Christian Nern

SOC – Potenziale in der Cyber Security voll ausschöpfen

Die BaFin hat in den Bankenaufsichtlichen Anforderungen an die IT (BAIT) Ende 2017 erstmalig Vorgaben gemacht, wie Banken ihre IT-Systeme ausstatten und die Informationssicherheit gewährleisten sollten. Mit der letzten Änderung im August 2021 hat sie diese noch einmal konkretisiert und schreibt zum Beispiel im neuen Kapitel „Operative Informationssicherheit" vor, dass Banken die Sicherheit ihrer IT-Systeme regelmäßig analysieren und kontrollieren müssen.

Als wirksames Tool für diese zeitnahe Analyse und etwaige Reaktion empfiehlt die BaFin eine „ständig besetzte zentrale Stelle, zum Beispiel in Form eines Security Operation Center (SOC)". Laut der Lünendonk-Studie 2022, in der 100 CIO, CTOs und CISO aus dem Finanzdienstleistungssektor befragt wurden, verfügen in Deutschland jedoch lediglich 40 Prozent der Unternehmen über ein SOC, weitere 35 Prozent planen den Aufbau eines SOCs und ganze 25 Prozent haben keins und planen auch keins.

Bedrohungen bei Banken nehmen zu

Dabei gewinnt das Thema zunehmend an Bedeutung, da Banken und andere Finanzdienstleister immer häufiger, auch getrieben durch die Ukraine-Krise beziehungsweise Corona und Remote-Arbeit, Ziel von Hackern werden. So nahm allein im Corona-Lockdown im Frühjahr 2020 die Zahl der Cyberangriffe auf Finanzinstitute im Vergleich zum Vorjahr um 238 Prozent[1)] zu. Das ist vergleichsweise wenig überraschend: Banken verfügen nicht nur über sehr sensible Kundendaten, sondern oftmals auch über einen Security-„Flickenteppich", inkonsistente Sicherheitsprozesse sowie wenig Automatisierung von Security-Systemen, weil sie sich darauf beschränken, die regulatorischen Mindestanforderungen zu erfüllen. Das ist sehr gefährlich, da etwaige Schäden sehr teuer werden und das Vertrauen der Kunden sowie die Reputation des Instituts nachhaltig erschüttern können.

> „Deutsche Banken brauchen einen Perspektivwechsel, um sich effektiv zu schützen."

Was deutsche Banken brauchen, um sich effektiv zu schützen, ist ein Perspektivwechsel: Anstatt reaktiv zu handeln und sich rein auf die regulatorischen Vorgaben zu fokussieren, sollten sie ihre Systeme und Sicherheitsmaßnahmen proaktiv an möglichen Bedrohungen ausrichten. Dafür brauchen sie eine Art Schaltzentrale, mit der sie ihre IT-Systemlandschaft überwachen, etwaige Bedrohungen erkennen und Angriffe abwehren sowie bei Bedarf sofort handeln können – ein Security Operations Center.

Aufbau des Security Operations Center

Um mit einem SOC eine nachhaltige und effektive Cyber Resilience aufzubauen, müssen Banken dieses zielgerichtet im Rahmen eines ganzheitlichen Ansatzes konzipieren. Dabei sollten Institute in vier Schritten vorgehen.

1. Zielbild: Im ersten Schritt müssen Banken definieren, was genau das SOC leisten soll und was nicht. Welchen Bedrohungen ist das Unternehmen ausgesetzt und gegen welche von ihnen will es sich schützen? Eine erste Orientierung kann dabei das MITRE ATT&CK Framework geben. Das Framework ist eine Wissensbasis von feindlichen Taktiken und Vorgehensweisen und kann somit einer umfassenden Bedrohungserkennung dienen.

2. Assets: Im zweiten Schritt müssen die Verantwortlichen festlegen, welche Assets, also welche Applikationen, Systeme, Infrastrukturkomponenten et cetera sie an das SOC anbinden beziehungsweise durch dieses überwachen lassen wollen. Um die Vielzahl anzubindender Assets zu bewältigen, ist eine Priorisierung jedoch unabdingbar –, zum Beispiel über die Erhebung ihrer Schutzbedarfe.

Durch diesen Ansatz ist es unter Umständen sogar möglich, dass auf bestimmte Assets zwar Bedrohungen einwirken, diese jedoch unter Betrachtung des Schutzbedarfs sowie der Wahrscheinlichkeit der Ausnutzung einer Schwachstelle im System nicht ins Gewicht fallen und das Asset somit aus Kosten-Nutzen-Gründen nicht in das SOC integriert werden sollte. Da inzwischen auch immer mehr Banken auf Cloud-Lösungen setzen[2)], müssen die Verantwortlichen hier auch definieren, ob und wenn ja welche Cloud-Services sie im SOC berücksichtigen müssen und wie sie diese integrieren.

3. Prozesse: Im dritten Schritt leiten sie ab, welche Sicherheitsprozesse im zukünftigen SOC zusammenlaufen beziehunsgweise durch dieses umgesetzt werden sollen. Hierzu gehören zum Beispiel die Integration beziehungsweise auch das Zusammenspiel des SOCs mit dem Security Information and Event Management (SIEM), dem Vulnerability Management, dem Information Security Incident Management sowie dem Identity and Access Management (IAM). Denn nur, wenn alle Prozesse ein gemeinsames Ziel verfolgen und ineinandergreifen, können Banken Vorgänge automatisieren und das Potenzial der zur Umsetzung und Unterstützung der Prozesse eingesetzten Tools vollständig ausschöpfen.

4. Umsetzung: Im letzten Schritt geht es darum, wie das SOC betrieben werden soll. Ein SOC sollte im Idealfall 365 Tage im Jahr rund um die Uhr aktiv sein. Diese Rund-um-die-Uhr-Überwachung kann die Bank entweder selbst übernehmen, damit einen Fremdbetrieb beauftragen oder sich für eine hybride Lösung entscheiden. Im Rahmen einer hybriden Lösung könnte das Institut das SOC zum Beispiel zu den Kerngeschäftszeiten betreiben und die Absicherung darüber hinaus in die Hände eines externen Dienstleisters geben. Bei den befragten Unternehmen der Lünendonk-Studie sind alle drei Varianten (inhouse, extern, hybrid) nahezu gleich vertreten. Demnach betreiben 31 Prozent ihr SOC inhouse, 31 Prozent hybrid und 38 Prozent vollständig über einen externen Partner. Als Faustregel gilt: Je größer die Informationssicherheitsabteilung eines Instituts ist, desto mehr Aufgaben des SOC kann es inhouse übernehmen.

Ganzheitliche Einbindung notwendig

Ein SOC funktioniert nur, wenn alle der Detection & Response zuzuordnenden Prozesse und Tools – zum Beispiel das Monitoring durch ein SIEM sowie die Reaktionsfähigkeit durch ein etabliertes Information Security Incident Mangement – auch miteinander „verdrahtet" sind. So enthält das SIEM zum Beispiel Erkennungsszenarien (auch Use Cases genannt), die aus Sicht der Sicherheit bedenklich sein können – zum Beispiel, wenn Benutzer sich zu merkwürdigen Zeiten einloggen oder ungewöhnlich große Datenmengen abgreifen. Anhand dieser Use Cases werden Kontrollprozesse und Alarme im SOC definiert, die dann manuelle oder automatische Vorgänge auslösen.

Das Zusammenspiel der einzelnen Aspekte lässt sich gut anhand eines Fußballspiels verbildlichen: In Fußballsprache entspricht das Unternehmen dem Stadion sowie die Systeme und Applikationen (inklusive Cloud) dem Spielfeld. Das IAM ist die Einlasskontrolle, die nur Zuschauer mit gültigem Ticket und aktive Akteure ins Stadion lässt, während das SOC als Schiedsrichter darauf achtet, dass alle Akteure sich an die Regeln halten.

„Cyber Security sollte in der Verantwortung der Unternehmensleitung liegen."

Die zentrale Herausforderung beim Aufbau eines SOC ist das Mindset zu Beginn: Viele Banken betrachten Security-Maßnahmen wie diese fälschlicherweise zunächst als Kostenpunkt, da ihre Einführung keinen direkten Businesserfolg liefert. Das ist jedoch zu kurz gedacht. Nicht nur, weil die Aufsicht eine „dem Stand der Technik entsprechende" Absicherung der IT-Infrastruktur und Informationen vorschreibt, sondern auch, weil moderne Kunden sicher sein wollen, dass ihre Daten bestmöglich geschützt sind.

Cyber Security sollte deshalb kein reines IT-Thema sein, sondern in der Verantwortung der Unternehmensleitung liegen. Denn der Vorstand muss bei einem etwaigen Sicherheitsvorfall sowohl der Aufsicht als auch seinen Mitarbeitern und Kunden gegenüber darlegen, wie es dazu kommen konnte und ob sein Institut alles Mögliche unternommen hat, um Angriffe von außen zu verhindern.

Änderung im Mindset

Darüber hinaus müssen auch die Fachabteilungen beim Aufbau des SOCs eingebunden werden. Denn sie arbeiten täglich mit den Systemen und wissen, für welche Tätigkeiten diese erforderlich sind und wer diese wann ausführt. Zudem ist es nur mit ihrer Hilfe möglich, eine sinnvolle und stringente Rechte- beziehungsweise Rollenvergabe im Rahmen des IAM zu definieren.

Christian Nern

Partner und Head of Security im Bereich Financial Services, KPMG AG Deutschland, München

Banken sind so stark im Fokus von Hackern wie nie zuvor. Für den Autor des vorliegenden Beitrags ist das wenig überraschend, denn seiner Feststellung nach verfügen Finanzdienstleister nicht nur über sehr sensible Kundendaten, sondern oftmals auch über einen Security-„Flickenteppich", inkonsistente Sicherheitsprozesse sowie wenig Automatisierung von Security-Systemen. Die Institute, so seine Kritik, würden sich darauf beschränken, die regulatorischen Mindestanforderungen zu erfüllen und machten sich so unnötig selbst angreifbar. Warum Banken also ein Security Operations Center (SOC) brauchen und wie sie dieses aufbauen können, erläutert folgender Beitrag. (Red.)

Ist ein SOC eingeführt und mit den übrigen Cyber-Security-Funktionen verzahnt, sind zwei Aspekte wichtig: Zum einen müssen die Institute ihre Systeme und Bedrohungen immer wieder überprüfen und bei Bedarf anpassen. Um etwaige Schwachstellen zu identifizieren, stehen ihnen verschiedene Testmethoden wie Security-Trainings mit Blue und Red Teams zur Verfügung.

Der Faktor Mitarbeiter

Ein weiterer essenzieller und vielfach unterschätzter Faktor ist eine Sensibilisierung und Schulung der Mitarbeiter: Dies ist nicht nur wichtig, weil menschliches Fehlverhalten ein großes Sicherheitsrisiko für viele Unternehmen darstellt, sondern vor allem, weil sensibilisierte Mitarbeiter dazu beitragen können, den Schaden etwaiger Sicherheitsvorfälle zu reduzieren. Sind sie zum Beispiel in der Lage, Angriffe wie Phishing als solches zu erkennen, können sie darüber sofort informieren und Gegenmaßnahmen einleiten.

Erfolgreiche Cyber Security startet mit dem richtigen Mindset und dem Bewusstsein, dass sie keine reine IT-Aufgabe, sondern eine strategische Entscheidung ist, die Banken proaktiv und im Zusammenspiel aus Vorstand, IT und Fachabteilungen angehen müssen. Dabei fungiert das SOC als Schaltzentrale in einem gesamtheitlichen Ansatz mit integrierten Prozessen und Tools, mit der Banken rund um die Uhr im Blick haben, was um sie herum passiert und bei Bedarf unverzüglich reagieren können. Im Falle eines Sicherheitsvorfalls gewährleisten aufeinander abgestimmte Funktionen und automatisierte Vorgänge eine angemessene Reaktion auf den Vorfall und somit letztendlich die Sicherheit der Daten und Informationen. Stimmen Mindset und integrierte Ausrichtung des SOC innerhalb eines ganzheitlichen Ansatzes, sind Banken bestmöglich gerüstet.

Fußnoten
1) Sicherheitsbericht „Modern Bank Heists 2020" von VMware Carbon Black https://www.carbonblack.com/resources/modern-bank-heists-2020/
2) Quelle: KPMG Cloud Monitor 2021, https://hub.kpmg.de/cloud-monitor-2021?utm_campaign=TECH%20-%20Studie%20-%20Cloud%20Monitor%202021&utm_source=aem