Cyber-Bedrohungen intelligent begegnen

Cyberangriffe haben ein Ausmaß erreicht, das Banken vor immer größere Herausforderungen stellt. Früherkennung, schnelle Analyse von Sicherheitsrisiken und Präventionsmaßnahmen werden immer essenzieller. Vielen Banken fehlen jedoch die Ressourcen sowie oftmals auch ein umfassendes IT-Security-Know-how, um angemessen auf die Bedrohungen zu reagieren. Frank Reiländer, Head of Cybersecurity bei CGI, gibt im gi-Geldinstitute-Interview Antworten auf wesentliche Sicherheitsfragen.

„Zukünftig ist zu erwarten, dass Banken das Thema IT-Sicherheit zu einer zentralen Eigenschaft ihrer Kernprodukte machen."
Frank Reiländer,
Head of Cybersecurity bei CGI

Der Finanzsektor gehört zu den Top Angriffszielen von Cyberkriminellen. Wo liegen denn die Hauptrisiken für Banken?
Reiländer: Das wertvollste Asset der Banken ist aus Kundensicht das Vertrauen in die Sicherheit der Geldanlagen. Gleichbedeutend mit einem Banktresor vor 20 Jahren ist es heute wichtig, dass alle Daten in einem virtuellen Safe liegen und somit geschützt sind. Allerdings finden Cyberkriminelle immer neue Wege, welche die Finanzwirtschaft in gefährliche Bedrohungslagen bringen. Der klassische „Fraud" – zu Deutsch „Betrug" – stellt einen wesentlichen Teil der operationellen und Compliance-relevanten Risiken dar. Dieser kann sowohl durch externe als auch interne Betrugsversuche wie die Weitergabe von datenschutzrelevanten Informationen oder die Durchführung unzulässiger Insidergeschäfte stattfinden. Jedes mit dem Internet verbundene Gerät ist ein potenzielles Einfallstor und muss geschützt werden. Hinzu kommt der Faktor Mensch, der eine nur schwer zu beeinflussende Variable und somit ein Risiko darstellt. Fallen beispielweise durch erfolgreiche Angriffe Zahlungssysteme temporär aus oder werden Datenschutzverstöße begangen, kann dies fatale Auswirkungen haben. Insbesondere, wenn eine Bank den Cyberangriff erst verspätet bemerkt, kann dies ungeahnte Ausmaße annehmen.

Banken gelten als unzureichend geschützt. Gibt es beim Thema IT-Sicherheit aus Ihrer Sicht Fortschritte? Wird die Finanzbranche resistenter?
Nicht zuletzt aufgrund der zunehmend strengeren Meldepflichten nehmen Banken die gegebene Bedrohungslage ernst. Wurden früher Zwischenfälle meist intern gelöst, werden heute nicht zuletzt aufgrund der Pflicht, die Datenschutzbehörde zu informieren, sicherheitsrelevante Vorfälle bekannt. Diese führen nicht nur zu Imageschäden der betroffenen Bank, sondern auch dazu, dass neue Angriffsarten publik werden und Nachahmer anziehen. Fortschritte gibt es jedoch gerade im Bereich von „Anti-Money-Laundering", also der Bekämpfung von Geldwäsche. Mit bewährten CGI-Lösungen wie HotScan360 wirken wir mit modernster Technik und automatisierten Prozessen der zunehmenden Komplexität von Finanzkriminalität entgegen. Zukünftig ist zu erwarten, dass Banken das Thema IT-Sicherheit zu einer zentralen Eigenschaft ihrer Kernprodukte machen, was man nicht zuletzt an häufig diskutierten Technologien wie Blockchain erkennt. Auch die Aufklärung der Mitarbeiter hat in den vergangenen Jahren stetig zugenommen. Durch die fortlaufende Schulung von Mitarbeitern und Dienstleistern wird versucht, das Risikobewusstsein hinsichtlich Compliance-Thematiken zu verbessern sowie den rechtlichen Vorgaben gerecht zu werden.

Nach welchen Kriterien sollten Banken ihre Security-Lösungen auswählen?
Banken sollten ihre Security-Lösungen risikobewusst nach Kriterien der Nutzbarkeit und Wirksamkeit auswählen. Grundsätzlich ist zwischen internen und kundenbezogenen Lösungen zu unterscheiden. Nach außen hin sollte die Lösung das Gefühl der Sicherheit vermitteln, jedoch keine weiteren Hürden wie Zusatzequipment, Registrierungen für Zertifikate oder Ähnliches aufweisen. Intern ist das Thema vielschichtiger. Hier transferieren die Mitarbeiter oft große Summen. Um Missbrauch vorzubeugen, sollten in diesen Bereichen Lösungen eingesetzt werden, die ein Vier-Augen-Prinzip unterstützen, das heißt eine Freigabe mit Autorisierung von dritter Seite. Wichtig aus Gründen der Nachvoll-

ziehbarkeit und Revisionsfähigkeit ist auch die durchgängige Protokollierung solcher Aktionen. Je nach Überwachungslösung kann dann schnellstmöglich ein Alarm ausgelöst werden.

Welche Rolle nimmt ein Security Operations Center (SOC) in der Gesamtstrategie eines Unternehmens ein?

Konkret geht es bei einem Security Operations Center um die strukturierte Erkennung von allgemeinen und speziellen Angriffen auf das Unternehmen und die Integrität der Daten. Neben den klassischen Angriffsszenarien von extern können auch die bankspezifischen Risiken in den Bereichen Wertpapierhandelsvorschriften, Betrugspräventionen intern und extern, Geldwäsche und Marktmachtmissbrauch überwacht werden. Cybersecurity sollte in Unternehmen als ganzheitliche Strategie betrieben werden und sich auf eigene Security- und Compliance-Abteilungen stützen. Diese werden oft durch externe Experten unterstützt, um spezifische Aspekte abzudecken. Eine Überwachung und Erstanalyse von Sicherheitsvorfällen im Rahmen eines ausgelagerten SOCs, das mit internen CERT (Computer Emergency Response Team)-Experten zusammenarbeitet, ist dabei ein wichtiger Trend, der sich im Bankensektor aktuell verstärkt durchsetzt.

Wie können Managed Security Services Banken konkret Schutz bieten?

Erfahrene Provider wie CGI bieten Cybersecurity-Lösungen als Managed Security Services an. Diese umfassen Infrastruktur-Dienstleistungen wie zum Beispiel PKI-Komponenten, Berechtigungs- und Firewall-Management sowie Managed Detection & Response (MDR). Dieser sogenannte SOC-as-a-Service-Ansatz integriert unter anderem Verwundbarkeits- und Risikoanalysen, Penetration Testing sowie Forensische Analysen. Um neben den allgemeinen Sicherheitsschwachstellen auch bankenspezifische Applikationen und missbräuchliche Nutzungen detektieren zu können, müssen entsprechende Use Cases erstellt werden. In einem typischen Migrationsszenario integrieren die Security-Spezialisten zunächst die Infrastrukturkomponenten, danach die allgemeinen Applikationen und zum Schluss die bankfachlichen Services in die Überwachung.

Skizzieren Sie bitte die Vorteile, die sich für den Nutzer der Services ergeben. Mit welchen Kosten ist zu rechnen?

Für den Nutzer des Services, also das beauftragende Unternehmen, ist der wesentliche Vorteil, dass er über den Service Zugang zu ausgewiesenem Experten-Know-How, hochentwickelten und bewährten Lösungen sowie ein professionelles Rund-um-die-Uhr-Management erhält. Die aus einer Ereignisüberwachung durch ein SOC resultierenden Meldungen entstehen aus der Natur der Sache heraus zu nicht vorhersehbaren Zeiten. Besprechungen und sonstige Aufgaben können nicht jederzeit unterbrochen werden, die Alarme würden in einem solchen Fall zunächst nicht bearbeitet. Eine dedizierte Mannschaft dafür vorzuhalten, ist kostenintensiv. Mit dem Managed Detection and Response Service, kurz MDR-Service, ist eine qualifizierte Erstanalyse, sprich ein Ausschluss von so genannten False Positives, eine Priorisierung gemäß Kritikalität und eine Alarmierung der definierten Ansprechpartner rund um die Uhr gewährleistet. Durch die global vernetzten SOCs und die in allen Industriezweigen und Public Services tätigen Cybersecurity-Spezialisten werden spezifische Erkenntnisse aus anderen Sektoren und Geografien zugänglich.

Diesen Service bietet CGI zu einem transparenten Festpreis an. Er kostet in den meisten Fällen nicht mehr als die Lizenzkosten für die ohnehin zu nutzende Software. Wir verfolgen einen ganzheitlichen Ansatz. Um ein konkretes Beispiel zu benennen: Nach kurzer Analyse konnten unsere Experten dem CERT eines Unternehmen, das seit geraumer Zeit zahlreichen Angriffen ausgesetzt war, bereits binnen Stunden helfen, einen zuvor unentdeckten Angriffsvektor zu erkennen und zusammen mit den internen Experten eine Abwehrstrategie planen.

Wie viele Banken vertrauen z.B. aktuell auf Managed Security Services eines SOC von CGI?

Zu den Kunden unserer Managed-Security- beziehungsweise MDR-Services zählen zahlreiche Unternehmen aus dem Finanzumfeld. Wir verfügen über eine umfangreiche Branchenerfahrung und unterstützen aktuell 50 Kunden im Bankenbereich.

Was unterscheidet CGI von anderen Anbietern?

Wir haben über 40 Jahre Erfahrung im Bankensektor und Security-Bereich. In Deutschland sind mehr als 600 Mitarbeiter auf Financial Services und mehr als 200 auf Cybersecurity spezialisiert. Unsere Fraud-Prevention- und Security-Lösungen erweitern wir stetig mit neuen Technologien, zum Beispiel mit künstlicher Intelligenz oder intelligenter Automatisierung, um Cyberkriminalität noch besser bekämpfen zu können. Zudem setzen wir mit einer eigenen Lösung, die Zugänge und Berechtigungen durch den Scan der Retina regelt, Projekte mit biometrischen Daten um. Im Bereich Cybersecurity verfügen wir über acht SOCs in Nordamerika, Europa und Deutschland. So bilden wir ein wichtiges Netz zum Wissens- und Erfahrungsaustausch für unsere Cyber-Experten weltweit.

Auf dieser Grundlage wehren wir Cyberangriffe nicht nur ab, sondern wir können Gefährdungslagen auch prognostizieren. Ziel ist es, den Angreifer aus dem Netz zu entfernen, sobald man ihn erkannt hat, und mit einer intelligenten Abwehr die Vorhersage von Aktionen und die gezielte Irreleitung des Einbrechers zu erreichen. Dazu werten wir die verfügbaren Wissensquellen inklusive Darknet-Scans aus. In unseren globalen Fachgruppen für Cybersecurity, Payments, Compliance und Banking findet daher ein permanenter Informationsaustausch statt, sodass alle Experten auf einem Kenntnisstand zu den aktuellen Themen in der Finanzbranche sind und unseren Kunden die bestmöglichen Lösungen anbieten können.