netwrix

itsa

Durchgängiger Schutz der Identitäten, sichere Verwaltung privilegierter Benutzer

Dirk Schrader
VP Security Research,
Netwrix

Typischer Angriff

AD ausspähen, um Benutzer, Server und Computer aufzuspüren.

Credentials stehlen.

Bei Systemen als legitime Benutzer anmelden.

Die Berechtigungen nutzen, um Daten zu stehlen, Systeme zu sabotieren (o.ä.)....

Solide Kontrolle über hybride AD erhalten, indem Sie proaktiv Sicherheitslücken identifizieren und abmildern

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

Wer hat zu viele Berechtigungen?

Wer kann sie in wenigen Schritten erlangen?

Welche Objekte sind veraltet und können bereinigt werden?

Welche Konten haben schwache Passwörter?

Ihre Werkzeuge:

- Netwrix StealthAUDIT
- Netwrix Auditor

Das Ergebnis:

Verstehen Sie, was in Ihrem AD vorhanden ist, wie AD konfiguriert ist und wer Zugriff auf was hat.

Erkennen Sie Risiken wie schwache Passwörter, übermäßige Privilegien und unsichere DC-Konfigurationen.

Sie können sicher sein, dass Ihr Active Directory vor Sicherheitsvorfällen geschützt ist

IDENTIFY | **PROTECT** | DETECT | RESPOND | RECOVER

Wie lassen sich strenge Kennwortrichtlinien durchsetzen?

Wie verhindert man unzulässige AD- und GPO-Änderungen?

Wie minimiert man Sicherheitsrisiken im Zusammenhang mit privilegiertem Zugriff?

Ihre Werkzeuge:

- Netwrix StealthINTERCEPT
- Netwrix GroupID
- Netwrix Change Tracker
- Netwrix Privilege Secure

Das Ergebnis:

- Bereinigen Sie veraltete Konten und leere Gruppen.
- Erzwingen Sie sichere Passwörter.
- Beseitigen Sie ständige Privilegien.
- Härten Sie DC-Sicherheitskonfigurationen.
- Blockieren Sie riskantes Verhalten.

Sicher sein, dass Bedrohungen rechtzeitig erkannt werden und Angriffe unterbunden

IDENTIFY | PROTECT | **DETECT** | RESPOND | RECOVER

Gibt es bösartige Akteure, die sich unkontrolliert im Netzwerk bewegen?

Gibt es eine ungewöhnlich hohe Anzahl fehlgeschlagener Anmeldungen?

Ungeplante Änderungen an den DC-Konfigurationen?

Ihre Werkzeuge:

- Netwrix StealthDEFEND
- Netwrix Change Tracker

Das Ergebnis:

Erkennen Sie verdächtiges Verhalten und fortgeschrittene Bedrohungen in Echtzeit.

Reduzieren Sie die Auswirkungen von Active Directory-Sicherheitsvorfällen

IDENTIFY | PROTECT | DETECT | **RESPOND** | RECOVER

Wie lässt sich ein AD-Vorfall schneller eindämmen, als es menschlich möglich ist?

Wie hat sich ein Vorfall genau abgespielt?

Ihr Werkzeug:

Netwrix StealthDEFEND

Das Ergebnis:

- Schnelle Eindämmung von Bedrohungen durch automatische Reaktionen.
- Vereinfachen Sie die Untersuchung von Vorfällen und treffen Sie fundiertere Reaktionsentscheidungen.

Sicherstellung der Kontinuität durch schnelles Rollback und Wiederherstellung von Active Directory

IDENTIFY | PROTECT | DETECT | RESPOND | **RECOVER**

Wie kann man sich von unzulässigen AD-Änderungen ohne Ausfallzeiten erholen?

Wie kann man verhindern, dass sich ähnliche Vorfälle wiederholen?

Ihr Werkzeug:

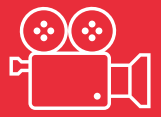
Netwrix Recovery for Active Directory

Das Ergebnis:

- Machen Sie unerwünschte AD-Änderungen rückgängig und stellen Sie ganze AD-Domänen wieder her.
- Nutzen Sie die gewonnenen Erkenntnisse, um zu verhindern, dass sich ähnliche Vorfälle wiederholen.

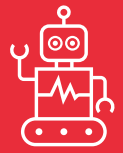
Was noch? Mehr am Stand 7A-320

Credential Management



Session Recording

Cloud Workloads



Application Management

Ecosystem Integrations

Access Certification

netwrix

Netwrix
Data Security Made Easy

Vielen Dank