proofpoint.

Proofpoint Identity Threat Defense-Plattform

Stoppen von Rechteerweiterungen und lateralen Bewegungen

Produkte

- Proofpoint Shadow
- Proofpoint Spotlight

Wichtige Vorteile

- Erkennung, Priorisierung und Behebung von Identitätsschwachstellen
- Informationen zu Risiken durch privilegierte Identitäten und mögliche Angriffspfade in Ihrer Umgebung
- Überblick über Identitätsschwachstellen in Active Directory, Entra ID, AWS Identity Center, Okta, PAM-Systemen, Endpunkten und LAPS
- Automatische Behebung von Identitätsschwachstellen auf Endpunkten
- Frühzeitige Erkennung von Angreifern und schnellere Untersuchung von Bedrohungen
- Einsatz agentenloser Technologien, die Angreifer nicht umgehen können
- Schließung von Lücken, die bei Signatur- und verhaltensbasierter Bedrohungserkennung entstehen
- Integration mit Proofpoint TAP, TAP ATO und NPRE
- Möglichkeit zur Bereitstellung per SaaS

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Angriffe werden immer raffinierter und gezielter, doch die Lösungen, die uns vor solchen Angriffen schützen sollen, können nicht mit den Bedrohungen mithalten.[1] Der Trend lässt vermuten, dass Angreifer ihre Taktiken, Techniken und Prozeduren (TTPs) standardisieren und nun Identitäten ins Visier nehmen. Unternehmen ist es jedoch noch nicht gelungen, die Angriffskette zuverlässig zu unterbrechen. Fakt ist aber, dass Identitäten ein wichtiger Teil der Angriffsoberfläche sind und stärker in den Fokus rücken müssen.

Die Proofpoint Identity Threat Defense-Plattform bietet End-to-End-Schutz vor Identitätsbedrohungen. Mithilfe der Komponenten Proofpoint Shadow und Proofpoint Spotlight ermöglicht sie die Erkennung und Behebung von Identitätsschwachstellen, agentenlose täuschungsbasierte Erkennungen sowie die Erfassung forensischer Daten. Die Plattform hilft Ihnen bei der Erkennung, Priorisierung und Behebung anfälliger Identitäten sowie bei der Erkennung und Abwehr aktiver Bedrohungen.

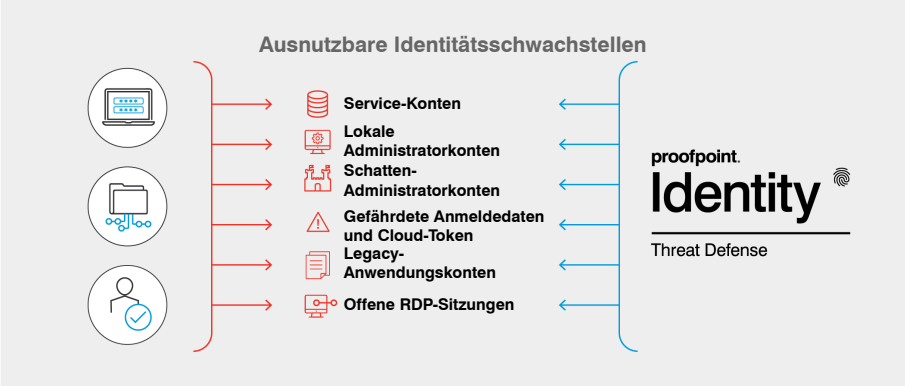

Abb. 1: Proofpoint Identity Threat Defense und ausnutzbare Identitätsschwachstellen.

1 Einige dieser Lösungen umfassen IAM (Identitäts- und Zugriffsverwaltung), MFA (Multifaktor-Authentifizierung), EDR (Endpunkterkennung und Reaktion), SIEM (Sicherheitsinformations- und Ereignis-Management) sowie XDR (erweiterte Erkennung und Reaktion).

In der Identitätskrise

Die meisten Unternehmen setzen auf Active Directory. Doch 79 % dieser Unternehmen sind in den letzten zwei Jahren Opfer einer identitätsbezogenen Kompromittierung geworden. Laut dem Verizon DBIR wurden bei 94 % der erfolgreichen Angriffe Active Directory und privilegierte Identitäten ausgenutzt, um Berechtigungen zu eskalieren. Dabei setzen die Angreifer auf verschiedenste Tools wie Bloodhound, Cobalt Strike, Mimikatz und ADFind, um privilegierte Identitäten schnell auszunutzen. Diese Tools erschweren zudem die Erkennung der Angriffe.

Untersuchungen von Proofpoint zeigen, dass jeder sechste Endpunkt in Unternehmen (Clients und Server) Identitätsschwachstellen aufweist – selbst dann, wenn herkömmliche Lösungen für Identitäts- und Zugriffsverwaltung (IAM) implementiert sind. Angreifer nutzen diese Schwachstellen, um Administratorberechtigungen zu erlangen. Wenn sie zum ersten Mal einen Host erreichen, handelt es sich bei diesem Host selten um das eigentliche Ziel. Auf der Suche nach den kritischsten IT-Assets (auch Tier 0 genannt) versuchen sie, sich lateral im Netzwerk zu bewegen. Sobald sie an ihrem Ziel angelangt sind, können sie Daten exfiltrieren oder auch Ransomware-Angriffe starten.

Abb. 2: Proofpoint Identity Threat Defense-Plattform.

Viele Identitätsschwachstellen haben ihren Ursprung in normalen Geschäfts- und IT-Prozessen wie diesen:

- **Benutzernamen und Kennwörter:** Anwendungen speichern diese Daten oft auf Endpunkten wie Browsern, SSH, FTP, PuTTY und Datenbanken. PAM-Systeme schützen diese Anmeldedaten nicht.
- **Domain-Administrator-Anmeldedaten:** Diese Daten bleiben nach einer Remote-Support-Sitzung manchmal im Systemspeicher zurück. Oft werden sie auch im Cache eines ungeschützten Service-Kontos gespeichert.
- **Schatten-Berechtigungen:** Die Konfiguration von Identitätsverzeichnisobjekten und Gruppen in Active Directory kann sehr schwierig sein, sodass Anwendern mitunter unbeabsichtigt übermäßige „Schatten-Berechtigungen“ zugewiesen werden.

Ein End-to-End-Überblick über Identitätssicherheit

Bei erfolgreichen Angriffen werden Lücken in der Verwaltung und in Schutzmaßnahmen ausgenutzt. Unsere Plattform unterstützt Sicherheitsverantwortliche mit folgenden Möglichkeiten bei der Erkennung und Vermeidung dieser Lücken:

1. **Erkennung:** Sicherheitsverantwortliche profitieren von der kontinuierlichen Erkennung und einem aktuellen Überblick über Identitätsschwachstellen in Active Directory, Entra ID, AWS Identity Center, Okta und Endpunkten.
2. **Priorisierung und Behebung:** Sie erhalten eine Liste der Schwachstellen, priorisiert nach den Schwachstellen, die zuerst behoben werden müssen. Das Spektrum dieser Risiken reicht von „nicht kritisch“ bis „dringend“. Sicherheitsverantwortliche können die automatische Behebung von Identitätsschwachstellen direkt in der Plattform aktivieren und außerdem Ausnahmeregeln einrichten, die mit den Sicherheitsrichtlinien Ihres Unternehmens übereinstimmen.
3. **Erkennung und Reaktion:** Sicherheitsverantwortliche sehen, wenn Angreifer in Ihrer Umgebung aktiv sind. Mithilfe agentenloser Täuschungsmaßnahmen können sie Aktivitäten wie Kerberoasting, Password Spraying, Missbrauch privilegierter Konten und vieles mehr erkennen. Darüber hinaus können Sicherheitsverantwortliche dank automatisiert erfasster forensischer Daten die Reaktion Ihres Unternehmens auf aktive Bedrohungen lenken.

MEHR ERFAHREN

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

0213-003-04-04 6/24