E-BOOK

Identitäten mit Proofpoint sichern

Konkrete Anwendungsszenarien und Kundenberichte

proofpoint.

Einleitung

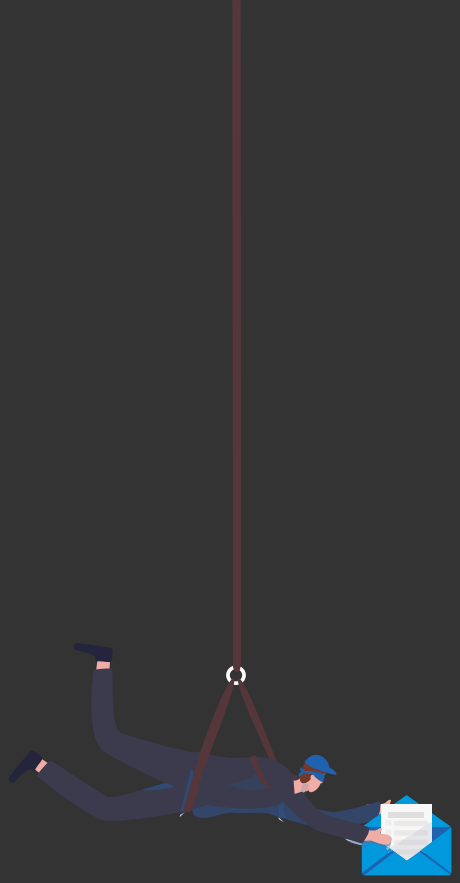
Rechteerweiterungen und laterale Bewegungen stellen für die meisten Sicherheitsteams eine ständige Herausforderung dar – selbst in den größten Unternehmen der Welt. Ein Blick auf Microsoft genügt. Im Januar 2024 gab das Unternehmen bekannt, dass es von einer berüchtigten Gruppe von Bedrohungsakteuren kompromittiert wurde, hinter der Russland stehen soll.

Die Angreifer nutzten ein ungeschütztes altes Testkonto aus. Nach dessen Kompromittierung erweiterten sie ihre Berechtigungen und bewegten sich lateral durch die Microsoft-Cloud-Systeme. Und hier liegt der Hase im Pfeffer: Weil sie sich als legitime Anwender ausgaben, blieben sie mehr als einen Monat lang unerkannt.[1]

Kompromittierungen dieser Art zeigen die Schwäche in der Mitte einer Angriffskette. Hier missbrauchen Angreifer kompromittierte Konten, um die nächsten Verteidigungslinien eines Unternehmens zu durchbrechen. Dafür nutzen sie Konfigurationsfehler aus und suchen nach Identitätsschwachstellen, um Zugriff auf Konten mit immer höheren Berechtigungen zu erlangen.

Rechteerweiterungen und laterale Bewegungen

1 Bleeping Computer: „Microsoft Reveals How Hackers Breached Its Exchange Online Accounts“ (Microsoft gibt bekannt, wie Hacker Exchance-Online-Konten kompromittieren konnten), Januar 2024.



Dieser Teil der Angriffskette spielt bei Cyberangriffen eine wichtige Rolle. Mit einer gestohlenen Identität können Angreifer sich als legitime Anwender ausgeben und dadurch quasi unsichtbar werden. Dadurch haben sie fast völlige Handlungsfreiheit und können Kennwörter zurücksetzen, Richtlinien ändern, Software installieren und Daten extrahieren oder für Lösegeldforderungen verschlüsseln.

Aber wie können wir sie stoppen?

Mit Proofpoint Identity Protection können Sie die Analysen durchführen, mit denen sich angreifbare Identitäten finden und korrigieren lassen, bevor sie Angreifern in die Hände fallen. Doch das ist nicht alles. Darüber hinaus können Sie damit aktive Angreifer enttarnen, die in Ihre Umgebung gelangt sind.

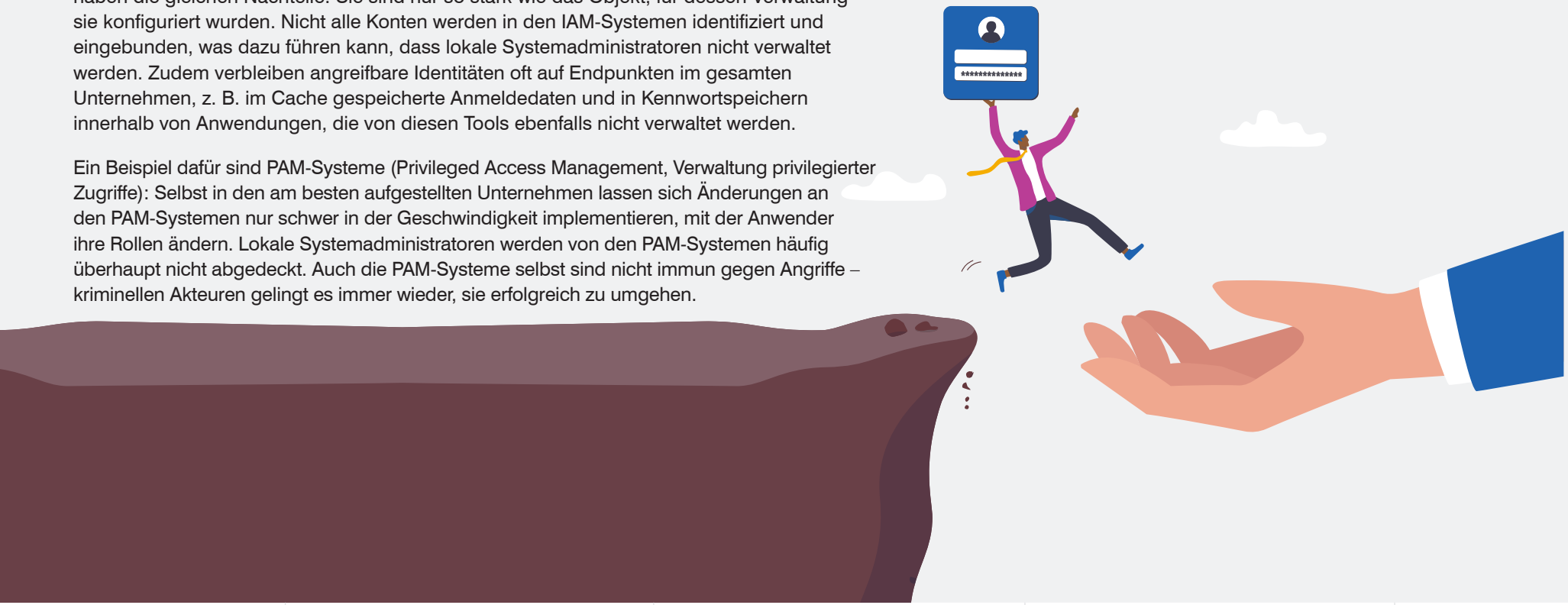
In diesem E-Book stellen wir drei Anwendungsszenarien vor, die Ihnen die Funktionsweise von Proofpoint Identity Protection verdeutlichen. Zudem zeigen wir anhand realer Fallbeispiele von Kunden, welche Vorteile unsere Lösung in Aktion bietet.

ANWENDUNGSSZENARIO 1:

Von IAM-Tools hinterlassene Sicherheitslücken schließen

Alle gängigen IAM-Tools (Identity Access Management, Identitäts- und Zugangsverwaltung) haben die gleichen Nachteile: Sie sind nur so stark wie das Objekt, für dessen Verwaltung sie konfiguriert wurden. Nicht alle Konten werden in den IAM-Systemen identifiziert und eingebunden, was dazu führen kann, dass lokale Systemadministratoren nicht verwaltet werden. Zudem verbleiben angreifbare Identitäten oft auf Endpunkten im gesamten Unternehmen, z. B. im Cache gespeicherte Anmeldedaten und in Kennwortspeichern innerhalb von Anwendungen, die von diesen Tools ebenfalls nicht verwaltet werden.

Ein Beispiel dafür sind PAM-Systeme (Privileged Access Management, Verwaltung privilegierter Zugriffe): Selbst in den am besten aufgestellten Unternehmen lassen sich Änderungen an den PAM-Systemen nur schwer in der Geschwindigkeit implementieren, mit der Anwender ihre Rollen ändern. Lokale Systemadministratoren werden von den PAM-Systemen häufig überhaupt nicht abgedeckt. Auch die PAM-Systeme selbst sind nicht immun gegen Angriffe – kriminellen Akteuren gelingt es immer wieder, sie erfolgreich zu umgehen.



Zusammenfassung

Eine Kfz-Finanzierungsfirma nutzt Proofpoint, um ihre Sicherheitsvorkehrungen durch eine Risikomanagement-Komponente zu verstärken.

Kundenprofil

Industrie: Finanzen

Mitarbeiter: 9.000

Ort: Weltweit

Lösungen

Produkt: Proofpoint Identity Protection

Komponente: Proofpoint Spotlight

Wie hilft Proofpoint

Eine Komponente von Proofpoint Identity Protection ist Proofpoint Spotlight. Damit ist es möglich, angreifbare Identitäten zu finden und Sicherheitslücken bei diesen Identitäten zu schließen, bevor Angreifer sie ausnutzen. Dazu scannt Proofpoint Spotlight Ihre Endpunkte, IAM-Systeme und Identitäts-Repositorys auf nicht verwaltete, falsch konfigurierte und ungeschützte Identitäten. Die Ergebnisse dieser Scans werden in einem leicht verständlichen Bericht präsentiert, der alle verfügbaren Angriffspfade anzeigt und die Identitäten auflistet, die Sie zuerst korrigieren sollten.

Proofpoint in Aktion

Eine Kfz-Finanzierungsfirma verstärkt ihre Sicherheitsvorkehrungen, um Identitäten besser zu schützen.

Der weltweit tätige Kfz-Finanzierer hatte über 30 Jahre hinweg eine große und komplexe IT-Infrastruktur aufgebaut. Im vorhandenen PAM-System wurden jedoch nur wenige Konten für die alten Anwendungen verwaltet. Einige Service- und Administratorkonten konnten überhaupt nicht im Tresor gespeichert werden. Aufgrund dieser Konstellation konnte die Firma weder ihre privilegierten Anmeldedaten und Identitäten vollständig verwalten, noch alle Identitätsrisiken erkennen.

Bei einer routinemäßigen Überprüfung des Ansatzes, den die Firma bei der automatisierten Risikobewertung verfolgte, stellte das IT-Sicherheitsteam fest, dass es keine Möglichkeit zur Verwaltung auftretender Identitätsrisiken gab. Deshalb entschied sich das Team für Proofpoint Spotlight, um diese Sicherheitslücke zu schließen. Proofpoint wurde zügig in die AD-Infrastruktur (Active Directory) und die Endpunkte der Firma (Clients und Server) integriert und scannte alle Endpunkte, das PAM-System sowie weitere Identitäts-Repositorys auf Schwachstellen.

Die IT-Sicherheitsexperten der Firma setzten mit dem Team, das für die Schließung von IT-Schwachstellen zuständig war, regelmäßige Meetings zur Besprechung der gewonnenen Erkenntnisse an. Beide Teams beschlossen, Änderungen gemeinsam vorzunehmen, um Identitätsrisiken zu minimieren. Die Teams verfolgten auch, wie die Änderungen im zeitlichen Verlauf wirkten.

Nach mehr als einem Jahr mit Proofpoint Spotlight vermeldeten sie beeindruckende Ergebnisse. Es traten zwar weiterhin im Wochentakt verschiedene neue kritische Probleme auf, aber man verfügte nun über neue Prozesse, mit denen sich diese Probleme schnell beheben ließen.

„[Proofpoint Spotlight] hat uns neue Einblicke ermöglicht. Wir wussten zwar schon vorher, dass wir Identitätsrisiken priorisieren müssen, hatten aber einfach keinen Ansatzpunkt."

– Assistant Vice President, Verantwortlicher für IT-Schwachstellen bei Kfz-Finanzierungsfirma

Die wichtigsten Punkte

Eine einzige Identitätsschwachstelle kann Ihre gesamte Umgebung lahmlegen. Deshalb brauchen Sie Tools, die Ihre Identitätsschwachstellen aufdecken können. Denn nur so können Sie Risiken erkennen, im Laufe der Zeit minimieren und tausende Identitätslücken schließen, bevor sie von Angreifern ausgenutzt werden.

Identitätsrisiken werden oft durch komplexe AD- und Identitätssysteme begünstigt und verändern sich ständig.

In der Regel ermöglicht niemand die Kompromittierung einer Identität aus einer bösen Absicht heraus. Wahrscheinlicher ist es, dass jemand einfach einen Fehler macht oder in Eile war.

ANWENDUNGSSZENARIO 2:

Red-Team-Übungen „gewinnen“

Auch wenn die Verteidigung einmal versagt, sind die echten Gewinner von Red-Team-Übungen jene Firmen, die damit ihre Sicherheitslage verbessern. Zwar fühlt es sich sicherlich nicht gut an, wenn eine Übung nicht verwaltete oder falsch konfigurierte Identitäten in Ihrer Umgebung zu Tage fördert, aber keine falsche Scham – es geht fast allen so. Erstaunliche 95 % aller Red-Teams finden bei ihren Übungen ungeschützte Anmeldedaten von Domain-Administratoren.[2]

2. Studie von Illusive.

Zusammenfassung

Das SOC-Team einer Privatkundenbank nutzt Proofpoint, um mehrere Versuche eines Red-Teams abzuwehren, sich bei kritischen Konten anzumelden und Server zu kompromittieren.

Kundenprofil

Industrie: Finanzen

Mitarbeiter: 1.000

Ort: EMEA

Lösungen

Produkt: Proofpoint Identity Protection

Komponente: Proofpoint Shadow

Wie hilft Proofpoint

Proofpoint Identity Protection kann Angriffe in der Mitte der Angriffskette erkennen und verhindern, dass ein Red-Team seine Mission unerkannt fortsetzt.

- **Proofpoint Shadow** baut ein dichtes Labyrinth aus Fake-Daten und falschen Netzwerkpfaden zu scheinbar sensiblen Assets und verteilt sie dann im ganzen Unternehmen. Selbst die raffiniertesten Red-Teams können nicht erkennen, was echt und was falsch ist. Sie können es nur herausfinden, wenn sie die ausgelegten Köder aufnehmen – und damit die Sicherheitsteams auf ihre Fährte bringen. In diesem Netz der Illusionen können sie sich den wirklich kritischen IT-Assets kaum unerkannt nähern.
- **Proofpoint Spotlight** kann alle nicht verwalteten, falsch konfigurierten und ungeschützten Identitäten in Ihrer Umgebung finden. Damit können Sie sie korrigieren, bevor das Red-Team – oder ein Bedrohungsakteur – die Chance ergreift und sie ausnutzt.

Proofpoint in Aktion

Eine große Privatkundenbank wehrt zwei Red-Team-Angriffe ab und geht als Sieger hervor.

Eine große Privatkunden- und Investmentbank hatte mehrere Verteidigungslinien mit Sicherheitskontrollen und verschiedenen Tools für die Abwehr von Malware auf Endpunkten aufgebaut. Da die Zahl hochentwickelter hartnäckiger Bedrohungen (APTs) jedoch ständig zunahm, wollte sie neue Erkennungsfunktionen hinzufügen und installierte deshalb Proofpoint Shadow. Kurz danach engagierte die Bank eine namhafte Firma für Penetrationstests, um ihr Netzwerk testen zu lassen. Der Clou war, dass die Firma nicht wusste, dass Proofpoint schon auf die Kompromittierungsversuche warten würde.

Vor Beginn des Penetrationstests verteilte Proofpoint Shadow Fake-Daten, die für Angreifer attraktiv sein könnten, auf jedem Endpunkt im 5.000 Knoten großen Netzwerk der Bank. Die Daten wurden so getarnt, als würden sie zu einer Bankumgebung gehören, einschließlich falscher Anmeldedaten.

Am ersten Tag des Tests erkannte Proofpoint Shadow, dass ein falscher Anwender („User A“) sich an schädlichen Aktivitäten auf einem der Citrix-Server der Bank versuchte. Daraufhin sammelte Proofpoint Shadow Details zum Wer, Was, Wann und Wo des Angriffs und informierte das SOC- und das Incident-Response-Team.

Bei ihren Untersuchungen stellten die Teams fest, dass die Penetrationstester schädliche Tools im Netzwerk der Bank installiert hatten und versuchten, weitere Fake-Konten zu nutzen – die sie nach der Initial-Kompromittierung „gefunden“ hatten –, um ihren Angriff fortzusetzen. Die Penetrationstester hatten keine Ahnung, dass sie von den Verteidigern bereits entdeckt wurden.

Am 22. Tag sendete Proofpoint Shadow dann eine weitere Warnung nach einer schädlichen Aktivität von „User A“. Diesmal war jedoch ein anderer Server betroffen. Als das SOC-Team eine zweite forensische Analyse durchführte, erkannte es hartnäckige Versuche, sich über diesen Server bei kritischen Konten anzumelden. Der Angreifer hatte den Alarm unwissentlich durch zwei verschiedene Sätze falscher Anmeldedaten ausgelöst.

Die wichtigsten Punkte

Wenn Ihr SOC-Team Red-Team-Übungen gewinnt, steigt die Wahrscheinlichkeit, dass es auch echte Cyberkriminelle stoppen kann, die Ihre Umgebung angreifen.

Wenn die SOC- und IT-Sicherheitsteams verdächtige Verhaltensweisen frühzeitig erkennen, können sie Angreifer stoppen, bevor diese sich lateral bewegen und kritische IT-Assets einer Firma erreichen. Im Rahmen dieser Erkennungen müssen auch wertvolle Daten gesammelt werden, damit die Teams die Angriffe forensisch analysieren können. Dies erleichtert die wirksame Reaktion und Minimierung der Auswirkungen.

Die Erkennung eines Versuchs, das Kennwort eines falschen Kontos zu knacken, führt zu einer sehr zuverlässigen Warnung – ein hundertprozentiges True Positive für eine schädliche Aktivität im Netzwerk.

ANWENDUNGSSZENARIO 3:

Hybride Identitäten in AD und Entra ID sichern

Active Directory (AD) ist ein Eckpfeiler der IT-Infrastruktur moderner Unternehmen. Laut einigen Schätzungen nutzen 90 % aller Unternehmen AD als primäre Methode für die Authentifizierung und Autorisierung von Anwendern. Und da immer mehr Unternehmen in die Cloud wechseln, wird Microsoft Entra ID (ehemals Azure AD) immer präsenter.

Diese Tools sind zwar sehr beliebt, aber auch berüchtigt für ihre komplizierte Verwaltung und Pflege. Diese Schwierigkeiten kommen zum großen Teil daher, dass es mit fast jeder Stelle, jeder Person und jedem Gerät im Netzwerk Berührungspunkte gibt. Ebenso wie bei den IAM-Tools sind diese Schwierigkeiten ein konstanter Faktor, weil sich Berechtigungen, Anwender und Unternehmen ständig ändern. Hinzu kommt, dass nicht jede Identität abgedeckt ist. Ein Beispiel dafür sind im Cache gespeicherte Anmeldedaten auf Endpunkten, die von AD und Entra ID nicht verwaltet werden – und auch von keinem IAM-System. Dadurch sind diese Anmeldedaten völlig ungeschützt.

Zusammenfassung

Eine Banken-Holding nutzt Proofpoint, um die Sicherheitslage eines neuen Tochterunternehmens zu analysieren, und entdeckt auf deren Workstations 3.000 Domain-Administrator-Konten.

Kundenprofil

Industrie: Finanzen

Mitarbeiter: 25.000

Ort: USA

Lösungen

Produkt: Proofpoint Identity Protection

Komponente: Proofpoint Spotlight

Wie hilft Proofpoint

Proofpoint Spotlight scannt Active Directory, Entra ID und mehrere andere Identitäts-Repositorys und findet Konten mit übermäßigen Berechtigungen, nicht verwaltete Identitäten auf Endpunkten und privilegierte Identitäten, die weder im PAM- noch in anderen IAM-Systemen verwaltet werden. Damit erhalten Sie die Chance, diese Elemente zu korrigieren, bevor sie in die falschen Hände geraten.

Zudem liefert Proofpoint Spotlight Bottom-Up- und Top-Down-Ansichten aller Risiken im Zusammenhang mit nicht verwalteten, falsch konfigurieren und ungeschützten Identitäten. So können Sicherheitsteams die Angriffspfade sehen, die Cyberkriminelle nutzen könnten, um Ransomware auszuführen und Daten zu stehlen.

Proofpoint in Aktion

Eine Holding analysiert die Identitätsrisiken eines neuen Tochterunternehmens, um die Übernahme sicher abzuschließen.

Eine Banken-Holding mit ca. 200 Milliarden US-Dollar Anlagevermögen und 1.000 Niederlassungen übernimmt etwa aller drei Jahre eine neue Bank. Nach jeder Übernahme führt das IT-Team die Systeme, Software, Daten und Prozesse zusammen. Zuvor muss die Holding aber noch die Sicherheitslage der übernommenen Bank analysieren. In diesem Fall hatte das Team weniger als vier Monate Zeit für seine Analyse.

Anhand der Identitätssicherheit lassen sich Rückschlüsse auf die gesamte Sicherheitslage einer Bank ziehen. Das IT-Team der Holding wusste, dass es einen guten Eindruck von der Lage erhalten würde, wenn es die Identitätsschwachstellen der neuen Bank aufdeckt.

Vor der Übernahme hatte das Team Proofpoint Identity Protection bereits sechs Monate lang eingesetzt, um seine eigenen Workstations und Identitäts-Repositorys zu scannen, und war daher bereits mit den wertvollen Einblicken vertraut. Deshalb entschied es sich dafür, Proofpoint Spotlight auch für die Analyse bei der übernommenen Bank zu nutzen.

„Ich bin froh, dass wir [Proofpoint Spotlight] eingesetzt haben. Jeder hat die Vorteile gesehen. Die Lösung liefert uns das Drehbuch für alle weiteren Übernahmen."

– Director of Cybersecurity Engineering

Nachdem die Proofpoint-Lösung die IT-Umgebung des neuen Tochterunternehmens gescannt hatte, stellte sie eine Risikobewertung mit verschiedenen detaillierten Identitätsrisikobereichen zusammen. Ein Bereich fiel dabei sofort ins Auge: Auf den Workstations wurden enorme 3.000 aktive Domain-Administrator-Konten gefunden. Wenn auch nur eines dieser Konten von einem Angreifer kompromittiert gewesen wäre, hätte das Team die Kontrolle über die ganze Umgebung verloren.

Angesichts der schlechten Sicherheitshygiene bei der neuen Bank beschloss der Vorstand der Holding, dass das Risiko zu groß war und die beiden IT-Umgebungen zumindest vorläufig separat weiterbetrieben werden sollten. Ohne Proofpoint wäre es deutlich schwerer gewesen, den vom IT-Team für notwendig gehaltenen verstärkten Schutz zu rechtfertigen.

Die wichtigsten Punkte

Oft ergeben sich Identitätsrisiken aus normalen Geschäfts- und IT-Prozessen, die viele Jahre lang genutzt wurden. Dies macht sie so schwer zu erkennen und so leicht zu übersehen, was insbesondere für Umgebungen gilt, die im Rahmen einer Übernahme erworben werden.

Active Directory, Entra ID, Endpunkte und andere Repositorys müssen kontinuierlich auf Identitäts-schwachstellen gescannt werden. Ein Angreifer muss lediglich eine einzige Workstation mit einem Administratorkonto kompromittieren, um die Kontrolle über eine ganze Umgebung zu übernehmen.

Fazit

Auch wenn die meisten Unternehmen ihre Umgebungen regelmäßig auf angreifbare Software und Anwendungen prüfen, lassen sie dabei oft angreifbare Identitäten außer Acht – obwohl diese unglaublich wertvoll sind. Tatsächlich handelt es sich bei Identitäten in vielerlei Hinsicht um die wertvollsten Assets eines Unternehmens, weil sie Berührungspunkte mit allen anderen digitalen Ressourcen haben.

Ihr Schutz könnte also nicht wichtiger sein. Cyberkriminelle haben heute Zugang zu einer breiten Palette an Tools, mit denen sie Anmeldedaten schnell, einfach und effektiv ausnutzen können. Noch problematischer ist, dass Unternehmen ihre Verwendung nur schwer erkennen können.

Sie können die Angriffskette nur unterbrechen, wenn Sie Identitäten ebenso umfangreich schützen wie jede andere wertvolle Ressource Ihres Unternehmens. Dies beginnt mit dem Ergreifen proaktiver Maßnahmen und bedeutet, dass die anfälligen Identitäten korrigiert werden müssen, bevor Angreifer sie finden, und dass Täuschungsmanöver notwendig sind, um Angreifer zu entdecken, bevor sie echten Schaden anrichten können.

Weitere Informationen dazu, wie Proofpoint Sie beim Schutz Ihrer Identitäten-unterstützen kann, erhalten Sie unter https://www.proofpoint.com/de/products/identity-protection.

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.

0513-002-04-01 4/24