



Zscaler Risk360™: Bessere Geschäftsergebnisse bei weniger Sicherheitsrisiko

Quantifizieren, Visualisieren und Beheben von Risiken

⋯ Betriebswirtschaftliche Herausforderung

Sicherheitsbeauftragten fehlt bislang eine zuverlässige sowie nachprüfbare Methode, um Cybersicherheitsrisiken datengestützt zu quantifizieren, zu beheben und zu melden. Bisher gibt es keinen allgemeinen Standard für die Quantifizierung von Sicherheitsrisiken und ihre potenziellen finanziellen Auswirkungen. Konsistente Ansätze zur Erfassung und statistischen Normalisierung von Daten zur Erstellung umsetzbarer Risk Scores sucht man ebenfalls vergeblich im Dickicht der Drittanbieter-Tools zum Management von Schwachstellen, Sicherheitsrisiken und Angriffsflächen, CMDBs, GRC-Systemen und Sicherheitskontrollen. Die fehlende Möglichkeit, Cyberrisiken konsistent zu quantifizieren und zu bewältigen, verschlechtert die Fähigkeit der Organisationen, ihr Cyberrisiko langfristig zu reduzieren.

Lösung: Zscaler Risk360 zur leistungsstarken Quantifizierung und Bewältigung von Risiken

Zscaler Risk360 ist ein leistungsstarkes Framework zur Behebung von Cybersicherheitsrisiken durch zuverlässige Quantifizierung und Visualisierung. Das Risk360-Modell erstellt mit Echtzeitdaten aus externen Quellen und Ihrer Zscaler-Umgebung ein detailliertes Profil Ihres aktuellen Risikostatus.

Dabei werden über 100 datengestützte Faktoren aus allen vier Phasen eines Cyberangriffs berücksichtigt.

Wie funktioniert Risk360?

Risk360 berücksichtigt über 100 Einzelfaktoren innerhalb der Cybersicherheitsumgebung der betreffenden Organisation und liefert Schätzwerte zur Quantifizierung potenzieller finanzieller Verluste, Erkenntnisse zu den wichtigsten Risikofaktoren, Empfehlungen für Untersuchungsverfahren, Trend- und Branchenvergleiche sowie verwertbare Folien für Vorstandspräsentationen.

Das Modell erstellt Risikobewertungen zu allen vier Phasen eines Cyberangriffs — von der externen Angriffsfläche über die Kompromittierung des Netzwerks und lateralen Ausbreitung bis hin zur Datenexfiltration — sowie für alle Elemente Ihrer IT-Umgebung (Ressourcen, Anwendungen, interne und externe User).

Kernfunktionen von Risk360

Umfassender, standardisierter Risk Score zur Bewertung des unternehmensspezifischen Gesamtrisikos unter Berücksichtigung von Informationen aus Zscaler-Kontrollen und relevanten Drittanbieter-Tools

Schätzung des finanziellen Risikos durch Cyberangriffe mit Monte-Carlo-Ergebnisspannen.

Messung von Risikotrends im Zeitverlauf zur Bewertung Ihrer Maßnahmen zur Risikobewältigung sowie der Entwicklung Ihres Cyberrisikos im Vergleich zu Mitbewerbern

Ihr Risk Score wird in Bewertungen für die vier Einzelphasen eines Cyberangriffs aufgeschlüsselt:

- **Externe Angriffsfläche:** Bewertung und Darstellung der externen Angriffsfläche, aufgeschlüsselt nach ausnutzbaren Sicherheitsrisiken, Schweregraden sowie öffentlich sichtbaren Servern und Ressourcen
- **Risiko von Kompromittierungen:** Informationen zum Risiko von Kompromittierungen durch Angreifer über schädliche Dateien, Patient-Zero-Bedrohungen und infizierte User
- **Potenzielle laterale Ausbreitung:** Bewertung des Reifegrads der Segmentierungskontrolle für alle Unternehmensbereiche
- **Risiko von Datenverlusten:** Auskunft über das Risiko von Datenexfiltrationen für einzelne User, Geräte und Anwendungen

Detaillierte Visualisierung von Risiken für unterschiedliche Einflussfaktoren und Entitäten (interne und externe User, Anwendungen, Ressourcen)

Umsetzbare Empfehlungen mit detaillierten Workflows zur schnellen Behebung des Risikos von Angriffen/Kompromittierungen

Vorstandsberichte, Risikokartierung und hilfreiche Tipps mit einer speziellen Funktion für den Export von Vorstandsberichten und KI-gestützten Sicherheitsbeurteilungen unter Anwendung von Risiko-Frameworks wie MITRE Attack, NIST CSF und SEC-Vorgaben (SEC Regulation S-K Item 106).

Hauptvorteile

- ❖ **Leistungsstarke Risikoquantifizierung** zur Verfolgung von Cyber- und Finanzrisiken
- ❖ **Erkenntnisse zu den wichtigsten Risikofaktoren** sowie Optionen zur Aufschlüsselung der Einflussfaktoren
- ❖ **Automatisierter Prozess zur Messung des Cyberrisikos** als weitaus effizientere Alternative gegenüber einer manuellen Berechnung mithilfe von Spreadsheets und Drittanbieter-Tools
- ❖ **Verbesserter Sicherheitsstatus** durch proaktive Minderung von Risikofaktoren für alle Geräte, Systeme, Daten und User mit nur wenigen Klicks
- ❖ **Produktivere Risikokommunikation** mit der Führungsebene anhand einheitlicher Risikobewertungen unter Anwendung von Risiko-Frameworks und SEC-Vorgaben.

Weitere Informationen
zu Risk360 finden Sie auf
unserer [Webseite](#).