Guida 2025 per gli addetti alla sicurezza

Rafforzate il futuro dei vostri sistemi di difesa

State al passo con i vettori di attacco emergenti e i nuovi metodi usati dai criminali per sfruttare vecchie vulnerabilità. Iniziate a leggere queste informazioni tratte dalla nostra guida per gli addetti alla sicurezza.

Organizzate i vostri sistemi di difesa con la sicurezza approfondita

Tre pilastri fondamentali da considerare

Gestione dei rischi, che assegna una priorità alle risposte in base alla probabilità che si verifichi una specifica minaccia e in base alla possibilità che la risposta riduca le vulnerabilità della vostra organizzazione

Architettura di rete, che implementa un sistema di sicurezza multilivello tramite i firewall, la segmentazione e i controlli degli accessi per difendervi dalle violazioni e per contenerle

Sicurezza degli host, che protegge i singoli dispositivi dai malware e dagli accessi non autorizzati tramite aggiornamenti di sistema, software antivirus, firewall e controlli degli accessi

Dove potrebbero nascondersi i malware?

I principali protocolli che hanno condotto a problemi legati alle porte nel 2024

58,0% SMB (Server Message Block)

14,5% RDP (Remote Desktop Protocol)

12,9% SSH (Secure SHell)

Cosa possono fare i criminali una volta all'interno di una VPN?

- Usare un server di autenticazione remoto per autenticare gli utenti
- Abusare di un'autenticazione legittima
- Usare server di autenticazione fittizi
- Estrarre e decrittografare i segreti dei file di configurazione

Come prevenire le vulnerabilità XSS

- Aggiungere la codifica dell'output a tutti i parametri controllati dall'utente
- Difendersi con la revisione del codice e le soluzioni WAF (Web Application Firewall)
- Bloccare le reali tattiche dei criminali come il furto di cookie, il defacement dei siti web e gli attacchi XSRF (Session Riding)/CSRF (Cross-Site Request Forgery)

Perché i criminali prendono di mira i container?

I ricercatori di Akamai hanno scoperto varie vulnerabilità e tattiche presenti in Kubernetes, che, se sfruttate, possono condurre a:

- Esfiltrazione dei dati
- Escalation dei privilegi
- Esecuzione di codice remoto

Come combinare misure proattive con azioni tempestive

Adottare queste quattro misure fondamentali:

- Implementare le pratiche di igiene informatica ovunque
- Suddividere l'ambiente in modo coerente con varie piattaforme di sicurezza
- Focalizzarsi attentamente sui servizi business-critical
- Disporre di un partner o un team di risposta agli incidenti affidabile e disponibile su richiesta

Scaricate la guida 2025 per gli addetti alla sicurezza