proofpoint

KUNDENBERICHT

Kfz-Finanzierungsfirma nutzt Proofpoint zur Erweiterung des Programms zur Schwachstellenverwaltung auf Identitätsrisiken

Die Herausforderung

- Erfassung von Identitätsrisiken im Programm zur Schwachstellenverwaltung
- Legacy-Anwendungen werden von der vorhandenen Lösung zur Verwaltung privilegierter Zugriffe nicht sinnvoll unterstützt
- Fehlender kontinuierlicher Überblick über Risiken durch privilegierte Identitäten

Die Lösung

Proofpoint Identity Threat Defense

- Proofpoint Spotlight

Die Ergebnisse

- Neues Bewusstsein für erhebliche Identitätsrisiken
- Sofortige Verbesserung der Risikolage
- Umfassendes Programm zur Schwachstellenverwaltung deckt nun den Angriffsvektor Nr. 1 ab: Identität

Das Unternehmen

Dieser weltweite Anbieter für Kfz-Finanzierungslösungen hat mehr als 9.000 Angestellte und Niederlassungen in Nord- und Südamerika sowie in Asien. Das Unternehmen arbeitet sowohl mit Verbrauchern als auch mit Kfz-Händlern zusammen und bietet Kauffinanzierung und Leasing-Programme an. Zum Portfolio gehören auch kommerzielle Kreditprodukte für Händler, mit denen diese ihr Geschäft finanzieren und ausbauen können. Das Unternehmen verwaltet einen Asset-Bestand in Höhe von etwa 60 Milliarden US-Dollar.

Die Herausforderung

Das Unternehmen verfügt über eine große und heterogene IT-Infrastruktur, was zu Problemen mit langjährig eingesetzten Anwendungen führt. Trotz einer implementierten Lösung zur Verwaltung privilegierter Zugriffe (Privileged Access Management, PAM) werden zahlreiche Legacy-Anwendungen nicht geschützt – insbesondere solche, deren Upgrade zu teuer ist oder die eigentlich außer Betrieb genommen werden sollen. Betroffen waren zudem Service- und Administratorkonten, die nicht zuverlässig geschützt werden konnten. Aus diesem Grund konnte das Unternehmen seine privilegierten Anmeldedaten und Identitäten nicht zuverlässig kontrollieren und besaß auch keinen ausreichenden Überblick über potenzielle Identitätsrisiken – weder für IT-Administratoren noch für reguläre Anwender.

Der Senior Vice President für Global Cybersecurity Strategy and Operations erklärt dazu: „Wenn große lokale Infrastrukturen seit Jahren auf Active Directory laufen, wirken sich vor langer Zeit getroffene Entscheidungen bis heute aus. Das führt zu Schwachstellen und zahlreichen technischen Schulden. Zudem wird die Komplexität durch Cloud-Migration, Fusionen und Übernahmen erhöht.“

Die Lösung

Das Unternehmen betrachtete Proofpoint Identity Threat Defense als wichtige Erweiterung der eigenen umfassenden Strategie zur Schwachstellenverwaltung. Bisher konzentrierte man sich bei der Behebung von Sicherheitslücken auf CVEs und CWEs. Gleichzeitig war den Verantwortlichen bewusst, dass Fehler bei der Identitätskonfiguration zu potenziellen Risiken führten. Deshalb wurde eine umfassende Überwachung für alles implementiert, das potenziell zu Cybersicherheitsrisiken führen kann – unabhängig davon, ob es dazu eine CVE gibt. Auf Grundlage des OSI 7-Schichtenmodells richtete das Unternehmen seinen automatisierten Risikoanalyseansatz neu aus, um die gesamte IT-Umgebung abzudecken. Dabei zeigte sich, dass die Identitätsrisikoverwaltung fehlte.

„Das Proofpoint-Tool hat uns neue Einblicke verschafft. Wir wussten zwar schon vorher, dass wir Identitätsrisiken priorisieren müssen, hatten aber einfach keinen Ansatzpunkt."

AVP für IT-Schwachstellen

Diese Lücke wurde Anfang 2021 durch die Implementierung von Proofpoint Identity Threat Defense geschlossen. Diese Lösung zur Identitätsrisikoverwaltung integriert sich in die AD-Infrastruktur (Active Directory) des Unternehmens und scannt regelmäßig alle Endpunkte. Mithilfe der gewonnenen Erkenntnisse wird ein Repository aller Identitätsrisiken erstellt, das per API abgerufen werden kann. Das IT-Sicherheitsteam analysiert diese Erkenntnisse und trifft sich regelmäßig mit dem Team für Schwachstellenbehebung, um gemeinsam Änderungen zur Risikominimierung in der Umgebung umzusetzen. Laut dem AVP für IT-Schwachstellen trägt diese Zusammenarbeit Früchte: „Gemeinsam mit der IT-Abteilung liefern wir die besten Ergebnisse."

Für die Maßnahmen zur Schwachstellenbehebung gelten vom jeweiligen Schweregrad abhängige SLAs, sodass kritische Fälle priorisiert werden.

Die Ergebnisse

Unmittelbar nach der Implementierung konnte das Unternehmen Verbesserungen bei seiner Risikolage feststellen. Nachdem das Produkt nun ein Jahr lang im Einsatz ist, werden meist mehrere neue Probleme pro Woche gefunden und schnell gelöst. „Üblicherweise sind das keine Fälle von Böswilligkeit, sondern Gedankenlosigkeit – jemand macht einen Fehler oder ist in Eile."

Auf die Frage, was das Team ohne die Proofpoint-Lösung tun würde, fällt die Antwort schwer, da nur diese Lösung solche identitätsbezogenen Erkenntnisse (insbesondere für Endpunkte) liefert. Dazu erklärt der AVP für IT-Schwachstellen: „Es gibt zum Beispiel keine andere Möglichkeit, ein in PuTTY gespeichertes Kennwort zu sehen."

Der Senior Vice President für Global Cybersecurity Strategy and Operations fügt hinzu: „Die Vorteile zeigen sich gerade bei Fusionen und Übernahmen – bei einem Scan vor und nach der Integration. Dank der Lösung kann ich sehen, wie sauber die Umgebung des neuen Unternehmens ist und welche technischen Schulden bestehen."

„Die Vorteile zeigen sich gerade bei Fusionen und Übernahmen – bei einem Scan vor und nach der Integration. Dank Proofpoint Identity Threat Defense kann ich sehen, wie sauber die Umgebung des neuen Unternehmens ist und welche technischen Schulden bestehen."

Senior Vice President für Global Cybersecurity Strategy and Operations

Auf die Frage, ob er Proofpoint Identity Threat Defense anderen Kunden empfehlen würde, betont er: „Angesicht des erfolgreichen Einsatzes und unserer neuen Ausrichtung kann ich diese Lösung allen empfehlen, die Schwachstellen beheben möchten. Dieses Tool bietet enorme Vorteile bei der Visualisierung von klassischen Sicherheitslücken, Identitätsschwachstellen und Konfigurationsfehlern."

Er fügt hinzu: „Eine einzige Identitätsschwachstelle kann eine gesamte Umgebung lahmlegen. Daher ist jede Information darüber von Vorteil, besonders wenn ich die Risiken sehe und sie im Laufe der Zeit immer weiter reduzieren kann. Wir konnten hunderttausende Türen fest verschließen, was ein enormer Erfolg ist."

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.

0613-003-04-01 06/24