19.05.2020
von

Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten

Gastbeitrag von Andreas Krautscheid, Hauptgeschäftsführer Bundesverbande deutscher Banken, und André Nash, Associate Director, Themengruppe Banktechnologie und Sicherheit, Bundesverband deutscher Banken in BaFin Perspektiven, Ausgabe 1|2020

Kurzgefasst

Cybermisiken sind für die gesamte Kreditwirtschaft eine ernste Herausforderung. Um den technischen Wettlauf gegen professionelle Cyberkriminelle auch künftig zu gewinnen, braucht es vor allem eins: eine stärkere internationale Zusammenarbeit. Gastbeitrag von Andreas Krautscheid, Hauptgeschäftsführer, und André Nash, Associate Director, Themengruppe Banktechnologie und Sicherheit, in BaFin Perspektiven, Ausgabe 1|2020.

Schlagworte

Cybersicherheit
Phishing
Krautscheid
Cyberkriminalität
Dossier Cybercrime
Cyberattacken
Künstliche Intelligenz
Sicherheit
BaFin
Dossier ECSM

1 Einleitung

2 Gewachsene Expertise - Banken sind von „Stunde null“ an dabei

3 Unsicherheitsfaktor Mensch

4 Bedeutung von Informationsaustausch und Netzwerken steigt

5 Regulierungsmaßnahmen müssen harmonisiert werden

6 Technischer Wettlauf erfordert nationale und internationale Zusammenarbeit

1 Einleitung

Die Coronakrise hat uns wieder einmal vor Augen geführt, welche Schlüsselfunktion Banken ausüben und dass sie eine zentrale Verantwortung in der Volkwirtschaft haben. Das Bankgeschäft muss funktionieren; Beeinträchtigungen oder gar massive Störungen müssen unter allen Umständen verhindert werden.

In den vergangenen Jahren hat die Gefahr von Cyberattacken auf Deutschlands Wirtschaft und damit auch auf den Finanzsektor erheblich zugenommen. Die beiden wesentlichen Gründe hierfür liegen auf der Hand: zum einen die digitale Transformation sämtlicher Bereiche unseres Gesellschafts- und Wirtschaftslebens sowie eine stärkere Vernetzung der Unternehmen, durch die beständig neue Einfallstore für Angreifer geschaffen werden; zum anderen die zunehmende Professionalisierung der Cyberkriminellen, die ihr technologisches Waffenarsenal kontinuierlich aufrüsten. Nicht ohne Grund werden Cyberangriffe gegenwärtig als das größte operationelle Risiko im Finanzsektor gesehen.

Schon heute sind die digitalen Systeme vieler Unternehmen, nicht zuletzt der Kreditinstitute, so komplex, dass es schlicht unmöglich ist, generell jeden Angriff zu verhindern. Hinzu kommt, dass Fortschritte im Bereich künstliche Intelligenz (KI) neue und perfektionierte Attacken ermöglichen. So wurden im vergangenen Jahr verstärkt Fälle von Telefonbetrug registriert, bei denen die Täter mit Hilfe von KI Stimmen manipulierten und so den Versuch unternahmen, Mitarbeiter von Unternehmen zu täuschen und Gelder zu ergaunern. Für 2020 wird mit einem deutlich höheren Einsatz solcher Deepfakes gerechnet, zu denen auch gefälschte Videos zählen. Hier wird auf KI zurückgegriffen, um dynamisch Daten zu verändern. Angriffe autonom durchführen werden diese Systeme jedoch vorerst nicht. Denn noch bedarf es zu einem wesentlichen Teil der menschlichen Intelligenz, um Sicherheitslücken zu finden, Angriffsszenarien zu entwerfen und Attacken tatsächlich durchzuführen.

Während die aktive Ausnutzung von Sicherheitslücken also vorerst eine menschliche Domäne bleibt, ist das Aufspüren von Bugs und deren Beseitigung eine Stärke autonomer, auf KI basierender Systeme. In welche Richtung die Entwicklung gehen kann, zeigt ein reales Beispiel: Auf einer DARPA - Hacker-Konferenz fand ein System in einer vorab präparierten Testumgebung einen Bug, von dem der Veranstalter nichts wusste, und startete eine erfolgreiche Attacke gegen ein anderes System. Ein drittes System hat dies beobachtet, den Angriff „reverse engineered“, den Bug gefunden, einen Patch geschrieben und bei sich selbst installiert – alles innerhalb von 20 Minuten. So sieht die Realität heute noch nicht überall aus, aber es wird deutlich, wohin sich solche Ansätze künftig entwickeln werden.

Daneben gibt es noch einen weiteren potenziellen Risikoherd: Die Banken haben IT-Systeme zunehmend auf eine vergleichsweise kleine Zahl von IT-Dienstleistern verlagert und nehmen obendrein verstärkt Cloud-Dienstleistungen in Anspruch. Ein Ausfall oder die eingeschränkte Verfügbarkeit eines Dienstleisters durch einen Cyberangriff könnte daher erhebliche Auswirkungen haben. Um beim Beispiel Cloud zu bleiben: Die Vorteile und Potenziale einer Einbindung von Cloud-Lösungen in die Bankprozesse und -systeme liegen auf der Hand. Da die Angebotsseite – mit gerade einmal einer Handvoll relevanter, globaler Cloud-Dienstleister – recht übersichtlich ist, droht hier jedoch eine hohe Konzentration vieler Banksysteme auf wenige Cloudsysteme. Und trotz der Fähigkeit der einzelnen Cloudsysteme, über eine Netzwerkarchitektur die Ausfallrisiken so stark zu streuen, dass Ausfälle fast unmöglich sind, können Einschränkungen in der Praxis doch auftreten. So waren im Sommer 2019 beispielsweise mehrere Google-Dienste, die über die Cloud des Internetkonzerns betrieben werden, zeitweise ausgefallen. In Summe drohen nicht nur finanzielle oder Reputationsschäden für die einzelne Bank, sondern auch systemische Schäden für den gesamten Finanzsektor. Aus diesem Grund ist das gesamte System gefordert, die Bedrohungslage laufend zu analysieren und Maßnahmen koordiniert zu ergreifen.

2 Gewachsene Expertise - Banken sind von Stunde null an dabei

Cyberrisiken sind für die gesamte Kreditwirtschaft eine ernstzunehmende Herausforderung. Aber: Kreditinstitute verfügen auch über eine besondere Expertise zum Schutz ihrer technischen Infrastrukturen. Seit Beginn des Online-Bankings im November 1980 – also seit fast 40 Jahren – stellen Cyberangriffe ein relevantes Thema für unsere Mitgliedsinstitute dar. Die kontinuierliche Weiterentwicklung der Sicherheitssysteme zum Schutz der Kundendaten und des Kundenvertrauens genießen schon seit langer Zeit höchste Priorität bei den Banken. Dies spiegelt sich auch in den Investitionen wider, die in diesem Bereich getätigt werden. Einer weltweiten Umfrage des Cybersicherheitsunternehmens Kaspersky zufolge sind

Banken bei den Investitionen in Cybersicherheit pro Mitarbeiter führend.

3 Unsicherheitsfaktor Mensch

Das sicherste technische System kann allerdings keinen ausreichenden Schutz bieten, wenn die Nutzer dieses Systems die grundlegenden Sicherheitsanforderungen nicht beachten. Denn das vielleicht größte Einfallstor für Cyberattacken ist der Mensch selbst. Angriffspunkte sind Einzelpersonen, über deren Zugangsdaten Cyberkriminelle versuchen, Zugriff auf Konten oder Banksysteme zu bekommen. Das Spektrum der Attacken reicht von breit gestreuten Phishing -E-Mails bis hin zu gezielten Angriffen auf einzelne, speziell ausgewählte Personen, die teilweise über viele Monate ausspioniert werden (Spear-Phishing-Angriffe). Banken betreiben deshalb zurecht einen hohen Aufwand für Schulungen, Awareness-Kampagnen und Aufklärungsarbeit, um Mitarbeiter und Kunden kontinuierlich zu informieren und zu sensibilisieren.

4 Bedeutung von Informationsaustausch und Netzwerken steigt

Inzwischen ist die unternehmens- und sektorübergreifende Vernetzung der Cybersicherheitsverantwortlichen genauso wichtig wie ihre IT-Kompetenz. Das Information Sharing ist ein wesentliches Instrument bei der Abwehr und Bekämpfung von Cyberangriffen. Eine kurzfristige Benachrichtigung der Community bei einem aktuell stattfindenden Angriff versetzt die Branche in Alarmbereitschaft und ermöglicht, dass die Abwehrsysteme sehr schnell auf die konkreten Angriffsvektoren eingestellt werden können. Und auch der Austausch über ausgewertete Vorfälle ist für die Banken unerlässlich, um den bestmöglichen Schutz sicherzustellen. Schadsoftware kann manchmal wochen- oder monatelang vor anderen verborgen werden. Ein möglicher Schaden tritt dann auf, wenn diese Software aktiv und der Angriff durchgeführt wird – dann schlagen die Abwehrsysteme an. Kann diese Software jedoch im Vorfeld durch Systemanalysen – aufgrund von ausgetauschten Informationen – identifiziert werden, hilft dies bei der Abwehr und auch bei der Prognose weiterer möglicher Angriffsszenarien. Darüber hinaus leisten diese Informationen einen erheblichen Beitrag für die Prävention weiterer Angriffe, indem sie Teil der ständigen Weiterbildung von Mitarbeitern und IT-Sicherheitsexperten werden. Und auch für die Strafverfolgung von Angreifern sind die zu den Attacken gesammelten Daten relevant, denn nicht selten führen sie zur Ergreifung von Cyberkriminellen.

Der freiwillige, regelmäßige Austausch von Informationen zwischen Banken, Sicherheits- und Strafverfolgungsbehörden reicht allein jedoch nicht aus. Auf verschiedenen Plattformen werden heute zahlreiche Informationen zu aktuellen Angriffen, neuer Schadsoftware und laufenden Phishing-Kampagnen oftmals ungefiltert ausgegeben. Aufgrund der enormen Menge weltweiter Cyberaktivitäten ist die Masse dieser Rohdaten aller-

dringt so groß, dass dies ihren Nutzen zugleich in Frage stellt. Denn bevor Informationen in die Abwehrsysteme einer Bank einfließen können, müssen der Angriff analysiert und die notwendigen Abwehrmaßnahmen mit Blick auf die eigenen Systeme bewertet werden, um neue Risiken durch Systemanpassungen zu vermeiden. Daher besteht Bedarf an besser gefilterten und bereits ausgewerteten Informationen, die für die eigenen Systeme relevant sind – und das so zeitnah wie möglich.

Es gibt ein weiteres Problem: Leider führt die zunehmend unübersichtliche IT-Sicherheitsregulierung im Finanzsektor zu Unsicherheiten darüber, welche Informationen (noch) mit wem geteilt werden dürfen. Um die Möglichkeiten insbesondere auch für einen grenzüberschreitenden Austausch zu verbessern, wäre es hilfreich, Inkonsistenzen und Interpretationsspielräume – insbesondere, wenn es sich um personenbezogene Daten handelt, – zu adressieren. Aus diesem Grund bemüht sich die Finanzdienstleistungsbranche um Rechtssicherheit hinsichtlich der Möglichkeiten für Finanzinstitute, Informationen über Betrugsbedrohungen innerhalb der Branche auszutauschen. Hier brauchen wir EU-weit einheitliche Rahmenbedingungen, die ausdrücklich den Austausch bestimmter Informationen und Erkenntnisse zwischen privaten Einrichtungen sowie zwischen dem privaten und dem öffentlichen Sektor erlauben. Generell gilt: Die Verflechtung der staatlichen und der privatwirtschaftlichen Sicherheitsereignis- und Reaktionsteams in den Unternehmen mit den (Sicherheits-)Behörden ist eine wesentliche Voraussetzung, um mögliche Großereignisse bewältigen zu können. Ereignisfeststellung, -bewertung und gegebenenfalls die Krisenreaktion sind in der Cybersicherheit eine Gemeinschaftsaufgabe und müssen auch als solche bewältigt werden.

5 Regulierungsmaßnahmen müssen harmonisiert werden

Die zunehmenden Cyberangriffe auf Banken sind in den vergangenen Jahren auch zu einem immer wichtigeren Thema für die Aufsichtsbehörden geworden, da sie die Stabilität des Finanzsektors gefährden können. Auf europäischer Ebene haben die Europäische Zentralbank (EZB) und die Europäische Bankenaufsicht (EBA) inzwischen ihre jeweiligen Vorstellungen zur Erhöhung der Cyberwiderstandsfähigkeit des Finanzsektors konkretisiert. Und auf EU-Ebene haben Europäischer Rat und Europäisches Parlament unter anderem die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie), die Zweite Zahlungsdiensterichtlinie (PSD2) und den Cyber Security Act beschlossen.

Grundsätzlich decken sich die Anforderungen der Aufsicht mit den Bestrebungen und Aktivitäten der Banken. Allerdings sind die Regulierungsvorgaben der einzelnen Aufsichtsbehörden oftmals nicht aufeinander abgestimmt. Die Folge: Der Aufwand, den die Kreditinstitute zu erbringen haben, ist enorm. Banken müssen gegenüber jeder einzelnen Behörde nachweisen, dass sie die Anforderungen erfüllt haben; obendrein müssen sie umfangreiche Fragenkataloge beant-

wohl und denselben Vorfall auf unterschiedlichen Formularen an mehrere Meldestellen senden. Dass dies nicht sinnvoll sein kann, liegt auf der Hand. Es wäre sehr viel effizienter, die hierfür notwendigen Ressourcen direkt in die Verteidigungssysteme zu stecken. Eine Harmonisierung der Vorgaben und eine organisierte Meldestruktur für die Nachweiserbringung und das Reporting sind daher zwingend erforderlich. Sie würden zu einem insgesamt höheren Sicherheitsniveau, zu angemessenen Aufsichtspraktiken und zugleich zu einem niedrigeren Verwaltungsaufwand führen. Die aktuelle öffentliche Konsultation der Europäischen Kommission zur Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen zeigt, dass diese Notwendigkeit von Aufsicht und Politik erkannt wird. Nur: Was folgt daraus? Es wäre keine gute Nachricht, wenn als Ergebnis zwar neue Regulierung auf die Banken zukäme, die notwendige Komplexitätsreduzierung aber ausbliebe.

Harmonisierung ist im Übrigen auch bei den Threat Intelligence-based Ethical Red Teamings, den TIBER-Tests, ein wichtiges Thema. Diese simulierten Hacker-Angriffe basieren auf einem Rahmenwerk der Europäischen Zentralbank: Während die EZB sich auf die Finanzmarktinfrastrukturen fokussiert, setzen die nationalen Zentralbanken und Aufsichtsbehörden diesen Testansatz für die jeweiligen Banken in den einzelnen Mitgliedstaaten um. Hier sehen wir derzeit allerdings noch zahlreiche ungeklärte Aspekte, beispielsweise hinsichtlich einer möglichen Zertifizierung der testenden Unternehmen (Red-Teams) oder der Vergleichbarkeit der jeweiligen nationalen Tests. Im Sinne des angestrebten harmonisierten Ansatzes wäre es wichtig, dass ein in einem Land durchgeführter Test durch die anderen EU-Mitgliedstaaten anerkannt wird, um doppelte Tests und unnötige Mehraufwendungen zu vermeiden. Darüber hinaus ist für die global agierenden Häuser wichtig, dass eine Vergleichbarkeit – bestenfalls Anerkennung – von TIBER mit den jeweiligen Test-Ansätzen außereuropäischer Länder gewährleistet wird, zum Beispiel mit dem CBEST-Rahmenwerk der Bank of England.

6 Technischer Wettlauf erfordert nationale und internationale Zusammenarbeit

Es ist absehbar, dass die Banken im Jahr 2020 mit deutlich raffinierteren und womöglich größeren Cyberangriffen rechnen müssen als in der Vergangenheit. Da sich die Täter technologisch weiterentwickeln und inzwischen in etwa das Niveau der nationalen Sicherheitsbehörden erreicht haben, müssen alle Kräfte gebündelt werden. Nur wenn Wissen geteilt und Innovationen gefördert werden, wird es gelingen, den Kriminellen einen Schritt voraus zu sein. Dabei darf der globale Aspekt nicht vernachlässigt werden. Cyberangriffe auf Banken können von überall auf der Welt aus gestartet werden – und globale Auswirkungen auf das Finanzsystem haben. Der einzig sinnvolle Weg ist daher eine international koordinierte Vorgehensweise. Banken, Sicherheitsindustrie sowie die relevanten

nationalen und supranationalen Behörden müssen an einem Strang ziehen.