Redaktionsgespräch mit Christian Nern

„Nicht das Budget ist ausschlaggebend, sondern die Effektivität in der Umsetzung“

Herr Nern, die Corona-Krise hat die Digitalisierung bei den Banken gezwungenermaßen forciert. Nicht nur an der Schnittstelle zum Kunden, auch das Arbeiten im Homeoffice hat innerhalb der Banken einen digitalen Schub gebracht. Die meisten Banken haben das gut hinbekommen, oder?

Ja, definitiv – was vorher aufgrund von Remote-Zugängen und sensiblen Daten undenkbar war, hat von einem Tag auf den anderen nahezu reibungslos funktioniert. Im Zuge dessen haben vielen Banken nachgebessert: Sie haben VPN-Dienste (Virtual Privat Network) implementiert und beispielsweise Verhaltensmuster im Security Operations Center (SOC) angepasst. Zudem haben sie die IT-Infrastruktur um skalierende Lösungen sowie Dienste zur Videokommunikation und Collaboration Tools erweitert.

Die Banken und Versicherungen müssen sich damit auseinandersetzen, wie sie langfristig mit diesen Entwicklungen umgehen. Sie müssen in eine moderne IT-Security-Architektur investieren und die Mitarbeiter im Umgang damit schulen. Statt Insellösungen sollten sie auf einen ganzheitlichen Sicherheitsansatz setzen, der die Cloud berücksichtigt. Nun gilt es, die neu geschaffenen Strukturen auf stabile Beine zu stellen.

Auch der allgemeine Trend – schon vor Corona – hin zur verstärkten Auslagerung von Daten in die Cloud ist dadurch verstärkt worden. Das eröffnet aber auch Angriffsvektoren für Cyberkriminelle. Wie gut haben die deutschen Kreditinstitute die Sicherheit da im Griff?

Wir lesen derzeit fast täglich von Cyberangriffen und oftmals ist der Finanzbereich im Visier. So stiegen zum Beispiel laut dem Sicherheitsbericht „Modern Bank Heists 2020“ von VMware Carbon Black während des ersten Lockdowns im Frühjahr 2020 Attacken auf den Finanzbereich um 238 Prozent gegenüber dem Vorjahr an. Eine explizite Cloud Security ist für Banken also extrem wichtig, dennoch wird das Thema immer noch sträflich vernachlässigt. Zwar wissen die Institute um die Bedrohung, dennoch beschränken sich die meisten darauf, die regulatorischen Mindestanforderungen zu erfüllen. Sie sehen IT-Security in erster Linie als Kostenfaktor. Doch das ist der falsche Ansatz, denn kommt es tatsächlich zu einem Sicherheitsvorfall, müssen Banken mit hohen finanziellen Schäden rechnen.

„Eine explizite Cloud Security ist für Banken und Versicherungen extrem wichtig.“

Wie beeinflusst der Standort des Cloud-Betreibers die Sicherheit der Daten eines Kreditinstituts?

Es geht weniger um den Standort als darum, welche Zugriffsrechte der Cloud-Provider hat und wo die Daten gespeichert werden. Bei der Umfrage zur Integration von Public-Cloud-Lösungen im KPMG Cloud Monitor 2021 gaben 81 Prozent der befragten Großunternehmen an, dass sie Schwierigkeiten bei der Umsetzung der Compliance-Anforderungen hatten. 84 Prozent taten sich bei den Security-Anforderungen schwer und zwei Drittel kämpften mit Herausforderungen bezüglich der Geschäfts- und IT-Prozesse.

Wichtig ist also, welche Server-Standorte der Cloud-Betreiber nutzt. Auf die Dienste US-amerikanischer Cloud-Anbieter zu verzichten, ist hingegen keine Option; auch wenn das Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) vom vergangenen Jahr (Juli 2020) die Nutzung verkompliziert hat. Finanzinstitute müssen die Datenflüsse analysieren und sämtliche Datentransfers wie in die USA (mittels Abfrage der Fachbereiche und/oder Dienstleister) abklären. Zum Schutz stehen mehrere Handlungsoptionen bereit wie ergänzende Vertragsklauseln, Verschlüsselung oder Pseudonymisierung.

Wie bewerten Sie vor diesem Hintergrund die unter anderem von der Commerzbank initiierte European Cloud User Coalition und auch das GAIA-X-Projekt?

Eine Best-Practice-Plattform, wie sie die Commerzbank geschaffen hat, halte ich für eine gute Idee. Denn hier können sich die Banken über ihre Erfahrungen austauschen – etwa wie sie die Regulatorik umsetzen oder welche Anforderungen sie an Cloud-Provider stellen. Da es sich niemand leisten kann, Dienste und Systeme komplett neu aufzusetzen, sind solche Erfahrungswerte viel wert.

GAIA-X betrachte ich mit gemischten Gefühlen. Ich glaube nicht, dass wir eine deutsche Cloud brauchen. Zum einen gibt es nach wie vor Private Clouds und Hosting-Angebote, zum anderen liegt der große Vorteil der Cloud eben darin, weltweit und über verschiedene Kunden hinweg zusammenzuarbeiten. Warum sollte man sich dahingehend durch eine lokal begrenzte Cloud wieder einschränken? Viel wichtiger ist in dem Zusammenhang, dass klar geregelt wird, wie die Datenhaltung, die Regulatorik, die Compliance-Vorgaben oder auch die Zugriffsrechte und technischen Umsetzungen mit Verschlüsselung beim jeweiligen Cloud-Provider erfolgen.

täte ihnen ein Perspektivwechsel gut: Sie sollten ihre Maßnahmen auch an der Bedrohungslage – also an der konkreten Bedrohung – ausrichten. Einen Überblick über mögliche Risiken bietet beispielsweise das MITRE Attack Framework. Basierend darauf sollten Institute überprüfen, wie gut sie abgesichert sind, um dann effektive Lösungen zu implementieren.

Das trifft auch für kleinere Banken zu, denn nicht das Budget ist ausschlaggebend, sondern die Effektivität in der Umsetzung der Lösungen. Sie sind dahingehend gefordert, Prozesse gezielt zu automatisieren und/oder bestimmte Aufgaben auszulagern. Managed Security Services sind für sie ein probates Mittel, um ihre IT-Architektur abzusichern.

„Ich glaube nicht, dass wir eine deutsche Cloud brauchen."

Auch wenn die Corona-Pandemie gerade deutlich abebbt, dürfte klar sein, dass die Homeoffice-Quote bei den Kreditinstituten höher bleiben wird als vor der Pandemie. Was können Banken tun, um dauerhaft beim Remote Access der Mitarbeiter gut gesichert zu sein?

Banken müssen wissen, was im Innern vor sich geht. Dafür benötigen sie eine klar geregelte und moderne IT-Architektur mit Sicherheitslösungen wie einem Security Operation Center (SOC), einem Security Information and Event Management (SIEM) sowie einem integrierten Identity and Access Management (IAM) inklusive PAM-Systemen (Privileged Access Management). Die IT-Tools allein reichen aber nicht. Entscheidend ist, dass die Sicherheitsprozesse harmonisiert sind und die IT-Security-Systeme automatisiert zusammenlaufen.

Was können Institute noch tun, um dem Ganzen mit einer ganzheitlichen Strategie zu begegnen, vor allem auch kleinere Institute, ohne riesiges IT-Budget?

Viele Banken richten ihre Sicherheitsstrategie allein an der Regulatorik aus, dabei

Sie haben auch das Identity and Access Management angesprochen. Wie sollte das ausgestaltet sein, um möglichst wenig Angriffsfläche zu bieten?

In Banken und Versicherungen geben Policy, Governance und Aufsicht den regulatorischen Rahmen vor, wie Zugriffsrechte zu vergeben sind – etwa durch das Need-to-know-Prinzip und die Funktionstrennung. Ein ausgewogenes Identity and Access Management (IAM) setzt sich zu 70 Prozent aus fachlichen Komponenten und zu 30 Prozent aus technischen Anwendungen zusammen. Ein holistischer Ansatz ist für die reibungslose Funktion des IAM unumgänglich. Deshalb erstellen Banken in einem ersten Schritt ein einheitliches, unternehmensweites Berechtigungskonzept, das notwendige Prozesse und Kontrollen – wie Rezertifizierungen und Joiner-Mover-Leaver – berücksichtigt.

Zudem ist es wichtig, einen Überblick über die Systeme zu gewinnen, um im Sinne eines ganzheitlichen Ansatzes eine homogene IT-Landschaft zu schaffen. Anschließend lassen sich bedarfsabhängig, zeitgesteuert und automatisiert Nutzerkonten erstellen sowie Berechtigungen basierend auf Business-Rollen vergeben. Die Vergabe erfolgt anhand der drei Kritikalitätsklassen „Standard", „wesentlich" und „privilegiert". Zudem wird zwischen zwei Account-Typen unterschieden: Accounts ohne privilegierte Rechte und Accounts mit privilegierten Rechten. Die Berechtigungsprozesse werden dann

Christian Nern

Partner, KPMG AG Wirtschaftsprüfungsgesellschaft, München

Den plötzlichen Übergang hin zum Homeoffice infolge der Pandemie sieht Nern bei den Banken als gelungen an. Doch er fordert die Institute dazu auf, darüber nachzudenken, wie sie langfristig damit umgehen und die neuen Strukturen mit moderner Security-Technologie wie zum Beispiel SOC, Maßnahmen für Cloud Security oder Zugriffs- und Identitätenmanagement auf stabile Beine zu stellen. Auch beim Thema Sicherheit bei der Cloud-Nutzung sieht er Nachholbedarf: IT-Security würde nur als Kostenfaktor betrachtet und dabei nur die regulatorischen Mindestanforderungen erfüllt. Nern warnt davor, dass Kreditinstitute mit hohen Schäden rechnen müssen, wenn es tatsächlich zu einem Sicherheitsvorfall käme. Für eine gute Idee hält er die European Cloud User Coalition der Commerzbank, da die Institute hier ihre Erfahrungen austauschen könnten. Hingegen zeigt er sich der deutschen Cloud-Initiative Gaia-X gegenüber skeptisch. Insgesamt fordert er, dass Banken ihre gesamte Sicherheitsstrategie weniger an der Regulatorik ausrichten sollten, sondern vielmehr an der konkreten Bedrohungslage. (Red.)

letztlich End-to-End über den gesamten Leistungsschnitt hinweg in technischen Lösungen umgesetzt. Für eine pragmatische Umsetzung mit fokussierten Ergebnissen in Financial Services helfen auch vorkonfigurierte Lösungspakete. Diese bestehen aus fachlichen und technischen Templates sowie Vorgehensmodellen auf Basis von Erfahrungswerten und IT-Lösungen wie Sailpoint oder CyberArk.

Spielt auch nach der Automatisierung von Prozessen und effektivem Identity and Access Management der Faktor Mensch eine Rolle?

„2021 werden IT- und Cyberrisiken bei der BaFin noch stärker in den Fokus rücken."

Die alte Regel hat immer noch Bestand: Die größte Gefahr bei Hackerangriffen geht zu 50 Prozent von der Architektur und zu 50 Prozent vom Menschen aus. Dabei werden die Angriffsarten immer raffinierter und intelligenter – was es Mitarbeitern mitunter erschwert, den Angriff als solchen zu erkennen und sich entsprechend zu schützen.

Phishing E-Mails sind mittlerweile so professionell geworden, dass Opfer leicht darauf hereinfallen können. Bei sogenannten Targeted Attacks spionieren Hacker zielgerichtet ihre Opfer aus und planen präzise den passenden Zeitpunkt für einen Angriff. Damit wird der Mensch zur Schwachstelle, wie etwa beim CFO-Fraud.

Was können die Kreditinstitute tun, um den Angriffsvektor Mensch weniger angreifbar zu machen?

Prävention heißt das Zauberwort: Banken müssen ihre Mitarbeiter für die IT-Security sensibilisieren. Das beginnt bereits damit, dass Angestellte ihre Hardware und Software aktuell halten, indem sie regelmäßig System-Updates durchführen. Zudem müssen sie geschult werden, Angriffe wie Phishing zu erkennen und Notfall-Übungen machen. Dazu gehören etwa Sicherheits- und Penetrationstests, bei denen Sicherheitsexperten im sogenannten Red Team in die Rolle der Angreifer schlüpfen. Die internen IT-Experten einer Bank versuchen, diese Cyberangriffe abzuwehren und die eigenen IT-Security-Systeme zu schützen.

Darüber hinaus ist der Austausch mit anderen Instituten wichtig, um über die Bedrohungslage sowie Schutzmechanismen informiert zu bleiben und gegebenenfalls gemeinsam an einem Vorfall zu arbeiten. Ein Beispiel dafür ist das German Competence Centre against Cyber Crime (G4C). Hier tauschen sich Banken regelmäßig mit dem Bundeskriminalamt über Thread-Vektoren und Security-relevante Themen aus.

Auch die deutsche Bankenaufsicht hat dieses Problem schon erkannt. Erwarten Sie hier zusätzliche regulatorische Vorgaben?

In diesem Jahr hat die BaFin IT- und Cyberrisiken zu einem der Schwerpunkte des Aufsichtshandelns erklärt. Das Thema ist vor allem aufgrund der Pandemie in den Fokus gerückt, denn während der Lockdowns haben die Menschen Digitalangebote von Finanzinstituten intensiver als zuvor genutzt. Aus Sicht der Banken wird es daher immer wichtiger, Sicherheitsprozesse zu automatisieren. Die BaFin wird künftig verstärkt prüfen, ob Regularien eingehalten und automatisiert umgesetzt werden. Sie werden die Zusammenarbeit der Fachbereiche, den Umgang mit Sicherheitsvorfällen und die Absicherung der Systeme beurteilen und ein Auge darauf haben, wie Drittanbieter an die bankeneigene IT-Security angebunden werden.

In welche Richtung es geht, verdeutlicht zum Beispiel die Ergänzung der „Bankaufsichtlichen Anforderungen an die IT" (BAIT), die die operative IT-Sicherheit in den Fokus nimmt. Banken finden hier klare Vorgaben zur technischen Umsetzung der Außen- und Innenabsicherung von IT-Systemen gegen Cyberangriffe. Als Sicherheitsmaßnahme empfiehlt sich zum Beispiel die Integration eines Security Information and Event Managements (SIEM) sowie eines Security Operation Centers (SOC).

Was kann die Politik tun, um die IT-Sicherheit im Finanzsektor zu verbessern?

Aktuell geschieht sehr viel über Regulierungen – aus meiner Sicht wäre es aber sinnvoller, wenn stattdessen die wichtigsten Security KPIs (Key Performance Indicator) den Rahmen vorgeben, die tagesaktuell direkt aus den IT-Systemen abgerufen werden können – Stichwort: Management oder CISO Cockpit. Die Politik sollte also als eine Art Security Cockpit fungieren, vergleichbar mit der Materialprüfung einer ISO-Norm. Für Banken hieße das, sich verstärkt um die Technik und Umsetzung der IT-Sicherheit zu kümmern, statt sich nur auf Vorgaben der Regulatorik zu konzentrieren.

„Aus Sicht der Banken und Versicherungen wird es immer wichtiger, Sicherheitsprozesse zu automatisieren."

Idealerweise schickt ein Kreditinstitut die Thread Reports, die Topthemen, regelmäßig an die BaFin, die damit einen branchenweiten Überblick über die Bedrohungs- und Sicherheitslage bekommt. Ähnlich geht das Bundesamt für Sicherheit in der Informationstechnik bereits vor: Es beobachtet, wo Cyberbedrohungen für Unternehmen lauern, und gibt entsprechende Empfehlungen. Banken könnten sich davon inspirieren lassen und so mit der BaFin zusammenarbeiten.