Guia dos guardiões da cibersegurança de 2025

Fortifique o futuro da sua defesa

Fique à frente de vetores de ataque emergentes — e das novas maneiras pelas quais os invasores estão explorando alvos antigos. Comece por estes destaques da nossa antologia: o Guia dos guardiões da cibersegurança.

Organize sua defesa com a segurança em profundidade

Três pilares a serem considerados

Gerenciamento de riscos que priorize as respostas com base na probabilidade de uma determinada ameaça e no potencial dessas respostas de reduzir o grau de vulnerabilidade da sua organização

Arquitetura de rede que implemente segurança em camadas por meio de firewalls, segmentação e controles de acesso para evitar e conter violações

Segurança de host que proteja dispositivos distintos contra malware e acesso não autorizado por meio de atualizações do sistema, software antivírus, firewalls e controles de acesso

Onde o malware pode estar se escondendo?

Principais protocolos de incidentes de porta aberta em 2024

58%
Protocolo SMB (Server Message Block)

14,5%
Protocolo RDP (Remote Desktop Protocol)

12,9%
Protocolo SSH (Secure Shell)

O que os invasores podem fazer depois de acessar uma VPN?

- Usar um servidor de autenticação remota para autenticar usuários
- Explorar autenticações legítimas
- Usar servidores de autenticação não autorizados
- Extrair e descriptografar segredos de arquivos de configuração

Evite vulnerabilidades de XSS

- Adicione codificação de saída a todos os parâmetros controlados pelo usuário
- Defenda-se com análise de código e firewalls de aplicativos da Web
- Detenha as táticas reais dos invasores, como roubo de cookies, desfiguração de websites e falsificação de solicitações entre websites/ montagem de sessão

Por que os invasores estão atacando contêineres?

Os pesquisadores da Akamai descobriram várias vulnerabilidades e táticas no Kubernetes que, quando exploradas, podem levar a estes casos:

- Exfiltração de dados
- Escalação de privilégios
- Execução remota de código

Combine medidas proativas com prontidão reativa

Coloque em prática estes quatro princípios fundamentais:

- Implemente a higiene cibernética em todos os ambientes
- Distribua seu ambiente consistentemente em níveis diferentes atrás de plataformas de segurança
- Mantenha grande foco em serviços críticos para os negócios
- Tenha à disposição uma equipe ou um parceiro confiável de resposta a incidentes

Baixe o Guia dos guardiões da cibersegurança de 2025