SOPHOS
Cybersecurity delivered.

Práticas recomendadas para proteger sua rede contra ransomware

Aumente sua proteção contra ransomware e outros ataques à rede

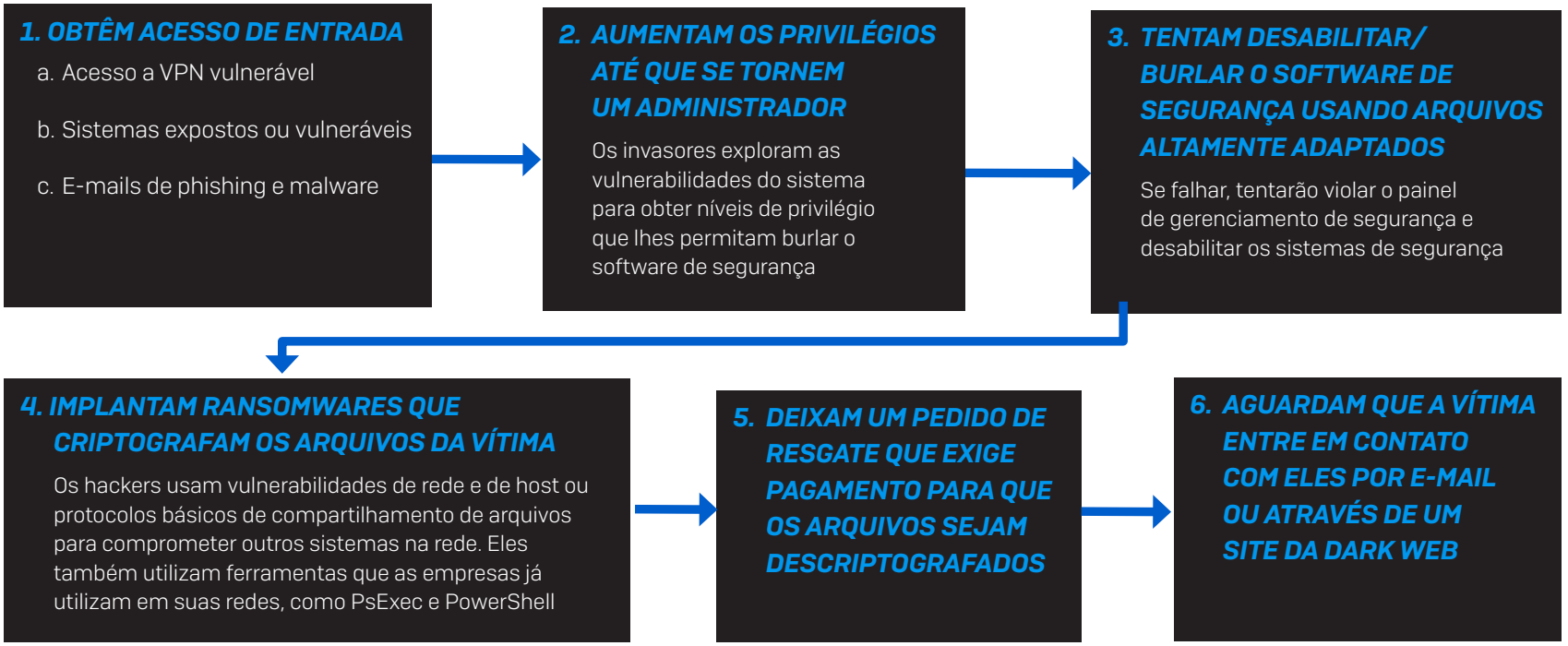
Documento técnico Sophos. Setembro, 2022

Os ataques de ransomware estão aumentando em volume e gravidade

66% das organizações foram atingidas por ransomware no ano passado, contra 37% em 2020.[1] Esse é um aumento de 78% em relação ao ano anterior, demonstrando que os adversários se tornaram consideravelmente mais capazes de executar ataques em escala do que nunca. A escalada do ransomware provavelmente também reflete o crescente sucesso do modelo de ransomware como serviço, ao reduzir o nível de habilidade necessário para implantar um ataque, amplia o alcance do ransomware.

Como funcionam os ataques de ransomware

Para saber como se proteger contra ataques de ransomware, primeiro precisamos examinar como eles funcionam. Um típico ataque direcionado de ransomware tem a seguinte estrutura:



Os ataques modernos de ransomware costumam usar ferramentas legítimas de TI e do usuário final, como VPN ou protocolo RDP (Remote Desktop Protocol) para obter acesso. Essas ferramentas são usadas por funcionários autorizados como parte de seu trabalho, dificultando a detecção inicial de ataques modernos de ransomware. A raiz do problema está no excesso de confiança implícita no uso dessas ferramentas — supõe-se que qualquer pessoa capaz de acessar uma VPN ou RDP seja confiável, uma prática que tem se mostrado imprudente.

1 O Estado do Ransomware 2022, Sophos - Pesquisa independente com 5.600 profissionais de TI em 31 países.

Como prevenir ataques de ransomware

Existem três medidas de segurança de rede que podem ajudar a mitigar o risco de um ataque de ransomware.

1. Eliminar a exposição do acesso remoto

Muitos acreditam que uma rede virtual privada (VPN) protege contra ataques de ransomware. Esse mito está incorreto, sendo a VPN um vetor de ataque fácil de usar para agentes mal-intencionados. É claro que esse vetor de ataque ganhou ainda mais apelo recentemente por meio da enorme proliferação do uso de VPN de acesso remoto, quando milhões de funcionários passaram a trabalhar em casa nos últimos dois anos. Os invasores percebem que essas redes domésticas são pouco protegidas e vulneráveis, o que as torna alvos fáceis.

Um dos ataques de ransomware mais importantes em 2021 envolveu uma organização de oleodutos nos EUA, que observou o fornecimento de combustível interrompido para a maioria de seus clientes nas regiões leste e sul do país. Durante o ataque, os criminosos cibernéticos exploraram uma VPN de acesso remoto.

A maioria dos clientes VPN desatualizados também contém vulnerabilidades que podem ser exploradas, aumentando ainda mais o desafio de proteger a rede contra ameaças externas. Isso levou organizações reguladoras como o FBI, o Departamento de Segurança Interna e a CISA (Agência de Segurança Cibernética e Infraestrutura) a emitir avisos sobre a possibilidade de ataques à infraestrutura VPN de acesso remoto.

Prática recomendada — Substituir a VPN de acesso remoto pela ZTNA

A ZTNA (Zero Trust Network Access) é o substituto moderno da VPN de acesso remoto. Ela elimina a confiança inerente e o amplo acesso que a VPN oferece, em vez de usar os princípios de Zero Trust — confie, mas confira. A ZTNA oferece segurança aprimorada, gerenciamento facilitado, melhor visibilidade e uma melhor experiência do usuário quando comparada à VPN de acesso remoto.

A ZTNA elimina clientes VPN vulneráveis, usa autenticação multifator (MFA) e integridade do dispositivo para controlar o acesso, além de fornecer acesso apenas a aplicativos de rede específicos, microssegmentando de modo efetivo a rede. Trata-se de algo tão relevante que a Casa Branca criou uma exigência de arquitetura de Zero Trust que deve ser cumprida por todas as agências federais até 2024.

Elimine a exposição com sistemas de área de trabalho remota (RDP) expostos e outros sistemas

Ferramentas como a RDP, a VNC (Virtual Network Computing) e outras soluções de gerenciamento remoto permitem que a equipe remota acesse e gerencie sistemas. Infelizmente, sem as devidas proteções, essas ferramentas oferecem também caminhos convenientes para os invasores lançarem ataques de ransomware.

Não proteger a RDP e outras soluções de gerenciamento remoto pode abrir as portas a ataques de ransomware. Os criminosos cibernéticos costumam usar varredura em massa ferramentas de ataque de força bruta que tentam centenas de milhares de combinações de nomes de usuário e senhas até chegar às credenciais corretas. Algumas vezes, eles usam essas credenciais para lançar imediatamente um ataque. Outras vezes, eles podem vender essas credenciais para outro grupo de invasores.

"Vocês têm uma antiga vulnerabilidade Log4j crítica que não foi corrigida no Horizon; foi assim que conseguimos fazer nossa primeira investida de acesso. Fizemos uma varredura em massa e vocês apareceram. Não foi intencional. Já dentro da sua VM do Horizon, fizemos o despejo das credenciais, obtivemos um administrador de domínio, quebramos o hash e [conseguimos] obter acesso mais profundo."

Essa é uma citação de invasores de ransomware bem-sucedidos descrevendo como obtiveram acesso

A citação acima é de um grupo de agentes de ameaças que extorquiu uma organização depois de obter acesso por meio de uma vulnerabilidade não corrigida no VMware Horizon descoberta por meio de uma varredura em massa. Ela ressalta a importância de manter o firmware e o software do sistema atualizados e com patches em dia.

Prática recomendada — Eliminar o acesso externo direto

Proteja o acesso a sistemas remotos bloqueando todo o acesso por meio de um firewall e habilitando apenas o acesso via ZTNA. Isso remove efetivamente o acesso externo direto.

Verifique todas as regras de firewall para garantir que nenhum sistema de gerenciamento remoto ou RDP seja exposto por meio de encaminhamento de porta ou regras de NAT. Além disso, garanta que o acesso seguro seja rigidamente controlado por meio da ZTNA. Esse procedimento certifica-se de que apenas usuários e dispositivos autorizados que comprovaram sua identidade com MFA e status de integridade possam obter acesso.

Considere também novas tecnologias de autenticação segura, como o Windows Hello para Empresas. Obviamente, mantenha sua infraestrutura atualizada e com patches em dia para evitar que vulnerabilidades antigas se tornem alvos fáceis.

2. Impedir a entrada de malware e ransomware por meio de phishing e downloads

Outro antigo vetor de ataque que induz os usuários a responderem a e-mails de phishing e/ou abrirem e-mails maliciosos. Atualmente, é preciso que um firewall moderno, endpoint e proteção de mensagens funcionem em conjunto com a mais recente tecnologia de Machine Learning e sandbox para identificar ameaças direcionadas em evolução que tentam acessar sua rede. O ideal é interromper essas ameaças antes que elas entrem na rede ou isolá-las e impedir que elas movam depois de se estabelecer em sua rede.

Prática recomendada — Usar proteção contra ameaças de dia zero

Para manter essas ameaças fora das caixas de entrada dos usuários, certifique-se de ter a proteção de mensagens mais recente contra phishing e e-mails maliciosos. Certifique-se também de ter a tecnologia de inspeção profunda de pacotes (DPI) em seu firewall, incluindo descriptografia TLS 1.3 para inspecionar cargas criptografadas, análise de Machine Learning para novas ameaças de dia zero e sandbox para avaliar arquivos recebidos no tempo de execução. Ensine seus usuários a identificar possíveis ameaças de phishing. Além disso, garanta que seus endpoints tenham a melhor proteção disponível contra roubo de credenciais, explorações e ransomware.

Para isolar as ameaças que entram na rede e impedir que elas se movam, há várias práticas recomendadas que abordaremos na próxima seção.

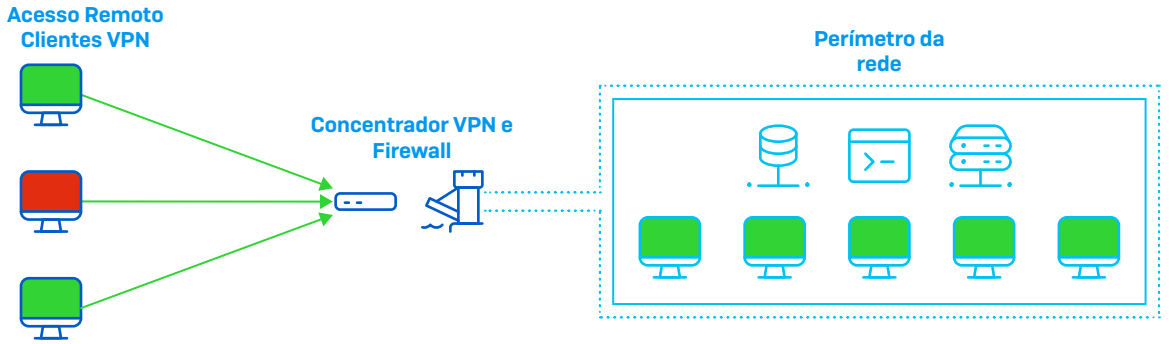
5 Playbook dos Adversários Ativos 2022 – Sophos

3. Limitar o acesso mais profundo à rede

Durante um ataque de rede, é vital que sua solução de segurança de rede limite a movimentação da ameaça pela rede — ou seu acesso mais profundo à rede.

Infelizmente, a maioria das redes é similar a uma fortificação medieval, com uma proverbial muralha de castelo e um fosso formando um perímetro seguro em torno dos recursos da rede. Uma VPN equivale a uma guarita de acesso para usuários autorizados entrarem nesse perímetro seguro. Porém, depois que criminosos cibernéticos acessam uma rede, eles têm acesso total a tudo o que está dentro do perímetro. Essa mesma liberdade de movimentação dentro de uma rede também se aplica a ameaças como ransomware.

Os criminosos cibernéticos usam o RDP e outros sistemas de gerenciamento, bem como dispositivos não gerenciados, como pontos de entrada. Eles também usam esses pontos de entrada para obter acesso mais profundo à rede.



Prática recomendada — microssegmentar a rede

Isso é crítico em redes modernas, juntamente com o Zero Trust. Há três práticas recomendadas que você deve usar para arquitetar sua rede:

1. **Segmente sua rede.** Crie pequenas zonas ou VLANs e conecte-as usando switches gerenciados e um firewall para aplicar proteção antimalware e IPS entre segmentos. Isso permite identificar e bloquear ameaças que tentam obter acesso mais profundo à rede.
2. **Use ZTN.** Microssegmente seus aplicativos de rede e permita que apenas usuários autorizados acessem os recursos de que precisam. Assim, se um dispositivo do usuário for comprometido e uma ameaça não for detectada, a ameaça poderá ser eliminada rapidamente. O Sophos ZTNA vai um passo além ao remover completamente o acesso caso um dispositivo seja comprometido.
3. **Use uma tecnologia como o Sophos Synchronized Security.** O Synchronized Security permite responder automaticamente a uma ameaça ativa na rede, permitindo que ela seja isolada e impedida de obter acesso mais profundo à rede. Ele é capaz de identificar imediatamente uma ameaça e notificar dispositivos íntegros para ignorar qualquer tráfego de um host comprometido, enquanto os Sophos Switches descartam automaticamente os pacotes de um dispositivo afetado e o Sophos Firewall limita ainda mais o acesso do host comprometido a outras partes da rede.

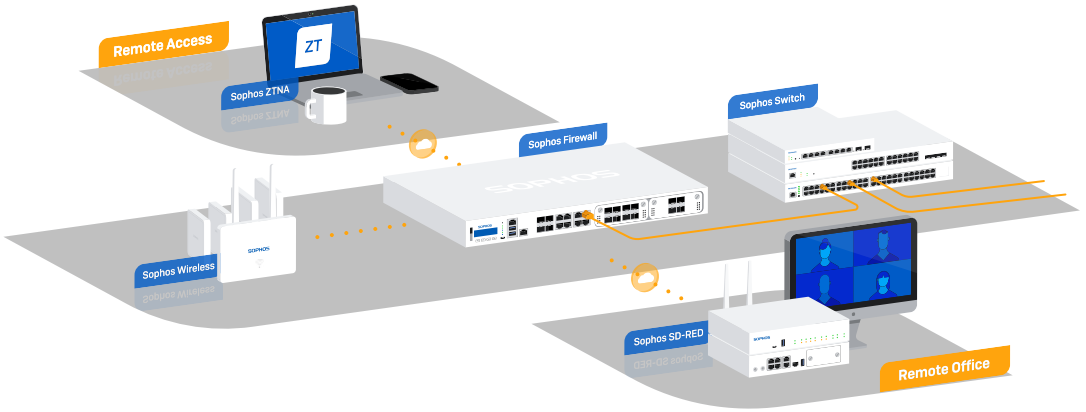
Práticas recomendadas de segurança de rede para proteção contra ransomware

Em resumo, estas são as práticas recomendadas que você pode usar para proteger sua rede contra ransomware e outras ameaças cibernéticas:

- **Microssegmente a rede.** Isso permite limitar o acesso mais profundo de ameaças à rede. Use o Sophos ZTNA para microssegmentar o acesso aos seus aplicativos de rede. Use ainda o Sophos Firewall e o Sophos Switch para microssegmentar seus recursos de rede internos. E use o Sophos SD-RED para segmentar e conectar com segurança dispositivos e locais remotos.
- **Substitua a VPN de acesso remoto pela ZTNA.** Elimine um vetor de ataque comum removendo clientes VPN antigos potencialmente vulneráveis. Atualize para uma solução ZTNA moderna, como o Sophos ZTNA, que se integra à proteção de endpoint de última geração da Sophos para proteger adequadamente o dispositivo do usuário, suas identidades, seu acesso a aplicativos e dados e sua rede com um único agente gerenciado em um único console, de um só fornecedor.
- **Implemente a proteção mais forte possível.** Você deve implementar o mais alto nível de proteção em seu firewall, endpoints, servidores, dispositivos móveis e acesso remoto.
  - Garanta que seu firewall tenha inspeção TLS 1.3, IPS NextGen e DPI de fluxo com Machine Learning e sandbox para proteção contra as ameaças de dia zero mais recentes. O Sophos Firewall inclui todas essas tecnologias e as integra perfeitamente para fornecer proteção e desempenho potentes, para que você obtenha o máximo valor do seu investimento em firewall.
  - Assegure também que seus endpoints tenham recursos modernos de proteção de última geração para se proteger contra roubo de credenciais, explorações e ransomware. A Sophos é classificada consistentemente como a principal fornecedora de soluções de proteção de endpoint de última geração. Cobrimos seus endpoints, dispositivos móveis e servidores e permitimos que você os gerencie no mesmo console de gerenciamento de nuvem que o restante de seus produtos Sophos.
- **Reduza a área de superfície de ataque cibernético.** Analise as regras de firewall e elimine qualquer acesso remoto ou acesso ao sistema RDP por meio de VPN, NAT ou encaminhamento de porta. Certifique-se ainda de que quaisquer fluxos de tráfego estejam devidamente protegidos. O Sophos Firewall facilita esse processo graças à sua visibilidade superior, painéis, relatórios e recursos de gerenciamento de regras.
- **Mantenha seu firmware e software atualizados e com patches em dia.** Trata-se de algo particularmente importante para qualquer infraestrutura de rede, como firewall ou software de acesso remoto ou clientes, mas também é importante para todos os seus sistemas, pois cada atualização inclui patches de segurança essenciais para vulnerabilidades já detectadas. A Sophos permite manter todos os seus produtos de segurança cibernética atualizados automaticamente.
- **Use MFA.** Garanta que sua rede opere em um modelo de Zero Trust, em que cada usuário e dispositivo precise ganhar confiança continuamente, verificando sua identidade. Além disso, imponha uma política de senha forte, e considere adotar soluções de autenticação como o Windows Hello para Empresas. Todos os produtos Sophos aceitam MFA de seu provedor de autenticação preferencial.

- **Responda instantaneamente a ataques cibernéticos.** Use tecnologias de automação e conhecimento humano para acelerar a resposta e a correção de incidentes cibernéticos.
  - Garanta que sua infraestrutura de segurança de rede o ajude a responder automaticamente a ataques ativos para que você possa isolar um host comprometido antes que ele cause sérios danos. Somente o Sophos Synchronized Security é capaz de fornecer o nível de resposta de que você realmente precisa, e quando você precisa.
  - Implante um serviço de detecção e resposta gerenciadas (MDR), como o Sophos MDR. Com o Sophos MDR, uma equipe de especialistas em ameaças monitora e responde constantemente a incidentes antes que eles se tornem problemas, para que você não precise se preocupar.

Proteja a rede com Sophos



A Sophos fornece tudo o que você precisa para proteger totalmente sua rede contra ataques, incluindo firewalls, ZTNA, switches, wireless, dispositivos de borda remotos, proteção de mensagens, MDR e proteção de endpoint Next-Gen para todos os seus dispositivos e servidores. E o que é melhor: tudo é gerenciado em um único console de gerenciamento de nuvem, o Sophos Central, e se integra para fornecer a Sophos Synchronized Security e detecção e resposta a ameaças entre produtos ou detecção e resposta estendidas (XDR).

O Synchronized Security garante que seus produtos Sophos compartilhem constantemente dados de telemetria e integridade, assim você pode responder rapidamente a ataques cibernéticos. Quando um host comprometido é detectado, os endpoints íntegros automaticamente ignoram o tráfego, os switches descartam pacotes do host comprometido e o firewall bloqueia o acesso a outras partes de sua rede até que o problema seja resolvido. Nenhum outro sistema de segurança de rede se iguala a isso — tornamos a segurança cibernética mais fácil e eficaz.

O Sophos XDR é a única solução XDR do setor que sincroniza firewall nativo, endpoint, servidor, e-mail, nuvem e segurança do Microsoft 365 para fornecer uma visão completa do ambiente da sua organização. Ele oferece um conjunto de dados rico e uma análise profunda para detecção, investigação e resposta a ameaças para equipes dedicadas do centro de operações de segurança e administradores de TI.

Se você imagina que a segurança cibernética é muito complexa, difícil e muda muito rápido para gerenciá-la de maneira eficaz, deixe isso com a gente. O Sophos MDR protege mais de 11.000 organizações em todo o mundo, fornecendo caça e neutralização de ameaças 24 horas por dia, fornecidas por uma equipe global de especialistas em ameaças.

Conclusão: A Sophos oferece um portfólio de produtos e serviços de segurança cibernética que permitem proteger facilmente sua rede contra ransomware.

Saiba como a Sophos pode proteger sua rede em www.sophos.com

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2022-09-12 PTBR-WP (DD)

SOPHOS