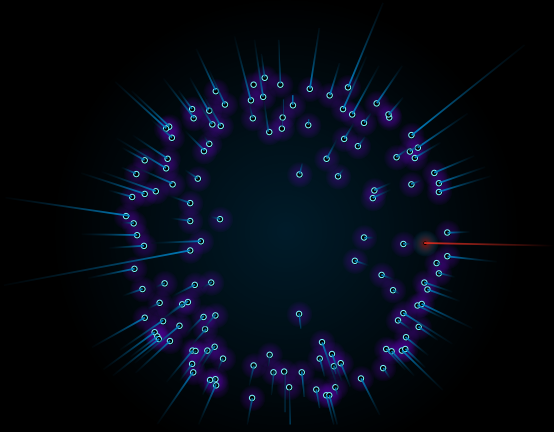
Verizon Risk Report

Messen Sie den ROI im Bereich Sicherheit durch praxistaugliche Daten, aus denen Risiken und Sicherheitslücken deutlich werden und die Ressourcen für Verbesserungen aufzeigen.

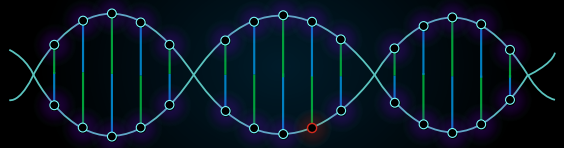


Phase eins: Den Wald vor lauter Bäumen sehen

Die Outsider-Perspektive

Mit dieser Methode wird Ihr Unternehmen aus Sicht eines Außenstehenden bewertet. Mit der Unterstützung von BitSight werden Daten von öffentlichen Quellen aus dem Internet gesammelt. Um eine Punktzahl für den Sicherheitsstatus zu ermitteln, werden externe Risikovektoren ausgewertet. Über das Unified Security Portal von Verizon wird täglich ein vollautomatisierter Bericht bereitgestellt.

- Basiert auf über 200 öffentlichen Datenquellen im Internet
- Automatisierter täglicher Bericht
- Zu den Datenquellen gehören BitSight, Recorded Future und der Verizon Data Breach Investigations Report (DBIR)

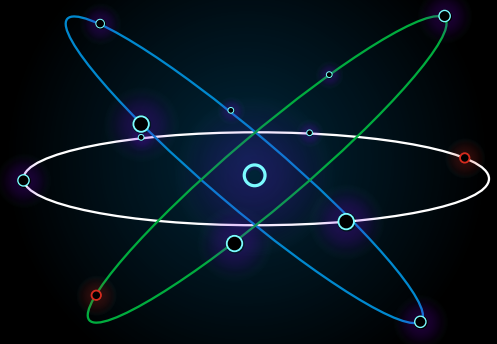


Phase zwei: Ein MRT für Ihr Unternehmen

Die Insider-Perspektive

In Phase zwei des Verizon-Risikoberichts wird die Punktzahl für Ihren Sicherheitsstatus durch eine interne Bewertung verfeinert. Dabei wird auf Ihren Endgeräten und in Ihrer Infrastruktur automatisch nach Malware, unerwünschten Programmen und Tools mit doppeltem Verwendungszweck gesucht.

- Baut auf der ersten Phase auf und berücksichtigt zusätzlich Daten, die im Unternehmen selbst gewonnen wurden
- Wertet Endgeräte und Infrastruktur aus, um den Sicherheitsstatus zu beurteilen und Risiken aufzudecken
- Zu den Datenquellen gehören neben allen Quellen der ersten Phase Tanium und Cylance



Phase drei: Sicherheitskultur und -prozesse

Die 360° Perspektive

Echte Transparenz erhält man, wenn externe und interne Risikobewertungen mit einer Tiefenanalyse der Sicherheitskultur und der sicherheitsrelevanten Prozesse des Unternehmens kombiniert werden. Auch die Beurteilung dieser Kultur und Prozesse stützt sich auf automatisierte Tools, die in Kombination mit menschlicher Intelligenz ein umfassendes Bild des Sicherheits- und Risikostatus vermitteln.

- Vervollständigt das in Phase eins und zwei erhaltene Bild unter Berücksichtigung von Sicherheitsverhalten, -kultur, -prozessen und -richtlinien
- Umfasst Professional Services von Verizon im Umfang von 100 Stunden zur Unterstützung der Verbesserungen des Sicherheitsstatus
- Ermöglicht eine ganzheitliche Beurteilung des Sicherheitsstatus

verizon

Weitere Informationen finden Sie unter **enterprise.verizon.com/de-de/products/**

Bedrohungsvektoren nach Phasen

Phase 1

Die Outsider-Perspektive

Schließt die Bewertung externer Risikovektoren durch BitSight ein. Diese Vektoren werden nach betroffenen Systemen, mangelnder Sorgfalt, Nutzerverhalten und öffentlichen Datendiebstählen unterteilt.

- Botnet-Infektionen
- Verbreitung von Spam
- Malware
- Unerwünschte Kommunikation
- Möglicherweise infiltrierte Systeme
- Offene Ports
- TLS/SSL-Zertifikate/Konfiguration
- Header von Webanwendungen
- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Patching-Frequenz
- Server-, Desktop- und Mobilgerätesoftware
- Unzureichend gesicherte Systeme
- DNSSEC-Datensätze
- Domain-Squatting
- Gemeinsame Nutzung von Daten
- Öffentlich preisgegebene Anmeldedaten
- Öffentliche Datendiebstähle

Phase 2

Die Insider-Perspektive

Enthält die externen Risikovektoren aus Phase eins, ergänzt durch die von Tanium und Cylance beigesteuerten Risikovektoren. Diese zusätzlichen Vektoren werden nach Schadsoftware, unerwünschten Programmen, Tools mit doppelter Verwendung und Infrastrukturproblemen unterteilt.

- Unerwartet ausgeführte Dienste
- Genutzte Software, deren Support ausgelaufen ist
- Anfällige Firmware-Versionen
- Schlecht gewartete Systeme
- WLAN-Netzwerke mit sichtbaren Endpunkten
- In zwei Netzwerkumgebungen eingebundene Geräte (Dual Homed)
- Ungewöhnliche Verbindungen
- Anomalien/falsch konfigurierte Kennwort- und Auditrichtlinien
- Fehlverhalten auf Seiten der Nutzer
- Probleme mit SSL-Zertifikaten
- Netzwerksegmentierung
- Nicht genehmigte, bestehende Verbindungen
- Anwendungsrisiken
- Anomalien, die auf Bedrohungen hinweisen könnten
- Endgeräte mit generischer Malware, Ransomware, Trojanern, falschen AV-Programmen, Hintertüren, Viren, Download-Trojanern, Rootkits, Infostealer-Viren, Reste von Viren, Würmern, Angriffsversuchen, Dropper-Software oder Bots
- Endgeräte mit generischen, vermutlich unerwünschten Programmen, Adware, Spielen, Keygens, Symbolleisten, Tools zur Skripterstellung, Tools für den Fernzugriff, beschädigte potenziell unerwünschte Programme (PUPs), Hacker-Tools oder portable Anwendungen
- Endgeräte mit Tools zur doppelten Verwendung, Tools für den Fernzugriff, Passwortknacker, Software zum Entfernen des Kopierschutzes (Cracking) oder Überwachungstools

Phase 3

Die 360° Perspektive

Enthält die externen Risikovektoren aus Phase eins, die internen Risikovektoren aus Phase zwei und wird ergänzt durch Sicherheitskultur- und prozessbezogene Risikovektoren, die aus einem auf den Kunden abgestimmten Audit von Verizon stammen. Zu diesen ergänzenden Bedrohungsvektoren gehören:

- Externe Schwachstellen
- IP-Reputation
- NetFlow
- Webanwendungen
- Interne Schwachstellen
- E-Mail-Filter
- Firewall
- Endpunktsysteme
- Phishing
- Hardwareprobleme
- Richtlinien, Prozesse und Verfahren
- WLAN

verizon

Weitere Informationen finden Sie unter **enterprise.verizon.com/de-de/products/**