Leitfaden für Abwehrspezialisten 2025

Schützen Sie sich jetzt und in Zukunft

Bleiben Sie den aufkommenden Angriffsvektoren immer einen Schritt voraus – und seien Sie bereit für neue Angriffstechniken auf alte Ziele. Beginnen Sie mit diesen Highlights aus unserer Reihe mit Leitfäden für Abwehrspezialisten.

Organisieren Sie Ihre Abwehr mit umfassenden Sicherheitsmaßnahmen

Diese drei Eckpfeiler müssen berücksichtigt werden:

Risikomanagement, bei dem Reaktionen basierend auf der Wahrscheinlichkeit einer bestimmten Bedrohung und dem Potenzial der Reaktion zum Schutz des Unternehmens ergriffen werden

Eine Netzwerkarchitektur, die mehrschichtige Sicherheit durch Firewalls, Segmentierung und Zugriffskontrollen implementiert, um Sicherheitsverletzungen abzuwehren und diese einzudämmen

Hostsicherheit, die einzelne Geräte durch Systemupdates, Antivirussoftware, Firewalls und Zugriffskontrollen vor Malware und unbefugtem Zugriff schützt

Wo könnte sich Malware verstecken?

Häufigste Protokolle bei Open-Port-Vorfällen im Jahr 2024

58,0 % Server Message Block (SMB)

14,5 % Remote Desktop Protocol (RDP)

12,9 % Secure Shell (SSH)

Was können Angreifer tun, sobald sie sich in einem VPN befinden?

- Remote-Authentifizierungsserver zur Authentifizierung von Nutzern verwenden
- Die legitime Authentifizierung missbrauchen
- Nicht autorisierte Authentifizierungsserver verwenden
- Konfigurationsdatei-Geheimnisse extrahieren und entschlüsseln

Verhindern Sie XSS-Schwachstellen

- Versehen Sie alle nutzergesteuerten Parameter mit Ausgabecodierung
- Schützen Sie sich mit Codeprüfung und Web Application Firewalls
- Stoppen Sie Taktiken von Bedrohungsakteuren wie Cookie-Diebstahl, Website-Defacement und Session Riding/Cross-Site Request Forgery

Warum zielen Angreifer auf Container ab?

Forscher von Akamai haben mehrere Schwachstellen und Taktiken in Kubernetes entdeckt, die bei Ausnutzung Folgendes ermöglichen:

- Datenextraktion
- Umgehung von Berechtigungen
- Remotecodeausführung

Kombinieren Sie proaktive Maßnahmen mit reaktiver Bereitschaft

Setzen Sie diese vier Grundprinzipien um:

- Implementieren Sie überall Cyberhygiene
- Implementieren Sie immer eine Sicherheitsplattform vor Ihrer Umgebung
- Konzentrieren Sie sich auf geschäftskritische Services
- Setzen Sie auf ein vertrauenswürdiges Team oder einen Partner

Laden Sie den Leitfaden für Abwehrspezialisten 2025 2025 herunter