Ransomware Exposure Assessment

In nur 30 Tagen: Vom Ransomware-Ziel zur Festung!

Reduzieren Sie die möglichen Auswirkungen einer Ransomware Attacke auf ein Minimum – und das in nur einem Monat

Ransomware-Gruppen arbeiten mit Hochdruck daran, Ihre wichtigsten Daten auszuspionieren, um damit ihre Chancen auf eine satte Lösegeldzahlung zu erhöhen. Dabei kommen vermehrt Double Extortion Methoden zum Einsatz, bei denen sensible Daten vor der Verschlüsselung kopiert werden. Die Erpresser haben dann ein zusätzliches Druckmittel, indem sie mit der Veröffentlichung dieser Daten drohen. Auf ihrem Raubzug ins Innere Ihrer IT-Infrastruktur halten sich die Angreifer bedeckt und verbreiten sich im Netzwerk aufgrund von Fehlkonfigurationen, ungepatchten Schwachstellen und falsch verwalteten Anmeldeinformationen.

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

- schnell und unkompliziert herausfinden möchten, wo die Gefährdung durch Ransomware-Angriffe am größten ist
- mögliche Gegenmaßnahmen sinnvoll priorisieren möchten, um das Risiko von Ransomware-Angriffen sofort zu reduzieren
- die längerfristigen Schritte zur besseren Kontrolle der hybriden Angriffsfläche verstehen wollen
- das Unternehmensrisiko verstehen und aus der Sicht des Angreifers betrachten können wollen
- die Erfolgsaussichten von Ransomware- und anderen Angriffen verringern möchten

Wie funktioniert das Ransomware 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

94%

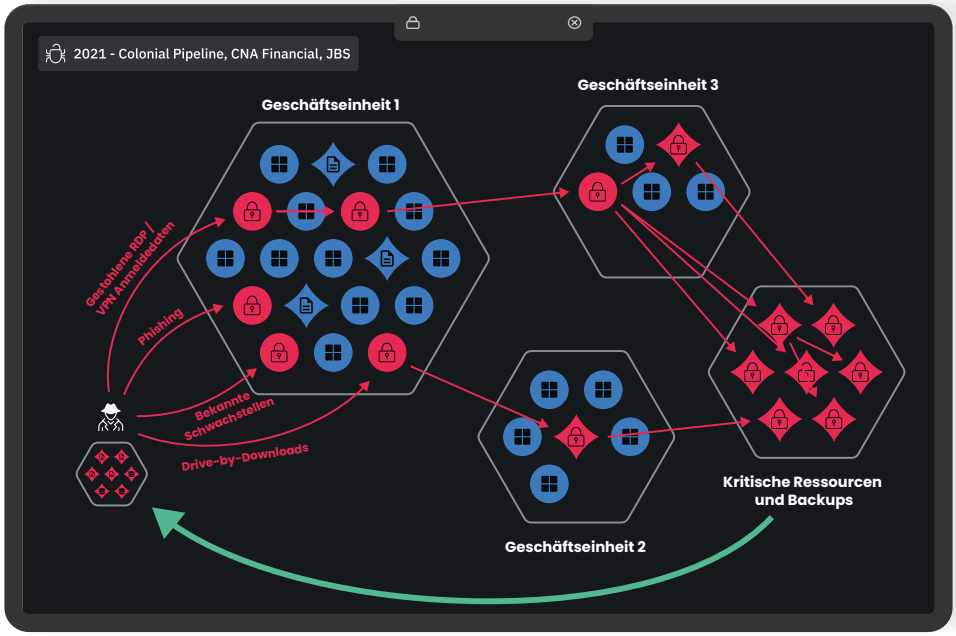
Von dem initialen Einfallstor aus können 94% aller kritischen Ressourcen in weniger als 4 Schritten erreicht werden.

75%

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



Die frühzeitige Übersicht über alle möglichen Ransomware Angriffswege und Cyber-Gefährdungen in Ihrem Netzwerk wird Ihnen helfen, Prioritäten zu setzen und sich mit Ihren Ressourcen auf die Behebung der Sicherheitsprobleme zu fokussieren, die die größten Auswirkungen auf den Erfolg oder Misserfolg eines Ransomware-Angriffs haben.

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