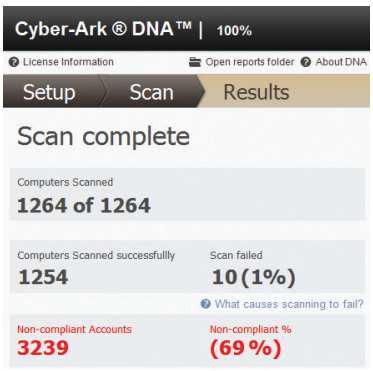
Discovery & Audit

Mit Cyber-Ark DNA™ können Sie:

- Privilegierte Benutzerkonten finden
- Sicherheitsrisiken durch privilegierte Konten klar einstufen
- Verlässliche und umfassende Audit-Informationen sammeln
- Projekte, Budgets und Ressourcen für die Problemlösung präzise planen



Erfassen Sie den Status Ihrer privilegierten Konten auf einfache Weise.

DIE HERAUSFORDERUNG

In jedem größeren Unternehmen stellen privilegierte und administrative Benutzerkonten ein erhebliches Sicherheitsrisiko dar. In den meisten Unternehmen gibt es mehr gemeinsam genutzte und technische Konten als Mitarbeiter. Privilegierte Shared Accounts finden sich auf stationären PCs, Notebooks und Servern, in Datenbanken und Applikationen, auf Sicherheits- und Netzwerkgeräten, in virtuellen Maschinen und Cloud-Anwendungen. Das Unternehmen muss in der Lage sein, diese Konten durch einen einfachen Netzwerkscan zu identifizieren und zentral zu verwalten.

Die IT-Umgebung eines großen Unternehmens besteht aus Hunderten oder Tausenden von Systemen, die über eine Vielzahl von privilegierten und administrativen Identitäten verwaltet werden – zum Beispiel Administratoren- und Dienste Konten in Windows, lokale privilegierte Konten auf Desktops, Root-Konten in UNIX/Linux, root in ESX, system/sys in Oracle-Datenbanksystemen, sa in MSSQL usw. Diese oft gemeinsam genutzten, privilegierten Konten sind aufgrund ihrer umfassenden Berechtigungen ein häufig genutztes Einfallstor für Cyber-Angriffe, die vertrauliche Daten und Unternehmenswerte beschädigen, zu Betriebsausfällen führen und den Ruf des Unternehmens schädigen können.

Dokumentationslücken und auf viele Abteilungen, Standorte und Geräte verteilte Daten machen es sehr schwierig, den Überblick über jedes einzelne privilegierte Konto im Netzwerk zu behalten. Unternehmen sind oft überrascht von der Anzahl ungenutzter Konten, die auf ausrangierten Systemen schlummern oder deren Benutzer das Unternehmen längst verlassen haben. Fusionen und Übernahmen lassen die Zahl der Konten nur noch weiter anwachsen.

Fehlendes Wissen darüber, wo genau privilegierte Konten anzufinden sind, führt zu verschiedenen Problemen:

- **Sicherheits- und Risikomanagement:** Das Sicherheits- und IT-Personal kann die Risiken nicht vollständig überblicken und daher das Risikomanagement auch nicht verbessern.
- **Audits und Compliance:** Prüfer haben Schwierigkeiten dabei, umfassende, gründliche und zuverlässige Informationen für ihre Audits zu erheben.
- **Projektplanung:** Zur Problemlösung erforderliche Kosten und Ressourcen sind schwer zu prognostizieren.

DIE LÖSUNG

Cyber-Ark Discovery & Audit (Cyber-Ark DNA™) bietet eine einfach zu bedienende Lösung, die potenzielle Probleme mit privilegierten Konten aufzeigt.

Von einem Windows-Desktop aus gestartet, fordert Cyber-Ark DNA™ den Benutzer auf, einige einfache Fragen zur Systemumgebung zu beantworten, um eine automatische Suche nach privilegierten Konten durchzuführen. Sobald der Scan abgeschlossen ist, wird Auditoren und Sicherheitsverantwortlichen in einer Zusammenfassung die Anzahl der privilegierten Konten in der Zielumgebung mitgeteilt.

Der automatisch erzeugte, übersichtlich gestaltete Report bietet dem Unternehmen sehr schnelle Erkenntnisse zum Stand der privilegierten Konten im eigenen Netzwerk, ohne Agenten auf den Zielsystemen zu installieren und ohne nennenswerte Netzwerkbandbreite zu beanspruchen. Cyber-Ark DNA liefert darüber hinaus einen ausführlichen Bericht zum Status der privilegierten Konten. Für jedes Konto werden dabei die relevanten Compliance-Informationen hervorgehoben.

Cyber-Ark®
Security That Empowers People™

Verschaffen Sie sich eine Übersicht über Ihre privilegierten Konten für Audits und Risikobewertungen: Cyber-Ark DNA™ identifiziert privilegierte Konten mit Management- oder Compliance-Problemen.

Computer Name	Account Name	Compliance status	Password Age
ProdSRV_01	Administrator	Non-compliant	308
ProdSRV_01	Guest	NA	0
ProdSRV_011	tester	Compliant	13
ProdDB_04	mysqladmin	Non-compliant	751
ProdDB_04	sysadmin	Non-compliant	235
ProdDB_04	serviceadmin	Non-compliant	671
ProdVM_12	vm	Non-compliant	241

Report zum Status privilegierter Konten (Muster)

SPEZIFIKATIONEN

Cyber-Ark DNA™ läuft

- auf Windows 7

Zielsysteme

PCs:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Server:

- Windows 2000
- Windows 2003
- Windows 2008/R2
- Windows 2012

Netzwerkprotokolle

- Windows Datei- und Druckerfreigabe
- Windows (WMI)

Gescannte Daten

Windows-Konten:

- Windows-Domänenkonten
- Lokale Windows-Konten

Dienste Konten:

- Windows-Services
- Scheduled Tasks

DIE VORTEILE

Cyber-Ark DNA™ beantwortet unter anderem folgende Fragen:

- Auf welchen Zielservern sind privilegierte Konten vorhanden?
- Welche persönlichen Administratorkonten wurden auf den Servern angelegt?
- Welche privilegierten Konten verstoßen gegen die Kennwortrichtlinien des Unternehmens, z. B. durch Kennwörter, die älter als 90 Tage sind?
- Haben externe Mitarbeiter auf den Servern zusätzliche privilegierte Benutzerkonten angelegt?
- Gibt es »Hintertüren« in Form von Anwendungskonten für Produkte, die nicht mehr in Betrieb sind?

Die Scanergebnisse verkürzen und vereinfachen die Erfassung und Analyse von privilegierten Konten, ermöglichen einen reibungsloseren und oft auch umfassenderen Audit- und Risikobewertungsprozess und versetzen Auditoren und Sicherheitsverantwortliche in die Lage, das Problem privilegierter Konten im Unternehmen effektiv zu analysieren und zu bewerten.

Cyber-Ark DNA™ unterstützt durch wertvolle Informationen folgende Prozesse im Unternehmen:

Risiken erkennen und beziffern durch Erfassung der Existenz und des Status jedes einzelnen privilegierten Kontos

Durch zielgenaues Reporting über privilegierte, persönliche oder gemeinsam genutzte Konten kann das Unternehmen unbekannte oder nicht ordnungsgemäß verwaltete Konten problemlos lokalisieren und Risiken schnell und einfach erkennen.

Bei der Auditvorbereitung wertvolle Zeit und Kosten sparen

Auditoren erhalten einen zuverlässigen und umfassenden Überblick über privilegierte Konten. Dadurch entfällt die oft schwierige und zeitraubende manuelle Ermittlung und Zuordnung dieser Informationen.

Die Problematik privilegierter Konten berechenbar machen

Ein klarer und zuverlässiger Überblick über Umfang und Status von privilegierten Konten liefert eine betriebswirtschaftliche Rechtfertigung für ein besseres Risikomanagement, die Optimierung der Betriebsabläufe und eine genauere Projektplanung.

DIE LEISTUNGSMERKMALE

Zu den wichtigsten Merkmalen von Cyber-Ark DNA™ gehören:

- **Bedienerfreundliches, nicht intrusives Scannen** - Cyber-Ark DNA ermöglicht schnelles Scannen bei geringer Bandbreitenauslastung und minimalem Netzwerk- und CPU Ressourcenverbrauch auf den Active-Directory Domänencontrollern und Zielsystemen. Alle Scans werden ausschließlich im read-only Modus ausgeführt, ohne in die Umgebung einzugreifen.

  In drei einfachen Schritten und ohne jeglichen Installationsbedarf wird das Unternehmensnetz auf privilegierte und gemeinsam genutzte Konten auf PCs und Servern gescannt.

- **Übersichtliche Darstellung** - Nach dem Scan Vorgang wird Anzahl und Compliance-Status privilegierter Konten in einer übersichtlichen Zusammenfassung präsentiert.

- **Detaillierte Berichterstattung und Kennzeichnung** - Ein ausführlicher Bericht mit Export- und Filteroptionen gibt eine verlässliche Antwort auf die Frage nach der Existenz und dem Status jedes einzelnen privilegierten Kontos innerhalb des Unternehmens. Der Bericht kennzeichnet Auditergebnisse wie zum Beispiel ungenügend verwaltete privilegierte Konten, um auf potentielle Risiken hinzuweisen.

DAS ERGEBNIS

Die Lösungen von Cyber-Ark für die Kontrolle privilegierter Benutzerkonten und Sessions bieten einen umfassenden Schutz dieser Konten und eine lückenlose Nachvollziehbarkeit aller administrativen Aktivitäten. Cyber-Ark DNA™ erkennt privilegierte Konten durch einen einfachen Scan, die Cyber-Ark Privileged Identity & Session Management Suite ermöglicht die automatische Verwaltung dieser Konten. Durch ein kontinuierliches Management aller privilegierten Benutzerkonten sorgt Cyber-Ark damit für Audit-Compliance sowie einen umfassenden Schutz gegen Cyberattacken.