THREATQUOTIENT™

ThreatQ™ für Finanzdienstleister

Finanzdienstleister sind ein attraktives und lukratives Ziel für Cyberangriffe. Bereits seit drei Jahren führen sie die Liste der am häufigsten angegriffenen Branchen an[1] und die Kunden verzeichnen 65 % mehr Cyberangriffe als bei allen anderen Branchen.[2]

Trotz regelmäßiger Tests und Simulationen der Reaktionsmaßnahmen auf Zwischenfälle sowie einer der schnellsten Erkennungs- und Reaktionsgeschwindigkeiten kommt es immer noch zu Kompromittierungen und Sicherheitsverletzungen bei Finanzinstituten. Die durchschnittlichen Kosten, die der Finanzdienstleistungsbranche durch Cyberkriminalität entstanden, stiegen auf 18,37 Millionen Dollar – die höchsten Kosten aller Branchen.[3] Neben den eigentlichen gestohlenen Geldern fließen in diese Summe auch die Kosten für Erkennung, Reaktion und Benachrichtigung über die Sicherheitsverletzung, Bußgelder und Gerichtsverfahren sowie entgangene Geschäfte ein. Im Falle einer Sicherheitsverletzung verzeichnen Finanzdienstleister nach Gesundheitsunternehmen zudem die zweithöchste Kundenabwanderungsrate.[4]

WICHTIGE HERAUSFORDERUNGEN

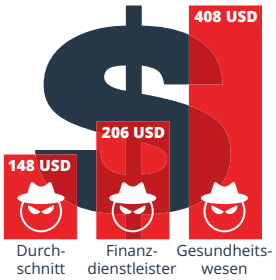
ZUNAHME DER ANGRIFFSFLÄCHEN

Kunden erwarten, dass Services rund um die Uhr verfügbar sind – auf jedem Gerät und an jedem Ort. Bedrohungsakteure unterbrechen die Geschäftsabläufe mit DDoS-Angriffen (Distributed Denial-of-Service). Solche Angriffskampagnen können mit Drittanbieter-Tools und Services relativ leicht durchgeführt werden und gehören für die Opfer zu den kostenintensivsten Angriffsformen. Zunehmend greifen die Bedrohungsakteure auch die sozialen und mobilen Netzwerke an, mit denen die Unternehmen ihre Kunden ansprechen sowie unterstützen und die sie auch für den Geschäftsbetrieb verwenden. Sie nutzen dabei die Tatsache aus, dass nur wenige Finanzinstitute diese Vektoren in ihrem Bedrohungsmodell berücksichtigen. Dabei setzen sie auf Phishing-Betrug, Social-Engineering-Angriffe sowie Malware, um Finanzbetrug zu begehen, der Marke zu schaden oder sogar Personen physisch zu bedrohen. Zum Schutz ihrer wachsenden Angriffsflächen benötigen Finanzinstitute einen Überblick über ihre gesamte Infrastruktur sowie einen proaktiven und antizipierenden Ansatz für das Schließen von Lücken in ihren Schutzmaßnahmen.

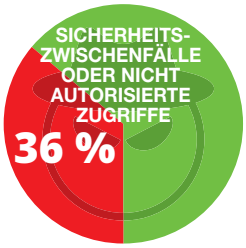
ATTRAKTIVE ZIELE

Cyberkriminelle greifen Finanzinstitute an, weil hier das große Geld zu holen ist und sie sich auf verschiedene Weise bereichern können. Dazu nutzen sie nicht nur aktiv Schwachstellen in Geldautomaten aus, sondern missbrauchen auch Netzwerke wie SWIFT (Society for Worldwide Interbank Financial Telecommunication), um Banken direkt zu bestehlen oder aus anderen Quellen gestohlene Gelder heimlich zu transferieren. Hinzu kommt, dass sich Bankkontodaten, Zahlungskartendaten sowie weitere personenbezogene Kundeninformationen schnell monetarisieren lassen. Die meisten Sicherheitsanalysten leiden unter einer wahren Flut an Warnmeldungen und benötigen eine Möglichkeit, sich auf relevante Bedrohungen mit hoher Priorität konzentrieren sowie verbesserte Funktionen zur Bedrohungssuche nutzen zu können.

KOSTEN PRO KOMPROMITTIERTEM DATENSATZ



Mit 206 US-Dollar hat die Finanzdienstbranche die zweithöchsten Kosten pro kompromittiertem Datensatz (Durchschnitt: 148 US-Dollar).[4]



Im Jahr 2018 verzeichneten etwa 36 % der Finanzinstitute einen Sicherheitsvorfall oder entdeckten nicht autorisierten Zugriff auf ihre Infrastruktur (24 % Steigerung gegenüber 2017).[5]

Banken und Finanzdienstleister waren im vergangenen Jahr das Ziel von 25,7 % aller Malware-Angriffe und damit mehr als jede andere Branche.[6]

ANGRIFFE AUF WEBANWENDUNGEN

Finanzdienstleister stellen mithilfe von Webanwendungen zahlreiche Online- und digitale Services für ihre Mitarbeiter und Kunden zur Verfügung. Mit diesen Anwendungen können Benutzer mithilfe ihrer Browser Daten aus und in Datenbanken übertragen. Bedrohungsakteure nutzen Schwachstellen in diesen Anwendungen sowie in den Zugriffsgeräten aus, um Netzwerke und Systeme zu infiltrieren und vertrauliche Daten sowie Gelder zu stehlen. Angesichts der Vielfalt der Angriffe auf Webanwendungen benötigen Finanzinstitute einen Echtzeitüberblick über die Vorgehensweise der Gegner und Kampagnen sowie über die Nutzung der eigenen Infrastruktur, damit die Reaktionen und Gegenmaßnahmen beschleunigt werden können.

„Wir verfügen nun über IoC-Daten aus vertrauenswürdigen Quellen, die proaktiv in die Überwachungslisten zur Bedrohungserkennung bei verschiedenen internen Sicherheitslösungen integriert werden, wobei keine tägliche Überwachung durch die Teammitglieder benötigt wird. Darüber hinaus können wir ausgewählte Daten in das speziell für deren Nutzung ausgelegte Tool exportieren, sodass wir keine großen Datenmengen im Netzwerk übertragen müssen, was die Systeme verlangsamen würde."

– Leiter Bedrohungsabwehr,
Fortune 500-Finanzdienstleister

GEORDNETERE SICHERHEITSABLÄUFE BEI FINANZDIENSTLEISTERN

Eine zuverlässige Bedrohungsdatenplattform liefert Finanzdienstleistern den Kontext sowie die Möglichkeiten zur Priorisierung, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams und Schulungen für fortlaufende Verbesserungen erforderlich sind. Sie müssen keine bestehenden Sicherheitsinfrastrukturen oder Abläufe ändern, da alle Tools und Technologien nahtlos mit der offenen Architektur von ThreatQ zusammenarbeiten.

MIT THREATQ MEHR ERREICHEN:

- **KONSOLIDIERUNG** aller Quellen für externe (z. B. FS-ISAC) und interne (z. B. SIEM) Bedrohungs- und Schwachstellendaten in einem zentralen Repository
- **AUSSORTIERUNG** nicht relevanter Informationen und einfache Navigation in enormen Mengen von Bedrohungsdaten zur Konzentration auf wichtige Ressourcen und Schwachstellen
- **PRIORISIERUNG** der Aspekte, die in Ihrer Umgebung am wichtigsten sind
- **PROAKTIVE SUCHE** nach böswilligen Aktivitäten, die auf Kontodaten-Kompromittierung, Zahlungskartenbetrug, DDoS-Angriffe sowie andere Schäden für Kunden und Händler hinweisen können
- **KONZENTRATION** auf bekannte Sicherheitsschwachstellen, die derzeit aktiv ausgenutzt werden und die Vorschriften-Compliance und Sicherheitslage beeinträchtigen können
- **SCHNELLERE ANALYSE** und Reaktion auf Angriffe gegen mehrere Ziele (z. B. Geldautomaten, das SWIFT-Netzwerk, Webanwendungen, neue digitale Kanäle und unterstützende Infrastruktur)
- **AUTOMATISCHE** Einbindung von Bedrohungsdaten in Erkennungs- und Reaktionstools

Fordern Sie eine Live-Demo für ThreatQ Platform und ThreatQ Investigations an: threatq.com/demo

1 IBM: „2019 IBM X-Force Threat Intelligence Index", https://www.ibm.com/account/reg/us-en/signup?formid=urx-36763

2 Die Weltbank: „Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision", 2018, http://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision

3 Accenture: „The Cost of Cybercrime", 2019 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

4 IBM: „2018 Ponemon Cost of a Data Breach Study", https://www.ibm.com/security/data-breach

5 Security Boulevard: „Cybersecurity Investment to Shoot Up in Financial Industry in 2019; Top Firms Already Spend $1 Billion", https://securityboulevard.com/2018/12/cybersecurity-investment-to-shoot-up-in-financial-industry-in-2019-top-firms-already-spend-1-billion/

6 Helpnetsecurity: „Which cyber threats should financial institutions be on the lookout for?", https://www.helpnetsecurity.com/2019/04/30/2019-cyber-threats-finance/

ÜBER THREATQUOTIENT™

ThreatQuotient hat sich das Ziel gesetzt, die Effizienz und Effektivität von Sicherheitsabläufen mithilfe einer bedrohungsbasierten Plattform zu verbessern. Durch die Integration der bestehenden Prozesse und Technologien eines Unternehmens in eine zentrale Sicherheitsarchitektur beschleunigt und vereinfacht ThreatQuotient die Untersuchungen sowie die Zusammenarbeit innerhalb von und zwischen Teams und Tools. Dank Automatisierung, Priorisierung und Visualisierung verringern die Lösungen von ThreatQuotient die Menge nicht relevanter Informationen und heben Bedrohungen mit hoher Priorität hervor, damit begrenzte Ressourcen ihren Schwerpunkt auf diese Gefahren legen können und bei Entscheidungen unterstützt werden. ThreatQuotient hat seinen Hauptsitz in Nord-Virginia (USA) sowie internationale Zweigstellen in Europa und im APAC-Raum. Weitere Informationen finden Sie unter https://threatquotient.com.

ThreatQ-for-Financial-Services_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885