Nicht ob, sondern wie: Studie von YesWeHack zeigt, wie die Finanzbranche von Cyberangriffen getroffen wird

Top 5 der häufigsten Angriffsszenarien bei Banken, Versicherungen und Finanzdienstleistern. © YesWeHack

Es geht nicht darum, ob ein Finanzinstitut von einem Cyberangriff getroffen wird – sondern wie. Eine aktuelle Studie von YesWeHack, Europas führender Bug-Bounty-Plattform, in Zusammenarbeit mit Foundry zeigt den Status Quo in Sachen Cyberattacken auf Banken, Versicherungen und Finanzdienstleister der DACH-Region. Zentrale Erkenntnis: Nahezu jedes Unternehmen ist betroffen. Hacker setzen zudem auf komplexere Angriffsszenarien. Die Studie deckt auf, in welchem Umfang Finanzinstitute in den vergangenen Monaten das Ziel von Cyberangriffen waren, welche Methoden Hacker bisher angewendet haben und welche für die kommenden Monate erwartet werden.

Fast jedes Unternehmen in der Finanzbranche betroffen

Lediglich rund sieben Prozent der Studienbefragten gaben an, in den letzten zwölf Monaten keinem Cyberangriff zum Opfer gefallen zu sein. Mit 76 Prozent verzeichnete die Mehrheit der Befragten zwischen einer und 20 erfolgreicher Attacken. Jedes zehnte Finanzinstitut (11 Prozent) hatte mit 21 bis 50 Attacken zu kämpfen, rund vier Prozent sogar mit über 50. Die Größe des Unternehmens spielt dabei eine wichtige Rolle: In der Umsatzklasse unter einer Milliarde Euro verzeichnete nur rund jede sechste Firma mehr als zehn Angriffe (17 Prozent), in der Umsatzklasse über zehn Milliarden Euro ist es schon fast jede zweite (46 Prozent).

Komplexität der Angriffe nimmt zu

Hacker haben verstanden, dass sie mit einfachen, altmodischen Taktiken kaum noch Erfolge erzielen können, da ihre Ziele davor immer besser gewappnet sind. Komplexe Szenarien, wie etwa Angriffe über die Geschäftslogik (Business Process Compromise), werden daher häufiger genutzt, wie knapp 53 Prozent der Befragten bestätigen. Dabei suchen Hacker gezielt nach Schlupflöchern in den Unternehmensprozessen im Sinne von Logikfehlern, die sie für ihre Zwecke ausnutzen können. 51 Prozent der Befragten berichten von Credentials-Diebstahl, insbesondere durch Social-Engineering-Angriffe wie Phishing. Auf Platz drei der häufigsten Angriffsszenarien liegt Ransomware mit knapp 39 Prozent, gefolgt von Insider Threats mit 38 Prozent und Attacken auf Datenbanken (beispielsweise über Brute-Force-Angriffe) mit 37 Prozent.

Die Unternehmensgröße ist auch hier entscheidend: Business Process Compromise betrifft rund 50 Prozent der Firmen mit über 1.000 Beschäftigten, aber nur rund 35 Prozent der Firmen mit weniger als 500 Angestellten. Phil Leatham, Senior Account Executive von YesWeHack Deutschland, erläutert: „Wenn Unternehmen wachsen, nimmt die Anzahl und die Komplexität von Prozessen exponentiell zu, was vermutlich zu mehr Schwachstellen führt.“ Credentials-Diebstahl sind dagegen eher die kleineren Unternehmen ausgesetzt (52 Prozent vs. 37 Prozent). „Ähnliche Resultate sehen wir auch bei unseren eigenen Bug-Bounty-Programmen in den Branchen Banken, Finanzen und Versicherungen“, bestätigt Leatham.

Ransomware auf dem Vormarsch

Zusammen mit Ransomware belegen diese beiden Angriffsszenarien auch die ersten drei Plätze, wenn es darum geht, welche Methoden in der Finanzbranche besonders zugenommen haben: Knapp 54 Prozent der Befragten gaben an, dass Business Process Compromise in den letzten beiden Jahren gestiegen bis stark gestiegen sei. „Ein Grund für diesen Anstieg ist sicher, dass die Entwicklung von Anwendungen meist auf der Basis moderner Frameworks erfolgt, die sicherer sind und weniger technische Schwachstellen beinhalten – abgesehen natürlich von Ausnahmen, wie etwa der Log4Shell-Sicherheitslücke. Im Gegenzug werden Unternehmensprozesse immer komplexer, die Digitalisierung nimmt zu, was zu Sicherheitslücken führt, die für Hacker besonders lukrativ sind“, so Leatham. Rund 51 Prozent bestätigen eine Zunahme bei Credentials-Diebstahl und rund 50 Prozent bei Ransomware, ein deutlich lukrativeres und weniger gefährliches Geschäft für Cyberkriminelle.

Jeder zweite Befragte (51 Prozent) geht davon aus, dass Ransomware in den kommenden zwölf Monaten noch zunehmen bis stark zunehmen wird. Eine ähnliche Entwicklung wird für Angriffe auf Webanwendungen (48 Prozent) sowie auf Datenbanken (46 Prozent) vorhergesagt.

Unternehmen sind gerüstet

Die Komplexität der Angriffe nimmt zu, aber Banken, Versicherungen und Finanzdienstleister sind dafür gerüstet: Nur rund ein Prozent der Institute erfüllen die neuesten „Bankaufsichtlichen Anforderungen an die IT“ – kurz BAIT – noch nicht. Diese schreiben regelmäßige Schwachstellen-Scans, Penetrationstests bzw. Simulation von Angriffen vor. 71 Prozent prüfen ihre IT-Systeme und Anwendungen mithilfe einmaliger Penetrationstests unabhängiger Dienstleister, 60 Prozent mithilfe einmaliger Tests durch unternehmenseigene Prüfer. 39 Prozent setzen auf eine

regelmäßige Überprüfung im Rahmen von Bug-Bounty-Programmen externer Dienstleister. In vielen Unternehmen werden mehrere Prüfszenarien umgesetzt.