SentinelOne

Singularity | RANGER. AD Assessor

Sicherheits-Checkliste für das Active Directory

Bedrohungsakteure lenken ihre Aufmerksamkeit immer mehr auf identitätsbasierte Angriffsflächen und nehmen dabei vor allem lokale und in der Cloud gehostete AD-Umgebungen (Active Directory) ins Visier. Da AD-Administratoren jedoch betriebliche Anforderungen und restriktive Sicherheitsmaßnahmen unter einen Hut bringen müssen, erweist sich die Absicherung dieser Umgebungen als echte Herausforderung.

Es gibt viele Lösungen zum Schutz von lokalen und Azure AD-Infrastrukturen. Allerdings fällt es Sicherheitsexperten häufig schwer, die passende Lösung für das Risikoprofil eines konkreten Unternehmens zu finden.

Anhand der folgenden Checkliste können Sicherheitsteams in Unternehmen Risiken und Lücken in ihren Schutzmaßnahmen für das Active Directory aufdecken.

Wichtige Fragen rund um den Schutz des Active Directory

Cyber-Hygiene für das lokale und Cloud-basierte Active Directory

- Gibt es eine Liste aller Benutzer- und Gerätekonten?
- Gibt es eine Liste aller Privilegien und Berechtigungen jedes Kontos?
- Wurde eine Least-Privilege-Richtlinie für alle Konten implementiert?
- Werden die AD-Sicherheitseinstellungen regelmäßig überprüft und bewertet?
- Werden Kerberos-Schwachstellen im AD regelmäßig bewertet?
- Sind die AD-Server vor den neuesten CVEs und anderen Schwachstellen geschützt?
- Werden die Vertrauensbeziehungen in allen Gesamtstrukturen regelmäßig überprüft?

Identifizierung von Angriffsindikatoren

- Werden Versuche, AD-Daten zu erfassen, erkannt oder gestoppt?
- Sind Audit-Richtlinien aktiviert?
- Werden die Audit-Protokolle in regelmäßigen Abständen analysiert?
- Haben Sie einen Überblick über die Replikation von Domänenverzeichnissen?
- Haben Sie einen Überblick über Versuche, Benutzer- und Gruppenberechtigungen zu erkennen?
- Haben Sie einen Echtzeit-Überblick über massenhafte Änderungen am AD?
- Können Angriffe wie Kerberoasting und DCShadow in Echtzeit erkannt werden?

Schutz von lokalen und Azure AD-Konten

- Werden Kontoberechtigungen regelmäßig überprüft und für jedes Konto bewertet?
- Werden Dienstkonten und privilegierte Konten regelmäßig überprüft und bewertet?
- Ist der Umfang und die Zahl privilegierter Konten beschränkt?
- Werden Delegierungen regelmäßig überprüft und bewertet?
- Sind die Kennwortrichtlinien angemessen und werden sie regelmäßig bewertet?
- Kann die Nutzung des integrierten AD-Administratorkontos in Echtzeit erkannt werden?

Erkennung von Endpunkt-Angriffen

- Können von Endpunkten ausgehende Versuche zur Erfassung von Informationen und Erkennung des AD erkannt werden?
- Gibt es Sicherheitskontrollen, die AD-Erkennungsanfragen, die von Endpunkten stammen, auf eine falsche Fährte führen?
- Werden AD-Anmeldedaten auf Endpunkten gespeichert? Wenn ja, sollten diese entfernt werden?
- Haben Sie einen Überblick über privilegierte oder gefährdete AD-Anmeldedaten, die auf Endpunkten gespeichert sind und von Angreifern für laterale Bewegungen missbraucht werden könnten?
- Haben Sie einen Überblick über Versuche, delegierte Konten mit speziellen Berechtigungen zu erkennen?

Definitionen

Cyber-Hygiene für das lokale und Cloud-basierte Active Directory

Anhand der Punkte in der Checkliste können Schwachstellen im Active Directory aufgedeckt werden, die Angreifer zur Kompromittierung der Umgebung nutzen könnten. Die Identifizierung und Behebung dieser angreifbaren Schwachstellen ist ein entscheidender Schritt bei der umfassenden Absicherung der AD-Infrastruktur.

Schutz von lokalen und Azure AD-Konten

Kontorichtlinien und -einstellungen haben Einfluss darauf, in welchem Umfang Angreifer eine bestimmte AD-Identität – ob lokal oder in Azure – missbrauchen können. Jedes Konto sollte überprüft und bewertet werden, um sicherzustellen, dass es nur über die für die jeweilige Funktionen nötigen Berechtigungen verfügt. Dies gilt besonders für privilegierte Konten sowie für Konten mit delegierten Administratorrechten (Schatten-Administratorkonten).

Identifizierung von Angriffsindikatoren

Bei vielen Unternehmen gibt es keine Kontrollen zur Erkennung von Angriffsaktivitäten, die AD-Daten ins Visier nehmen. Dazu gehören zum Beispiel das Zusammentragen von Daten sowie Angriffe mit Rechteausweitung (z. B. Kerberoasting). Unternehmen sollten Maßnahmen ergreifen, mit denen sie Angriffe auf das Active Directory erkennen können (z. B. indem sie Änderungen am AD prüfen und daraufhin bewerten, ob die Aktionen auf einen Angriff hindeuten).

Innovativ. Vertrauenswürdig. Anerkannt.

Gartner

Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen

MITRE ENGENUITY

Rekordergebnis bei der ATT&CK-Bewertung

- 100 % Schutz. 100 % Erkennung.
- Höchste analytische Abdeckung 3 Jahre in Folge
- 100 % Echtzeit und keinerlei Verzögerungen

Gartner peerinsights 4,9

99 % der Gartner Peer Insights™

EDR-Analysten empfehlen SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

Informationen zu SentinelOne

SentinelOne ist Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller, umfangreicher und genauer, als das mit ausschließlich manuellen Technologien möglich ist. Die Singularity XDR-Plattform bietet Ihnen Echtzeit-Transparenz und intelligente KI-gestützte Reaktion. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733