Jamie Collier

Cyberkriminalität – **aktuelle Bedrohungen**, Angreifer **und Gegenmaßnahmen**

Der neueste M-Trends-Bericht von Mandiant bestätigt, dass Gewerbe und professionelle Dienstleistungen sowie die Finanzbranche im Jahr 2021 am häufigsten Ziel von Hackerangriffen waren (jeweils 14 Prozent). Der Bericht basiert auf Ermittlungen von vorderster Cyberfront und der Bekämpfung von folgenreichen Angriffen weltweit. Ein Vergleich der Ergebnisse zeigt, dass jedes Jahr weltweit dieselben Branchen ins Visier genommen werden. Die beiden Hauptgründe: die fortgeschrittene digitale Transformation und die immer wichtiger werdende Vernetzung.

„Cybersicherheit ist ein Thema für das Topmanagement."

Diese Faktoren vergrößern die Bedrohungslandschaft und je stärker die internen Computernetzwerke des Finanzsektors miteinander verflochten sind, desto anfälliger werden sie für Angriffe von außen. Die gute Nachricht ist, dass Sicherheitsverantwortliche das Problem gezielt angehen können. Dazu müssen sie die neuesten Informationen über potenzielle Angreifer haben und die von ihnen verwendeten Techniken, Taktiken und Verfahren (TTPs) im Detail kennen.

Cybersicherheit wird zur Chefsache

In den vergangenen Jahren hat sich der Fokus vieler Hackergruppen verlagert. Insbesondere im Finanzsektor setzen sie am häufigsten Ransomware ein. Nachdem sie sich so Zugriff auf die Computernetzwerke eines Unternehmens verschafft haben, verschlüsseln sie wichtige Daten oder ganze Systeme und nehmen diese in „Geiselhaft". Anschließend erhalten die betroffenen Kreditinstitute eine Lösegeldforderung.

Solche Ransomware-Attacken waren in der Vergangenheit häufig das Ergebnis von Malware-Spamming, also der massenhaften Verbreitung von Schadsoftware. Mittlerweile lässt sich ein neues Muster erkennen: der gezielte und teilweise monatelang vorbereitete Angriff auf sorgfältig ausgewählte Institute.

Die wichtigsten Bedrohungen für den Finanzsektor

Das verändert die Sichtweise, die Banken auf das Thema haben sollten. Geraten sie ins Visier von Cyberkriminellen, liegt nicht länger ein zufälliges, singuläres Ereignis zugrunde. Vielmehr handelt es sich um ein strategisches Problem. Damit verändert sich auch die Zuständigkeit in den Kreditinstituten: Cybersicherheit ist nicht nur ein Thema für die IT-Abteilung, sondern auch für das Topmanagement auf Vorstands- und Aufsichtsratsebene.

Für die Gefahrenabwehr gilt einmal mehr die bewährte Regel: Kenne deine Feinde besser, als sie sich selbst kennen. Zwar ändern Cyberkriminelle ihre Taktiken regelmäßig, es lassen sich aber dennoch ganz bestimmte Muster identifizieren. Wer diese Muster kennt, zum Beispiel weil er sich der Expertise von Threat Intelligence bedient, also dem Wissen über die Vorgehensweisen von Angreifern, kann die richtigen Dinge priorisieren und die richtigen Hebel in Bewegung setzen, um seine Netzwerke vor den größten Gefahren zu schützen.

Finanziell motivierte Angriffe machten wie in den Vorjahren auch im Jahr 2021 den Großteil der Angriffe aus: 3 von 10 Angriffen zielten auf monetäre Gewinne ab. Dazu wurden Methoden wie Erpressung, Lösegeldforderung, Diebstahl von Zahlungskarten und illegale Überweisungen eingesetzt.

Hacker nehmen für Ransomware-Attacken viel Vorbereitungszeit in Kauf. Sie bewegen sich in den Netzwerken ihrer Opfer oft lange unbemerkt, bis sie schließlich zuschlagen. Sie lernen die Systeme genau kennen und identifizieren die Netzwerkbereiche, die für das Unternehmen überlebenswichtig sind und deren Manipulation besonders schmerzt. Entsprechend hoch kann das Lösegeld ausfallen. Über die vergangenen Jahre sind die Erpressungsgelder drastisch gestiegen. Zuweilen suchen sich Hacker auch Insider aus der Organisation, die ihnen Zugang verschaffen.

Hinzu kommt, dass sich spezialisierte Hackergruppen immer häufiger zusammenschließen, um den maximalen Nutzen aus ihren jeweiligen Stärken zu ziehen und noch komplexere Angriffe wie Kompromittierungen der Lieferkette durchführen

zu können. Zu einem zusätzlichen Problem kann sich eine solche Kooperation entwickeln, wenn es zum Streit zwischen einzelnen Gruppen kommt, obwohl gefordertes Lösegeld gezahlt wurde. Unternehmen sollten keine Ehre unter Dieben erwarten: Es ist schon vorgekommen, dass die versprochene Freigabe der gestohlenen Daten nicht erfolgte und das erpresste Kreditinstitut zum Kollateralschaden eines hackerinternen Konflikts wurde.

Erpressung

Ein weiterer Trend: Ransomware-Attacken werden immer häufiger als vielschichtige Erpressungsversuche geplant. Die Verschlüsselung wichtiger Systeme bildet hierbei nur die erste Stufe des Angriffs. Die zweite Stufe ist die Drohung, geheime Informationen zu veröffentlichen. Dies führt zu einer strategischen Bedeutsamkeit für das erpresste Kreditinstitut: Wenn Hacker die Presse und die Öffentlichkeit direkt darauf aufmerksam machen, dass sie im Besitz wichtiger, auch für die Kunden der Kreditinstitute kompromittierender Informationen sind, kann dies die Reputation des Unternehmens nachhaltig schädigen.

„Die Preisgabe sensibler Informationen kann gefährlicher sein als eine diskret abgewickelte Erpressung."

Die Ankündigung der Preisgabe sensibler Informationen kann gefährlicher sein als eine diskret abgewickelte Erpressung. Hier haben es Finanzinstitute dann mit einem interdisziplinären Abwehrkampf zu tun, der neben der IT-Abteilung und dem Vorstand unter anderem auch die Öffentlichkeitsarbeit und die Rechtsabteilung mit einschließt.

Hackergruppen nutzen eine Vielzahl von Angriffsmustern, um sich Zugang zu verschaffen und Kreditinstitute zu kompromittieren:

– Zero-Day-Exploits sind meist sehr simple Software-Sicherheitslücken, die dem Hersteller noch nicht bekannt sind und für die es deshalb auch keinen Patch oder ein Update gibt. Hacker nutzen ihren Wissensvorsprung, um über die Sicherheitslücke Schadsoftware in das Netzwerk einzuschleusen. Vor allem chinesische Hackergruppen haben solche Sicherheitslücken in der Vergangenheit immer wieder ausgenutzt, sogar um in Netzwerke von Regierungsorganisationen einzudringen.

– Lieferketten-Angriffe gehören zu den neueren Trends. Die zunehmende Spezialisierung der Angreifer und der Zusammenschluss einzelner Hackergruppen mit unterschiedlichen Fähigkeiten haben ihnen neue Möglichkeiten eröffnet. Statt etwa eine Bank anzugreifen, wird ein Unternehmen infiltriert, dessen Software bei möglichst vielen Kreditinstituten verwendet wird. Über diese Lieferkette dringt der Hacker dann in viele andere Institute ein. Man könnte sagen: Statt sich den Schlüssel für ein Unternehmen zu besorgen, stehlen die Hacker den Generalschlüssel. Ein bekanntes Beispiel ist der Einbruch von mutmaßlich russischen Hackern in mehrere Behörden- und Unternehmensnetzwerke über eine Hintertür in der Software des IT-Unternehmens SolarWinds Ende des Jahres 2020.

– Beim Web-Skimming „phischen" Hacker die Zahlungsmitteldaten von Kunden auf Webshops oder Bezahlseiten ab und stehlen ihnen anschließend Geld. Das geschieht meist über einen Lieferketten-Angriff, bei dem der Schadcode über einen zuvor infiltrierten Drittanbieter auf der Website des E-Commerce-Händlers ausgeführt wird. Da die Bankdaten ihrer Kunden auf diese Weise gestohlen werden, sind auch die Kreditinstitute selbst von diesem Angriff betroffen.

– Der Diebstahl von Kryptowährungen ist für Hacker auf zweierlei Weise interessant: Sie stehlen die Währung, um sich zu bereichern, aber sie nutzen die schwer nachvollziehbaren Bewegungen von Kryptowährungen auch, um damit Geld zu waschen. Opfer dieser Diebstähle sind nicht nur die Besitzer von Bitcoin, Ethereum und Co., sondern auch deren Emittenten.

Die überwiegende Mehrheit der finanziell motivierten Operationen wird von aufstrebenden Cyberkriminellen durchge-

Dr. Jamie Collier

Senior Threat Intelligence Advisor, Mandiant, London

Kreditinstitute geraten verstärkt ins Visier von Hackern weltweit. Die große Vernetzung der Kreditwirtschaft, die zunehmende Digitalisierung sowie die Fülle von sensiblen Daten machen die Institute zu einem lohnenswerten Ziel. Dabei reicht die kriminelle Motivation von rein finanziellen Interessen über Rufschädigung bis hin zu Destabilisierung der Wirtschaftssysteme und psychologischer Kriegsführung, wie der Autor anhand des aktuellen M-Trends-Berichts ausführt. Die gute Nachricht: Banken können sich wehren, wobei Cybersicherheit zur Chefsache werden muss. Bei der Abwehr von Angriffen, seien es Spionage- oder Ransomware-Attacken, gilt laut Autor: Je besser die Strategien der Angreifer bekannt sind, desto effektiver können sie abgewehrt werden. Um den Angriffslebenszyklus zu schwächen, sollten auch die Abwehrmaßnahmen mehrstufig sein, beispielsweise indem Netzwerke mit unterschiedlichen Barrieren versehen werden. Gleichzeitig empfiehlt der Autor die Hinzuziehung externer Experten, die die Systeme permanent auf Schwachstellen testen und so die Resilienz der Kreditinstitute erhöhen. (Red.)

führt. Der Finanzsektor ist jedoch auch staatlichen Bedrohungen ausgesetzt. Groß angelegte Hackerangriffe werden oftmals von staatlich unterstützten Gruppen begangen. Die Hauptakteure sind die „Big Four" China, Iran, Nordkorea und Russland. Was ist ihre Motivation? Sie kann sehr unterschiedlich sein, wie Beispiele aus Nordkorea und Russland zeigen.

Vermehrt staatlich unterstützte Hackerangriffe

Im Fall von Nordkorea sind es vor allem politische und finanzielle Motive, die denen von nicht staatlich unterstützten Cyberkriminellen ähneln. Das Regime in Pjöngjang ist aufgrund von Sanktionen von so vielen Geldströmen abgeschnitten, dass Cyberoperationen ein immer wichtigeres Mittel der Staatsfinanzierung geworden sind. Zudem leidet die Wirtschaft stark unter der Corona-Pandemie, was einen weiteren Anreiz für Cyberaktivitäten zur Geldbeschaffung bietet. So geht zum Beispiel die groß angelegte Attacke mit der Schadsoftware WannaCry, die 2017 hunderttausende Computer in 150 Ländern befiel und unter anderem das britische Gesundheitssystem NHS oder die Deutsche Bahn infizierte, vermutlich auf eine nordkoreanische Hackergruppe zurück.

> „Groß angelegte Hackerangriffe werden oftmals von staatlich unterstützten Gruppen begangen."

Im Fall von Russland sind viele Cyberangriffe politisch motiviert. Viele Attacken der Vergangenheit waren gezielt auf eine Destabilisierung der Ukraine ausgerichtet. Seit Beginn der Krise in der Ukraine setzen Hacker vor allem Wiper Malware ein, die wichtige Daten in den gehackten Netzwerken einfach löscht. Teilweise kam es auch zu vergleichsweise technisch einfachen Attacken auf ukrainische Kreditinstitute mit der Zielsetzung, die Bevölkerung zu verunsichern. Wenn beispielsweise viele Ukrainer die Nachricht erhalten, dass sie keinen Zugang mehr zu ihren Bankkonten hätten, verbreitet sich schnell Panik.

Kreditinstitute können sich wehren

Cyberattacken sind auch Teil der psychologischen Kriegsführung. Es ist durchaus wahrscheinlich, dass russische Hacker auch hierzulande mit ähnlichen Methoden angreifen – als Vergeltungsmaßnahme für die Sanktionen gegen Russland und die Unterstützung, die Deutschland der Ukraine gewährt.

Hacker greifen Computersysteme häufig in mehreren Phasen an. Sie müssen ein Einfallstor ausfindig machen, die richtigen Subsysteme finden, Daten stehlen und verschlüsseln, Malware einschleusen und können erst dann zum großen Schlag ausholen. Diese Schritte kann man als „Angriffslebenszyklus" bezeichnen.

> „Um Attacken in den verschiedenen Phasen abfangen zu können, sollten auch Gegenmaßnahmen mehrstufig sein."

Vom Opfer zum aktiven Akteur

Um Attacken in den verschiedenen Phasen abfangen zu können, sollten auch die Gegenmaßnahmen mehrstufig sein. Zum Beispiel, indem die Netzwerke mit unterschiedlichen Barrieren versehen werden, welche die Hacker daran hindern, die nächste Stufe ihres Angriffsplans zu starten. Möglich ist dies beispielsweise mittels einer systematischen Risikobewertung der eigenen IT-Infrastruktur und der anschließenden Installation von individuell ausgewählten Cybersicherheitslösungen.

Zu wissen, wie aktive Hackergruppen in den einzelnen Szenarien agieren, erlaubt es IT-Security-Spezialisten, Kreditinstitute gegen eingeschleuste Malware zu immunisieren und sie zum Schutz ihrer Systeme zu befähigen. Wer externe Experten hinzuzieht, kann sicherstellen, dass diese die Systeme testen und sichert sich gleichzeitig das notwendige Wissen, um einer immer stärker ausdifferenzierten Bedrohung entgegentreten zu können.

Somit ergibt sich neben dem technischen auch ein wichtiger psychologischer Nutzen: Kreditinstitute sind nicht mehr länger nur in der Opferrolle, sondern aktive Akteure, die ihre Cyberresilienz stärken und ihre sensiblen Daten – und die ihrer Kunden – nachhaltig schützen.