Guide 2025 à l'usage des gardiens de la sécurité internet

Fortifiez votre défense pour l'avenir

Restez à l'affût des nouveaux vecteurs d'attaque et des façons dont les anciennes cibles peuvent être exploitées. Commencez par ces points forts de notre anthologie du Guide à l'usage des gardiens de la sécurité internet.

Organisez vos efforts de défense avec la sécurité en profondeur

Trois pierres angulaires à prendre en compte

La gestion des risques qui hiérarchise les réponses en fonction de la probabilité d'une menace particulière et de la capacité de cette réponse à réduire la vulnérabilité de votre organisation

L'architecture réseau qui met en œuvre une sécurité à plusieurs niveaux au moyen de pare-feux, d'une segmentation et de contrôles d'accès afin de se défendre contre les violations et de les contenir

La sécurité de l'hôte qui protège les terminaux individuels contre les logiciels malveillants et les accès non autorisés grâce à des mises à jour du système, des logiciels antivirus, des pare-feux et des contrôles d'accès

Où les logiciels malveillants peuvent-ils se cacher ?

Principaux protocoles pour les incidents de ports ouverts en 2024

58,0 %
Server message block (SMB)

14,5 %
Remote Desktop Protocol (RDP)

12,9 %
Secure shell (SSH)

Que peuvent faire les pirates une fois à l'intérieur d'un VPN ?

- Utiliser un serveur d'authentification distant pour authentifier les utilisateurs
- Abuser de l'authentification légitime
- Utiliser des serveurs d'authentification indésirables
- Extraire et décrypter les secrets des fichiers de configuration

Prévenir les vulnérabilités XSS

- Ajouter l'encodage de sortie sur tous les paramètres contrôlés par l'utilisateur
- Se défendre avec une révision du code et des pare-feux d'applications Web
- Arrêter les tactiques réelles des acteurs malveillants telles que le vol de cookies, le détournement de sites Web et la falsification de session/de requête intersite.

Pourquoi les pirates ciblent-ils les conteneurs ?

Les chercheurs Akamai ont découvert de multiples vulnérabilités et tactiques dans Kubernetes qui, lorsqu'elles sont exploitées, peuvent entraîner :

- Exfiltration de données
- Élévation des privilèges
- Exécution de code à distance

Combiner des mesures proactives avec une préparation réactive

Appliquer ces quatre principes fondamentaux :

- Mettre en œuvre la cyberhygiène partout
- Placer systématiquement votre environnement derrière des plateformes de sécurité
- Se concentrer sur les services critiques de l'entreprise
- Disposer d'une équipe d'intervention en cas d'incident ou d'un partenaire de confiance

Télécharger le guide 2025 à l'usage des gardiens de la sécurité internet