Active Directory Exposure Assessment

In nur 30 Tagen:
Kontrolle und Sicherheit für Ihre Identitätsinformationen

Identifizieren Sie Active Directory-Schwachstellen in einem einzigen konsolidierten Angriffspfad, um Ihre Cyber-Resilienz zu erhöhen – und das in nur einem Monat

Das Active Directory ist ein beliebtes Ziel für Angreifer, die sich Zugriff mit Domain-Administrator-Berechtigungen verschaffen wollen. Ein Angreifer, der ein Active Directory kompromittiert hat, kann dies nutzen, um sich weitere Zugriffsprivilegien zu erteilen, bösartige Aktivitäten im Netzwerk zu verbergen, bösartigen Code auszuführen und sogar in die Cloud-Umgebung vorzudringen.

Unser Active Directory Exposure Assessment kombiniert die Attack Path Management Technologie des Marktführers XM Cyber mit dem Expertenwissen unserer IT-Sicherheits-Spezialisten, um Ihnen in kürzester Zeit die bestmöglichen Ergebnisse zu liefern.

Das Active Directory Exposure Assessment eignet sich besonders für Unternehmen, die:

- Active Directory-bezogene Angriffe in On-Premise- und Cloud-Umgebungen verhindern wollen
- ihre Sicherheitsreaktionen auf Änderungen im Active Directory verbessern wollen
- eine proaktive Active Directory-Risikoanalyse in Echtzeit durchführen möchten

Wie funktioniert das Actice Directory Exposure Assessment?

PLANUNG UND EINRICHTUNG

- Detaillierte Planung von Angriffsszenarien, abgestimmt auf Unternehmensziele
- Schnelle Bereitstellung der Attack Path Management SaaS-Plattform
- Integration bei den Cloud-Providern
- Verteilung der Sensoren

BEWERTUNG

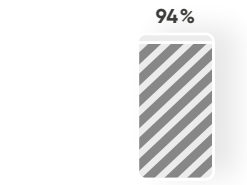
- Kontinuierliche Simulation von Angriffspfaden auf sensible Daten
- Aufdeckung aller versteckten Angriffspfade und hochriskanten Knotenpunkte

DOKUMENTATION

- Technischer Bericht und Management Summary
- Konkrete Anleitungen für echte umsetzbare Gegenmaßnahmen
- Priorisierung der Gegenmaßnahmen mit Fokus auf Kritikalität und Kosten

Swiss IT Security Group
www.sits-group.ch
CH: xmcyber@sits.ch
DE: sales@sits-d.de

JETZT ANFRAGEN UND INDIVIDUELL BERATEN LASSEN

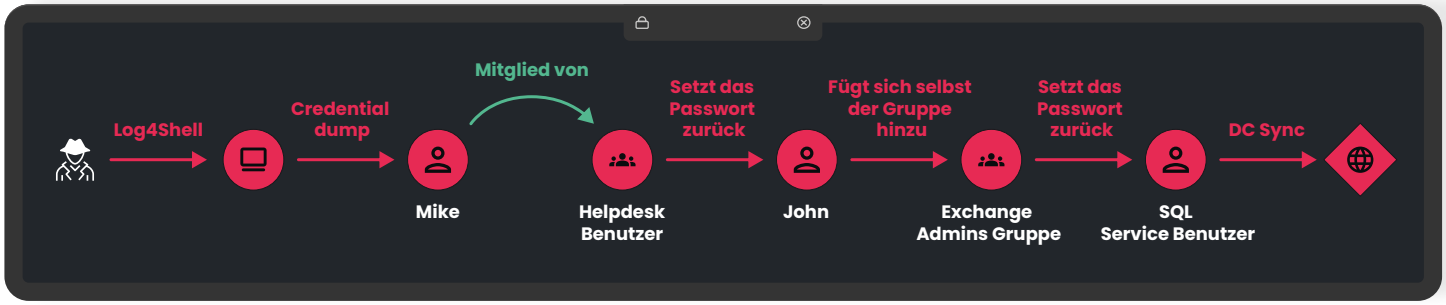


Von dem initialen Einfallstor aus können 94% aller kritischen Ressourcen in weniger als 4 Schritten erreicht werden.

In ihrem aktuellen Sicherheitsstatus können 75% der kritischen Ressourcen eines Unternehmens kompromittiert werden.

Sofort verwendbare Ergebnisse

1. Sehen Sie Ihr Netzwerk mit den Augen eines Hackers
2. Erfahren Sie, was Sie als erstes beheben müssen
3. Verstehen Sie Ihren aktuellen Sicherheitsstatus
4. Lassen Sie sich von Sicherheitsexperten bei der Analyse und der praktischen Umsetzung unterstützen



Finden Sie heraus, wie ein Angreifer eine Schwachstelle ausnutzt, um

- einen Active Directory Account zu hacken,
- anschließend trotz einer eigentlich sicheren Konfiguration seine Privilegien zu erweitern und damit
- die Unternehmensdomäne zu kompromittieren.

Warum Attack Path Management?

- **Kontinuierliche und sichere** Sicht auf die Risiken
- Präzise **Priorisierung** auf Basis des Risikos
- Wirtschaftlich sinnvolle **Maßnahmenplanung**
- Reduzierung der Angriffsfläche in **hybriden Cloud** Umgebungen
- **Sicherheits-Score** und Trendanalyse

Swiss IT Security Group
www.sits-group.ch
CH: xmcyber@sits.ch
DE: sales@sits-d.de

JETZT ANFRAGEN UND INDIVIDUELL BERATEN LASSEN

2023-08