Cybersicherheits-lösungen für die Finanzbranche

Finanzinstitute bleiben ein attraktives Angriffsziel

Cyberkriminelle haben die Finanzbranche nach wie vor im Visier. Laut dem Data Breach Investigations Report 2017[1] von Verizon® liegt die Branche bei bestätigten Angriffen auf Platz 1, bei Ransomware-Kampagnen befindet sie sich unter den ersten Drei und bei Sicherheitsvorfällen aller Art unter den ersten Vier. Im Vorjahr hatte die Branche bereits ähnlich abgeschnitten.

Eine wahre Schatzkammer

Im Finanzsektor bieten sich Hackern viele Möglichkeiten. Sie können Geldautomaten knacken und Bargeld stehlen, aber auch aus den vielfältigen Daten Profit schlagen, die in Finanzinstituten gespeichert sind, darunter personenbezogene Daten, Angaben zu Transaktionen und Vermögenswerten sowie vertrauliche Informationen zu Investitionsstrategien, potenziellen Fusionen und Akquisitionen. Diese Daten lassen sich beispielsweise durch Identitätsdiebstahl, Bereicherung mithilfe von nicht öffentlichen Informationen, Kontoübernahmen oder direkte Überweisungen zu Geld machen.

Heterogene Infrastrukturen

Die meisten Finanzinstitute nutzen zudem eine Mischung aus zahlreichen unterschiedlichen Technologien verschiedener Anbieter und selbst entwickelten Lösungen. Einige davon sind möglicherweise veraltet oder wurden bei Akquisitionen übernommen und werden nur noch minimal unterstützt und gepflegt. Dadurch werden die Umgebungen insgesamt anfälliger und damit attraktiver für Angreifer, denn sie müssen nur eine einzige Schwachstelle auf einem Gerät finden, um sich Zugang zur gesamten Unternehmensumgebung zu verschaffen.

Defense-in-Depth-Ansatz

Ironischerweise rückt der Finanzsektor auch aufgrund seiner Vorliebe für die Defense-in-Depth-Strategie in das Visier der Hacker. Die Branche und ihre Regulierungsbehörden empfehlen diesen Ansatz schon seit Langem. Die Herausforderung besteht jedoch in der Implementierung und Integration mehrerer Sicherheitslösungen von diversen Anbietern. Wenn diese nicht korrekt miteinander verknüpft werden, entstehen Lücken, die die Angreifer ausnutzen können.

Größte Sorgen der Finanzdienstleister

Ein schwerwiegender Sicherheitsvorfall schädigt nicht nur das Markenimage, den guten Ruf und die Marktkapitalisierung, sondern kann auch dazu führen, dass ein Finanzinstitut das Vertrauen seiner Kunden verliert. Um die Bedeutung der Cybersicherheit im Finanzsektor erneut zu unterstreichen, haben Regulierungsbehörden in New York und Hongkong neue Cybersicherheitsvorschriften für die Branche erlassen. Diese fordern eine aktive Beteiligung der Vorstände. Organisationen wie FINRA (Financial Industry Regulatory Authority) und SWIFT (Society for Worldwide Interbank Financial Telecommunications) haben angesichts der zunehmenden Bedrohungen in der Branche ebenfalls genauer definiert, welche Erwartungen sie hinsichtlich der Cybersicherheitsmaßnahmen an ihre Mitglieder stellen.

Bedrohungen in der Finanzbranche 2016 und 2017 (YTD*)

Top-5-Bedrohungen 2016	Top-5-Bedrohungen 2017 (YTD)
1. Locky	1. CerberSage_Distribution
2. Hancitor	2. Adwind
3. Cerber	3. ZyklonHTTP
4. Vawtrak	4. PdfDocmDropper
5. LokiBot	5. Locky

*27. Oktober 2017

Sicherheit der Endpunkte und Peripheriegeräte im Bankwesen

Da Endpunkte Zugang zu den vertraulichen Daten eines Unternehmens (zum Beispiel Finanzdaten, personenbezogene Daten der Kunden und Kartendaten) bieten, ist die Endpunktsicherheit ein wichtiger Aspekt des Sicherheitsstatus eines Finanzinstituts. Aufgrund der großen Zahl und Vielfalt der Endpunkte in einem typischen Unternehmensnetzwerk ist die Endpunktsicherheit jedoch eine komplexe Herausforderung. Neben den von der IT-Abteilung verwalteten Laptops, PCs und Servern werden eventuell auch private Geräte der Mitarbeiter und branchenspezifische Technologien wie Geldautomaten, Scheckscanner und spezielle Drucker für Sparbücher oder Debitkarten eingesetzt.

1. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Einige dieser Endpunkte werden vom Hersteller möglicherweise nicht mehr unterstützt, zum Beispiel Geldautomaten oder andere ältere Geräte mit dem Betriebssystem Windows® XP. Cyberkriminelle können den unzureichenden Endpunktschutz ausnutzen, um Malware einzuschleusen, Fernzugriff zu erlangen, Anmeldedaten zu stehlen und dann die nächste Phase ihres Angriffs zu starten.

Größere Verbreitung von Ransomware

Ransomware hat sich zu einer äußerst lukrativen Angriffsmethode entwickelt und in den vergangenen Jahren immer wieder Schlagzeilen gemacht. Andere Branchen wurden eventuell häufiger angegriffen und haben in den Medien für mehr Aufsehen gesorgt, doch auch der Finanzsektor blieb nicht verschont. Wie oben erwähnt nennt der „Data Breach Investigations Report 2017" von Verizon nur zwei Branchen, in denen es mehr Ransomware-Angriffe gab als im Finanzwesen. Eine Reihe von Finanzinstituten war beispielsweise von den WannaCry- und NotPetya-Kampagnen 2017 betroffen. In manchen Fällen wurde Ransomware als Ablenkungsmanöver eingesetzt, während der eigentliche Angriff an einer anderen Stelle im anvisierten Unternehmen stattfand. Sicherheitsverantwortliche in der Finanzbranche sollten die Entwicklung neuer Angriffsmethoden und Ransomware-Varianten unbedingt im Auge behalten und ihre Sicherheitsstrategien entsprechend aktualisieren, denn in diesem Bereich sind weitere Bedrohungen zu erwarten.

Schutz von E-Mail-Systemen und Abwehr von Phishing-Angriffen

E-Mails werden von Cyberkriminellen gern als Einfallstor genutzt. Laut Bedrohungsdaten, die Unit 42 (das Threat-Intelligence-Team von Palo Alto Networks®) im Laufe des Jahres 2017 sammelte, wurden 96 Prozent der Cyberangriffe im Finanzsektor über E-Mails gestartet.

E-Mails stellen eine besondere Herausforderung dar, da sie menschliche Schwächen ausnutzen. Auch mit noch so vielen Cybersicherheitsmaßnahmen lässt sich nicht verhindern, dass hin und wieder fragwürdige E-Mails im Posteingang der Mitarbeiter landen. Zudem müssen einige Mitarbeiter, zum Beispiel im Kundendienst, in der Personalabteilung und in der Finanzabteilung, im Rahmen ihrer Arbeit E-Mails mit unbekanntem Absender öffnen. Daher sind Schulungen zur Schärfung des Sicherheitsbewusstseins äußerst wichtig. Sie sollten Mitarbeiter darüber informieren, worauf sie bei E-Mails achten müssen, um nicht auf Phishing-Kampagnen oder schwerwiegendere Angriffe hereinzufallen.

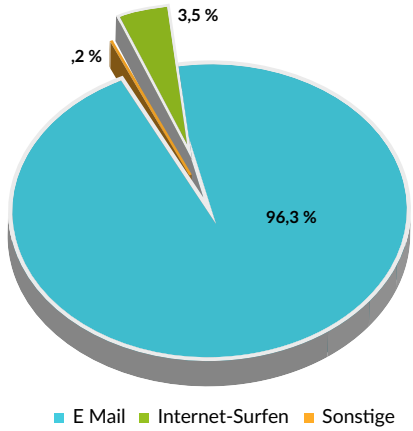

Abbildung 1: Im Finanzsektor beginnen über 96 Prozent der Cyberangriffe mit einer E Mail

Finanzinstitute können auch sogenannte „Red-Team-Übungen" durchführen. Dabei versuchen Experten, andere Mitarbeiter dazu zu verleiten, vorgetäuschte Phishing-E-Mails zu öffnen. Viele Unternehmen nutzen solche Planübungen, um ihren Mitarbeitern in einem realistischen Szenario Erfahrung im Umgang mit potenziell gefährlichen E-Mails zu vermitteln. Auf diese Weise können sie auch feststellen, welche Mitarbeiter von einer weiteren Schulung profitieren würden. Doch auch mit regelmäßigen Sicherheitsschulungen werden einige schädliche E-Mails in die Unternehmenssysteme gelangen.

Schutz der Finanz-Websites und Kundendaten

Die Cybersicherheit im Finanzsektor ist oft ein Balanceakt zwischen einfachem Zugriff und starker Sicherheit. Um wettbewerbsfähig zu bleiben, müssen Finanzinstitute die Erwartungen ihrer Kunden erfüllen und ihnen über das Internet oder Mobilanwendungen unmittelbaren Zugriff auf ihre Kontodaten bieten.

Wie bei E-Mails müssen Unternehmen auch bei kundenorientierten Websites und Mobilanwendungen teilweise auf das richtige Verhalten der Endbenutzer vertrauen. Mit Richtlinien für starke Passwörter und Zwei-Faktor-Authentifizierung haben sie jedoch zwei Möglichkeiten, sicherheitsbewusstes Verhalten zu fördern. Natürlich sollte die Internetpräsenz eines Finanzinstituts auch Schutzmaßnahmen auf Netzwerkebene umfassen. Firewalls und Technologien zur Erkennung und Abwehr von Eindringlingen gehören dabei zur Mindestausstattung.

Integrierte Sicherheitsplattformen verfügen über mehrere Sicherheitsebenen

Es gibt nicht das einzelne Sicherheitssystem und keine Punktlösung, mit der sich Finanzinstitute zuverlässig vor allen Cybersicherheitsrisiken schützen können. Sicherheitslücken auf Endpunkten, Phishing-Kampagnen, Diebstahl von Anmeldedaten, Ransomware-Angriffe und Schwachstellen auf Websites werden auch in Zukunft für Probleme sorgen. Zudem entwickeln Angreifer beständig neue Cybersicherheitsbedrohungen.

Konventionelle Punktlösungen haben ausgedient

Die Cybersicherheitsstrategien vieler Finanzinstitute sind veraltet. Sie setzen Punktlösungen verschiedener Anbieter für bestimmte Aufgaben ein, darunter Firewalls, netzwerk- und endpunktbasierte Antivirenprogramme und Systeme zur Erkennung und Abwehr von Eindringlingen. Obwohl nach wie vor verschiedene Infrastrukturbereiche und -komponenten geschützt werden müssen, ist dieser Ansatz nicht mehr zeitgemäß. Auch wenn eine Defense-in-Depth-Strategie mit Lösungen mehrerer Anbieter umgesetzt werden soll, müssen die einzelnen Ebenen genau definiert und alle Punktlösungen nahtlos miteinander verknüpft werden, damit keine Lücken entstehen.

Angesichts der aktuellen Bedrohungslage ist ein mehrschichtiger Cybersicherheitsansatz erforderlich, der auf nativ miteinander integrierten Sicherheitspunkten basiert, die umgebungsweit Bedrohungsdaten untereinander austauschen. Das heißt: Sobald eine Bedrohung an einem Ort, beispielsweise auf einem Endpunkt, erfasst wird, muss die Plattform in der Lage sein, sie überall abzuwehren, also im gesamten Netzwerk und in der Cloud. Das zeichnet eine effektive Sicherheitsplattform aus.

Anforderungen an eine umfassende Sicherheitsplattform

Die meisten Finanzinstitute setzen nach wie vor auf Sicherheitsmaßnahmen am Perimeter und nutzen ein flaches internes Netzwerk. Dadurch sind jedoch viele Systeme, auf denen geschäftskritische Informationen und personenbezogene Daten der Kunden gespeichert werden, anfällig für Cyberangriffe. Eine effektive Sicherheitsplattform beinhaltet Tools, mit denen jede Komponente der Rechenumgebung geschützt werden kann. Dazu gehören verwaltete Endpunkte wie PCs und Server, das Netzwerk selbst und Aktivitäten des Unternehmens in der Cloud.

> *„Dank Palo Alto Networks können wir jetzt den Datenverkehr bis auf die Anwendungsebenen filtern. Außerdem bietet Palo Alto Networks Sicherheitsprofilfunktionen wie Antiviren- und Anti-Spyware-Lösungen, VPN, URL-Filterung und WildFire-Funktionen, die bei der Abwehr bekannter und unbekannter Bedrohungen helfen."*
>
> – Filipus H. Suwarno, Leiter der Abteilung für Technologiesicherheit und Governance, Bank OCBC NISP

Eine integrierte Sicherheitsplattform vertraut bei der Abwehr von Cyberangriffen nicht nur auf ein einziges Tool oder eine einzige Lösung, sondern kombiniert diverse Tools und Strategien im gesamten Unternehmen, die zum Schutz vor Cyberangriffen miteinander interagieren. Umfassende Sicherheitsplattformen bieten Hunderte Funktionen, die wir hier nicht alle erläutern können. Nachfolgend sind daher die acht grundlegenden Funktionen in vier übergeordneten Kategorien aufgelistet.

Automatische Abwehrmaßnahmen

- **Koordination der Aktionen an allen Sicherheitspunkten durch den Austausch von Bedrohungsdaten:** Durch die native Integration aller Sicherheitspunkte auf der Plattform können Bedrohungsdaten nahtlos vom Netzwerk an die Endpunkte übertragen werden und umgekehrt. Dadurch wird sichergestellt, dass bei einer Anomalie in einem Bereich der Sicherheitsplattform schnell das gesamte Netzwerk informiert wird und überall entsprechende Abwehrmaßnahmen eingeleitet werden.
- **Automatische Abwehr in Echtzeit:** Viele Finanzinstitute verfügen nicht über ausreichend Mitarbeiter mit den erforderlichen Spezialkenntnissen, um die zahlreichen Cyberangriffe auf ihr Netzwerk manuell abzuwehren. Mit einer Sicherheitsplattform, die über eine Funktion für den Austausch von Bedrohungsdaten verfügt, können viele Aktivitäten automatisiert und das Sicherheitsteam entlastet werden.

Unternehmensweiter Einsatz von Sicherheitsmaßnahmen der nächsten Generation

- **Unternehmensintern verwaltete Endpunktsicherheitslösungen auf allen Endpunkten.** Auf allen verwalteten Geräten in der Umgebung sollte ein innovativer Endpunktschutz installiert werden, der Malware, Exploits und bisher unbekannte Bedrohungen effektiv abwehren kann.
- **„Zero Trust"-Ansatz für die Netzwerksicherheit:** In einer Zero-Trust-Netzwerkarchitektur wird kein Element standardmäßig als vertrauenswürdig eingestuft, nicht einmal der interne Netzwerkverkehr. Das Grundprinzip lautet „niemals vertrauen – immer prüfen".[2] Dazu müssen alle legitimen Geschäftskontakte und zulässigen Verkehrsströme im Netzwerk im Detail bekannt sein. Wird dieser Ansatz korrekt und effizient umgesetzt, ist er ein äußerst effektives Mittel zur Abwehr von Ransomware und anderen Bedrohungen. Eine Sicherheitsplattform bietet über Firewalls der nächsten Generation umfassende Einblicke und eine Anwendungstransparenz, mit denen ein Zero-Trust-Netzwerk zur Realität werden kann.

> *„Als wir die Lösung von Palo Alto Networks noch nicht hatten, haben die riesigen Datenmengen unser Sicherheitsteam oft überwältigt, ohne ihnen genug Anhaltspunkte für schnelle Maßnahmen zur Abwehr von Cyberbedrohungen zu geben. Der Ansatz von Palo Alto Networks und die neueste Version von PAN-OS haben Ordnung in das Chaos gebracht. Jetzt können wir die Nadeln im Heuhaufen finden und unser Netzwerk besser schützen."*
>
> - Dallan M. Wagner, Information Security Engineer, Academy Mortgage Corporation

- **Risikominderung für Geräte, die noch nicht gepatcht wurden oder für die es keine Patches gibt:** Finanzinstitute sind in der Regel schon aus Wettbewerbsgründen an neuen Technologien interessiert. Dennoch sind vielerorts auch veraltete Geräte im Einsatz, die keinen Herstellersupport

2. Palo Alto Networks, „Network Segmentation/Zero Trust" o. J., Auszug aus https://www.paloaltonetworks.com/solutions/initiatives/network-segmentation

mehr erhalten. Ein Beispiel dafür sind Geldautomaten, auf denen noch Windows XP läuft. Auf anderen Geräten werden verfügbare Patches möglicherweise nicht zeitnah eingespielt. In beiden Fällen entstehen Einfallstore, die von Angreifern ausgenutzt werden können. Ein innovativer Endpunktschutz mit mehrschichtigen Maßnahmen zur Abwehr von Malware und Exploits ist effektiver als herkömmliche Antiviren- oder Anti-Malware-Lösungen. Außerdem ist er Teil einer Sicherheitsplattform, die durch den Austausch von Bedrohungsdaten neue Bedrohungen noch besser erkennen und abwehren kann.

Funktionen, die unachtsame Nutzer schützen

- **Schutz vor Diebstahl von Anmeldedaten zur Verhinderung von Phishing-Angriffen:** Eine Funktion zur Verhinderung des Diebstahls von Anmeldedaten ist nur auf den wenigsten Firewalls der nächsten Generation vorhanden. Wenn Mitarbeiter Phishing-E-Mails erhalten, verhindert eine solche Funktion automatisch die Übermittlung unternehmensinterner Benutzernamen und Passwörter an schädliche Websites. So lässt sich verhindern, dass Unachtsamkeit bei E-Mail-Angriffen und Phishing-Kampagnen ausgenutzt wird.
- **Integration eines innovativen Malware-Sandboxing-Service:** Eine Firewall der nächsten Generation kann Bedrohungen wie E-Mails mit potenziell schädlichen Anhängen erkennen, die von einem Netzwerkbereich in einen anderen übertragen werden. Derartige Anhänge können dann automatisch an einen Sandboxing-Service gesendet werden, der die Datei in einer sicheren Umgebung öffnet und auf schädliche Funktionsweisen überprüft. Dies ist eine weitere Möglichkeit, um E-Mail-Angriffe zu vereiteln, bei denen Unachtsamkeit ausgenutzt wird.

> *„[W]ir haben eine Lizenz erworben, um den kompletten WildFire-Service zur Prüfung und zum Extrahieren aller Anhänge nutzen zu können, die wir erhalten oder über Lösungen wie Dropbox herunterladen. ... [S]chon während der ersten Woche haben wir mehrere Dinge gefunden, die zuvor vermutlich unbemerkt in unser Intranet gelangt wären und sich dort möglicherweise ausgebreitet hätten. Unsere vorhandenen Antiviruslösungen haben uns auf keinen dieser Anhänge aufmerksam gemacht. Nur mit WildFire konnten wir sie als schädlich erkennen."*
>
> - Lance Spencer, Lead Data Security Engineer, Northwest Bank

Optimale Transparenz im Netzwerk

- **Einblicke in den Netzwerkverkehr in Echtzeit oder nahezu in Echtzeit:** Eine Sicherheitsplattform, die dem Unternehmen einen umfassenden Einblick in den Netzwerkverkehr verschafft, bietet einen enormen Mehrwert. Wenn Sicherheitsteams einen umfassenden Überblick über die Datenverkehrsströme, die aktiven Anwendungen und das Gefahrenpotenzial der Benutzer haben, können sie die aktuelle Sicherheitslage viel besser einschätzen.

Was bedeutet das für Finanzinstitute? Ein Sammelsurium aus älteren Punktlösungen bietet keinen ausreichenden Schutz vor Cyberangriffen mehr. Das gilt für Schwachstellen auf Endpunkten oder im Kundenportal ebenso wie für Ransomware- und Phishing-Angriffe. Eine mehrschichtige Sicherheitsplattform mit nativ integrierten Sicherheitspunkten im gesamten Netzwerk, in der Cloud und auf allen Endpunkten ermöglicht einen automatischen Schutz vor Cyberbedrohungen, den keine Kombination aus Punktlösungen erreichen kann.

Weitere Informationen dazu, wie die Sicherheitsplattform der nächsten Generation von Palo Alto Networks Finanzinstitute schützen kann, finden Sie auf unserer Website.

https://www.paloaltonetworks.com/solutions/industries/enterprise/fin-serv

3000 Tannery Way
Santa Clara, CA 95054

Allgemeine Anfragen: +1 408 753 4000
Vertrieb: +1 866 320 4788
Support: +1 866 898 9087

www.paloaltonetworks.com