KLARHEIT SCHAFFEN

Die Bedrohungslage für Finanzdienstleister Report 2021

Aufschlussreiche Erkenntnisse von Countercept

WITH secure

Zusammenfassung

Methodik

Ziel dieses Berichts ist es, eine Zusammenfassung der Kernthemen sowie der größten Bedrohungen für den Sektor der Finanzdienstleistungen zu bieten. Der Report basiert auf Interviews mit Threat-Intelligence-Experten sowie Führungskräften aus dem Bereich Cybersicherheit in EU-Banken, EU-Finanzaufsichtsbehörden sowie globalen Investment- Organisationen.

WithSecure™ erarbeitete die wichtigsten Sicherheitsthemen und Informationen zur Bedrohungslage auf Basis dieser Gespräche sowie auf Grundlage der eigenen Erfahrungen, die WithSecure™ im Rahmen der Managed Services und der Consulting-Projekte im Sektor der Finanzdienstleistungen gesammelt hat. Der Bericht stützt sich auch auf Bedrohungsdaten aus WithSecure™-Quellen sowie auf frei verfügbare Informationen.

Wesentliche Einschätzungen

- Die Supply Chain war das Thema mit der höchsten Priorität für die von WithSecure™ befragten Finanzdienstleistungsunternehmen. Staatlich organisierte Bedrohungsakteure wie NOBELIUM dominieren derzeit diesen Bereich. Eine besorgniserregende Entwicklung ist jedoch die hohe Verbreitung dieser Techniken und Vorgehensweisen unter weiteren cyberkriminellen Gruppierungen, wie die Ransomware-Gruppierung REvil mit den jüngsten Supply-Chain-Attacken auf Kaseya gezeigt hat. **WithSecure™ hält es für wahrscheinlich, dass einige Cyberkriminelle und Bedrohungsakteure die Fähigkeiten und die Absicht haben, in Zukunft Supply-Chain-Angriffe durchzuführen, die sich auf Finanzunternehmen auswirken könnten**.

- Cloud Computing war das Thema mit der zweithöchsten Priorität für die Finanzdienstleister, die von WithSecure™ befragt wurden. Die Unternehmen hoben hervor, dass die unterschiedlichen Strategien für die Einführung von Cloud Computing, fehlende Funktionen für die Überwachung und Bedrohungserkennung sowie der Mangel an Fachkräften und Expertise eine große Herausforderung für sie darstellen. **Nach Einschätzung von WithSecure™ werden staatlich organisierte Bedrohungsakteure ihre Fähigkeiten weiter ausbauen, um Cloud-Offensiven starten zu können. Weitere, cyberkriminelle Gruppierungen werden folgen. Dabei wird die Cloud nicht nur durch direkte Kompromittierungen der Cloud-Infrastruktur bedroht sein. Die Cloud ist auch das Endziel der Bedrohungsakteure, die die On-Premises-Infrastrukturen von Unternehmen angreifen und sich dann weiter über die Netzwerke hinweg ausbreiten, wie die NOBELIUM- Kompromittierungen gezeigt haben**.

- Vor dem Hintergrund der zunehmenden Ausnutzung von Schwachstellen durch staatlich organisierte Bedrohungsakteure und andere Cyberkriminelle haben Finanzdienstleister mehr und mehr Schwierigkeiten, die Schwachstellen in ihrer Infrastruktur effektiv zu bewältigen. Die Daten von WithSecure™ sowie frei verfügbare Informationen deuten darauf hin, dass die Ausnutzung von Schwachstellen einer der wichtigsten Angriffsvektoren bei vielen schwerwiegenden Cyberattacken ist. **Die Einführung effektiver Asset-Management-Strategien in Finanzdienstleistungsunternehmen ist daher für die langfristige Resilienz sehr bedeutend**.

- Technologien wie SWIFT, Open Banking sowie Geldautomaten stellen ein fortdauerndes Risiko für Finanzorganisationen dar, da sich die gegnerischen Technologien und eingesetzten Angriffstechniken kontinuierlich weiterentwickeln. Auch Angriffe im Zusammenhang mit Kryptowährungen haben zugenommen. Die Sicherung der Infrastruktur für digitale Währungen ist eine wichtige Entwicklung, da die Zentralbanken ihre Bestände an Kryptowährungen erhöhen und ihre eigenen digitalen Währungen einführen. **Die Absicherung der Technologien für Kryptowährungen wird in Zukunft ein wichtiger Trend im Sektor der Finanzdienstleistungen sein**.

- Die von WithSecure™ befragten Finanzdienstleistungsunternehmen betrachteten Ransomware als die größte Bedrohung. Der Grund hierfür ist die wahrgenommene Wirkung, die ein Ransomware-Angriff auf die Resilienz eines Unternehmens haben kann. Hierzu zählen erhebliche finanzielle Schäden, Beeinträchtigungen des Geschäftsbetriebs sowie der Reputationsverlust. **Die Ausnutzung von Schwachstellen ist eine auffällige Entwicklung, die früher ausschließlich staatlich gestützten Bedrohungsakteuren vorbehalten war und heute immer häufiger von Ransomware-Akteuren eingesetzt wird. Nicht nur ein direkter Ransomware-Angriff auf ein Finanzdienstleistungsunternehmen hat negative Auswirkungen, sondern auch ein Angriff auf einen Lieferanten oder Partner. Denn auch so kann es zu erheblichen Unterbrechungen des Geschäftsbetriebs und Ausfallzeiten kommen, die dann**

wiederum den Geschäftsbetrieb von Finanzdienstleistern beeinträchtigen. Unternehmen sollten sicherstellen, dass sie die Entwicklungen der Vorgehensweise dieser kriminellen Gruppierungen im Auge behalten. Sie sollten sich weiterhin darauf konzentrieren, sowohl die Angriffsvektoren einzudämmen und zu entschärfen als auch die Auswirkungen zu reduzieren, falls diese Gruppierungen sich bereits Zugang zu ihren Netzwerken verschaffen konnten.

- Finanziell motivierte, staatlich gestützte Gruppierungen stehlen auch weiterhin Geld aus Bankautomaten, kompromittieren die von Banken betriebenen SWIFT-Endpunkte, und eignen sich illegal Kryptowährungen an. **Nach Einschätzung von WithSecure™ werden die Diebstähle von Kryptowährungen weiter zunehmen, da die Bestände der Banken an digitalen Währungen und Kryptowährungen wachsen. Staatlich gestützte Gruppierungen aus China und Russland haben ihre hochentwickelten Fähigkeiten, gesamte Lieferketten anzugreifen, bereits unter Beweis gestellt**. Beide Gruppierungen haben die Absicht, Regulierungsbehörden für Finanzdienstleistungen ins Visier zu nehmen, um an nachrichtendienstlich wertvolle Informationen zu gelangen. Zudem wurden staatlich gestützte Bedrohungsakteure aus China auch bei dem Versuch beobachtet, Daten von Finanzdienstleistern des privaten Sektors zu stehlen, um politische und wirtschaftliche Ziele zu verfolgen.

Kernthemen:

Supply Chain

Die jüngsten, hochkarätigen Supply-Chain-Vorfälle wie SolarWinds und Kaseya haben das öffentliche Bewusstsein für die Supply Chain als Angriffsvektor geschärft. Die Absicherung gegen diesen Angriffsvektor war für nahezu alle Finanzunternehmen, mit denen WithSecure™ gesprochen hat, das wichtigste Anliegen und der strategische Schwerpunkt. Ein Unternehmen, mit dem WithSecure™ sprach, hat ein Projekt gestartet, um nicht nur seine Drittanbieter, sondern auch seine Viertanbieter zu klassifizieren. Diese Arbeit konzentrierte sich darauf, ein Verständnis für die gesamten, vorgelagerten Abhängigkeiten von Lieferanten und Partnern zu entwickeln, die für diese Organisation ein hohes Risiko darstellen könnten. Anhand dieses Bildes könnte das Unternehmen dann die Risiken auf Basis der Lieferantenauswahl steuern, und die konzentriertenAbhängigkeiten reduzieren.

ENISA, die Agentur der Europäischen Union für Cybersicherheit, veröffentlichte kürzlich eine Untersuchung von 24 Supply-Chain-Angriffen, die in den vergangenen 18 Monaten durchgeführt wurden. In diesem Bericht definierte die ENISA eine neue Taxonomie für die Diskussion von Supply-Chain-Angriffen und unterteilte das Thema in vier Schlüsselbereiche.

In der Diskussion über den Kaseya-Angriff war auffallend, dass Verwirrung darüber bestand, wie dieser Supply-Chain-Angriff zu klassifizieren sei. Die ENISA-Taxonomie zur Definition der verschiedenen Elemente eines Supply-Chain-Angriffs soll dazu beitragen, mehr Klarheit in diese Diskussionen zu bringen und Organisationen bei der Entwicklung ihrer Strategien zur Abwehr dieser Bedrohungen zu unterstützen. Der ENISA-Bericht hebt hervor, dass die meisten Supply-Chain-Angriffe das Vertrauen, das in Lieferanten und Partner gesetzt wird, ausnutzten, und sich auf den Code der Drittanbieter konzentrierten, um deren Kunden zu kompromittieren. Zudem setzten die Angreifer Malware ein, und zielten darauf ab, sich Zugang zu den Geschäftsdaten der Kunden zu verschaffen. Obwohl Datenverluste für alle Unternehmen ein großes Problem darstellen, sind die Auswirkungen eines solchen Angriffs unterschiedlich schwerwiegend – je nachdem, wer das Opfer ist.

Eine besorgniserregende Entwicklung bei Supply-Chain-Angriffen ist die Tatsache, dass diese Vorgehensweise nicht mehr ausschließlich von staatlich organisierten Bedrohungsgruppen genutzt wird, sondern auch von anderen Cyberkriminellen. Der Angriff auf die Kaseya-Supply-Chain, bei dem die Kunden von MSSPs, die Kaseya VSA-Appliances betreiben, kompromittiert wurden, wurde dem Ransomware-Bedrohungsakteur REvil zugeschrieben[1].

Obwohl der Supply-Chain-Angriff nicht den gleichen Grad an Technik aufwies wie andere Supply-Chain-Angriffe – beispielsweise der Angriff auf die Kunden von SolarWinds –, zeigte er doch ein hohes Maß an technologischen und operativen Fähigkeiten. WithSecure™ geht davon aus, dass einige kriminelle Bedrohungsakteure die Absicht und auch die Möglichkeiten haben werden, künftig Supply-Chain-Angriffe durchzuführen, die Auswirkungen auf Finanzorganisationen haben könnten.

Der ENISA-Bericht führt etwa die Hälfte der untersuchten Supply-Chain-Angriffe auf staatlich finanzierte APT-Aktivitäten zurück. Diese Gruppierungen haben klar bewiesen, dass sie diese Angriffe mit einem hohen Maß an technischen und operativen Fähigkeiten durchführen können. Da ihre Motivation in der Regel Spionage ist, stehen Finanzorganisationen nicht im Mittelpunkt des Interesses. Es ist jedoch davon auszugehen, dass Finanzunternehmen die Zielkriterien einiger dieser kriminellen Gruppierungen erfüllen könnten, da sie als kritische nationale Infrastruktur (CNI: Critical National Infrastructure) eingestuft werden. Der jüngste Vorfall mit SolarWinds hatte Auswirkungen auf einige staatliche Finanzinstitute. Dies untermauert die Einschätzung, dass ein konkretes Risiko besteht, dass Eindringlinge künftig auch die Schwachstellen von Finanzinstituten ausnutzen und Daten sammeln könnten.

[1] https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-incident

Die Erkenntnisse von WithSecure™:

Die Ereignisse der vergangenen 18 Monate haben deutlich gemacht, dass Unternehmen ihren Ansatz für die Supply-Chain-Sicherheit überdenken müssen. Der herkömmliche Ansatz – die Einhaltung der Compliance-Vorgaben sowie die Nutzung von Fragenbögen zur Sorgfaltspflicht – mag den Verantwortlichen im Unternehmen ein Gefühl der Sicherheit vermitteln, trägt in der Realität jedoch wenig zum Schutz der Unternehmen vor Supply-Chain-Angriffen bei. Es ist wichtig, dass Finanzdienstleistungsunternehmen stets in Betracht ziehen, dass es bei ihren Lieferanten und Partnern zu Sicherheitsverstößen kommen kann. Sie müssen sich darüber im Klaren sein, dass Lieferanten und externe Partner Zugang zu ihren Umgebungen haben, und die Auswirkungen einer möglichen Kompromittierung dieser Organisationen berücksichtigen. Die Entwicklung von Sicherheitsmechanismen zur Eindämmung der Auswirkungen dieser Angriffe sowie eine offene Kommunikation mit den Lieferanten über deren Sicherheit sind wichtige Schritte, um die Abwehr künftiger Supply-Chain-Angriffe zugewährleisten.

Cloud Computing

In allen von WithSecure™ befragten Finanzinstituten ist eine stetig zunehmende Nutzung von Cloud-Infrastrukturen zu beobachten. Sicheres Cloud Computing ist – nach dem Schutz der Supply Chain – das zweitwichtigste Thema, auf das sich Finanzinstitute konzentrieren. Die Meinungen über langfristige Strategien für die Cloud-Nutzung gehen auseinander, wobei sich einige Unternehmen wie BNP Paribas, Citi und Standard Chartered auf die Nutzung von On-Premises-Clouds festgelegt haben[2]. Diese Banken zögerten, ihre Daten an Cloud-Service-Provider auszulagern. Sie machen sich Sorgen über das Risiko von Sicherheitsverstößen, über die Abhängigkeit von einem einzelnen Anbieter sowie über das mögliche Einschreiten der Aufsichtsbehörden in Bezug auf den Speicherort der Daten. Neue Gesetze, wie der vorgeschlagene Digital Operational Resilience Act (DORA)3, bieten einige regulatorische Leitlinien für Unternehmen, umfassen aber auch Einschränkungen für potenzielle Cloud-Service-Provider[4]. Im Gegensatz dazu nutzen andere Unternehmen mehrere Public-Cloud-Provider: Das Unternehmen HSBC hat in den vergangenen zwei Jahren beispielsweise vertragliche Vereinbarungen mit den Cloud-Service-Providern Google, AWS und Microsoft geschlossen[5]. Zudem haben einige neuere Fintech-Unternehmen ihr gesamtes Geschäftsmodell auf die Cloud ausgerichtet und arbeiten vollständig in der Cloud – mit nahezu keiner oder vollkommen ohne On-Premises-Infrastrukturen.

In allen Consulting-Projekten sowie in allen Interviews mit den Finanzdienstleistern konnte WithSecure™ feststellen, dass die Unternehmen bei der Absicherung dieser neuen Technologien vor großen Herausforderungen stehen. Mit der zunehmenden Nutzung der Cloud steigt auch die Menge an sensiblen Daten, die in cloudbasierten Umgebungen gespeichert wird. Gleichzeitig steigt damit die Notwendigkeit, diese Daten zu schützen. Viele der namhaften Cloud-Service-Provider verfügen über Telemetrie- sowie unterstützende Funktionen, um eine Überwachung zu ermöglichen. Finanzdienstleister wissen jedoch aufgrund der mangelnden Expertise oftmals nicht, wie sie diese Funktionen effektiv zum Schutzihrer Umgebungen einsetzen können.

[2] https://www.digfingroup.com/hsbc-cloud/
[3] https://www.withsecure.com/gb-en/consulting/our-thinking/exploring-dora
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
[5] https://www.digfingroup.com/hsbc-cloud/

In diesem Jahr gab es Veröffentlichungen zu mehreren neuen Cloud-Bedrohungen, die mit immer neuen Techniken und neuer Malware einhergingen. In den Gesprächen, die WithSecure™ mit Finanzdienstleistern geführt hat, standen die von NOBELIUM eingesetzten Techniken im Vordergrund. In der jüngsten Angriffsoffensive gelang es NOBELIUM, in die Cloud-Infrastruktur eines Opfers einzudringen, indem es ADFS-Trusts ausnutzte und neue SAML-Token fälschte, um sich im Netzwerk des Opfers auszubreiten und dort verbleiben zu können[6]. Diese „Golden SAML"-Angriffe[7] waren eine neue Technik und kamen für die meisten Unternehmen, die keine Erkennungsmechanismen für diese Art von Bedrohung hatten, überraschend.

Die jüngsten vier OMIGOD-Schwachstellen[8] in Microsofts Open-Management-Infrastructure-Framework (OMI) haben deutlich gezeigt, dass auch diese Infrastruktur – wie jede Technologie – Sicherheitslücken hat und angreibar ist. Darüber hinaus entwickeln Bedrohungsakteure neue technische Fähigkeiten, um Cloud-Services anzugreifen. So wurde in diesem Jahr die erste „cloudnative" Malware entdeckt, die unter dem Namen Siloscape auf Windows-Container abzielt[9]. Die Malware ist darauf ausgelegt, eine Backdoor in mangelhaft konfigurierten Kubernetes-Clustern zu öffnen, um schadhafte Container auszuführen. Mit den entsprechenden Privilegien würde dies den Diebstahl von Anmeldedaten ermöglichen, um sich in der Cloud-Umgebung eines Opfers zu bewegen und auf das schlussendliche Ziel hinzuarbeiten – seien es finanzielle Motive oder Spionage.

[6] https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps; https://us-cert.cisa.gov/ncas/alerts/aa21-008a
[7] https://www.sygnia.co/golden-saml-advisory
[8] https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/
[9] https://unit42.paloaltonetworks.com/siloscape/

Die Erkenntnisse von WithSecure™:

Nahezu alle von WithSecure™ befragten Branchenexperten äußerten Bedenken hinsichtlich der Sicherheit von Cloud-Infrastrukturen in den kommenden 12 Monaten, insbesondere da Cloud Computing für viele Unternehmen zum Standard wird – oder bereits ist. Mit zunehmender Cloud-Nutzung werden mittlere bis große Unternehmen mit Hunderten von Workloads in der Cloud vor der Herausforderung stehen, ihre Aktivitäten sicher zu skalieren. Auch die Absicherung von Software-as-a-Service (SaaS) wird für die meisten Unternehmen des Finanzsektors zunehmend zum Problem werden, da es immer mehr unterschiedliche Lösungen und Nischenprodukte gibt, die aufgrund mangelnder Erfahrung und Erkenntnisse nicht ausreichend geschützt sind.

WithSecure™ empfiehlt Unternehmen daher, Fachwissen und Rat einzuholen, um eine bedarfsgerechte, sichere Konfiguration umzusetzen. Für Unternehmen, die eine eigene Bedrohungserkennung für die Cloud entwickeln, kann die cloud-spezifische Bedrohungssimulation mit einem Purple Team eine wertvolle Möglichkeit sein, um Erkennungsfunktionen zu entwickeln und zu validieren. Die Zusammenarbeit in solchen Projekten kann auch dazu beitragen, das Know-how in den Unternehmen zu vertiefen, um den Fachkräftemangel, der in der gesamten Branche herrscht, oder auch mögliche Qualifikationsdefizite zu überbrücken.

Aufgrund der Weiterentwicklung der Cloud-Nutzung geht WithSecure™ davon aus, dass zunächst staatlich organisierte Bedrohungsakteure Cloud-Offensiven starten werden, und mehr und mehr Cyberkriminelle sich dieses Know-how dann aneignen werden. Das Bedrohungsszenario für Cloud Computing umfasst nicht nur direkte Angriffe auf Cloud-Infrastrukturen. Bedrohungsakteure nutzen auch die On-Premises-Infrastrukturen, breiten sich in den Unternehmensnetzwerken aus und greifen dann die Cloud an, wie im Fall der NOBELIUM-Kompromittierungen zu sehen war.

Schwachstellen und Legacy-Infrastrukturen

Die Risiken, die von Legacy-Software und Legacy-Anwendungen ausgehen, waren ein wichtiges Thema für die von WithSecure™ befragten Finanzdienstleister, die sich aufgrund wichtiger betrieblicher Abhängigkeiten nicht von diesen Infrastrukturen trennen können. Der Sektor der Finanzdienstleistungen ist in Bezug auf Standards und Praktiken für die Cybersicherheit relativ stark reguliert, steht aber immer noch vor erheblichen Herausforderungen bei der Identifizierung der gefährdeten Assets und beim Schwachstellen-Management in oft sehr großen, komplexen und verteilten Umgebungen.

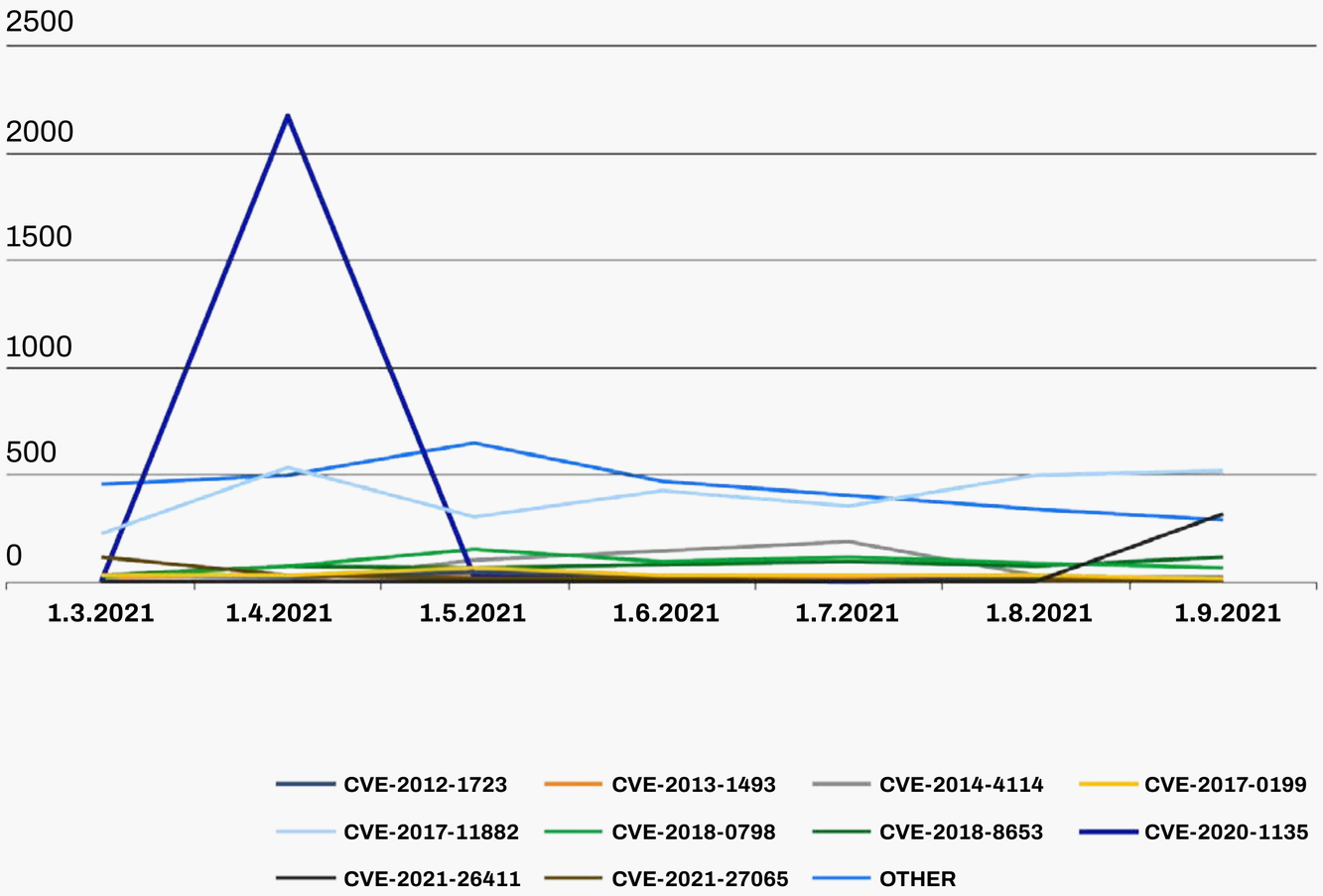
Im Juli veröffentlichten die US Cybersecurity and Infrastructure Security Agency (CISA), das Australian Cyber Security Centre (ACSC), das britische National Cyber Security Centre (NCSC) und das US Federal Bureau of Investigation (FBI) einen Bericht[10] über die 30 größten Schwachstellen, die von Bedrohungsakteuren in den Jahren 2020 und 2021 routinemäßig ausgenutzt wurden. Der Bericht hebt hervor, dass Bedrohungsakteure weiterhin gezielt Schwachstellen in nach außen gerichteten Technologien ausnutzen. Zu den im Jahr 2021 am häufigsten ausgenutzten Schwachstellen gehören die in Microsoft (Exchange), Pulse Secure, Accellion, VMware und Fortinet-Geräten.

Die öffentliche Berichterstattung über die Ausnutzung dieser Schwachstellen zeigt, dass einige Organisationen im Sektor der Finanzdienstleistungen von Bedrohungsakteuren kompromittiert wurden, die diese Angriffsvektoren nutzten. So war beispielsweise eine nicht gepatchte, kritische Schwachstelle in Pulse Secure VPN-Servern wahrscheinlich der Angriffsvektor, der bei einem REvil-Ransomware-Angriff im Jahr 2020 gegen das Devisenhandelsunternehmen Travelex in London eingesetzt wurde[11]. Der Angriff zwang das Unternehmen, alle Operationen in 30 Ländern einzustellen[12]. Varianten der Ransomware DarkSide wurden erkannt, als sie eine SonicWall-VPN-Schwachstelle ausnutzten, um Ziele in den USA zu hacken[13]. Der Hack der Cayman Bank – ausgeführt von Phineas Fisher – zielte auf ein Banken-Netzwerk ab, das eine anfällige SonicWall-VPN-Appliance nutzte. Dies zeigt deutlich, dass VPN-Schwachstellen immer noch eine beliebte Möglichkeit sind, Finanzdienstleistungsunternehmen zu kompromittieren[14].

Ebenfalls auf der Liste der von der CISA identifizierten Schwachstellen stand CVE-2017-11882, ein 17 Jahre altes Problem der Speicher-Korruption in Microsoft Office (einschließlich Office 365). Die WithSecure™-Telemetrie identifiziert diese als eine der am häufigsten ausgenutzten Schwachstellen auf Windows-Endgeräten im vergangenen Jahr. Diese Schwachstelle kann bei Phishing-Kampagnen ausgenutzt werden und erfordert nur geringe Interaktionen seitens des Benutzers. Sie wurde in der Vergangenheit von finanziell orientierten Bedrohungsakteuren wie der Cobalt Group genutzt[15].

[10] https://us-cert.cisa.gov/ncas/alerts/aa21-209a
[11] https://portswigger.net/daily-swig/travelex-ransomware-attack-pulse-secure-vpn-flaw-implicated-in-security-incident
[12] https://www.bitdefender.com/blog/hotforsecurity/pulse-secure-vpn-server-exploit-opens-the-way-for-sodinokibi-ransomware-travelex-falls-victim
[13] https://www.securitynewspaper.com/2021/05/12/darkside-ransomware-affiliates-are-using-sophos-firewall-and-vpn-vulnerability-to-hack-researchers-track-down-5-affiliates-of-them
[14] https://github.com/Alekseyyy/phineas-philes/blob/master/cayman-english.md
[15] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wil[d]

Die am häufigsten ausgenutzten Schwachstellen, die von WithSecure™ zwischen März 2021 und September 2021 erkannt wurden



*Details zu CVE-2012-1723: https://nvd.nist.gov/vuln/detail/CVE-2012-1723

National Vulnerability Database: https://nvd.nist.gov/vuln/full-listing

Die Erkenntnisse von WithSecure™:

Die WithSecure™-Daten aus Incident-Response-Projekten untermauern die Relevanz der Ausnutzung von Schwachstellen, wobei die nach außen gerichteten Schwachstellen ein weit verbreiteter Angriffsvektor für alle Bedrohungsakteure sind. Vor allem in den vergangenen 12 bis 18 Monaten konnte WithSecure™ beobachten, dass die Ausnutzung von Schwachstellen im Rahmen von Ransomware-Attacken in Zahl und Geschwindigkeit stark zunimmt.

WithSecure™ empfiehlt Unternehmen, Tests der externen Angriffsfläche durchzuführen, um ihre Gefährdungslage zu verstehen sowie Sicherheitsverletzungen und Schwachstellen zu identifizieren und zu beseitigen. Es wird immer Bereiche eines Perimeters geben, die exponierter sind als andere. Das sind beispielsweise Assets, die aus geschäftlichen Gründen nicht aus dem öffentlichen Bereich genommen werden und deren Angriffsflächen nicht reduziert werden können. Wissen Unternehmen, wo diese Schwachstellen liegen, können sie potenzielle Angriffspfade kartieren und ihr Engagement für die Erkennung von Bedrohungen und die Reaktion darauf verstärken. So haben beispielsweise die Untersuchungen des WithSecure™-EASM-Teams (EASM: External Attack Surface Management) ergeben, dass die E-Mail-Anmeldedaten einiger Unternehmen einer weitaus höheren Gefährdung ausgesetzt sind als zu erwarten war. Es gibt zwar nicht zwingend Patches, die dieses Problem beseitigen. Aber diese Informationen können in Phishing-Awareness-Schulungen und Sicherheitstrainings sowie in die Unternehmenskultur einfließen, um eine stabile und sichere Organisation zu schaffen.

Technologien für Finanzdienstleister

Technologien, die von Finanzdienstleistern eingesetzt werden, wie SWIFT und Open Banking, waren das letzte zentrale Thema in den Gesprächen, die WithSecure™ mit den Unternehmen aus diesem Sektor führte. Angriffe auf diese Technologien sorgen für Schlagzeilen, da sie relativ neu sind und von der breiten Öffentlichkeit als Bankraub betrachtet werden. Da für diese Angriffe hohe technische Fähigkeiten erforderlich sind, werden diese in erster Linie von staatlich organisierten Gruppierungen mit fortgeschrittenen Kenntnissen und erheblichen Ressourcen durchgeführt. Wie im Abschnitt über „Staatlich organisierte Akteure“ erörtert wird, haben nordkoreanische Gruppierungen die Absicht und Fähigkeit unter Beweis gestellt, die SWIFT-Infrastruktur mit Netzwerken aus Kriminellen auszunutzen, um Geld zu waschen, das an das DPRK-Regime zurückfließt[16].

SWIFT

SWIFT ist eine Telekommunikationsinfrastruktur für den Finanzsektor, die die Netzwerke der Banken miteinander verbindet, um den Nachrichtenaustausch und den weltweiten Geldtransfer zwischen Banken zu erleichtern. Die Angriffe auf SWIFT gehen mindestens bis auf das Jahr 2013 zurück, als Bedrohungsakteure SWIFT für die Abwicklung betrügerischer Banküberweisungen nutzten[17]. Der vielleicht bekannteste Fall war der Angriff einen nordkoreanischen Bedrohungsakteurs auf die Bank of Bangladesh im Jahr 2016, bei dem 150 Millionen US-Dollar gestohlen wurden. Nach dem Angriff im Jahr 2016 kam es zu einer Häufung von Aktivitäten verschiedener Bedrohungsakteure, die auf die SWIFT-Infrastruktur von Banken in Russland, der Ukraine und Vietnam abzielten.

Nachdem die SWIFT-Banken das Customer Security Controls Framework (CSCF) eingeführt hatten, segmentierten sie ihre operativen Netzwerke mit der SWIFT-Infrastruktur und führten „sichere Zonen“ mit zusätzlichen Sicherheitsmaßnahmen sowie Überwachung in Echtzeit ein. Diese Maßnahmen haben die Möglichkeiten für Bedrohungsakteure eingeschränkt, von anderen exponierten Komponenten der Banken-Netzwerke in das SWIFT-System einzudringen und es zu nutzen. Dies hat dazu beigetragen, die Zahl der Angriffe zu reduzieren.

WithSecure™ ist der Ansicht, dass die Lockdown-Maßnahmen während der globalen Pandemie die Möglichkeiten der Bedrohungsakteure, logistische Ressourcen zu mobilisieren, die für die „Auszahlung“ aus betrügerischen SWIFT-Transaktionen erforderlich sind, wahrscheinlich weiter beeinträchtigt haben. Wie im Abschnitt „Staatlich organisierte Akteure“ dieses Berichts erörtert wird, hat auch die Verlagerung des Schwerpunkts von Lazarus auf Angriffe auf Kryptowährung-Infrastrukturen zum Rückgang der SWIFT-Angriffe beigetragen. Lazarus war bisher der Bedrohungsakteur, der am häufigsten für Angriffe auf SWIFT verantwortlich gemacht wurde.

Open Banking

Open Banking ist ein Standard, der Organisationen dabei unterstützen soll, die zweite Zahlungsdiensterichtlinie (PSD2: Second Payment Services Directive)[18] zu erfüllen, um anderen Finanzorganisationen den Zugang zu den Daten der Banken zu ermöglichen. In der Öffentlichkeit ist wenig über die Ausnutzung von Open Banking bekannt. Mit dem Anstieg des Online-Bankings und der Zahl der Banken, die heute vollständig online operieren, wird diese Infrastruktur jedoch zunehmend eingesetzt. Open Banking ist in hohem Maße auf APIs angewiesen. Es gibt mehr und mehr Hinweise[19] darauf, dass mit der zunehmenden Verbreitung der APIs auch deren Ausnutzung über verschiedene Technologien hinweg steigt.

[16] https://us-cert.cisa.gov/northkorea
[17] https://www.withsecure.com/content/dam/withsecure/en/business/common/collaterals/withsecure-threat-analysis-swift.pdf
[18] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[19] https://salt.security/api-security-trends

Die Consultants von WithSecure™ haben zusammen mit Finanzdienstleistern, die eine Open-Banking-Infrastruktur nutzen, Bedrohungsmodellierungen durchgeführt. Sie sind zu dem Schluss gekommen, dass eine Ausnutzung erhebliche technische Fachkenntnisse oder Insiderwissen erfordern würde. WithSecure™ geht davon aus, dass die opportunistische Ausnutzung zunehmen könnte, wenn Open Banking von einem größeren Kreis von Organisationen übernommen wird, von denen viele nicht so strengen Vorschriften und Standards für die Cybersicherheit unterliegen. Transaktionsdaten sind wertvolle Informationen, die Aufschluss über die Lebensgewohnheiten und die finanzielle Situation geben, und von einem fähigen Bedrohungsakteur ausgenutzt werden können. WithSecure™ geht jedoch davon aus, dass der Missbrauch von Open-Banking-Infrastrukturen, der Finanzdienstleister ernsthaft beeinträchtigen könnte, nur dann zunehmen wird, wenn Bedrohungsakteure eine profitable Methode zur Monetarisierung der Daten finden.

Geldautomaten

Angriffe auf Geldautomaten stellen ein fortlaufendes operatives Risiko und einen Kostenfaktor für Banken dar. In den von WithSecure™ durchgeführten Interviews betrachteten die Unternehmen dies jedoch nicht als wachsendes Problem oder größere finanzielle Herausforderung im Vergleich zu anderen Risiken. In einem Bericht hielt die EU EAST Expert Group on ATM and ATS Physical Attacks (EGAP) Anfang des Jahres 2021 fest, dass die Zahl der physischen Angriffe auf Geldautomaten seit Beginn der Pandemie um 19 Prozent zurückgegangen ist, auch wenn die mit den Angriffen verbundenen Gesamtkosten konstant geblieben sind. Im Gegensatz dazu sind die Häufigkeit von logischen Angriffen und Malware-Attacken auf Geldautomaten im selben Zeitraum um 44 Prozent und die Gesamtkosten um 14 Prozent gestiegen[20]. Dabei vermerkte der Bericht jedoch auch, dass die meisten dieser Angriffe trotz dieses Anstiegs erfolglos blieben.

Es ist offensichtlich, dass einige Geldautomatenmodelle immer noch anfällig für Kompromittierungen sind. Da kriminelle Gruppierungen auch weiterhin neue Technologien und Malware entwickeln werden, werden sie weiterhin Wege finden, um die sich verändernde Angriffsfläche auszunutzen[21]. Das Incident-Response-Team von WithSecure™ hat im Jahr 2021 die Verwendung von einfacher Geldautomaten-Malware wie beispielsweise Alice[22] in Europa beobachtet. Das „Jackpotting“ von Geldautomaten kann Bedrohungsakteuren beträchtliche Einnahmen bescheren. So wurden in diesem Jahr zwei Personen verhaftet, die bei Angriffen auf Geldautomaten einer bestimmten Marke in mehr als sieben europäischen Ländern mindestens 230.000 Euro gestohlen haben[23]. Diese Verluste sind für Banken jedoch nicht sehr groß und bleiben aufgrund der physischen Menge an Bargeld, die sich in diesen Geräten befindet, begrenzt – eine Beschränkung, die für SWIFT-Angriffe oder Ransomware-Attacken nicht gilt.

Befähigte Bedrohungsakteure, wie beispielsweise staatliche gestützte Gruppierungen, die im Interesse der DPRK operieren, haben bereits erfolgreich Geldautomaten-Angriffe durchgeführt. In diesen FASTCash-Cyberangriffen kamen zehn verschiedene Malware-Samples zum Einsatz. Die Angreifer kompromittierten die Geldautomaten und die SWITCH-Application-Server, um betrügerische Transaktionen und Auszahlungen zu ermöglichen. Die Cybersecurity and Infrastructure Security Agency (CISA) erklärte, dass „Nordkorea seit Februar 2020 wieder Banken in mehreren Ländern angreift, um betrügerische, internationale Geldüberweisungen und Auszahlungen an Geldautomaten zu veranlassen. Das jüngste Wiederaufleben folgt auf eine Pause nach den Angriffen auf Banken Ende 2019“[24]. Diese Angriffe sind deutlich komplexer als die üblichen Jackpotting-Angriffe auf Geldautomaten und umfassen auch die Kompromittierung der Banking-Infrastruktur vor der Monetarisierung an Geldautomaten-Terminals. Die nachfolgende Abbildung 2 gibt einen beispielhaften Überblick über einen von der DPRK gestützten Angriff, der im Jahr 2020 gemeldet wurde.

[20] https://www.association-secure-transactions.eu/tag/atm-physical-attacks/
[21] https://www.finextra.com/newsarticle/36242/diebold-nixdorf-warns-banks-of-compromised-atms
[22] https://www.trendmicro.com/en_us/research/16/l/alice-lightweight-compact-no-nonsense-atm-malware.html
[23] https://www.europol.europa.eu/newsroom/news/russian-speaking-hackers-arrested-in-poland-over-atm-jackpotting-attacks
[24] https://us-cert.cisa.gov/ncas/alerts/aa20-239a

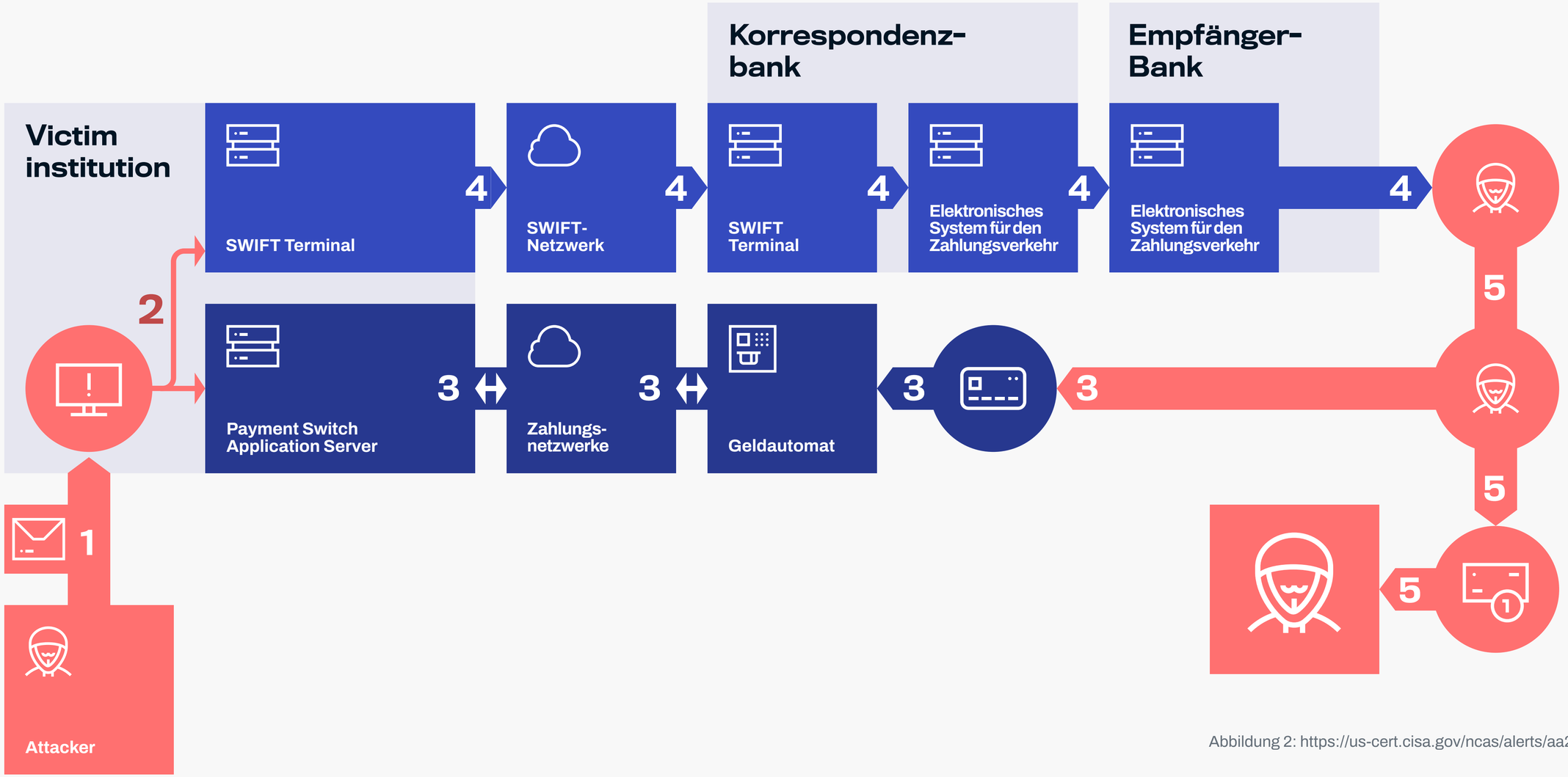


Abbildung 2: https://us-cert.cisa.gov/ncas/alerts/aa20-239a

Die Erkenntnisse von WithSecure™:

Der Trend, dass immer mehr Banken Kryptowährungen vorhalten, wird sich auch weiter verstärken. Die Zentralbanken in Ländern und Regionen wie den USA, Großbritannien, China und der EU haben bereits Vorschläge für ihre eigene, digitale Zentralbankwährung (CBDC: Central Bank Digital Currency) angekündigt. Daher wird die Absicherung von CBDC-Plattformen eine wichtige, technologische Entwicklung im Finanzdienstleistungssektor sein. Die Benutzerinteraktionen werden über mobile Anwendungen erfolgen, die kriminelle Organisationen oder staatlich gestützte Bedrohungsakteure voraussichtlich ebenfalls angreifen werden. Bedrohungsakteure, die auf CBDC-Plattformen abzielen, werden vermutlich finanzielle Motive verfolgen. Hierbei kann es sich beispielsweise um staatliche Gruppierungen wie aus der Demokratischen Volksrepublik Korea (DPRK) oder andere Cyberkriminelle handeln, die häufig betrügerische Angriffe auf bestehende Banking-Apps durchführen – mit Angriffswerkzeugen wie Click-Bots, mobiler Malware, Credential Stuffing, Overlay-Angriffen und Banking-Trojanern[25]. Darüber hinaus werden Geldwäsche und andere betrügerische Aktivitäten wahrscheinlich Bedrohungsakteure anziehen, die bereits mit Kryptowährungen vertraut sind und diese als eine attraktive Form der Währung ansehen, mit der sie arbeiten können.

[25] https://www.finextra.com/blogposting/20408/a-central-bank-digital-currency-challenges-and-opportunities26

Die größten Bedrohungen:

Cyberkriminalität

Alle Interview-Partner haben einen deutlichen Anstieg der Cyberkriminalität beobachtet, der von Phishing über die steigende Zahl an Initial-Access-Brokern (IABs) bis hin zu der damit verbundenen Bedrohung durch Ransomware reicht, die den befragten Finanzinstituten auch weiterhin große Sorgen bereitet. Auch die technischen Fähigkeiten einiger Cybercrime-Gruppen haben an Raffinesse gewonnen: Ein Befragter konnte feststellen, dass eine kriminelle Gruppierung in den vergangenen 12 Monaten erfolgreich die Multi-Faktor-Authentifizierung (MFA) umgangen hatte und so in der Lage war, Banking-Apps für Verbraucher zu kompromittieren.

Ransomware

In den Gesprächen, die WithSecure™ mit Finanzdienstleistern geführt hat, wurde Ransomware immer wieder als die Bedrohung mit der höchsten Priorität genannt. Der Grund hierfür ist die wahrgenommene Wirkung eines Ransomware-Angriffs auf die Resilienz eines Unternehmens: Ein Ransomware-Angriff kann zu erheblichen finanziellen Schäden, operativen Beeinträchtigungen sowie Reputationsverlust führen. Die kürzlich von Sophos veröffentlichten Statistiken stützen diese Wahrnehmung. So waren laut Sophos 34 Prozent der Finanzdienstleistungsunternehmen im vergangenen Jahr Ransomware-Angriffen ausgesetzt. 51 Prozent der Betroffenen gaben an, dass es den Cyberkriminellen gelungen ist, ihre Daten zu verschlüsseln[26]. Laut der Studie ließ sich zudem im Durchschnitt ein Drittel der Daten nicht wiederherstellen, obwohl die Finanzorganisationen das Lösegeld gezahlt hatten.

Das Risiko der Auswirkungen von Ransomware liegt nicht nur in direkten Angriffen auf Finanzdienstleister selbst. Auch Lieferanten und Partner können von Ransomware betroffen sein und erhebliche Unterbrechungen des Geschäftsbetriebs und Ausfallzeiten erleiden, die sich wiederum negativ auf den operativen Betrieb der Finanzdienstleister auswirken. Ransomware-Angriffe bergen somit nicht nur direkte, sondern auch indirekte Risiken – die Supply-Chain-Risiken, die aufgrund der Zusammenarbeit mit Lieferanten und Partnern auftreten und unmittelbare Auswirkungen auf die Finanzdienstleistungsunternehmen haben.

Die Bedrohungsakteure und das zugrundeliegende System, das Ransomware-Angriffe ermöglicht, haben sich in den vergangenen zwei Jahren in Umfang und krimineller Leistungsfähigkeit weiterentwickelt, wobei sich die führenden Bedrohungsakteure zunehmend spezialisieren und ihre technischen Fähigkeiten ausbauen. Auch die operativen Modelle und die Methoden für die Monetarisierung, wie beispielsweise die Erpressung mit gestohlenen Daten, haben sich weiterentwickelt, sodass die Kosten für Ransomware-Angriffe für die Unternehmen weiter steigen. Die Untersuchungen von Sophos haben ergeben, dass die durchschnittlichen Kosten eines Ransomware-Vorfalls für einen Finanzdienstleister 2,1 Millionen US-Dollar betragen – eine erhebliche Belastung für jedes Unternehmen.

[26] https://www.finextra.com/blogposting/20408/a-central-bank-digital-currency-challenges-and-opportunities26

Untersuchungen von WithSecure™ zeigen, dass Ransomware-Angriffe drei wesentliche Angriffsvektoren nutzen

- **Phishing:** Angreifer versuchen in der Regel, Ransomware-Malware direkt zu installieren, oder in Fällen, in denen die Clients über eine effektivere Filterung verfügen, Anmeldedaten durch Phishing zu sammeln, um Zugriff auf den Zielrechner zu erhalten.
- **Ungeschützte RDP-Server**: Angreifer versuchen oft, sich mit Brute-Force-Methoden Zugang zu verschaffen oder öffentlich gewordene Anmeldedaten zu nutzen.
- **Ausnutzung anfälliger Software:** Ransomware-Angriffe beginnen oft mit der Ausnutzung von anfälliger, nach außen gerichteter Software wie Firewalls oder VPN-Anwendungen.

Die zunehmende Ausnutzung von Schwachstellen ist eine auffallende Entwicklung, da diese Technik früher ausschließlich staatlich gestützten Bedrohungsakteuren vorbehalten war und nun auch häufiger von Ransomware-Angreifern eingesetzt wird. Wie bereits im Abschnitt „**Schwachstellen**“ erwähnt, haben Ransomware-Akteure[27], die Finanzdienstleister angriffen, Schwachstellen in SonicWall- und Pulse Secure VPN-Geräten ausgenutzt. WithSecure™ kann dies anhand von Incident-Response-Projekten sowohl für Finanzdienstleister als auch für Unternehmen in anderen Branchen bestätigen.

Traditionelle Banking-Trojaner wie TrickBot haben sich zu „Enablern“ von Ransomware entwickelt, wobei der Schwerpunkt nicht mehr auf den bisherigen Banking-Wurzeln liegt, sondern auf der Monetarisierung im Allgemeinen. Diese Entwicklung ist keine seismische Verschiebung, sondern verdeutlicht die Ertragskraft von Ransomware. Finanzdienstleister sollten sicherstellen, dass ihre Reaktionsmaßnahmen entsprechend aktuell sind, um diesen Malware-Familien und der veränderten Bedrohungslage Rechnung tragen zu können.

[27] https://withsecure.com/content/dam/WithSecure™/en/business/g/WithSecure™-threat-highlights-report-2021-08.pdf

Die Erkenntnisse von WithSecure™:

Ransomware

Die Auswirkungen von Ransomware werden auch in den nächsten 12 Monaten eine vorherrschende Bedrohung für Finanzdienstleister darstellen. Unternehmen sollten sicherstellen, dass sie die Entwicklungen der Vorgehensweise dieser kriminellen Gruppierungen im Auge behalten und sich weiterhin darauf konzentrieren, sowohl die Angriffsvektoren zu entschärfen als auch die Auswirkungen der Ausbreitung in ihren Netzwerken zu reduzieren. Realität ist, dass sie vermutlich irgendwann Opfer eines Angriffs werden, aber der Aufwand und die Kosten für die Behebung lassen sich mit angemessenen Maßnahmen für die Erkennung und Reaktion auf wenige Arbeitsstunden reduzieren.

Ransomware-Akteure konzentrieren ihre Bemühungen auf die einfachsten Ziele, die am ehesten bereit sind, ein Lösegeld zu bezahlen. Wie bereits erwähnt bedeutet dies, dass sich das Ransomware-Risiko für Finanzdienstleister auch auf die Supply-Chain erstreckt – das heißt, wenn Drittanbieter Opfer eines Angriffs werden. Diese Unternehmen investieren möglicherweise weniger in Cybersecurity-Maßnahmen als Finanzdienstleister, ein Angriff kann jedoch enorme Auswirkungen auf deren Business-Resilienz haben. Das Management dieses Supply-Chain-Risikos sowie die Annahme, dass Lieferanten und Partner kompromittiert werden könnten, wird sich als wertvoll erweisen, wenn Finanzdienstleister dies in die Entscheidungsfindung bei Beschaffungs- und Geschäftsprozessen einbeziehen.

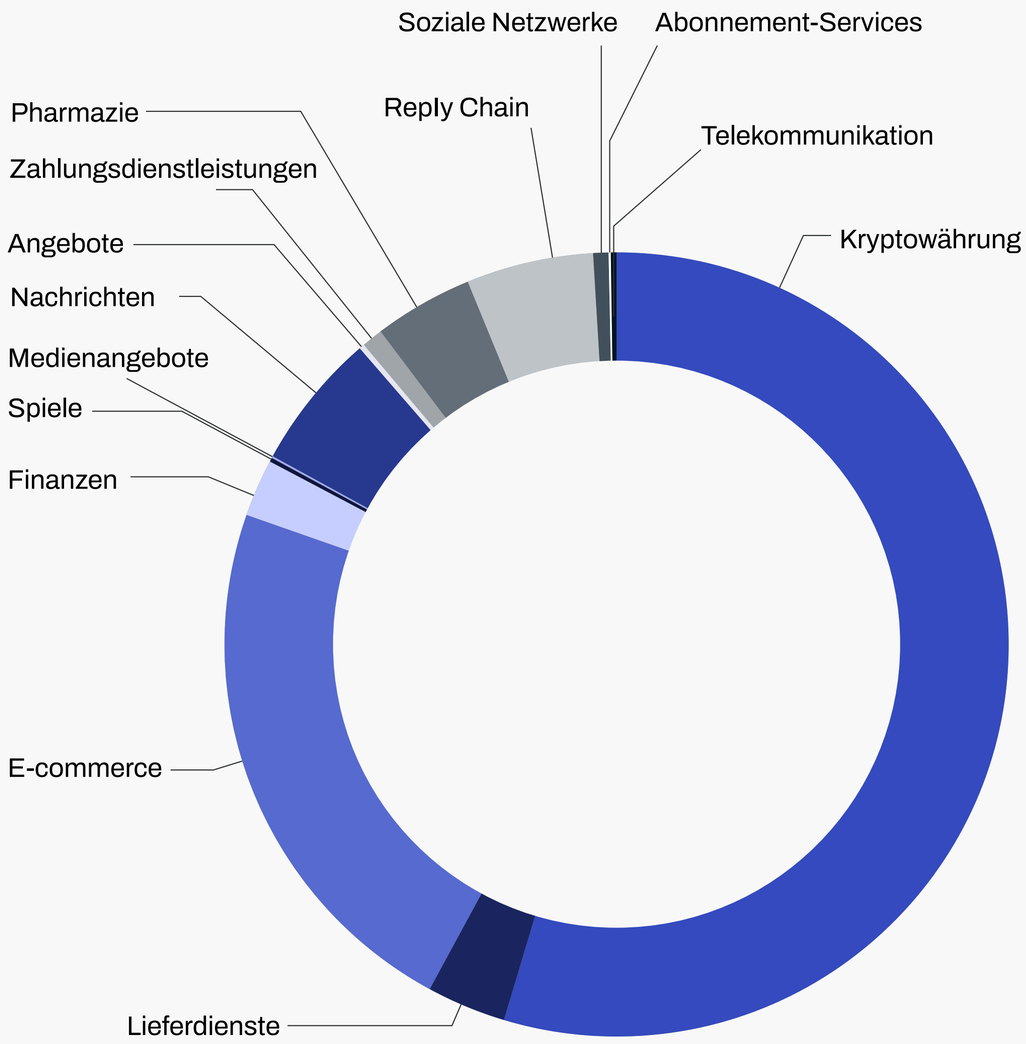
Phishing

Im vergangenen Jahr (2020) konnte WithSecure™ im Rahmen von Incident-Response-Fällen hochentwickelte Phishing-Kampagnen erkennen, die auf Finanzdienstleister abzielten und kompromittierte Konten nutzten, die dem Kunden des Zielunternehmens gehörten. „CEO-Fraud“ oder „Whale-Phishing“ wurde nur von einer Organisation, mit der WithSecure™ sprach, als besorgniserregend bezeichnet. Das Unternehmen gab an, dass dies zwar eine anhaltende Bedrohung sei, es in den vergangenen 12 Monaten jedoch zu keiner Eskalation kam.

Die meisten Unternehmen, mit denen WithSecure™ gesprochen hat, schätzten jedoch den Grad der Ausgereiftheit der Phishing-E-Mails, die sie gesehen hatten, als niedrig und nicht sehr zielgerichtet ein. Sie entsprachen den allgemeinen Phishing-Trends in Bezug auf das Thema, wie etwa Inhalte, die sich auf Covid bezogen. Dies steht im Einklang mit den Daten von WithSecure™. Diese zeigen, dass es sich meist um Standard-Phishing-Kampagnen handelt, die Adware, Malware und Credential-Harvesting (Diebstahl von Zugangsdaten) nutzen.

Eine staatliche Behörde für Cybersicherheit in Europa stellte einen enormen Anstieg an Cyberkriminalität fest, die sich gegen Verbraucher richtet. Insbesondere sei Smishing (Phishing über SMS-/Textnachrichten) „seit Oktober 2020 explosionsartig angestiegen… es dominiert unsere Arbeit“. Darüber hinaus wurde eine sehr gut organisierte Kampagne beobachtet, bei der in einer Woche ausschließlich ein bestimmtes Finanzunternehmen ins Visier genommen wurde und in der darauffolgenden Woche ein anderes Ziel der Kampagne war. Vor einer koordinierten Zusammenarbeit und einem Informationsaustausch zwischen dem privaten Sektor und staatlichen Organisationen wäre der Zusammenhang zwischen den Angriffen und der Verbreitung der Bedrohung durch koordinierte Phishing-Kampagnen nicht erkannt worden, was die Möglichkeiten zur Prävention und Reaktion auf die Bedrohung einschränkte. Dies unterstreicht den Wert der Zusammenarbeit und des Informationsaustauschs zwischen Finanzorganisationen.

Die häufigsten Spam-Themen, die WithSecure™ identifizieren konnte



Staatlich organisierte Akteure

In den Gesprächen, die WithSecure™ mit Finanzdienstleistern geführt hat, wurden staatliche Bedrohungsakteure als ein geringeres Risiko im Vergleich zu Ransomware-Akteuren eingestuft. Auf die Frage nach einer Begründung für diese Einschätzung gaben die Unternehmen an, dass sie wahrscheinlich nur ein drittrangiges Ziel für staatlich organisierte Akteure darstellen – abgesehen von den finanziell motivierten DPRK-Gruppen. Die staatlichen Bedrohungsakteure würden versuchen, sich Zugang zu Finanzaufsichtsbehörden oder Regierungsinstitutionen zu verschaffen, um sich Zugriff auf nachrichtendienstlich wertvolle Daten zu verschaffen. Die Auswirkungen für die Finanzdienstleister selbst wären geringer als bei einem Ransomware-Angriff.

Demokratische Volksrepublik Korea (DVRK)

Die staatlich gestützten Gruppierungen der DVRK sind die bekanntesten, die es auf Finanzdienstleistungen abgesehen haben. Der UN-Sicherheitsrat hat in der Vergangenheit über die kriminellen Methoden der DVRK berichtet, die darauf abzielen, „Gelder von Finanzinstituten und Kryptowährungsbörsen zu stehlen“[28], um die militärischen und nuklearen Programme des Regimes zu finanzieren. Diese Prioritäten bleiben für das DVRK-Regime bestehen und sind eine ständige Motivation für finanziell motivierte Cyberangriffe.

Seit dem Jahr 2015 ist die Lazarus-Gruppe (APT38) für die Auszahlungen an FASTCash-Geldautomaten sowie für den betrügerischen Missbrauch von kompromittierten SWIFT-Endpunkten, die von Banken betriebenen werden, verantwortlich. Laut CISA hat die Gruppierung BeagleBoyz, die Überschneidungen mit Lazarus aufweist, seit dem Jahr 2015 versucht, rund 2 Milliarden US-Dollar zu stehlen: „Sie haben kritische Computersysteme von Banken und anderen Finanzinstitutionen manipuliert und außer Betrieb gesetzt.[29]“

In den vergangenen zwei Jahren haben diese Gruppierungen ihren Schwerpunkt jedoch auf den lukrativen Diebstahl von Kryptowährungen verlagert. In einer weiteren Warnung [30] hat die CISA darauf hingewiesen, dass die Lazarus-Gruppe im vergangenen Jahr in mehr als 30 Ländern Malware eingesetzt hat, die sich als Handelsplattformen für Kryptowährungen getarnt hat. Auch WithSecure™ [31] konnte eine lang andauernde Kampagne der Lazarus-Gruppe identifizieren, die im Jahr 2020 auf Kryptowährungsorganisationen abzielte, um sich finanziell zu bereichern. ClearSky-Analysten stellten weitere Aktivitäten dieser Gruppierung fest, die sich auf den Diebstahl von Krypto-Wallets konzentrierten. Nach deren Schätzungen könnte dies zum Diebstahl von Hunderten von Millionen Dollar geführt haben[32].

Die von der Demokratischen Volksrepublik Korea unterstützten Bedrohungsgruppen haben eindeutig die klare Absicht und auch die Möglichkeiten, Angriffe auf Finanzdienstleistungsunternehmen durchzuführen, finanzielle Verluste und Kosten für die Wiederherstellung zu verursachen und dabei deren Ruf zu schädigen. WithSecure™ geht davon aus, dass sich die Entwicklung, Kryptowährungen zu stehlen, fortsetzen wird – insbesondere da die Bestände der Banken an digitalen Währungen und Kryptowährungen wachsen. Die Auswirkungen erfolgreicher Angriffe dieser Bedrohungsgruppen sind gravierend. Finanzunternehmen wären gut beraten, die Aktivitäten dieser Gruppierungen zu verfolgen und Maßnahmen zu entwickeln, um diesen Bedrohungen zu begegnen.

[28] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf
[29] https://us-cert.cisa.gov/ncas/alerts/aa20-239a
[30] https://us-cert.cisa.gov/ncas/alerts/aa21-048a
[31] https://labs.withsecure.com/assets/BlogFiles/withsecureLABS-tlp-white-lazarus-threat-intel-report2.pdf
[32] https://www.clearskysec.com/cryptocore-lazarus-attribution/

Russland

Die von Russland ausgehenden Bedrohungen im Zusammenhang mit dem Hackerangriff auf das SolarWinds-System[33] standen im Jahr 2021 in vielen Diskussionen im Vordergrund. Diese massive Cyberattacke hat das Risiko einer Supply-Chain-Kompromittierung und das hohe Maß an technischen Fähigkeiten, das russische Gruppierungen einsetzen können, deutlich gemacht. Die Attacken hatten auch einige Auswirkungen auf Finanzdienstleistungsunternehmen, zu den Opfern gehörten auch Zentralbanken. Die Absicht, Finanzdienstleister des privaten Sektors direkt zu kompromittieren, tritt jedoch weniger deutlich zu Tage.

In den Gesprächen, die WithSecure™ mit Finanzdienstleistern führte, herrschte Einigkeit darüber, dass die technischen Fähigkeiten von NOBELIUM, Angriffsvektoren in der Cloud und in Supply-Chains auszunutzen, es erfordern, diese Bedrohung zu beachten und in deren Bekämpfung zu investieren. Diese Einschätzung ist auch dadurch beeinflusst, dass die Befragten davon ausgehen, dass andere kriminelle Gruppierungen möglicherweise ebenfalls Finanzdienstleistungsunternehmen ins Visier nehmen, und ihre Methoden nachahmen. Der Kaseya-REvil-Angriff, der Anfang dieses Jahres ein Element der Supply-Chain betraf, könnte ein Indiz für den Versuch einer Nachahmung sein.

Die von Russland aus agierenden Bedrohungsakteure verfügen über ein hohes Maß an technischen Fähigkeiten, gezielte Angriffe mit Schwerpunkt auf Cloud-Infrastrukturen durchzuführen[34]. Die Kompromittierung staatlicher Finanzorganisationen birgt auch für private Finanzdienstleister ein Risiko, da die bei diesen Angriffen gestohlenen Informationen als Waffe gegen sie eingesetzt werden könnten. Diese Gruppierungen haben bisher keine klaren Absichten gezeigt, Finanzdienstleister des privaten Sektors ins Visier zu nehmen. Nach Einschätzung von WithSecure™ besteht jedoch eine begründete Wahrscheinlichkeit, dass Finanzdienstleister aufgrund der geopolitischen Dynamik und ihrer Rolle als CNI in Zukunft ins Visier dieser Gruppierungen geraten könnten. Finanzdienstleistungsunternehmen sollten sich dieser Bedrohungen und neuer technischer Methoden bewusst sein, die von anderen Bedrohungsgruppierungen in größerem Umfang genutzt werden könnten. Im Vergleich jedoch zu den Bedrohungen, die von Ransomware und von den DVRK-gestützten Gruppierungen ausgehen, sollten diese weniger Priorität haben.

[33] https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

[34] https://us-cert.cisa.gov/ncas/alerts/aa21-116a

China

In den Gesprächen mit WithSecure™ haben Finanzdienstleister Bedenken geäußert, dass vom chinesischen Staat gestützte Gruppierungen Zero-Day-Schwachstellen ausnutzen könnten. Die HAFNIUM-Angriffe, die Zero-Day-Schwachstellen des Microsoft Exchange Servers[35] ausgenutzt haben, sowie die Pulse Secure VPN-Angriffe[36] sind die jüngsten Belege für diese kriminellen Fähigkeiten. Berichten zufolge waren in beiden Fällen Finanzdienstleistungsunternehmen direkt von diesen Angriffen betroffen.

Vom chinesischen Staat unterstützte Bedrohungsakteure nutzen auch die Supply-Chain für die Kompromittierungen. Diese reichen mindestens bis in das Jahr 2017 zurück. Damals kompromittierte eine kriminelle Gruppierung mehr als 2,27 Millionen Avast-Nutzer und spielte ein schadhaftes Update ein. Ein kleiner Teil der Angriffsopfer wurde mit einem Second-Stage-Trojaner infiziert, vermutlich zu Spionagezwecken[37]. Jüngste Berichte haben wieder das Ausmaß der technischen Fähigkeiten dieser vom chinesischen Staat unterstützten Gruppierungen aufgezeigt. Bedrohungsakteure, die mit der chinesischen Volksbefreiungsarmee (PLA) in Verbindung stehen, verfügen dank einer Reihe staatlicher Ressourcen zudem über logistische Unterstützung, einschließlich des Einsatzes von HUMINT-Operationen (Human Intelligence) zur Ausnutzung von Computernetzwerken (CNE: Computer Network Exploitation)[38].

Im Jahr 2017 gab das Finanzdienstleistungsunternehmen Equifax bekannt, dass vom chinesischen Staat unterstützte Hacker die Kreditinformationen von 147,9 Millionen Amerikanern gestohlen haben[39]. Jüngste Aktivitäten wie die HAFNIUM-Angriffe auf Microsoft Exchange Server belegen die Absicht, Daten aus E-Mails der europäischen Bankenaufsichtsbehörde (EBA: European Banking Authority) zu sammeln[40]. Die EBA erfasst und speichert große Mengen sensibler Daten über Banken und deren Kreditvergabe. Berichten zufolge verblieb der Angreifer auf den E-Mail-Servern des Opfers und versuchte nicht, sich innerhalb des kompromittierten Netzwerks auszubreiten. Dies deutet darauf hin, dass das Ziel des Angreifers ausschließlich die Exfiltration von den Daten der E-Mail-Server war. Jüngsten Berichten zufolge besteht die Möglichkeit, dass die von HAFNIUM bei den Angriffen auf Microsoft Exchange Server gestohlenen Daten in Chinas KI-Wissensbasis eingespeist werden könnten[41].

Obwohl für diese Behauptung keine ausreichenden Beweise vorliegen, gibt es Anhaltspunkte dafür, dass vom chinesischen Staat unterstützte Cyberoperationen in den vergangenen Jahren große Mengen an personenbezogenen Daten von Bürgern gesammelt haben.

Diese staatlich unterstützten Cyberoperationen sind als eine Erweiterung der politischen, wirtschaftlichen und militärischen Agenda in China zu betrachten. WithSecure™ geht davon aus, dass Bedrohungsakteure, die im Auftrag der chinesischen Regierung operieren, Finanzorganisationen aus Spionagegründen ins Visier nehmen, um Informationen zu sammeln, die für den chinesischen Staat von nachrichtendienstlichem Wert sind. Dabei gehen diese Cyberoperationen über traditionelle nachrichtendienstliche Aktivitäten hinaus und umfassen auch wirtschaftliche Aspekte wie den Diebstahl geistigen Eigentums sowie die Sammlung personenbezogener Daten.

[35] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[36] https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html
[37] https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/
[38] https://asia.nikkei.com/Business/Technology/Japan-lashes-out-against-alleged-Chinese-military-cyberattacks
[39] https://www.#i.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020
[40] https://www.reuters.com/article/us-microsoft-hack-eba-idUSKBN2B01RP
[41] https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

Über WithSecure™

WithSecure™ ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endpoints und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ ist Teil der 1988 gegründeten F-Secure Corporation, die an der NASDAQ OMX Helsinki Ltd. gelistet ist.

W / T H
secure