proofpoint.

Insider Threats im Finanzdienst-leistungssektor

Schützen Sie sensible Daten und schützen Sie Ihre Reputation

Einführung

Finanzdienstleister gehören meist zu den ersten, die neue Cybersicherheits-technologien einführen. Doch trotz dieser Investitionen findet fast ein Viertel aller Sicherheitsverletzungen in dieser Branche statt. Zudem tragen Insider zu mehr als der Hälfte dieser Zwischenfälle bei.

Als Teil ihrer täglichen Arbeit haben die Mitarbeiter in diesem kritischen Sektor Zugang zu digitalen Geldströmen und wertvollen Kundendaten. Dadurch sind diese Personen ein inhärenter Risikofaktor für Ihr Unternehmen – und lukrative Ziele für kriminelle Akteure.

Einige Insider haben böswillige Absichten, während viele einfach nur fahrlässig handeln. Andere werden jedoch von externen Angreifern kompromittiert, die dadurch Zugriff auf vertrauliche Daten, Systeme und Ressourcen erlangen. Es ist kein Wunder, dass Insider-Bedrohungen ein so herausfordernder Bedrohungsvektor sind.

Dieses E-Book befasst sich mit dem Management von Insider-Bedrohungen aus der Perspektive der Finanzdienstleistungsbranche. Anhand von Praxisbeispielen aus den Bereichen Versicherung, Bankwesen und Vermögensverwaltung werden die Herausforderungen beim Umgang mit diesen Bedrohungen erörtert. Das E-Book zeigt außerdem, wie Proofpoint Ihnen helfen kann, Insider-Vorfälle schnell und effizient zu identifizieren, zu untersuchen und darauf zu reagieren.

24 % aller Sicherheitsverletzungen erfolgen in Finanzinstituten – und mehr als die Hälfte der Angriffe auf diese Unternehmen werden von Insidern verübt.[1]

[1] Verizon: „Data Breach Investigations Report 2017“ (Untersuchungsbericht zu Datenkompromittierungen 2017).

ABSCHNITT 1

Insider-Bedrohungen im dynamischen Finanzdienstleistungssektor von heute

Seit 2018 hat die Finanzdienstleistungsbranche eine Zunahme bei Insider-Bedrohungen um 20,3 % festgestellt.[2]

Jedes Unternehmen muss vertrauliche Informationen wie Kunden- und Firmendaten sowie geistiges Eigentum schützen. Das gilt sicher besonders für Banken, Kreditinstitute, Vermögensverwalter und Versicherungen.

Wie andere Branchen auch, bewegt sich der Finanzsektor hin zu dezentralen Mitarbeitermodellen. Gleichzeitig gewinnen Cloud-basierte Anwendungen zunehmend an Bedeutung. Durch diese konvergierenden Trends wird die Abwehr von Insider-Bedrohungen zusätzlich erschwert.

Die IT-Infrastruktur wird von einer größeren Bandbreite an Usern gemeinsam genutzt. In einem typischen Unternehmen können Auftragnehmer, Dienstleister, Partner und Mitarbeiter mit Remote-Zugang auf das Firmennetzwerk zugreifen. Das erschwert die Definition des Begriffs „Insider“.

Doch auch die Definition des Begriffs „Bedrohung“ ist nicht viel einfacher. Bei der Abwehr von Insider-Bedrohungen geht es nicht nur darum, User mit böswilligen Absichten zu stoppen, sondern auch um die Identifizierung und Eindämmung von Bedrohungen durch fahrlässig handelnde oder kompromittierte Endnutzer.

[2] Ponemon Institute: „2020 Cost of Insider Threats: Global Report“ (Kosten von Insider-Bedrohungen 2020: Weltweit).

ABSCHNITT 2

Insider-Risiko: Wer und was?

Insider-Risiken sollten im Fokus aller digital orientierten Unternehmen stehen. Das gilt ganz besonders für Finanzdienstleister.

Doch wo sollen sie anfangen? Der erste Schritt beim Aufbau eines Technologie-gestützten Programms zur Abwehr von Insider-Bedrohungen besteht in der Erkenntnis, *wer* und *was* zu Insider-Risiken gehört:

- Wen sollten Sie im Blick behalten?
- Was sollten Sie schützen?

Wen sollten Sie im Blick behalten?

Die Abwehr von Insider-Risiken beginnt mit der Identifizierung der Anwender, die das größte Risiko für Sicherheitsverletzungen „von innen" bergen. In jedem Unternehmen und jedem Bereich kann dies anders aussehen. Diese verbreiteten Kategorien von Usern sollten Sie berücksichtigen:

Nicht beim Unternehmen angestellte Anwender: Uneinheitliche, dynamische Liefer- und Serviceketten sind bei Finanzdienstleistungen üblich. Oft nutzen die Auftragnehmer, Dienstleister, Berater und Partner die selbe IT-Infrastruktur, wie die Mitarbeiter. All diese Personen stellen ein potenzielles Risiko dar.

Anwender mit privilegierten Zugriffen: Einige Mitarbeiter benötigen Zugriff auf geschützte Infrastrukturen und Informationen. Dazu gehören:

- IT-Administratoren
- Helpdesk-Mitarbeiter
- Callcenter-Mitarbeiter
- Finanzverwaltungen

Besonders gefährdete Mitarbeiter: Einige Anwender werden von der Personalabteilung möglicherweise aufgrund eines der folgenden Faktoren als besonders gefährdet eingestuft:

- Verhalten
- Änderung der Position
- Probleme bei Leistung oder Disziplin
- Gefahr der Abwanderung

Von Fusionen und Übernahmen betroffene Mitarbeiter: Die Finanzdienstleistungsbranche unterliegt kontinuierlichen Veränderungen. Unternehmen fusionieren oder werden übernommen, sodass die Zahl der autorisierten Anwender immer wieder variieren kann. Diese Veränderungen fordern kontinuierlich ein Höchstmaß an Aufmerksamkeit und unterliegen daher einem hohen Risiko.

Remote-Mitarbeiter: Immer mehr Angestellte arbeiten weltweit im Home Office oder an einem anderen Remote-Arbeitsplatz. Da sie sich damit außerhalb des geschützten Netzwerk-Perimeters befinden, steigt das Risiko eines Zwischenfalls.

Nicht nur böswillige Anwender erhöhen das Risiko

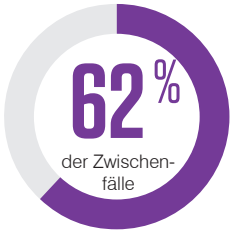
Der Begriff „Insider-Bedrohung" wird meist mit böswilligen Anwendern gleichgesetzt. Diese können durch finanziellen Gewinn, Vergeltungsmaßnahmen oder ausländische Einflüsse motiviert sein. Tatsache ist jedoch, dass fahrlässig handelnde oder kompromittierte Anwender häufiger Insider-Zwischenfälle verursachen.

Fahrlässige Anwender verwenden unter Umständen nicht genehmigte Prozesse und gefährden damit unwissentlich Ihre Infrastruktur oder Daten.

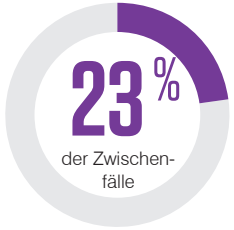
Kompromittierte Anwender stehen unter dem Einfluss externer Angreifer, zum Beispiel weil sie per Social Engineering zur Herausgabe von Daten verleitet wurden oder weil sie schlicht die Kontrolle über ihr Konto verloren haben.

Beachten Sie auf jeden Fall, dass fahrlässig handelnde und kompromittierte Anwender meist das größte Insider-Risiko darstellen.

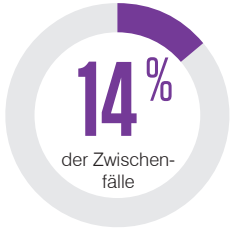
Fahrlässig handelnde Insider



Böswillige Insider



Kompromittierte Insider



Was sollten Sie schützen?

Ebenso wie die meisten Unternehmen setzen Finanzdienstleister auf stark abgesicherte digitale Transaktionen. Sie sind zusätzlich von der Integrität ihrer Mitarbeiter und der kundennahen IT-Infrastruktur abhängig. Diese Bereiche bereiten die größten Probleme:

Schutz vertraulicher Daten: Finanzdienstleister verwalten enorme Mengen an personenbezogenen Informationen wie Zahlungskartendaten (PCI) und – wie im Falle von Versicherungen – sensible Daten der Krankengeschichte des Patienten. Personenbezogene Informationen sind für Betrüger äußerst wertvoll und häufig das primäre Ziel von Datenschutzverletzungen.

Compliance: Die Finanzdienstleistungsbranche unterliegt zahlreichen Vorschriften und Compliance-Vorgaben, die festlegen, wie Unternehmen ihre Daten, Informationen und die Integrität ihrer Prozesse schützen sollen. Compliance-Lücken und Datenschutzverletzungen können enorme Kosten verursachen.

Finanzbetrug: Finanzdienstleister verwalten große Mengen an Transaktionen und Vermögen. Betrüger instrumentalisieren Arbeitnehmer und nutzen ihren Insider-Zugang, um durch eine Vielzahl von Machenschaften Geld zu stehlen.

Service-Unterbrechungen: Die Geschäftsabläufe der Finanzdienstleister sind von der IT-Infrastruktur abhängig, die die kundennahen und von Mitarbeitern genutzten Dienste unterstützen. Angreifer mit Insider-Zugriffen können Ihre Systeme beschädigen oder stören. Ausfallzeiten können zu Umsatzverlusten sowie zu verlorenen Geschäftschancen und Vertrauensverlust führen.

Schutz proprietärer Informationen: Der Wettbewerbsvorteil vieler Wertpapierfirmen hängt von deren proprietären Informationen und Handelsalgorithmen sowie davon ab, dass diese Daten zuverlässig geschützt bleiben.

Reputationsschaden: Die Reputation von Finanzdienstleistern basiert auf dem Vertrauen ihrer Kunden, Geschäftspartner und u. a. den Aufsichtsbehörden. Im Fall eines Sicherheitsverstoßes – vor allem wenn er durch einen Insider erfolgt – wird dieses Vertrauen verletzt. Ein Reputationsschaden ist die Folge.

ABSCHNITT 3

Die Vorteile von Insider Threat Management

Insider Threat Management (ITM) hilft dem IT-Security-Team, diesen einzigartigen Bedrohungsvektor in den Griff zu bekommen

Es kombiniert Elemente von Data Loss Prevention (DLP) und User Behavior Analytics (UBA), um das Risiko auf drei wichtige Arten zu reduzieren:

Identifizierung von Anwenderrisiken

ITM-Lösungen bieten IT-Security-Teams die Möglichkeit, potenzielle Sicherheitsverletzungen schnell zu erkennen. Effektive Tools helfen Ihnen, zwischen Falschmeldungen und Insider-Aktivitäten zu unterscheiden, die eine Nachverfolgung erfordern. Dazu ist es erforderlich, den gesamten Kontext der User-Aktivitäten und Datenbewegungen zu kennen – insbesondere bei Usern, die als hohes Risiko eingestuft werden.

Schutz vor Datenverlust

Die meisten Finanzunternehmen verfügen über Daten, die sie schützen müssen, zum Beispiel proprietäre Algorithmen, Geschäftsgeheimnisse, personenbezogene Informationen usw. Kein Finanzdienstleister kann es sich leisten, dass diese Daten die eigene Umgebung verlassen. Die Identifizierung und schnelle Schließung von Datenlecks ist eine Kernfunktion moderner ITM-Lösungen.

Schnellere Reaktion auf Zwischenfälle

Die Kosten von Bedrohungen durch Insider hängen maßgeblich davon ab, wie schnell die Reaktion auf den Zwischenfall erfolgt. Moderne ITM-Systeme tragen dazu bei, dass Sicherheitsteams bis zu 10 Mal schneller reagieren können. Mit der richtigen ITM-Lösung sind für Schritte, die andernfalls Tage oder Wochen dauern, nur noch wenige Minuten nötig. Durch die schnellere Untersuchung wird die Zeit bis zur Problemlösung deutlich verkürzt.

ABSCHNITT 4: Proofpoint ITM in Aktion

Reale Vorfälle

Weltweit tätiger Versicherungsmakler – besserer Überblick über Aktivitäten der verteilten Belegschaft

Die Herausforderung

Ein weltweit tätiger Versicherungsmakler wollte die Schadensfalldaten seiner Kunden schützen.

Dazu benötigte das Sicherheitsteam einen besseren Überblick über potenzielle Datenschutzverletzungen durch Insider. Das Unternehmen konnte die stark verteilte Belegschaft über eine Cloud-basierte Anwendung überwachen, doch die Überprüfung der Aktivitätsprotokolle der Anwendung – und die Rekonstruktion der tatsächlichen Ereignisse – war mit großem Zeit- und Arbeitsaufwand verbunden. Die über die Anwendung erfassten und verwalteten Daten unterlagen zudem Datenschutzgesetzen, was zusätzliche Sorgen mit sich brachte.

Die Lösung

Das Maklerunternehmen benötigte ein ITM-Tool, mit dem sich vertrauliche Daten überall proaktiv schützen lassen – unabhängig davon, wo sie gespeichert und übertragen werden und insbesondere auch auf Remote-Endgeräten. Dazu war ein besserer Überblick über die Interaktionen der Anwender mit den Daten sowie über die Aktivitäten auf Endgeräten notwendig. Gefordert war also eine Lösung, die riskantes Verhalten proaktiv erkennt, Compliance-Warnungen sendet und Audits für Compliance-Teams vereinfacht.

Das Ergebnis

Durch ITM profitiert das Unternehmen wie folgt:

- Erkennen Sie risikoreiche Bewegungen von Schadendateien aus Unternehmensanwendungen, auf Servern und aus Endgeräten heraus.
- Informieren und warnen Sie User bei richtlinienwidrigem Verhalten in Echtzeit.
- Stellen Sie bei der Untersuchung eines Alarms unwiderlegbare Beweise für das „Wer, Was, Wann, Wo, Warum und Wie“ zusammen. Bildschirmaufzeichnungen der Endpunktaktivität liefern den Kontext dessen, was vor und nach einer Verletzung geschah. Mit diesen Erkenntnissen lässt sich feststellen, ob die Aktivität durch fahrlässiges oder böswilliges Verhalten oder eine externe Kompromittierung erfolgte.
- Bewahren Sie einen detaillierten Prüfpfad der Aktivitäten von Mitarbeitern und Dritten auf, um finanzielle Compliance-Vorgaben zu erfüllen.

Unabhängiger Vermögensverwalter – Schutz des Vertrauens und der Assets von Kunden

Die Herausforderung

Unabhängige Vermögensverwalter müssen die vertraulichen und privaten Informationen ihrer Kunden zuverlässig schützen. Ihr Erfolg hängt vom Vertrauen ihrer Kunden ab.

Im Rahmen ihrer täglichen Arbeit haben die Mitarbeiter der Vermögensverwaltung täglich mit Daten von Privatkunden zu tun. Zu den Insidern gehören nicht nur Fondsmanager, Administratoren und andere Mitarbeiter, sondern auch externe Auftragnehmer. Die Firma sah sich ständigen Bedrohungen ausgesetzt – Cyberkriminalität, von Unternehmen und Staaten geförderte Spionage, Geldbetrug und vieles mehr.

Die Lösung

Das Unternehmen benötigte ein zuverlässiges Sicherheitssystem, das vor Cyberkriminalität und Finanzbetrug schützt. Zudem benötigte das IT-Security-Team eine einfachere Möglichkeit, potenziell riskante Aktivitäten – einschließlich Remote-Anwender und externe Parteien – im gesamten Unternehmen zu erkennen.

Das Ergebnis

Durch ITM profitiert das Unternehmen wie folgt:

- Vereinfachte Richtlinien zur akzeptablen Nutzung und Einhaltung von Compliance-Vorgaben
- Automatische Echtzeit-Erkennung riskanter Übertragungen sensibler und vertraulicher Informationen
- Vereinfachung der Untersuchung von Zwischenfällen, indem alle Datenbewegungen und Anwenderaktivitäten in Echtzeit korreliert werden; Bildschirm-Screenshots zu Endgeräteaktivitäten liefern unwiderlegbare Nachweise über die Aktivitäten der Anwender
- Speicherung eines detaillierten Auditprotokolls zu den Aktivitäten von Mitarbeitern und Dritten zur Einhaltung von Compliance-Vorschriften

Regionale Bank – Schutz der Callcenter vor Insider-Bedrohungen

Die Herausforderung

Eine regionale Bank musste ihre Callcenter in der Zeit der intensiven Home Office-Nutzung zuverlässig schützen.

Bei jedem Anruf greifen die Mitarbeiter auf die Daten des Bankkunden zu. Das Sicherheitsteam musste auch bei Mitarbeitern, die im Home Office arbeiten, weiterhin in der Lage sein, die Aktivitäten dieser Insider zu überwachen und auf potenzielle Zwischenfälle zu reagieren. Der Bank bereiteten vor allem die besonders gefährdeten Mitarbeiter mit Zugriff auf wertvolle private Informationen Sorgen, da diese gestohlen, kompromittiert oder manipuliert werden könnten. Das Team musste außerdem die Möglichkeit haben, bei einem Zwischenfall forensische Daten zu identifizieren, zu erfassen und weiterzugeben.

Die Lösung

Das Sicherheitsteam suchte eine Lösung, die anormales Verhalten in Echtzeit erkennt und zusätzlich die Datenerfassung und den Überblick über Mitarbeiter im Home Office gewährleistet, ohne die Produktivität und den Kundendienst zu beeinträchtigen.

Das Ergebnis

Durch ITM profitiert das Unternehmen wie folgt:

- Die Anwender sind widerstandsfähiger. ITM steigerte durch reale Insider-Bedrohungsszenarien das Sicherheitsbewusstsein und half der Bank, die eigenen Datenschutzrichtlinien deutlicher darzustellen.
- Auf Endgeräten wurden ressourcenschonende sogenannten Lightweight-Agents implementiert, die die Produktivität der Anwender nicht beeinträchtigen und die Geräte nicht ausbremsen.
- Riskantes Anwenderverhalten und riskante Datenübertragungen werden in Echtzeit erkannt.
- Personal- und Rechtsabteilung sowie Compliance- und IT-Teams arbeiten zusammen, um sich darüber abzusprechen, welche Anwender- und Dateidaten erfasst werden, welche Verhaltensweisen erkannt werden sollen und wie auf Zwischenfälle zu reagieren ist.
- Untersuchungen werden beschleunigt. ITM liefert kontextbezogene Bedrohungsdaten zum Anwender, vereinfacht die Erfassung von Nachweisen und optimiert die Zusammenarbeit zwischen Teams.

Schlussfolgerungen und Empfehlungen

Gründe für Proofpoint: ITM mit Best Practices von einem vertrauenswürdigen Berater

Ihre IT- und Sicherheitsteams sind jeden Tag intensiv damit beschäftigt, Cyberbedrohungen zu identifizieren, zu erkennen und abzuwehren. Mit Proofpoint Insider Threat Management (ITM) wird diese Aufgabe vereinfacht. ITM schützt Sie vor Datenverlust, Störungen und anderen Schäden, die durch böswillige, nachlässig handelnde und kompromittierte Anwender verursacht werden.

Unsere prämierte Lösung unterstützt bereits mehr als 1.200 führende Unternehmen in mehr als 100 Ländern:

- Schnellere Erkennung potenzieller Risiken für sensible und vertrauliche Informationen durch Insider-Bedrohungen
- Reduzierung der Häufigkeit, Schwere und Kosten für Zwischenfälle, indem die Zeit bis zur Reaktion verkürzt wird
- Produktivere Sicherheitsteams bei geringeren Kosten: Mit Proofpoint können Sie mehrere Technologien (z. B. anwenderbasierte Analysen und Endgeräte-DLP) zu einer ITM-Plattform konsolidieren

So unterstützen wir Sie:

- Wir erarbeiten gemeinsam mit Ihnen ein Proof-of-Concept, mit dem Sie Ihr ITM-Programm darstellen können.
- Wir unterstützen Sie bei Konzeption und Aufbau Ihres Programms zur Abwehr interner Bedrohungen. Dazu gliedern wir Ihre Initiativen in kleinere Projekte, die basierend auf riskanten Verhaltensweisen priorisiert werden. Das Proof-of-Concept hilft Ihnen, Ihr ITM-Programm zu visualisieren. Und mit unseren ITM Jump Start-Services können Sie schnelle Rendite erzielen.
- Mit unserem Proofpoint Security Awareness Training können Sie Ihre Anwender sensibilisieren und so deren Resilienz stärken.

Wir haben das gleiche Ziel wie Sie – den Schutz wertvoller Unternehmensressourcen und der Menschen, die sie produzieren.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

0512-002-01-01 10/21