Christian Kothe

Cybersicherheit – Bedrohungen besser verstehen und abwehren

Die Bedrohung der Finanzdienstleistungsindustrie durch Cyberattacken wächst fortlaufend in immer neuen Varianten. Das erfordert ein weltweit konzertiertes Vorgehen in der Finanzbranche. Für seine Mitgliedsinstitute in der ganzen Welt hat SWIFT dazu das „Customer Security Program" (CSP) entwickelt, das sie bei der Sicherung ihres operativen Umfelds gegen Cyberangriffe umfassend unterstützt. Anleitungen für die Praxis und ein Regelwerk obligatorischer Sicherheitsstandards sowie weitere Richtlinien decken die Transaktionskette im System der Kunden vollständig ab und helfen, Schwachstellen aufzudecken und zu beseitigen.

Um Einblick in die hinter den Cyberangriffen stehenden Kräfte zu gewinnen, deren Angriffsmuster zu identifizieren, eine gemeinsame Sprache rund um Cybersicherheit zu schaffen und so der Industrie zu einer noch besseren Cyberabwehr zu verhelfen, hat das „SWIFT Institute" zur Förderung von Forschungen für die Finanzindustrie drei unabhängige neue Studien in Auftrag gegeben.[1)] Die hierin vertretenen Ansichten spiegeln die Meinungen der Autoren und nicht unbedingt diejenigen von SWIFT oder dem SWIFT Institute wider. Im Folgenden werden die drei Papiere mit ihren wesentlichen Erkenntnissen und Aussagen vorgestellt.

Einblick in die Bedrohungslandschaft

„Forces Shaping the Cyber Threat Landscape for Financial Institutions" von William A. Carter[2)] zielt ab auf das Verständnis derjenigen Kräfte, die die Bedrohungslandschaft formen. Dahinter steht die Überzeugung, dass dieses Verständnis entscheidend ist für die Finanzinstitute, um ihre Gegner im Cyberspace einholen zu können und ihnen letztlich voraus zu bleiben.

Die in Finanznetzwerken zunehmend genutzten neuen Technologien und das Internet vergrößern das Feld für Cyberangreifer erheblich. Auch die Erfolgsanreize für Angriffe sind größer geworden und zwingen Banken, sich weitaus zahlreicherer und immer raffinierterer Attacken zu erwehren. Gegen neue Abwehrmaßnahmen variieren auch die Angreifer ihr Vorgehen, um sich neue Zugänge zu verschaffen.

Der gewöhnliche Betrug mit Verbraucherbank-Zahlkarten und Kreditkarten am Point of Sale (PoS) ist trotz abnehmender Dominanz noch vorherrschend, wenn auch Objekte und Taktiken sich ändern – Betrüger zielen zunehmend auf Mobilgeräte und Geschäftskunden. Die Digitalisierung verändert zudem die Geografie der Finanzkriminalität, indem sie Milliarden neuer Nutzer in den Entwicklungs- und Schwellenländern online stellt. Das verschafft Kriminellen neue Zielgebiete mit begrenztem Gefahrenbewusstsein und schwachen Abwehrmöglichkeiten. Die aufstrebenden Märkte in Asien sind derzeit Hauptziele, aber da auch Millionen neuer Kunden in Lateinamerika und Afrika online gehen, blühen dort ebenso kriminelle Gruppen auf.

Christian Kothe, Head of Markets & Initiatives EMEA, SWIFT, Frankfurt am Main

Für den interessierten Beobachter und Kunden ist es schon beängstigend, immer wieder von neuen Bedrohungen des digitalen Bankgeschäftes durch Cyberattacken zu hören. Aber auch Aufseher, Wissenschaftler und die Wirtschaft kümmern sich um das Thema und suchen die Strukturen der Angriffe zu verstehen und zu bekämpfen. So verweist der Autor anhand von drei aktuellen Studien seines Hauses nicht nur auf neue Cybergefahren für Finanzinstitute etwa durch unsichere Mobil- und IoT-Geräte, durch koordinierte Cyber-Großangriffe krimineller Organisationen und die Aktivitäten neuer Cybermächte, sondern er verweist auch auf erfolgversprechende Gegenmaßnahmen und Lösungsansätze. So konnten in drei Kategorien des Insiderverhaltens 54 Verhaltensmuster für Insiderbetrug mit den Quellen klassifiziert und in einer Liste zusammengefasst werden. Zur Abwehr der vielfältigen Angriffe plädiert er für eine enge Zusammenarbeit aller Beteiligten in der Finanzindustrie und darüber hinaus einschließlich eines Netzwerkes für den Austausch von Warnungen vor drohenden Cyberbetrugsaktivitäten (Red.)

Koordinierte Großangriffe

Während Betrugsverhütung und Verbrauchersicherheit gestiegen sind, haben Cyberkriminelle großangelegte koordinierte Angriffe auf die internen Netzwerke von Finanzinstitutionen gestartet. Ihr Ziel ist es, wenige, dafür aber sehr hohe Auszahlungen zu erbeuten anstelle vieler kleiner. Zudem ist Erpressung eine der großen Sorgen der Finanzinstitute, seit IoT-Botnetze (IoT - Internet of Things) und Massenaussendungen ausgeklügelter Ransomware Banken offline zu stellen drohen.

Kampagnen zur Warnung vor unvorsichtigem Anklicken unbekannter Links haben herkömmliche Phishing-Angriffe weniger wirkungsvoll gemacht. Angreifer versuchen daher immer häufiger, über vorgetäuschte Identitäten Zugang zu Banknetzwerken zu erhalten. Gelingt das, so kombinieren sie mehrere Cashout-Strategien, um Millionenbeträge abzuziehen. Die Banken sind dann vielschichtigen DDoS-Angriffen (DDoS – Distributed Denial of Service) ausgesetzt, mit denen Kriminelle die Spuren ihrer Datendiebstähle und betrügerischen Transaktionen mithilfe von Ransomware verwischen.

Die Cyberabwehr muss sich auch auf neue Gegner einstellen: Steigende geopolitische Spannungen zwischen existierenden Cybermächten führen zu verstärktem Ausspionieren von Finanzinstitutionen und zu Störattacken. Inzwischen haben sich auch nationalstaatliche Akteure auf finanziell motivierte Cyberkriminalität verlegt. Mit mehr als 30 Ländern, die in diese Entwicklung von Cyberfähigkeiten investiert haben, weitet sich die nationalstaatliche Bedrohungsszenerie dramatisch aus.

Zugleich hat die Verbreitung von leicht einsetzbarer Malware und Auftragshackern im Darknet einem weiten Kreis die Möglichkeit raffinierterer Attacken eröffnet. Was anfangs nur für staatliche Experten verfügbar war, ist nun auch organisierten Gruppen, die zum Teil mit Regierungen zusammenarbeiten, und gewöhnlichen Cyberkriminellen über offene Malware-Bibliotheken zugänglich. Automatisierung ermöglicht zudem, solche Ressourcen ohne viel Aufwand in großem Maßstab noch wirkungsvoller zu nutzen und die Abwehr weiter zu erschweren. Hochentwickelte Gruppen nutzen die Verbindungen zwischen den Finanzinstituten aus, indem sie über aufgebrochene Zugänge kleinerer Banken in Großbanken eindringen und diese ausrauben. Internationale Grenzhindernisse und fehlende Kompetenz in Entwicklungsländern erleichtern es ihnen, häufig unentdeckt davonzukommen.

Ansätze zur Abwehr erweitern

Im gleichen Maße, in dem die Cyberangreifer immer raffinierter und gezielter vorgehen, muss die Abwehr neue Wege zum Schutz des gesamten globalen Finanzsystems bis in die kleinsten Verknüpfungen hinein entwickeln – nicht nur im jeweils eigenen Netzwerk. Kleine und mittlere Finanzinstitute vor allem in Wachstumsmärkten sind allzu leichte Zugangspunkte für kriminelles Eindringen in das globale Finanzsystem. Führende Institute der Branche müssen dazu ihre kleineren Partner stärken und den Bewusstseins- und Kompetenzaufbau für Cyberabwehr in Schwellenländern unterstützen.

Cybergefahren für Finanzinstitute kommen zunehmend von unsicheren Mobil- und IoT-Geräten. Dafür brauchen Banken neue Abwehransätze bei Monitoring- und Authentifizierungstechniken ebenso wie neue Sicherheitslösungen für die Geräte außerhalb ihrer eigenen Netzwerke. Die Verbesserung der Ausbildung zur Abwehr von Cyberkriminalität und die Stärkung des Bewusstseins aller Internetnutzer sowie erhöhte Anstrengungen zum weltweiten Ausbau der Strafverfolgung sind ebenso entscheidend.

Gemeinsame Sprache für Cybersicherheit

„The Cyber Security Ecosystem: Defining a Taxonomy of Existing, Emerging and Future Cyber Threats" von Jason Ferdinand mit Richard Benham[3)] stellt eine neue Taxonomie zur Kategorisierung von Cyberbedrohungen, Cyberangriffen und wissensbasierten Regeln für die Cyberabwehr vor. Die Untersuchung zeigt, dass trotz vieler Fälle mit großer Medienresonanz und Druck von Branchengruppen die Notwendigkeit, Cybergefahren und damit verbundene Risiken zu verstehen, immer noch weithin nicht erkannt oder unter Organisationen nicht kommuniziert wird.

Diese Studie ist zwar zunächst für Banken und Finanzorganisationen gedacht, sie soll aber allen Organisationen Analysen und Anleitungen bieten, da auch diese als Firmenkunden mit Banken und Finanzen in Verbindung stehen. Die Finanzindustrie hat ureigenes Interesse daran, Organisationen bei der Verbesserung ihres Wissens und Handelns zu unterstützen. Der Ausgangspunkt für diese Untersuchung ist daher der Versuch, eine gemeinsame Sprache für den Bereich Cybersicherheit zu schaffen, um alle Organisationen beim Umgang mit Cybergefahren in ihrem Umfeld zu unterstützen und eine gehaltvolle Diskussion darüber innerhalb und zwischen den Organisationen zu ermöglichen.

Ökosystem der Sicherheit – fehlendes Wissen und Verständnis

Um das Feld der Cyberbedrohungen angemessen untersuchen zu können und von den Erkenntnissen der vielfältigen Informationsquellen aus Wissenschaft, Regierungen und Praxis zu profitieren, wird das Ökosystem der Cybersicherheit unter Verwendung der neuesten Taxonomien, Theorien und Absprachen aufgezeichnet. In dieses Ökosystem werden eine Terminologie und Klassifizierungen eingeführt, um die Verständigung durch eine gemeinsame Sprache zu fördern. Zudem wird eine aktualisierte Klassifizierung der Cyberangriffe innerhalb des Ökosystems vorgestellt, um die Entwicklung einer dynamischen Cyber-Widerstandsfähigkeit sowie wirkungsvolle Grundsatz- und Strategieentscheidungen zu ermöglichen. Der erste Abschnitt der Studie fasst die Vergangenheit der Cybersicherheit zusammen mit einem kurzen Überblick über das Ökosystem der Cybersicherheit auf Basis einer systematischen Literaturauswertung, in der die früheren Verständnisse und Erfahrungen aus der Landschaft der Cyberbedrohungen erforscht werden.

Im zweiten Abschnitt wird untersucht, wie die heute Verantwortlichen für das Management der Cybersicherheit diese Taxonomien, Modelle und Idealtypen in der Praxis einsetzen – mit einigen überraschenden Ergebnissen. Den Bemühungen der Finanzindustrie, der Regierungen und anderer zum Trotz scheint es Managern in Großbritannien immer noch an Wissen und Verständnis von Cyberbedrohungen zu mangeln. Da diese Studie sich im Rahmen der vorgegebenen Parameter auf Großbritannien konzentriert, könnten daran anschließende internationale Vergleichsstudien aufzeigen, wie repräsentativ die hier identifizierten Probleme sind, da es in vielen Ländern unterschiedliche Positionen und rechtliche Anforderungen gibt. Fehlendes Wissen und Verständnis kann die Folge mangelnder Aktivitäten zur Cybersicherheit sein und/oder Kommunikationsversagen. In jedem Fall erscheinen diese Ergebnisse jedoch bedenklich.

Der dritte Abschnitt führt die Erkenntnisse aus den vorigen Abschnitten zusammen und präsentiert neue Taxonomien der Cyberbedrohung und -angriffe sowie praktische Empfehlungen, wie Institute durch Verwendung einer gemeinsamen Sprache dynamische Cyber-Widerstandsfähigkeit aufbauen und erhalten können. Der vierte Abschnitt fasst die Schlussfolgerungen zusammen und gibt Empfehlungen für künftige Studien.

Verhaltensmuster beim Cyber-Cashout

„Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud" von Elizabeth M. Petrie und Casey D. Evans[3)] untersucht, warum Organisationen sowohl die Fähigkeit, bei Cyberbetrugsaktivitäten auftretende Verhaltensmuster zu erkennen, als auch eine Plattform zur Kommu-

nikation entsprechender Informationen an andere Organisationen brauchen, um vor Cyberbetrug zu warnen und Kriminellen zuvorzukommen.

Die Studie konzentriert sich darauf, Verhaltensmuster zu identifizieren, die typischerweise die Bemühungen von Kriminellen indizieren, mithilfe von Insidern einen betrügerischen Cashout zu erreichen. Sie verschaffen sich Zugang zu Infrastrukturen, Zielen und Tools mithilfe von Insidern und machen das zu Geld. Insider, die sich daran beteiligen, verfügen über eine Stellung, die es ihnen ermöglicht, Kundenkonten einzurichten, zu ändern oder zu löschen. Ihre Motive können finanzielle oder nichtfinanzielle Gründe haben und sie können von Außenstehenden oder persönlichen Bekannten angeworben worden sein. Die Studie unterteilt diese Bedrohung durch Insiderverhalten in drei Kategorien: Diebstahl persönlicher Informationen, Diebstahl geheimer Handelsdaten und Cashout-Aktivitäten durch Insiderhilfe bei Geldwäsche.

Indikatoren für Insiderbetrug

Indikatoren sind Verhaltensmuster wie unbegründeter Zugriff auf Kundeninformationen, Kopieren persönlicher Unterlagen außerhalb der Verantwortlichkeit, E-Mails mit Anhängen an persönliche Accounts oder Internetadressen, Beschaffung bankinterner Unterlagen über Handelsaktivitäten, Verbleiben im Büro lange nach Arbeitsende und Zugriff auf sensible Daten nach Arbeitsabschluss. „Gesäuberte" Laptops nach Beendigung von Tätigkeiten deuten darauf hin, dass Angestellte Daten stehlen mit der Absicht, diese an Kriminelle oder Wettbewerber weiterzugeben. Cashout-Aktivitäten durch Insider-Beihilfe zur Platzierung geraubter Mittel im Darknet gegen Bezahlung zeigen sich durch Zugriff auf ruhende Konten mit plötzlichen Bewegungen oder stets wechselnden Kundenmerkmalen.

Zur Kategorisierung der Verhaltensmuster wurden die Quellen betrügerischer Insideraktivitäten definiert wie Netzwerk-Zugangsdaten, persönliche Kundendaten, Kundenkonto-Bewegungen, E-Mails, Telefon- und Internetbrowser-Aufzeichnungen. Der Untersuchung liegt die Annahme zugrunde, dass kriminelle Cyberakteure unter einem „Shared Services"-Modell operieren, um Angriffsaktivitäten auszulagern. Daher wurden die Verhaltensmuster nur solchen Services zugeordnet, mit denen sie zu Geld gemacht werden können, sogenannten Cashout Services. 54 Verhaltensmuster für Insiderbetrug in den drei genannten Kategorien wurden mit den Quellen klassifiziert und in einer Liste zusammengefasst.

Netzwerk für Betrugswarnungen

Die Potenziale zur Nutzung einer bestehenden weltweiten Telekommunikationsplattform wie SWIFT wurden erforscht, um Warnungen vor drohenden Cyberbetrugsaktivitäten zu kommunizieren. Für einen Transfer von Warnungen vor Insider-Cyberbedrohungen über das SWIFT-Netzwerk mit dem hier vorgestellten „Insider Threat Report" (ITR) müssen alle Nutzer die Einhaltung bestimmter Sicherheitsstandards nachweisen sowie sichere Zugänge vorhalten und korrekt handhaben. An beiden Enden des Transfers müssen ausreichende Sicherungen zum Schutz der Informationen und unabhängige Verifizierungen der Datensicherheit des jeweiligen Partners implementiert sein. Sollte dieser Vorschlag für Cyberbetrugswarnungen umgesetzt werden, so wäre – vielfältigem Austausch mit SWIFT zufolge – das strukturierte Nachrichtenformat MT 998 höchstwahrscheinlich das geeignetste, um den ITR über das SWIFT-Netzwerk an die Mitgliedsbanken zu versenden.

Nur durch enge Zusammenarbeit mit allen Beteiligten kann sich die Finanzindustrie eine starke Position zur Minderung der Cyberbedrohung und zur Abwehr der vielfältigen Angriffe verschaffen. Das SWIFT Institute und die Autoren der Studien hoffen, mit deren Veröffentlichung einen substanziellen Beitrag dazu leisten zu können.

Fußnoten

1) Die vollständigen Studien können unter www.swiftinstitute.org/papers/ heruntergeladen werden.
2) William A. Carter ist Stellvertretender Direktor des Technologiepolitik-Programms am Center for Strategic and International Studies (CSIS), einer Nonprofit-Organisation mit Sitz in Washington D.C., USA.
3) Dr Jason Ferdinand ist Gründer der IKSM Ltd, Certified Public Accountants & Business Consultants, Providence, RI, USA. Richard Benham ist Professor in Residence am National Cyber Skills Centre, Malvern, UK, Visiting Professor für Cybersecurity an der University of Gloucestershire und der Coventry Business School, UK, sowie u.a. Gründer von The National Cyber Awareness Course, UK.
4) Elizabeth Petrie ist Director Cyber Threat Risk Management bei Citi, New York, NY, USA. Casey Evans ist Program Director an der Kogod School of Business, American University, Washington DC, USA.