Cloud Exposure Assessment

In nur 30 Tagen: Sicherheitsrisiken an Schnittstellen in Ihrer Hybrid-Umgebung eliminieren

Identifizieren Sie die Sicherheitslücken in Ihrer hybriden Cloud-Umgebung, die Angreifern Zugang zu Ihren kritischen Ressourcen ermöglichen und beheben Sie die wichtigsten davon – und das in nur einem Monat

Indem Unternehmen ihre IT auf hybriden Umgebungen aufbauen, entstehen ständig neue Sicherheitslücken. Cyber-Angreifer nutzen diesen Wandel, um in ein Unternehmen einzudringen, indem sie Fehlkonfigurationen, überprivilegierte Nutzerkonten, Schwachstellen und menschliche Fehler ausnutzen.

Unser Cloud 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 Cloud Exposure Assessment eignet sich besonders für Unternehmen, die:

- Schwachstellen identifizieren möchten, die sich aus Veränderungen in ihren AWS-, Azure- und GCP-Umgebungen ergeben
- den Umfang und die Kosten von Penetrationstests minimieren möchten
- die für die Minderung der größten Risiken erforderlichen Ressourcen reduzieren möchten

Wie funktioniert das Cloud 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

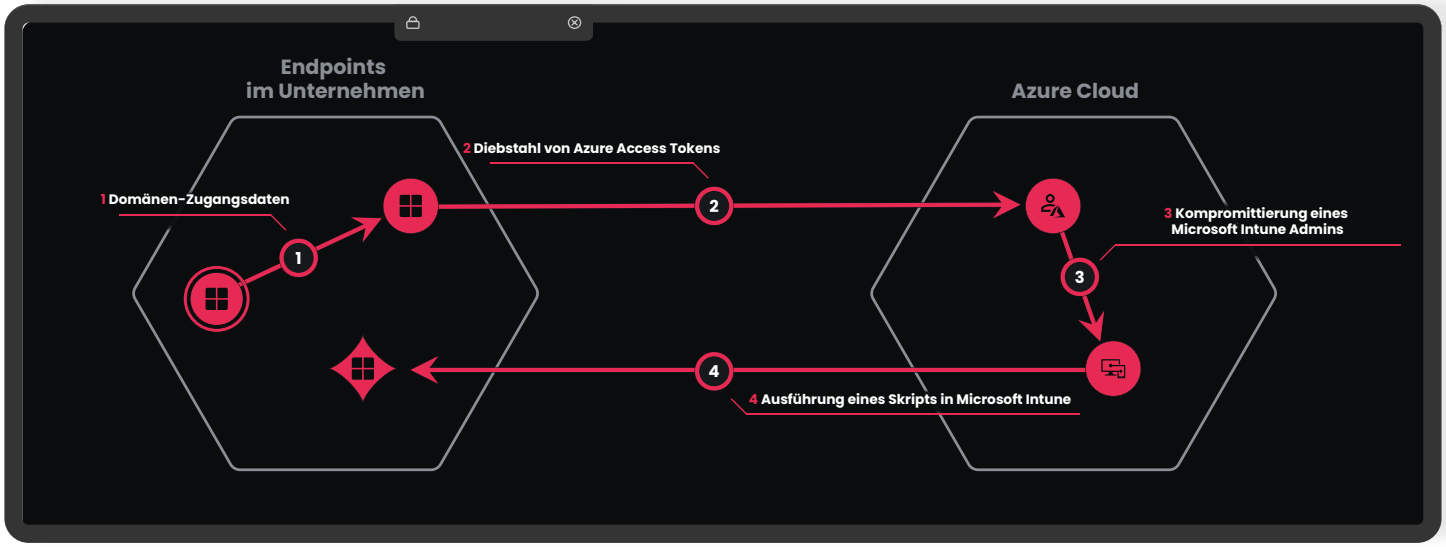
JETZT ANFRAGEN UND INDIVIDUELL BERATEN LASSEN

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 Angreifer von On-Premise zur Cloud und wieder zurück wechseln, um kritische Ressourcen 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