Cyber Risk Monitoring*

Informationsblatt

Umfassende Transparenz, tägliche Updates und praxisbezogene Daten: So ermitteln Sie, welchen Risiken Ihr Unternehmen ausgesetzt ist, evaluieren Ihren Sicherheitsstatus und maximieren den ROI.

Die Outsider-Perspektive: Den Wald vor lauter Bäumen sehen

Hier bewerten Sie Ihr Unternehmen aus Sicht eines Außenstehenden. 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, und über das Unified Security Portal von Verizon wird täglich ein vollautomatisierter Bericht bereitgestellt.

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

Risikovektoren

Schließt die Bewertung externer Risikovektoren durch BitSight ein und wird ergänzt durch Daten von Recorded Future (RF) und aus dem Verizon Data Breach Investigations Report (DBIR). Diese Vektoren werden nach betroffenen Systemen, mangelnder Sorgfalt, Nutzerverhalten und an die Öffentlichkeit weitergegebenen Informationen unterteilt.

- Botnet-Infektionen
- Verbreitung von Spam
- Malware
- Unerwünschte Kommunikation
- Möglicherweise infiltrierte Systeme
- Offene Ports
- TLS/SSL-Zertifikate und Konfiguration
- Header von Webanwendungen
- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Patching-Frequenz
- Software für Server, Desktops und Mobilgeräte
- Unzureichend gesicherte Systeme
- DNSSEC-Datensätze
- Dateifreigabe
- Offengelegte Anmeldedaten von Benutzern
- Schlagzeilenträchtige Datendiebstähle
- Bedrohungsdaten aus dem Dark Web

* Cyber Risk Monitoring wurde bisher unter der Bezeichnung „Verizon Risk Report“ angeboten

Die Insider-Perspektive: Ein MRT für Ihr Unternehmen

In der zweiten Phase des „Cyber Risk Monitoring“ wird die Punktzahl für Ihren Sicherheitsstatus durch eine interne Bewertung verfeinert. Bei dieser wird auf Ihren Endgeräten und in Ihrer Infrastruktur 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 auch Tanium und Cylance.

Risikovektoren

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 doppeltem Verwendungszweck und Infrastrukturproblemen unterteilt.

- Unerwartet ausgeführte Dienste
- Genutzte Software, deren Support ausläuft
- Anfällige Firmware-Versionen
- Unzureichend 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, Backdoors, Viren, Download-Trojanern, Rootkits, Infostealer-Viren, Resten 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, beschädigten potenziell unerwünschten Programmen (PUPs), Hacker-Tools oder portablen Anwendungen
- Endgeräte mit Tools für den Fernzugriff, Tools mit doppeltem Verwendungszweck, Passwortknackern, Software zum Entfernen des Kopierschutzes (Cracking) oder Überwachungstools

verizon

Die 360° Perspektive: Sicherheitskultur und -prozesse

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

- Vervollständigt das in Phasen eins und zwei erhaltene Bild durch Berücksichtigung von Sicherheitsverhalten, -kultur, -prozessen und -richtlinien
- Umfasst eine professionelle Beratung durch Verizon im Umfang von 100 Stunden zur Unterstützung bei der Umsetzung von Verbesserungen des Sicherheitsstatus
- Ermöglicht eine ganzheitliche Beurteilung des Sicherheitsstatus

Risikovektoren

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 Risikovektoren gehören:

- Externe Schwachstellen
- IP-Reputation
- NetFlow
- Webanwendungen
- Interne Schwachstellen
- E-Mail-Filter
- Firewalls
- Endpunktsysteme
- Phishing
- Bei einer Untersuchung der Hardware ermittelte Probleme
- Richtlinien, Prozesse und Verfahren
- WLAN

Vendor Risk Dashboard

Die weitläufige Nutzung von Outsourcing- und cloudbasierten Technologien bedeutet, dass moderne digitale Unternehmen unweigerlich in Kontakt mit Lösungen von Drittanbietern kommen. Das birgt natürlich Sicherheitsrisiken, da ein System immer nur so gut geschützt ist wie das schwächste Glied in der Kette. Eine Sicherheitsverletzung bei einem Ihrer Anbieter kann dazu führen, dass vertrauliche Geschäfts- und Kundendaten offengelegt werden, was wiederum dem Ruf Ihres Unternehmens schadet.

Deshalb ermöglichen wir Ihnen mit unserem Vendor Risk Dashboard, den Sicherheitsstatus Ihrer Anbieter und Partner im Blick zu behalten. So erhalten Sie anhand von maßgeschneiderten, praxisbezogenen Bedrohungsdaten und Risikowerten für relevante Drittanbieter einen umfassenden Überblick über Ihr eigenes Sicherheitsniveau.

Sie werden umgehend über Auffälligkeiten benachrichtigt und können so potenziellen Problemen vorbeugen, Ressourcen sinnvoll zuweisen und zusammen mit Ihren Partnern in der Lieferkette gegen besonders gefährliche Bedrohungen vorgehen. Die im Rahmen des Cyber Risk Monitoring generierten Berichte helfen zudem, das mit Firmenzusammenschlüssen verbundene Risikopotenzial einzuschätzen und empfohlene Strategien zur Risikominimierung besser zu verstehen.

Im Dashboard kann ein Anwender den Bedrohungsgrad und die branchenspezifische Sicherheitseinstufung für einen ausgewählten Anbieter einsehen. Es ist auch möglich, Anbieter in Gruppen zusammenzufassen, Bedrohungsfaktoren nach Rangfolge zu sortieren und verschiedene Diagramme mit den zusammengefassten Punktzahlen für alle Anbieter und Anbietergruppen anzuzeigen.

Portfolio Management

Portfolio Management ist ein optionaler Service, der Ihnen zum Beispiel ermöglicht, alle mit Ihrem Unternehmen verbundenen juristischen Personen (z. B. Niederlassungen) wahlweise im Überblick oder im Detail zu sehen. Sie können ganz leicht zwischen verschiedenen Ansichten wechseln (ohne sich ab- und wieder anzumelden) und haben so Ihr gesamtes Portfolio stets im Blick. Im Portfolio-Dashboard stehen verschiedene Diagramme mit Angaben zum Sicherheitsniveau und Bewertungen des Bedrohungsgrads zur Auswahl, während die Administrationsansicht eine Liste aller Tochterunternehmen und Niederlassungen in einer hierarchischen Struktur enthält.

Weitere Informationen

Cyber Risk Monitoring unterstützt Sie dabei, Ihre Sicherheitsstrategie optimal zu planen und zu messen. Weitere Informationen erhalten Sie unter enterprise.verizon.com/de-de/products/security/cyber-risk-monitoring

verizon

© 2020 Verizon. Alle Rechte vorbehalten. Der Name Verizon und das Verizon-Logo sowie alle anderen Namen, Logos und Slogans, die sich auf die Produkte und Dienste von Verizon beziehen, sind Marken und Dienstleistungszeichen oder eingetragene Marken und Dienstleistungszeichen von Verizon Trademark Services LLC oder seinen angeschlossenen Unternehmen in den USA und/oder anderen Ländern. Alle anderen Marken und Dienstleistungszeichen sind Eigentum ihrer jeweiligen Inhaber.