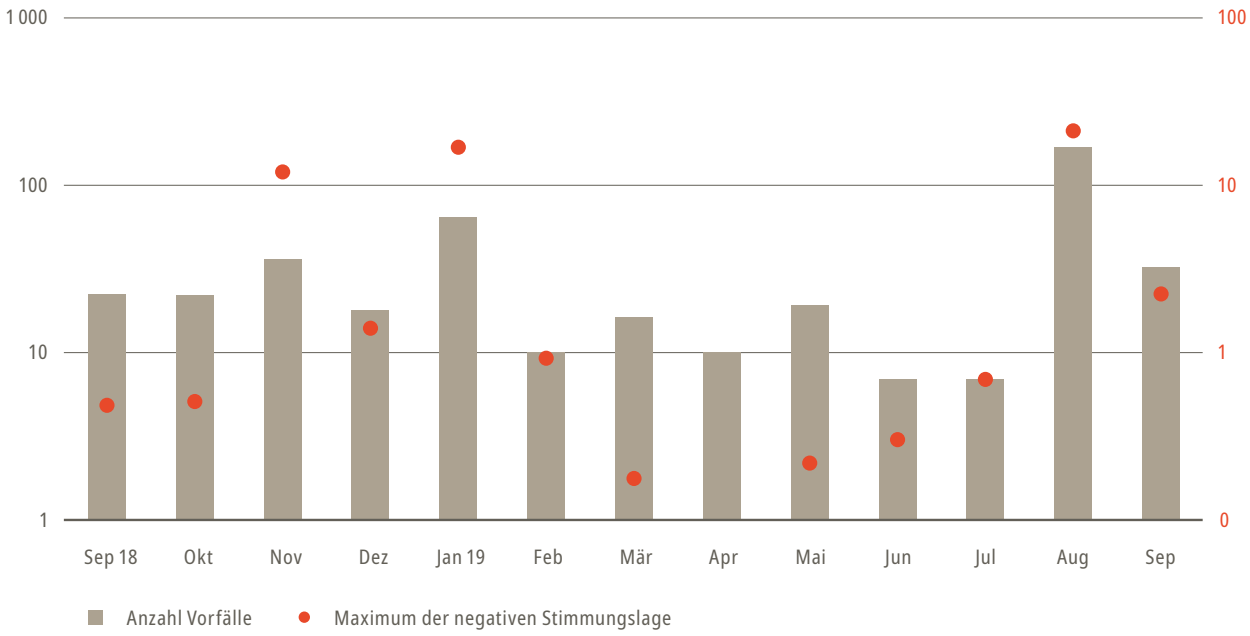
Deutschland

Mehrere Faktoren tragen in Deutschland zu einem erhöhten Risiko potenziell böswilliger Cyber-Aktivitäten bei. Ein wichtiger Umstand ist dabei die hohe Dichte an bedeutenden Finanzinstituten in Frankfurt – diese sind attraktive Ziele für fortgeschrittene Cyber-Kriminelle.

Es liegt auf der Hand, dass die hohe Konzentration an Rechenzentren, regionalen und globalen Hauptsitzen von Finanzinstituten gezielte Operationen und Angriffe nicht nur durch Cyber-Kriminelle, sondern auch durch staatlich unterstützte Gruppen anzieht. Dieses Risiko wird voraussichtlich auch in den kommenden Jahren – vor dem Hintergrund zunehmender geopolitischer Spannungen zwischen Russland und dem Westen sowie im Nahen Osten – nicht abnehmen.

Die Recherchen für diesen Report stellten konsistent russische Einflüsse im Hintergrund vermutlich staatlich geförderter Aktivitäten fest. Der Zuordnungsgrad dieser Fälle variiert zwar, ein Muster ist jedoch klar erkennbar. Durch Russland mitfinanzierte Bedrohungen sollten bei der Einstufung von Cyber-Risiken für die deutsche Finanzdienstleistungsbranche Anlass zu grösster Besorgnis geben.

Die Grafik unterhalb zeigt die auf den Deutschen Finanzplatz bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



Cyber-Event-Chronik Deutschland (Finanzen / Banken / Versicherungen)

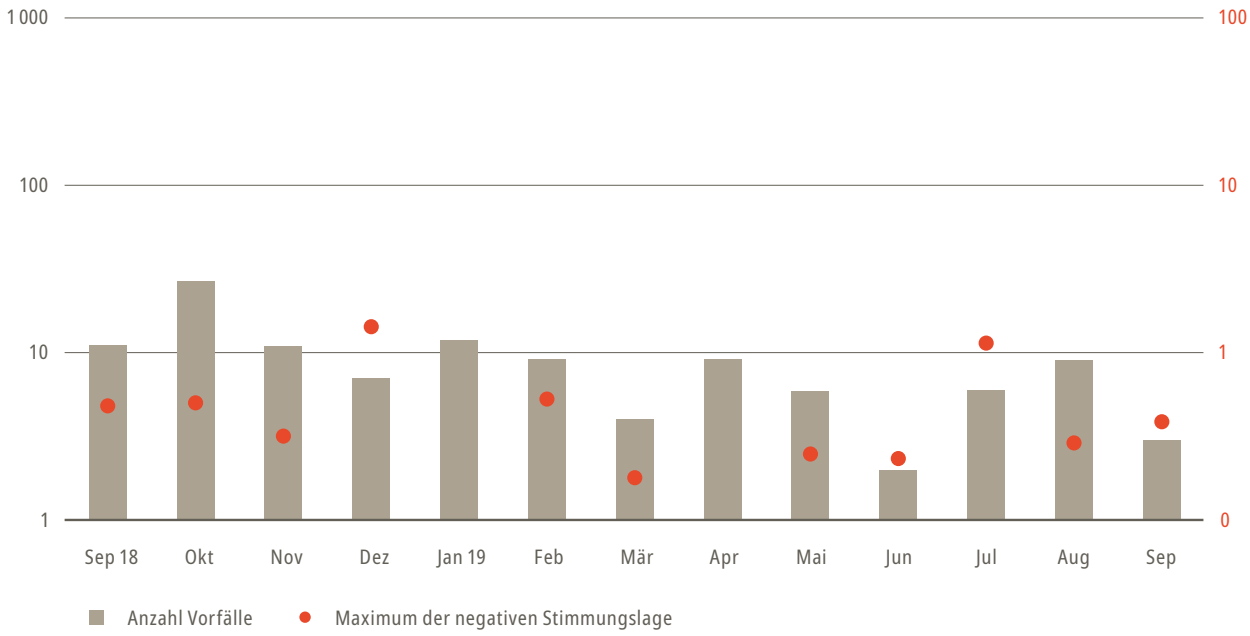
Niederlande

Im vergangenen Jahr liessen sich im Darkweb und in Untergrundforen häufige Verweise auf niederländische Organisationen finden. Die Organisationen wurden hauptsächlich im Zusammenhang mit dem Verkauf von Online-Banking-Anmeldeinformationen, gestohlenen Kreditkarteninformationen sowie Banking-Malware (beispielsweise Web Injects) genannt.

Daneben beobachteten die Sicherheitsexperten mehrfach, dass Cyber-Kriminelle Kontodaten und Kreditkartendaten zum Verkauf anboten, die sie höchstwahrscheinlich von Kunden niederländischer Finanzinstitute entwendet hatten.

Ähnlich den meisten anderen G20-Ländern, die in diesem Report beschrieben sind, wurden auch niederländische Finanzinstitute im vergangenen Jahr zunehmend Angriffsziel von staatlich unterstützten russischen und iranischen Gruppen. Mehrere andere Bedrohungsakteure, die schon in der Vergangenheit niederländische Organisationen angegriffen hatten, führten im vergangenen Quartal ebenfalls aktive Cyber-Kampagnen durch, in erster Linie mit finanziellen Motiven.

Die Grafik unterhalb zeigt die auf den Holländischen Finanzplatz bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



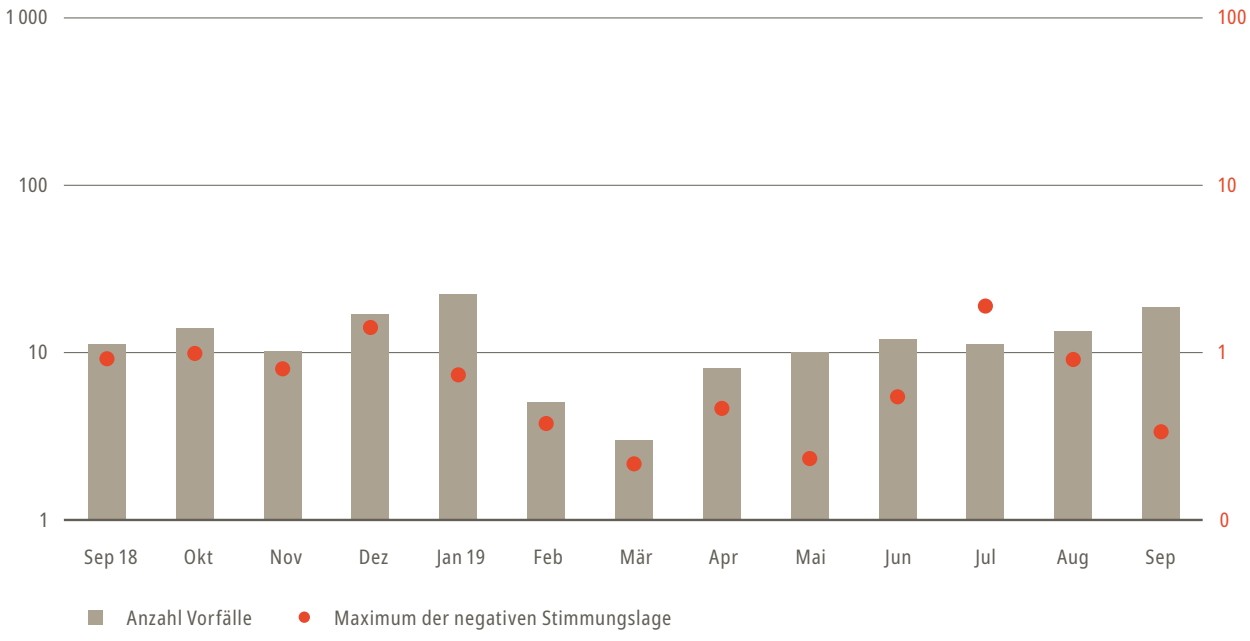
Cyber-Event-Chronik Niederlande (Finanzen / Banken / Versicherungen)

Frankreich

Im Jahr 2018 nahm die Anzahl der Malware-Angriffe auf Finanzinstitute weltweit zu. Insbesondere kamen dabei Banking-Trojaner zum Einsatz, die auf Websites, mobile Anwendungen von Finanzinstituten sowie POS- und Zahlungsverarbeitungssysteme von E-Commerce-Organisationen abzielten.

In der untersuchten Zeitspanne fand dieser Bericht in der französischen Finanzdienstleistungsbranche einen vorübergehenden Rückgang der Cyber-Angriffe zu Beginn des Jahres 2019. Über die gesamte Zeitspanne zeigte sich, dass Bedrohungsaktivitäten zugenommen hatten, die sich nicht gezielt an französische Organisationen richteten, sondern mehrere europäische Länder gleichzeitig betrafen.

Die Grafik unterhalb zeigt die auf den Französischen Finanzplatz bezogene Cyber-Angriffsaktivität die in Open Source Quellen erfasst wurde. Eine Erklärung wie die Grafik aufgebaut ist, findet sich in der Einleitung der Makro Analyse.



Cyber-Event-Chronik Frankreich (Finanzen / Banken / Versicherungen)

Mikroanalyse: der Schweizer Finanzsektor

Dieser Report wertet Daten von über 40 Finanzdienstleistungsinstituten in den Bereichen Versicherungen, Banken, Wertpapiere und Kapitalanlagen aus, die ihren Hauptsitz oder aber eine bedeutende Präsenz in der Schweiz haben. Er untersucht Cyber-Vorfälle, den Verlust oder Diebstahl von Anmeldedaten sowie Diskussionen im Darkweb und im kriminellen Untergrund, in denen diese Organisationen im vergangenen Jahr erwähnt wurden.

Der Grossteil der Cyber Security Verantwortlichen, die am Programm des Cyber Security Hub von SIX teilnehmen, wurde für diesen Bericht vertraulich befragt. Diese Interviews lieferten eine erhebliche Menge hochrelevanter Informationen zu Vorfällen und Beinahe-Zwischenfällen, die Unternehmen in den letzten zwölf Monaten erlitten haben. Um die Vertraulichkeit zu wahren, wurden alle Informationen nach ihrer Erfassung anonymisiert. Die einzelnen anonymisierten Beispiele in diesem Bericht enthalten keine Informationen, die aus dieser vertraulichen Datensammlung stammen. Um die Interessen der Mitglieder des Cyber Security Hub zu wahren, haben wir die mit uns im Vertrauen geteilten Informationen nur zur Gesamtanalyse verwendet.

Wesentliche Ermessungsentscheide

Die Analyse der gesammelten Informationen zeigte, dass Finanzunternehmen mit unterschiedlichen Merkmalen in der Regel auch unterschiedlichen Kombinationen von Cyber-Bedrohungen ausgesetzt sind. Basierend auf dieser Analyse gruppiert dieser Bericht Organisationen der Schweizer Finanzdienstleistungsbranche, die gemeinsame Charakteristiken und Bedrohungen aufweisen, in drei Kategorien:

Tier 3
- Versicherungen
- Investment Banking
- Wertpapiere und Handel

Im vergangenen Jahr waren Tier-3-Organisationen sowohl gezielten als auch generischen Phishing-Kampagnen ausgesetzt. Einige erlitten erhebliche Datenverluste, entweder direkt oder über Dritte. Tier-3-Organisationen werden im Darkweb kaum oder gar nicht erwähnt.

Tier 2
- Kleine und mittelgrosse Privatkundenbanken
- Finanzinfrastrukturanbieter (zum Beispiel SIX)
- Corporate Banking
- Vermögensverwaltung

Zusätzlich zu den in Tier 3 beobachteten Angriffskategorien erlebten Tier-2-Organisationen deutlich mehr Phishing-Kampagnen, gezielte Angriffe geringer Intensität und Erpressungsversuche.

Tier 1
- Grosse Retail-Banken

Zusätzlich zu den in Tier 2 und Tier 3 verzeichneten Angriffen waren Tier-1-Organisationen regelmässig gezielten Malware-Angriffen sowie allen Arten von Phishing-Versuchen ausgesetzt.

Zudem gab es mehrere gezielte Angriffe, in denen Banking-Malware und Trojaner implementiert wurden; diese Angriffe richteten sich gegen die Kunden von Tier-1-Organisationen und nicht gegen die Bankinstitute selbst. Es ist ersichtlich, dass jede Kategorie auch den Bedrohungen der jeweils niedrigeren Kategorien ausgesetzt ist. Beispielsweise ist eine Tier-2-Organisation mit allen Bedrohungen konfrontiert, die in Tier 3 beobachtet werden, sowie mit zusätzlichen Bedrohungen, die sich an Tier-2-Organisationen richten.

Vergleich der Schweiz mit ihren Nachbarn

Unsere Analyse legt nahe, dass die Schweizer Finanzdienstleistungsbranche weniger von Cyber Security Vorfällen betroffen ist als die ihrer Nachbarländer. In Abschnitt 1 sind weitere entsprechende Nachweise aufgeführt. Dies veranlasst zu der Frage, warum das so ist: Wenn sich die wichtigsten Gründe und Prinzipien identifizieren lassen, dann kann die breitere Community der Finanzdienstleister daraus lernen.

Zunächst einmal scheint es einen direkten Zusammenhang zwischen der Anzahl von Cyber-Angriffen und dem Ausmass des Privatkundengeschäfts zu geben. Je grösser die Reichweite einer Retail-Banking-Organisation, desto breiter ist ihre Angriffsfläche und desto höher die Anzahl der Vorfälle.

Obwohl die Schweiz mehrere hundert Finanzdienstleistungsorganisationen beherbergt, gibt es hier im Vergleich zu beispielsweise Frankreich, den Niederlanden, Deutschland oder Grossbritannien nicht viele bedeutende Privatkundenorganisationen. Im vergangenen Jahr haben die in der Schweiz existierenden grossen Retail-Banken die meisten Angriffe verzeichnet, was die von uns beobachtete Korrelation bestätigt.

Vermögensverwaltung und Private Banking in der Schweiz: gegen gezielte Angriffe gefeit?

Basierend auf den Daten, die aus vertraulichen Befragungen und Open-Source-Quellen zusammengetragen wurden, lässt unsere Analyse darauf schliessen, dass die Sektoren Vermögensverwaltung und Private Banking in Tier 2 im Vergleich zu anderen Finanzorganisationen erheblich weniger Cyber-Angriffen ausgesetzt sind.

Wir führen das relativ geringe Ausmass gezielter Angriffsversuche auf diese Sektoren darauf zurück, dass solche Cyber-Aktivitäten von den Angreifern weitaus mehr manuellen Arbeitsaufwand erfordern. Zudem sind diese Organisationen in der Schweiz in der Regel vergleichsweise klein und haben bewährte Schutzmechanismen entwickelt, um Bedrohungen einzudämmen. Aufgrund dieser Eigenschaften sind sie weitgehend gegen Angriffe isoliert.

Die Digitalisierung von Geschäftsprozessen, Outsourcing ins Ausland oder die Übertragung von Aufgaben an weniger qualifizierte Mitarbeiter würde automatisch das Risiko und die Wahrscheinlichkeit gezielter Angriffe erhöhen. Daher ist es wichtig, solche Initiativen hinsichtlich ihrer Chancen und Risiken zu bewerten und mit der Implementierung angemessener Sicherheitsmassnahmen zu kombinieren.

Über die Organisationsgrenzen hinaus: Kunden und Partner schützen

Cyber-Bedrohungen machen nicht an der Unternehmensgrenze halt. Die für diesen Bericht gesammelten Daten belegen, dass sich zahlreiche cyberkriminelle Aktivitäten eher an Kunden von Schweizer Finanzinstituten als an die Organisationen selbst richten. Beispielsweise sind gefälschte Bankanwendungen und gefälschte Webseiten so konzipiert, dass sie Bankkunden erfolgreich ködern und dem Angreifer direkt die gewünschten Informationen liefern, ohne dass er das Finanzinstitut selbst infiltrieren muss. Für Cyber-Kriminelle ist dies offenbar der bequemere Weg, verwertbare Finanzinformationen abzugreifen, die sich dann zu Geld machen lassen. Die für diesen Report durchgeführten Interviews untermauern, dass Angriffe auf Kunden, Dritte und nachgelagerte Unternehmen – und die Verhinderung solcher Angriffe – ein zentrales Anliegen für Schweizer Finanzdienstleistungsunternehmen sind.

Ausgewählte Erkenntnisse

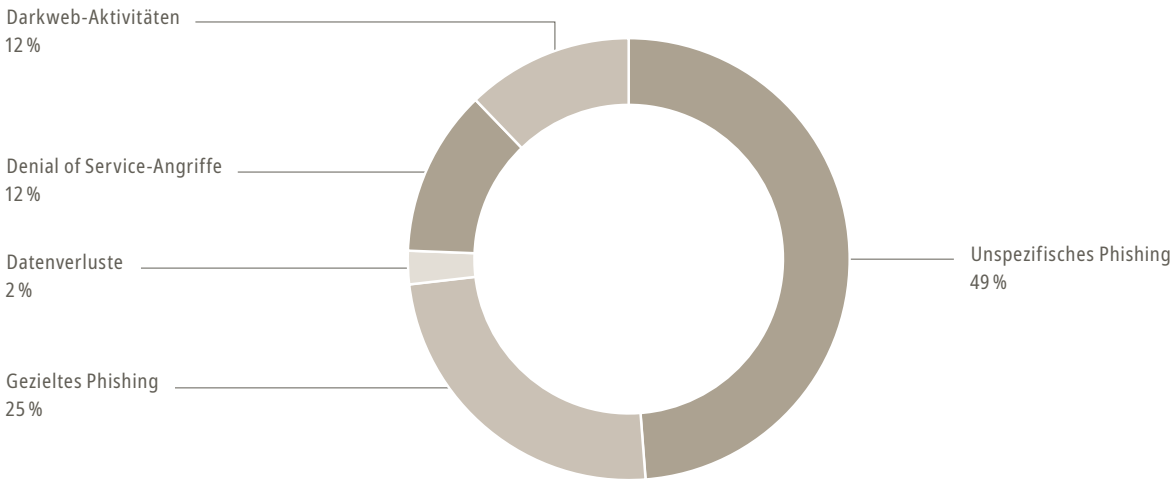
Die in diesem Abschnitt präsentierten Erkenntnisse basieren vornehmlich auf vertraulichen Interviews mit Mitgliedern des SIX Cyber Security Hub. Zusätzliche Informationen und Beispiele stammen aus Open-Source-Quellen. Dieser Bericht analysiert zwei Hauptfragen. Erstens: Wie unterscheiden sich Cyber-Angriffe in den einzelnen Kategorien – Tier 1 bis Tier 3 – nach Art und Umfang? Zweitens: Was können wir daraus lernen, wenn wir Darkweb-Konversationen über verschiedene Organisationen beobachten? Die hier dargestellten Ergebnisse sind als Interpretation bestimmter Trends auf Grundlage unserer Daten zu verstehen und nicht als akkurate Referenzwerte für vergleichbare Organisationen. Die aufgeführten Beispiele dienen der Veranschaulichung und beziehen sich nicht unbedingt auf Mitglieder des Cyber Security Hub.

Tier-3-Organisationen

Organisationen dieser Kategorie gehören zu den Bereichen Versicherungen, Investment Banking, Wertschriften und Handel innerhalb des Schweizer Finanzsektors. Im Gesamtvolumen der in dieser Kategorie gemeldeten Cyber-Vorfälle machten Phishing-Angriffe mit fast drei Viertel aller registrierten Vorfälle mit Abstand den grössten Anteil aus. Etwa zwei Drittel aller Phishing-Versuche waren unspezifische Phishing-Kampagnen, die sich nicht gezielt an die jeweilige Organisation richteten. Darkweb Abdeckung bezieht sich in diesem Zusammenhang auf jeder beliebigen Erwähnung der betreffenden Organisation im Darkweb. Für Organisationen mit starker internationaler Präsenz kann eine spezifische Erwähnung nicht dem Schweizer oder internationalen Teil der Organisation zugeordnet werden und wird daher in jedem Fall mitgezählt. Daher ergibt sich eine im Vergleich zu den anderen Kategorien scheinbar hohe Darkweb Abdeckung.

Einige erwähnenswerte und repräsentative Beispiele für Cyber-Vorfälle, von denen Tier-3-Organisationen im untersuchten Zeitrahmen betroffen waren:

– Die Erwähnung oder das Anbieten von Domains bestimmter Organisationen im Genesis Store (siehe Kasten).



Qualitatives Diagramm basierend auf anonymisierten SIX Cyber Security Hub Informationen

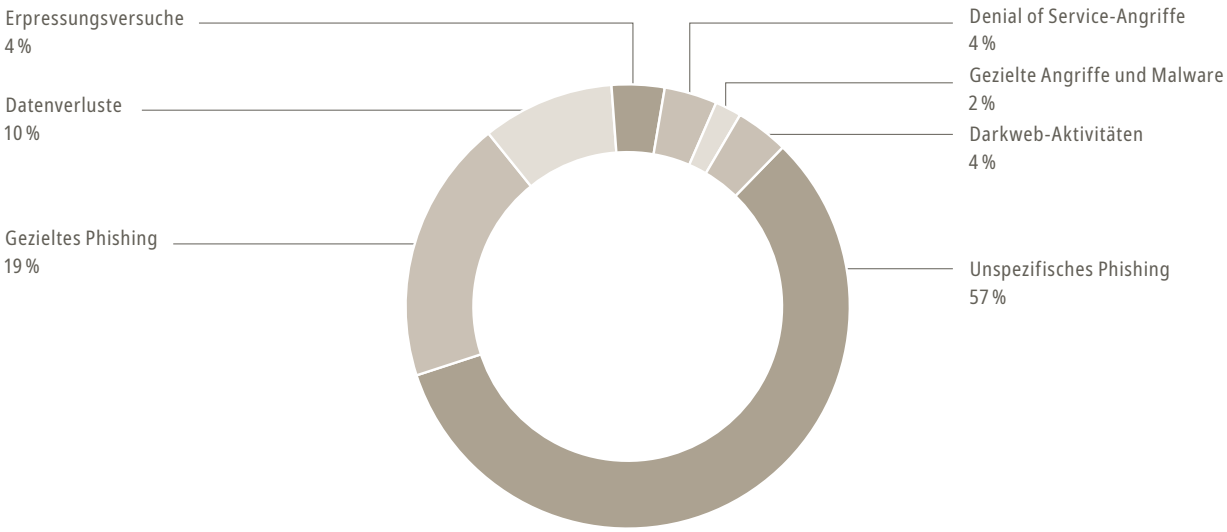
Der Genesis Store wird als Forum vom gleichnamigen Bedrohungsakteur Genesis Store betrieben. Der Genesis Store vertreibt die Browser-Fingerprints von manipulierten Host-Computern. Diese Computer wurden zunächst mit Malware infiziert und so in Bots verwandelt. Sie lassen sich dann für andere böswillige Aktivitäten wie DDoS-Angriffe (Distributed Denial of Service) nutzen. Gleichzeitig werden mit verschiedenen Methoden Informationen von der gekaperten Maschine gesammelt und in Darkweb- und Untergrundforen wie dem Genesis Store verkauft. Auf diese Weise hat der Käufer Zugriff auf eine Kombination aus Fingerprints, Cookies, Daten, die per Form Grabbing von Online-Formularen abgegriffen wurden, Anmeldeinformationen und anderen Daten, die sich im Browser des Opfers finden lassen. Cyber-Kriminelle können ein speziell für Chromium entwickeltes Browser-Plugin herunterladen, um die Daten des Opfers zu importieren. Anschliessend können sie sich in seinen Browser einloggen, um auf verschiedene Nutzerkonten zuzugreifen und Geld, persönliche Fotos, vertrauliche oder geschützte Dokumente sowie weitere Informationen zu stehlen.

Tier-2-Organisationen

Zu den Tier-2-Organisationen zählen kleine bis mittlere Retail-Banking-Organisationen, der Firmenkundenbereich, Vermögensverwaltungs- und Finanzinfrastrukturanbieter. Mehr als drei Viertel der Cyber-Angriffe auf die untersuchten Tier-2-Organisationen waren Phishing-Angriffe. Fast die Hälfte der übrigen Vorfälle waren Datenverluste, unter anderem auch der Verlust von Kredit- und Debitkarteninformationen. Eine weitere Aufschlüsselung der Phishing-Angriffe zeigt, dass es sich hier meist um unspezifische Phishing-Kampagnen handelte; ungefähr ein Viertel der Kampagnen waren gezielte Phishing-Versuche. In Übereinstimmung mit dem was für Tier 2 Organisationen bereits in diesem Kapitel beobachtet wurde, ist auch die Darkweb Abdeckung für Tier 2 Organisationen in unserer Stichprobe deutlich geringer als in den anderen Tiers.

Einige erwähnenswerte und repräsentative Beispiele für Cyber-Vorfälle, von denen Tier-2-Organisationen im untersuchten Zeitrahmen betroffen waren:

- Im März 2019 bekundeten im BHF-Forum tätige Akteure ihr Interesse daran, Geldautomaten einer Vermögensverwaltungs- und Firmenkundenbank zu kompromittieren.
- Verdacht auf Steuerung und Kontrolle des Netzwerkverkehrs per Command and Control (C&C) in der Infrastruktur einer Vermögensverwaltungs- und Firmenkundenbank im Zusammenhang mit einer bestimmten Malware-Gattung.
- Ein Nutzer im SkyFraud-Forum versuchte, Konto- oder Kartendaten zu verkaufen, die mit einer Vermögensverwaltungs- und Firmenkundenbank im Zusammenhang standen. Auf das ursprüngliche Angebot hin meldeten sich im Forum zwar keine interessierten Käufer, möglich ist aber, dass Interessenten den Verkäufer über die privaten Messaging-Kanäle des Forums kontaktierten, um ihre Anonymität zu wahren.
- Es wurden mehrere Ereignisse beobachtet, die auf eine offizielle Vermögensverwaltungs- und Firmenkunden-Domain im Genesis Store als Teil eines gebündelten Angebots verwiesen.
- Es gab bedeutende Denial of Service-Angriffe (DoS) auf eine Vermögensverwaltung und/oder Corporate Bank, die in mehreren Ländern ihren Ursprung hatten und sogar Satellitenverbindungen umfassten.
- Im Forum Joker's Stash sind zahlreiche gestohlene Karteninformationen verfügbar.



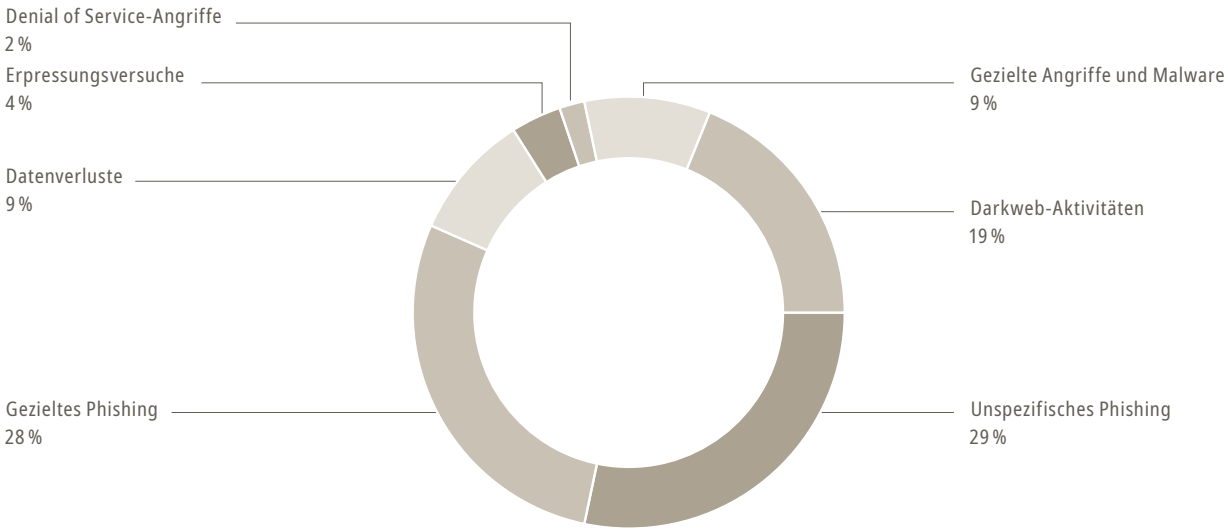
Qualitatives Diagramm basierend auf anonymisierten SIX Cyber Security Hub Informationen

Tier-1-Organisationen

Tier-1-Organisationen – grosse Retail-Banken in der Schweiz – waren am meisten von Phishing-Versuchen betroffen. Diese machten etwas mehr als die Hälfte aller Cyber-Angriffe in dieser Kategorie aus und verteilten sich mehr oder weniger gleichmässig auf generische und gezielte Phishing-Kampagnen. Die Erwähnung von Tier-1-Organisationen im Darkweb war nach dem Phishing das am häufigsten vorkommende Ereignis, gefolgt von gezielten anderen Angriffen.

Einige erwähnenswerte und repräsentative Beispiele für Cyber-Vorfälle, von denen Tier-1-Organisationen im untersuchten Zeitrahmen betroffen waren:

- Innerhalb eines Monats wurden mehr als 20 Typosquatting-Domains für eine Tier-1-Organisation registriert, in Vorbereitung auf gezielte Phishing-Angriffe.
- Regelmässig und übereinstimmend wurde berichtet, dass Produkte/Daten, die mit einer Retail-Bank im Zusammenhang standen, in populären Untergrundmärkten wie EpicMarket zum Verkauf angeboten waren. Dabei war in den letzten zwei Quartalen ein spürbarer Anstieg zu verzeichnen, wahrscheinlich, weil Strafverfolgungsbehörden weitere Webseiten stillgelegt hatten und Cyber-Kriminelle daraufhin nach alternativen Marktplätzen suchten.
- Mehr als 50’000 Kreditkartennummern einer Privatkundenbank sind über Kommunikationskanäle im kriminellen Untergrund verfügbar.
- Domains, die einer Retail-Bank angehören, werden im Genesis Store angeboten.



Qualitatives Diagramm basierend auf anonymisierten SIX Cyber Security Hub Informationen

Fazit

Wie die Makroanalyse zeigt, schneidet die Schweiz bei Cyber-Angriffen im Vergleich zu anderen G20-Staaten gut ab. Angesichts der Gesamtgrösse ihres Bankensektors im Vergleich zu anderen Ländern ist die Schweiz ein relativ seltenes Ziel für Cyber-Angriffe.

Dies ist zum Teil der Struktur der Schweizer Finanzdienstleistungsbranche zu verdanken. Grosse Retail-Banken verzeichnen die gezieltesten Angriffe, in der Schweiz gibt es jedoch stattdessen einen hohen Anteil an anderen Finanzdienstleistungsunternehmen. Auch solche Organisationen werden aber nicht gegen Cyber-Angriffe immun bleiben. Tatsächlich nimmt sowohl die Häufigkeit als auch die Komplexität der Attacken zu. Cyber-Kriminelle agieren dynamisch und suchen stets nach neuen Wegen, um Schwachstellen zu ihrem Vorteil auszunutzen, beispielsweise durch Erpressung.

Um gegenwärtigen und künftigen Cyber-Risiken zu begegnen, sollten die Finanzdienstleistungsunternehmen in der Schweiz ihre Cyber Security Aktivitäten koordinieren und das Erfassen wichtiger Bedrohungsinformationen erleichtern. Damit Schutzmassnahmen so effizient wie möglich sind, sollten sie zudem gemeinsame, landesweite Strategien für die Reaktion auf Cyber-Vorfälle (Incident Response) implementieren.

In der Mikroanalyse ergibt sich ein interessantes Muster für verschiedene Kategorien von Schweizer Finanzdienstleistungsunternehmen und -instituten. Das Bedrohungsspektrum jeder Kategorie baut auf jenem der vorhergehenden Kategorie auf und wird jeweils um neue Bedrohungsarten erweitert.

In allen Kategorien ist Phishing die häufigste Angriffsform. Der Prozentsatz der gezielten Phishing-Kampagnen steigt dabei von Kategorie zu Kategorie: von rund 30 % in Kategorie 3 auf über 50 % in Kategorie 1.

Darüber hinaus unterscheiden sich je nach Kategorie die Nennungen von Unternehmen im Darkweb in ihrer Struktur und Häufigkeit. Während dies zum Teil auf die spezifischen Aktivitäten der betroffenen Organisation zurückzuführen ist (etwa die Bereitstellung von Kreditkarten im Vergleich zur Vermögensverwaltung), spiegelt die Häufigkeit der Nennungen das Interesse der Cyber-Kriminellen an dieser Kategorie von Organisationen deutlich wider.

Schliesslich zielen Cyber-Kriminelle auch auf Kunden und Lieferanten ab, um mit relativ wenig Aufwand an Informationen zu kommen, die sich zu Geld machen lassen. Derzeitige Best-Practice-Anforderungen sehen vor, dass das Cyber Security Team eines Unternehmens ausdrücklich dafür verantwortlich ist, dieser Art von Risiko angemessen zu begegnen. Kundenbezogene Vorfälle schaden dem Vertrauen in das Unternehmen, worunter letztendlich der Ruf der gesamten Schweizer Finanzdienstleistungsbranche leidet. Daher liegt es in der gemeinsamen Verantwortung aller Institutionen in unserer Branche, die Häufigkeit und Auswirkung solcher Vorfälle so weit wie nur möglich einzudämmen.

Begriffe und Abkürzungen

APT	Advanced Persistent Threat
DDoS	Distributed Denial of Service
DoS	Denial of Service
IoT	Internet der Dinge
OSINT	Open Source Intelligence
PoC	Proof of Concept

SIX Group Services AG
Pfingstweidstrasse 110
Postfach
CH-8021 Zürich

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