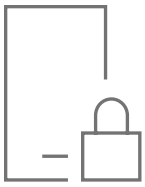
Microsoft Security

# Acompanhe um cenário de segurança cibernética que está mudando

# Sumário

# Introdução

**Acima de tudo, os CISOs devem lidar com um cenário de segurança cibernética de crescente complexidade.**



O papel de um CISO nunca foi fácil, mas parece estar ficando cada vez mais desafiador a cada dia. A descrição do trabalho é bastante completa:

- ✓ proteger os ativos digitais da organização
- ✓ promover boas práticas de segurança em toda a empresa
- ✓ compreender as necessidades e os riscos de unidades de negócios individuais
- ✓ envolver-se regularmente com os colegas da diretoria e o conselho de administração para ajudá-los a gerenciar estrategicamente o risco

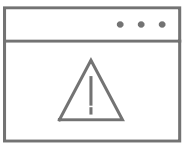
Acima de tudo, os CISOs devem lidar com um cenário de segurança cibernética de crescente complexidade. Os dias de proteção de ativos por trás de um perímetro fortificado já passaram há muito tempo. Os dados residem na nuvem, em pontos de extremidade e em toda a cadeia de suprimento, expandindo significativamente a superfície de ataque.

E agora, os CISOs devem lidar com as novas realidades de trabalho criadas por uma pandemia global. Um mundo no qual as equipes de trabalho inteiras eram subitamente obrigadas a trabalhar em casa aumenta significativamente as apostas para proteger dispositivos de ponto de extremidade, dados e infraestrutura de rede.

Portanto, é fundamental para os CISOs manterem-se atualizados sobre as ameaças que estão surgindo e, o mais importante, como a proteção contra ameaças está evoluindo para ajudar a manter as organizações seguras.

# Ameaças que estão surgindo

**Muitos criminosos online são atraídos por uma nova geração de técnicas de ataque "livres de malware".**



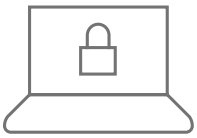
Assim como a distância mais curta entre dois pontos é uma linha reta, os criminosos cibernéticos terão cada vez menos trabalho para comprometer os sistemas e exfiltrar dados. Portanto, não deve surpreender ninguém que muitos criminosos online sejam atraídos por uma nova geração de técnicas de ataque "livres de malware". Por que escrever malware quando você pode penetrar em um sistema com código executado de credenciais gravadas em memória ou comprometidas?

"Tomei conhecimento de mais de uma violação em que o invasor usou abordagens livres de malware como adivinhação de senha em uma área de trabalho remota para obter primeiro acesso ao ambiente", disse Chris Clements, vice-presidente de arquitetura de soluções do Cerberus Sentinel, uma consultoria de segurança cibernética. "Os invasores então usaram funções internas do sistema para escalar seus privilégios e dar-lhes controle completo sobre todos os sistemas e dados na rede."

**Esses ataques podem ser devastadores,"** Clements acrescentou, **"pois os invasores estão imitando as mesmas atividades dos administradores de TI legítimos que o antivírus não foi projetado para parar."**

# Técnicas avançadas de phishing

**O phishing continua sendo uma ameaça popular, com os atores de ameaças adotando táticas avançadas para evitar as defesas tradicionais de rede.**



O phishing continua sendo uma ameaça popular, com os atores de ameaças adotando táticas avançadas para evitar as defesas tradicionais de rede. Eles estão se escondendo atrás de ofuscação de pacotes, criptografia, cargas de várias fases e DNS de fluxo rápido, onde botnets escondem sites de entrega de phishing por trás de uma rede de hosts comprometidos atuando como proxies.

Os ataques de ransomware também estão evoluindo. Os operadores mais sofisticados penetrarão um alvo e, em seguida, procurarão um parceiro que possa implantar seu ransomware no destino de forma personalizada. Por exemplo, os desenvolvedores do ransomware LockerGoga, que precisa de direitos administrativos para ser executado, têm sido conhecidos para analisar minuciosamente as defesas de um alvo que nem sequer se preocupam em ocultar seu aplicativo ruim porque sabem que essas defesas não detectarão isso.

Os invasores também estão usando ferramentas já instaladas em um sistema, como o PowerShell, para se espalhar em uma rede e ampliar a infestação. Esses intrusos “sobrevivem” quando penetram em um sistema, usando ferramentas e utilitários disponíveis publicamente para realizar suas finalidades. Esses ataques são difíceis de detectar porque, para os defensores, eles parecem ser uma atividade de rede normal.

# Explorações remotas crescentes

**De acordo com a KnowBe4, um provedor de conscientização de segurança, os ataques de email relacionados ao coronavírus cresceram 600% durante o trimestre que terminou em 30 de março de 2020.**

À medida que mais funcionários são forçados a trabalhar em casa devido à epidemia COVID-19, os trabalhadores remotos adicionam outra vulnerabilidade acentuada para as organizações. A rapidez da mudança para o trabalho remoto para muitas organizações deixou muitas equipes de segurança tentando acompanhar o passo para garantir que as políticas e proteções apropriadas estivessem em vigor. Não surpreendentemente, os atores maus também estão explorando a pandemia por meio da engenharia social. De acordo com a KnowBe4, um provedor de conscientização de segurança, os ataques de email relacionados ao coronavírus cresceram 600% durante o trimestre que terminou em 30 de março de 2020.

"Os vilões são oportunistas e usarão todas as chances de aproveitar as emoções aumentadas das pessoas em situações de crise, como esta, tentando atraí-los para clicar em um link malicioso ou fazer o download de um anexo atado com malware", disse o CEO da KnowBe4, Stu Sjouwerman.

# Defensores sitiados

**O cenário de ameaças em expansão coloca mais pressão nos CISOs para modernizar as operações de segurança para reduzir as ineficiências.**

O cenário de ameaças em expansão coloca mais pressão sobre os CISOs para modernizar as operações de segurança para reduzir as ineficiências, aumentar a visibilidade em toda a organização e tornar-se mais proativa na identificação e proteção contra ameaças.

Tradicionalmente, as equipes de segurança têm sido incumbidas de monitorar domínios específicos, sem interação ou integração. Esses silos podem impedir que os defensores vejam o contexto completo de um ataque até que seja tarde demais. Os invasores de hoje se movem tão rapidamente que, quando as equipes de SecOps reconhecem toda a extensão de um problema, seus sistemas podem já terem sido comprometidos.

Esse desafio é exacerbado por uma mistura cada vez maior de produtos e serviços de segurança. Normalmente, esses produtos usam portais, esquema de dados e metodologias diferentes. Monitorar dados em todos esses produtos manualmente pode atrasar os tempos de resposta e até mesmo perder elementos de um ataque em si.

**Um aumento nos produtos de segurança e nos dados coletados e analisados geralmente cria fadiga de alertas. Os analistas de segurança não podem possivelmente priorizar o volume de alertas que recebem para enfrentar as maiores ameaças. Nenhuma inteligência que estão coletando é acionável. Sem as ferramentas certas para ajudá-los a responder proativamente, antes ou como uma violação está ocorrendo e para bloquear ameaças persistentes, os defensores estão em clara desvantagem ao enfrentar adversários.**

# Uma nova era de proteção contra ameaças

**A segurança baseada em identidade é um componente fundamental de uma estrutura de segurança emergente conhecida como confiança zero.**

A proteção contra ameaças está evoluindo para enfrentar esses desafios, com métodos e tecnologias emergentes projetados para fortalecer as defesas tradicionais.

Por exemplo, os controles de rede começaram a ficar em segundo plano em relação à identidade como um meio para proteger os sistemas e os dados. Quando o paradigma de defesa centrado no perímetro e na arquitetura de TI compartilhava um intervalo comum de endereços IP, os controles de segurança eram orientados pela rede. À medida que a nuvem e as plataformas móveis tomaram dados fora do perímetro, as proteções de segurança também deviam se estender para fora da rede. Como resultado, as organizações estão explorando maneiras de reformular suas defesas em torno do contexto e da identidade.

Com o paradigma de perímetro, depois de conectado a um sistema, você foi considerado 100% confiável. Com o paradigma de identidade, o acesso a um sistema é limitado ao que o usuário precisa para fazer seu trabalho, e qualquer comportamento anômalo provocará alertas. A segurança baseada em identidade é um componente fundamental de uma estrutura de segurança emergente conhecida como confiança zero. Esse modelo é baseado na premissa de que a confiança não deve ser dada a nada dentro ou fora da organização. Tudo precisa ser verificado antes de acessar qualquer coisa.

# Mais ferramentas para defesa detalhada

**As equipes de segurança agora têm a capacidade de implantar recursos avançados de "caça" para erradicar violações sofisticadas.**

A proteção contra ameaças moderna requer controles de segurança que continuamente correlacionam e analisam variáveis relevantes quase em tempo real e decidem se uma identidade deve ser concedida ou negada o acesso. Essa necessidade está aumentando a urgência das organizações adotarem automação, inteligência artificial (IA) e machine learning (ML) em suas pilhas de segurança.

A IA e o ML desempenham funções críticas em operações de segurança cibernética porque possibilitam a análise de grandes quantidades de dados para padrões de atividade suspeitos e sinais de ameaça que os analistas humanos não podem ver até que seja tarde demais. Os algoritmos de ML podem transformar dados brutos de várias fontes em incidentes que dão aos defensores o tipo de visibilidade de que precisam para entender todo o contexto de um ataque e criar uma resposta direcionada.

IA, ML e automação também ajudam as organizações a se tornarem menos reativas e mais proativas na identificação e resposta à ameaças. As equipes de segurança agora têm a capacidade de implantar recursos avançados de "caça" para erradicar violações sofisticadas ou entender melhor como os ativos de sua organização se comportam. Essa abordagem aumenta a capacidade de uma organização se defender contra ataques persistentes e impedir que invasores obtenham um ponto de apoio para explorar dados e sistemas.

**O trabalho do CISO não está ficando mais fácil. Mas, com uma visão clara do cenário de cibersegurança em mudança e acesso a métodos de defesa em evolução, suas noites podem ser um pouco mais tranquilas.**

Saiba mais sobre como a IA, a automação e a integração ajudam a manter usuários, pontos de extremidade, aplicativos de nuvem e dados seguros.

Microsoft