proofpoint

KUNDENBERICHT

Bank beseitigt mit Proofpoint praktisch alle Identitäts-schwachstellen

Die Herausforderung

- Identifizierung potenziell ausnutzbarer Lücken zwischen mehrschichtigen Sicherheitskontrollen
- Beschleunigung von Behebungsmaßnahmen
- Zuvorkommen von Angriffen

Die Lösung

Proofpoint Identity Threat Defense-Plattform

- Proofpoint Spotlight
- Proofpoint Shadow

Die Ergebnisse

- Domain-Administratorrechte von 350 auf Null verringert
- Riskante Einfallstore zu den wichtigsten Assets identifiziert und geschlossen
- Größeres Vertrauen von Führungskräften und Vorstandsmitgliedern in unternehmensweite Kontrollen

Das Unternehmen

Diese Bank gehört einem multinationalen Finanzdienstleistungsunternehmen und verfügt über Niederlassungen in den USA. Zu ihrem Portfolio gehören Bankdienstleistungen, Kreditkarten, Darlehen und Vermögensverwaltung. Angesichts eines Asset-Bestands von mehreren Milliarden US-Dollar setzt die Bank alles daran, die Zahl von Cybersicherheitsschwachstellen so weit wie möglich zu minimieren.

Die Herausforderung

Das Cybersicherheitsteam der Bank ist verantwortlich für mehr als 10.000 Anwender-Endpunkte sowie für die Absicherung der Entwicklungs-, Betriebs- und Zugriffsprozesse. Es hatte eine mehrschichtige Sicherheitsumgebung mit Lösungen für Bedrohungserkennung und Cyberrisiko-Management aufgebaut, wobei zahlreiche Sicherheitsebenen voneinander isoliert waren. Lediglich die SIEM-Lösung der Bank deckte als „horizontale“ Ebene alle Kontrollen ab und führte Ereigniserfassung und Analysen durch. Trotz der hochentwickelten Schutzmaßnahmen fanden immer wieder hartnäckige Angriffe statt, die zeigten, dass kein Unternehmen gegenüber potentiellen Kompromittierungen immun ist.

„Ich wusste, dass es einige Schwachstellen geben würde, mit denen wir leben müssen“, erklärte der CISO. „Einige der Assets lassen sich nur schwer patchen, ohne den Betrieb zu unterbrechen, und perfekte Cyber-Hygiene ist schlicht unmöglich. Wir wollten Transparenz und Schutz für alle unsere Netzwerke und Endpunkte, um Lücken zu identifizieren, in denen unsere anderen Kontrollen möglichweise keinen ausreichenden Schutz bieten.“

Die Lösung

Der CISO erfuhr von seinen Branchenkollegen von Proofpoint Identity Threat Defense. Er wusste, dass die Plattform bei mehreren führenden Banken im Einsatz ist, hatte sie jedoch noch nicht in Aktion erlebt.

„Als ich die Proofpoint-Plattform im Einsatz erlebte, fand ich ihren Ansatz sehr sinnvoll“, betonte der CISO. „Sie bietet uns die Möglichkeit, unser Netzwerk mit den Augen eines Angreifers zu sehen.“

Proofpoint Shadow ist eine agentenlose Lösung, die Bedrohungsdaten verarbeitet und über die gesamte Infrastruktur hinweg ein Netz aus Täuschungen aufzieht. Die Lösung beschleunigt die Bedrohungserkennung deterministisch, indem Bedrohungen basierend auf Interaktionen der Angreifer mit Täuschungen identifiziert werden – im Gegensatz zu probabilistischen Ansätzen, die Signaturen und Verhaltensanalysen nutzen. Im Gegensatz zu anderen Täuschungstechnologien, die auf Agenten oder Honeypots setzen und sich dadurch verraten können oder sogar von Angreifern ausnutzen lassen, verhindert die agentenlose Proofpoint-Architektur eine Entdeckung. Der CISO und sein Team führten eine 60-tägige Proof-of-Concept-Phase mit Proofpoint durch und testeten die Lösung auf Herz und Nieren. Außerdem führten sie Penetrationstests durch, um die Lösung auszuhebeln – und die Penetrationstester scheiterten jedes Mal.

„Dank Proofpoint Identity Threat Defense haben wir größeres Vertrauen in unsere Sicherheitskontrollen. Durch die Lösung wurde der Schutz insgesamt messbar besser.“

Chief Information Security Officer

Mithilfe von Proofpoint Spotlight konnte das Team auch hochriskante Angriffspfade aufdecken, durch die Angreifer sich schnell durch das Netzwerk zu den wichtigsten Assets bewegen können. Die Lösung identifiziert kontinuierlich ungenutzte oder unnötige Zugriffsrechte sowie unzureichend geschützte Anmeldedaten, die Angreifer kompromittieren und missbrauchen könnten.

„Proofpoint Spotlight hat anhand tatsächlicher Cyberangriffsmuster schnell unsere schwerwiegendsten Lücken identifiziert“, erklärt der CISO. „Damit hatten wir die Beweise und den Kontext, um Behebungsmaßnahmen zu priorisieren und bei Bedarf weitere Sicherheitskontrollen zu optimieren.“

Um die maximale Effektivität der Lösung zu gewährleisten, wussten nur wenige Personen im Sicherheitsteam der Bank von ihrer Bereitstellung. Warnungen von Proofpoint Identity Threat Defense werden als Richtlinienverstöße eingestuft und an das SIEM-System geschickt. Ein IT-Analyst der Bank hat ausschließlich die Aufgabe, von der Plattform gemeldete „Richtlinienverstöße“ zu untersuchen. False Positives bereiteten den für die Bereitstellung der Lösung zuständigen Sicherheitsexperten keine Probleme – jede Warnung ist ein Hinweis auf echte laterale Bewegungsversuche unbekannter Personen im Netzwerk.

„Die von Proofpoint erfassten Informationen bieten wertvolle und relevante Erkenntnisse, mit denen wir unsere Führungskräfte überzeugen können."

Chief Information Security Officer

Die Ergebnisse

Sperrung von Domain-Zugriffen

Proofpoint Spotlight stellte unmittelbar nach der Bereitstellung Lücken in der Sicherheitshygiene fest, zum Beispiel Konfigurationsfehler und Probleme mit der Zugangskontrolle. Die Plattform führt kontinuierlich Erkennungen durch und ermöglicht selektive Automatisierung, sodass hochriskante Angiffspfade mühelos aufgedeckt und gesperrt werden. Dadurch konnte Proofpoint nicht nur Konten mit übermäßigen Rechten identifizieren, sondern auch die realen Netzwerkpfade anzeigen, mit denen Angreifer auf die wichtigsten Assets zugreifen. Dank dieser Transparenz erhielt das Team des CISOs den notwendigen Kontext, um genau zu festzustellen, an welchen Stellen scheinbar harmlose Verbindungen laterale Angreiferbewegungen ermöglichen. Dadurch konnte das Team nicht zwingend erforderliche Schnittstellen basierend auf Risikometriken und Auswirkungen auf Geschäftsprozesse und Workflows entfernen. Außerdem arbeitete der CISO mit dem IT-Team zusammen, um Berechtigungen in der gesamten Infrastruktur strategisch zu entfernen.

„Wir haben unsere Richtlinien optimiert und die Zahl der Domain-Administratorrechte von 350 auf Null reduziert", freut sich der CISO. „Umfassender Zugriff ist nur für einen begrenzten Zeitraum in einem Notfall verfügbar."

Durch die Möglichkeit zur schnellen und einfachen Erkennung ausnutzbarer Lücken erhält das Sicherheitsteam einen Vorsprung vor den Angreifern. Wenn Angestellte das Unternehmen verlassen, kann das Team mit deren Anmeldedaten herausfinden, wo diese Anmeldedaten genutzt wurden, und dadurch Lücken schließen, die andernfalls unentdeckt bleiben würden.

So gewinnen – und behalten – Sie das Vertrauen der Unternehmensführung

Die Proofpoint Identity Threat Defense-Plattform kann nicht nur laterale Bewegungen effektiv erkennen und das Team bei der Absicherung der Umgebung unterstützen, sondern auch die Kommunikation verbessern. Mit den umfangreichen Telemetriedaten und den Berichten der Proofpoint-Lösung konnte der CISO den Führungskräften und Vorstandsmitgliedern der Bank leicht verständliche Informationen und grafische Übersichten dazu geben, wie Angreifer vorgehen, warum laterale Bewegungen so gefährlich sind und wie die vorhandenen Schutzmaßnahmen die IT-Umgebung der Bank schützen.

Obwohl die Cybersicherheitsinfrastruktur der Bank bereits gut aufgestellt war, erhielt der CISO durch Proofpoint bessere Kontrolle, mehr Transparenz und die Möglichkeit, wichtige Informationen besser zu kommunizieren. Die Sicherheit der Bank wurde durch die Transparenz, die Behebungsmöglichkeiten und die Effektivität der Kontrollen entscheidend verbessert.

„Dank Proofpoint Identity Threat Defense haben wir größeres Vertrauen in unsere Sicherheitskontrollen", betont der CISO. „Durch die Lösung wurde der Schutz insgesamt messbar besser."

MEHR ERFAHREN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. 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 85 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten 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**.

proofpoint.

0613-002-04-01 06/24