CROWDSTRIKE

Interrompendo ataques à nuvem

6 FUNDAMENTOS PARA PROTEGER APLICAÇÕES NATIVAS DA NUVEM

Com a probabilidade de a adoção da nuvem continuar acelerando, a proteção dos ativos em nuvem será um aspecto crítico do suporte à transformação digital em organizações de qualquer tamanho, qualquer setor, em qualquer lugar do mundo. Mas abraçar a nuvem amplia a superfície de ataque e abre a porta para os adversários tirarem vantagem. O que você precisa saber para proteger seu negócio?

Quais são as consequências?
“Saída de dados, entrada de malware”

$4.24M é o custo médio de uma violação de dados em 2021: o maior aumento de custo de 1 ano em 7 anos[3]

40% das empresas relataram acesso não autorizado a aplicações e dados devido a configurações incorretas na nuvem[2]

38% das empresas relataram a introdução de malware devido a configurações incorretas na nuvem[2]

30% das empresas relataram a introdução de ransomware devido a configurações incorretas na nuvem[2]

Por que isso está acontecendo?

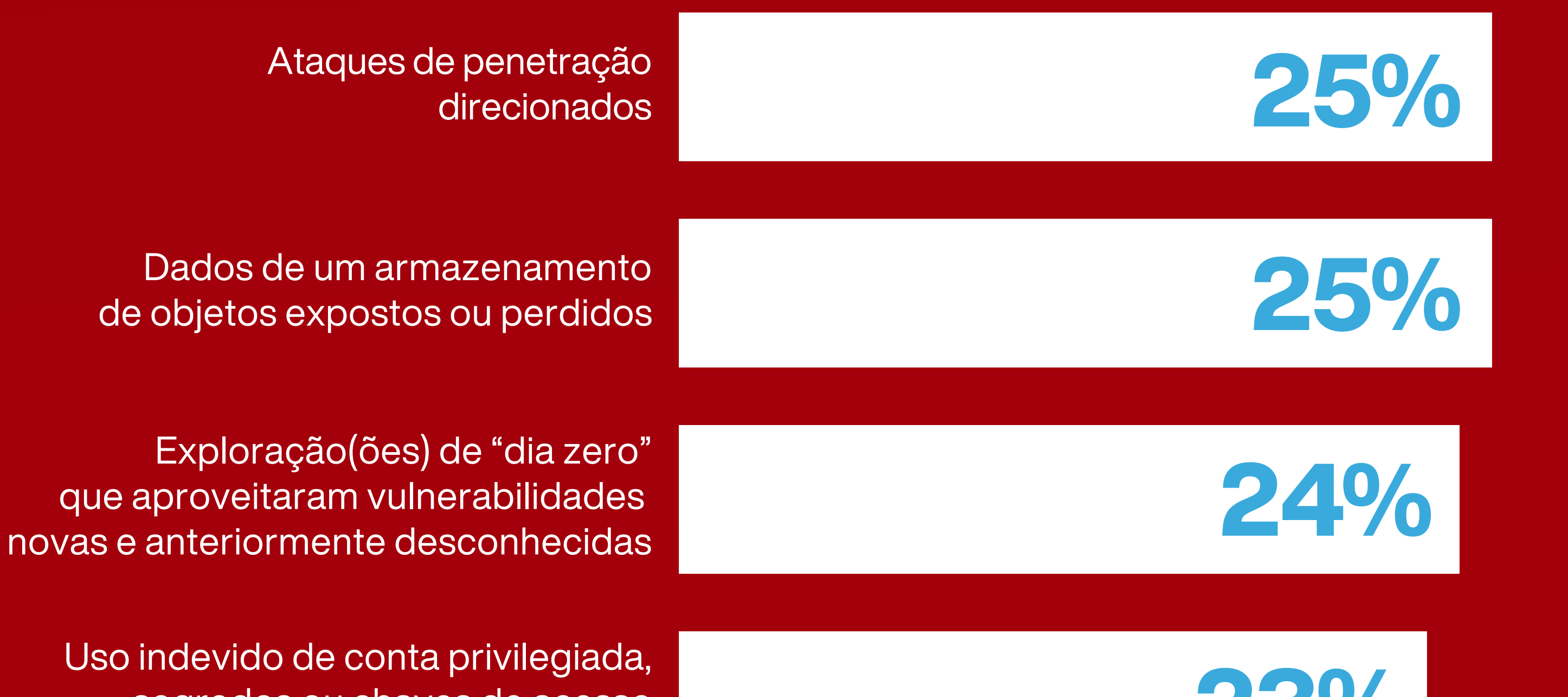
Shadow IT
- Falta de visibilidade
- Uso não autorizado
- Ativos não protegidos

Complexidade da nuvem
- Configurações incorretas
- Consistência de segurança
- Uso de APIs inseguras

Ameaças de Tempo de Execução
- Adversários
- APTs/exploits de dia zero
- Vulnerabilidades

Escassez de Habilidades
- IAM, gerenciamento de chaves
- Nuvem/segurança
- Responsabilidade compartilhada

A realidade de hoje:
Uma gama diversificada de ciberataques



Malware se deslocando lateralmente para workloads em nuvem	27%
Ataques de penetração direcionados	25%
Dados de um armazenamento de objetos expostos ou perdidos	25%
Exploração(ões) de “dia zero” que aproveitaram vulnerabilidades novas e anteriormente desconhecidas	24%
Uso indevido de conta privilegiada, segredos ou chaves de acesso através de credenciais roubadas	23%

Apesar de tudo isso, apenas **1 em cada 5 organizações** avalia regularmente sua postura geral de segurança na nuvem[4]

4 Principais prioridades para DevSecOps

#1 Criar consistência de segurança pelo data center e nos ambientes de nuvem pública e privada

#2 Automatizar a introdução de controles e processos através da integração com o ciclo de vida de desenvolvimento de software e ferramentas de CI/CD

#3 Aprimorar o conhecimento e a compreensão do modelo de ameaças e dos adversários para aplicações e infraestrutura nativas em nuvem

#4 Consolidar em uma plataforma para proteção de workloads em nuvem integrada, nativa da nuvem

6 Fundamentos para proteger aplicações nativas da nuvem

1 **Faça de erradicar vulnerabilidades a sua missão**
Conheça suas imagens. Entenda como são criadas e qual código é usado, incluindo software e configuração.

2 **Imponha imutabilidade para containers**
Fortaleça suas imagens, containers e hosts. Adote a automação para executar varredura contínua e implementar verificações à medida que você gerencia e se alinha com os regulamentos.

3 **Reduza a superfície de ataque antes do tempo de execução**
Adote uma abordagem “shift left” para a segurança para identificar e corrigir vulnerabilidades mais cedo. Integre com suas ferramentas de CI/CD como Jenkins ou Azure DevOps.

4 **Imponha o controle de acesso**
Garanta a segregação de funções do seu ambiente de container e integre ferramentas de controle de acesso com diretórios corporativos para obter gerenciamento de acesso detalhado e melhor visibilidade.

5 **Automatize a proteção do tempo de execução**
A imutabilidade dos containers permite uma identificação de ameaças mais rápida e precisa. Dimensione a proteção em tempo de execução por meio da automação da defesa contra ameaças e detecção de anomalias, com um baseline para comportamento de container.

6 **Audite, audite e audite de novo**
Tome medidas para minimizar a dispersão de containers e eliminar imagens e containers arriscados.

Fontes:
1. O estado da segurança em nuvem 2021 (Ermetic/IDC)
2. A maturação da segurança nativa em nuvem: Protegendo aplicações e infraestrutura modernas (ESG, março de 2021)
3. https://www.foley.com/en/insights/publications/2021/07/4-24m-now-the-average-cost-per-data-breach
4. Implementando melhores práticas da segurança em nuvem — agosto de 2020 (Tripwire)

Sobre a CrowdStrike

A CrowdStrike, líder global em cibersegurança, está redefinindo a segurança para a era da nuvem com uma plataforma de proteção de endpoint e workload criada do zero para impedir ataques. A arquitetura de um único agente leve da plataforma CrowdStrike Falcon® utiliza inteligência artificial (IA) em escala de nuvem, e oferece visibilidade e proteção em tempo real para toda a empresa, evitando ataques a endpoints e workloads dentro ou fora da rede. Alimentada pelo patenteado CrowdStrike Threat Graph™, a plataforma CrowdStrike Falcon correlaciona em tempo real mais de 1 trilhão de eventos mundiais relacionados a endpoints por dia, abastecendo uma das plataformas de dados para segurança mais avançadas do mundo.

CrowdStrike **Nós Interrompemos Ataques**