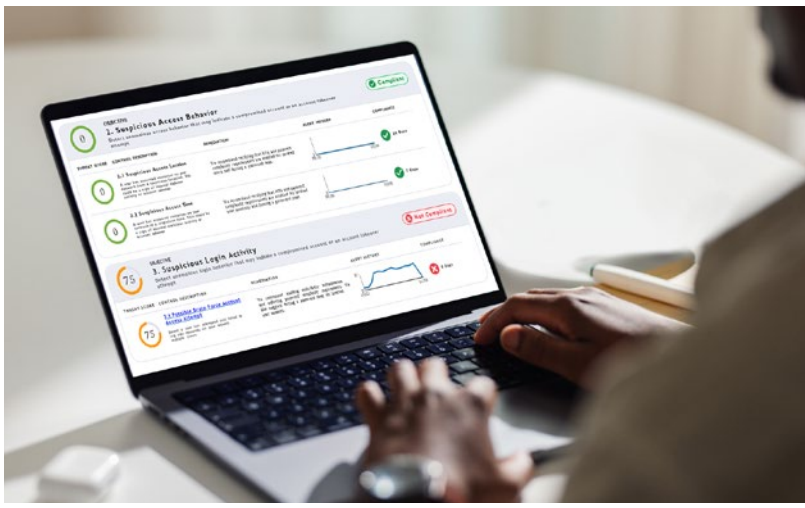
Erkennung von Risiken und Bedrohungen bei Microsoft 365



Einleitung

Es ist nicht leicht, den in der Microsoft 365 (M365) -Bereitstellung Ihres Unternehmens verborgenen Risiken und Bedrohungen auf den Grund zu gehen. M365 verfügt von Haus aus bereits über umfangreiche Sicherheitsfunktionen, die jedoch auch komplex und schwierig zu verwalten sind. Das Verständnis der Risiken und Bedrohungen in M365-Aktivitäten ist entscheidend für den Schutz Ihres gesamten Unternehmens und Ihrer Lieferanten, Partner und Kunden.

Durch die aktive Überwachung Ihrer M365-Bereitstellung mit automatisierten Risiko- und Bedrohungsberichten können Sie Schwachstellen oder Cyberangriffe identifizieren, die in der Komplexität von Microsoft Defender verloren gehen. Durch diesen proaktiven Ansatz können Cybersicherheitsexperten M365-Probleme beheben, bevor Schäden auftreten. Dadurch werden Integrität und Abwehr Ihrer Cybersecurity gestärkt.

Risiko- und Bedrohungsberichte für M365

ThreatSync+ SaaS beinhaltet Risiko- und Bedrohungsberichte für M365. Der Bericht bietet einen detaillierten Blick auf riskante und bedrohliche Aktivitäten sowie Verstöße gegen Richtlinienkontrollen bei M365-Anwendern. Am Anfang stehen Visualisierung und Zeitleiste aller M365-Bedrohungwerte und Trends auf der Grundlage von 15 Best-Practice-Kontrollrichtlinien. Der Bericht bietet einen detaillierten Blick auf jede der 15 Kontrollen, die vom System aktiv überwacht werden. Jeder Abschnitt der Kontrolleffektivität zeigt zu jeder überwachten Kontrolle den jeweiligen Bedrohungswert und die Trendlinie. Wenn Lücken oder Ausfälle festgestellt werden, wird eine Anleitung zur Behebung zur Verfügung gestellt.

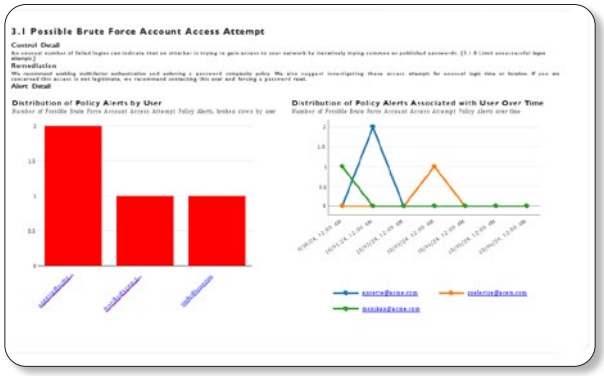
Der Bericht ist leicht konfigurierbar, um die spezifischen Anforderungen von Unternehmen oder Cyber-Abwehrprogrammen zu erfüllen. Neue Kontrollen können einfach in ThreatSync+ SaaS integriert und dem M365-Bericht hinzugefügt werden. Zweck ist es, M365-Probleme schnell und genau hervorzuheben, Managern eine Möglichkeit zum Festlegen von Sicherheitszielen für M365 zu geben und Fortschritte und Verbesserungen in Bezug auf diese zu verfolgen.

Der Bericht mit Risiken und Bedrohungen für Microsoft 365 ist eine umfassende Ressource, die detaillierte Einblicke in die Aktivitäten innerhalb Ihrer Microsoft 365-Bereitstellung bietet. Er bietet einen gründlichen Überblick über die Risiken und Bedrohungen im Zusammenhang mit allen 15 kritischen Kontrollen und Zielen und stellt sicher, dass Ihre Microsoft 365-Umgebung und -Anwender geschützt sind. Diese Erkenntnisse sind entscheidend für Ihr Cybersicherheitsprogramm, da sie die notwendigen Informationen liefern, um Ihr Sicherheitskonzept zu verstehen und Schritte zu dessen Verbesserung zu ermitteln. Die in dem Bericht enthaltenen konkreten Informationen können je nach den eingesetzten Kontrollen variieren, umfassen jedoch in der Regel:

- Eine priorisierte Ansicht der wichtigsten Bedrohungen für Ihre M365-Umgebung.
- Den Gefährdungsgrad eines jeden Risikos - in der Regel als kritisch, hoch oder mittel eingestuft.
- Eine Beschreibung jedes Risikos, einschließlich der Art, des Schweregrads und der potenziellen Auswirkungen.
- Empfehlungen zur Beseitigung der einzelnen Risiken, zum Beispiel das Installieren von Sicherheitsupdates, das Entfernen von Malware, das Isolieren von Geräten, das Ändern von Anmeldeinformationen oder das Konfigurieren von Sicherheitseinstellungen.

Beispiele für konkrete Sicherheitsrisiken, die bei der Bewertung ermittelt werden können:

- Externe Freigabe interner Dateien
- Verdächtige Dateiaktivität nach Rate
- Anonyme Dateiaktivität
- Öffentlich gemachte interne Dateien
- Brute-Force-Passwortangriff
- Verdächtige Admin-Änderungen, Rate
- Verdächtige Admin-Änderungen, Zeit
- Verdächtiger Zugriffspunkt
- Verdächtige Zugriffszeit
- Unmöglicher Weg/Zugang
- Verdächtige Zugriffsrate



Weitere Informationen über die Risiko- und Bedrohungsberichte für M365 von WatchGuard erhalten Sie bei Ihrem WatchGuard-Vertreter.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter watchguard.de.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 www.watchguard.de