SOPHOS
Cybersecurity evolved.

Minimizando o risco de ataques à cadeia de suprimentos: diretrizes e práticas recomendadas

Em dezembro de 2020, a notícia sobre um ataque cibernético à empresa de monitoramento de TI SolarWinds deu destaque aos ataques à segurança cibernética da cadeia de suprimentos, mas esse tipo de ataque não é um fenômeno recente. O fato é que, de modo inquietante, praticamente uma a cada 10 vítimas de ransomware (9%) disse que o ataque encontrou a sua porta de entrada através de um fornecedor terceirizado de confiança, de acordo com a pesquisa da Sophos de 2020, com 5.000 gerentes de TI em 26 países[1].

Mas o que é exatamente um ataque à cadeia de suprimentos e como funciona? Mais importante: o que você pode fazer para proteger a sua organização do impacto de um ataque à cadeia de suprimentos?

Essas e outras questões são respondidas aqui, neste documento.

1 O Estado do Ransomware 2020 – Sophos, 2020

Documento técnico Sophos. Abril, 2021

O que é um ataque à cadeia de suprimentos?

As organizações são, geralmente, dependentes de um fornecedor terceirizado para gerenciar toda ou parte de uma função de negócio em particular, como a infraestrutura de TI, por exemplo. Permitir que fornecedores terceirizados se conectem à sua rede beneficia os seus negócios, pois libera o seu pessoal interno, mas inerentemente traz riscos à segurança, expondo vulnerabilidades aos ataques à cadeia de suprimentos.

Em um ataque à cadeia de suprimentos, em lugar de se infiltrarem diretamente, os hackers exploram o acesso que os fornecedores terceirizados têm aos seus sistemas para montar uma base de operações no seu ambiente. Uma vez que adentrem o seu espaço, eles estão prontos para realizar qualquer atividade fraudulenta.

Ter apenas um fornecedor conectado à sua rede representa o risco de um ataque à cadeia de suprimentos. Entretanto, em média, as organizações de pequeno e médio porte relatam ter pelo menos três fornecedores que podem se conectar aos seus sistemas[2]. Proteger esses fornecedores conectados cria grandes desafios, aumentando a carga de trabalho para as equipes de TI. Para aumentar ainda mais o desafio, os ataques à cadeia de suprimentos são notoriamente difíceis de detectar, quanto mais de se defender, pois podem vir de qualquer parte da sua cadeia de suprimentos.

Tipos de fornecedores terceirizados

Provedores de serviços de TI e serviços profissionais são dois dos fornecedores terceirizados que mais comumente podem vir a se conectar à rede de uma organização.

Serviços profissionais

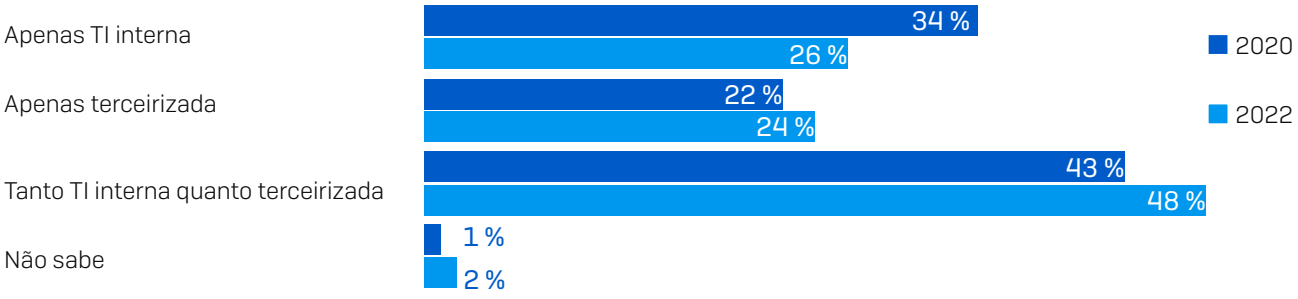
Serviços profissionais são bastante empregados pelas organizações para gerenciar de modo independente funções de negócios (ou parte delas) quando não têm o pessoal especializado e os conhecimentos necessários internamente. Tomemos como exemplo uma firma de contabilidade que precisa ter acesso a dados financeiros sigilosos (através de um software) para fornecer ao cliente análises e insights os quais foram encarregados de providenciar. Como você pode imaginar, um ataque cibernético de sucesso em tal organização poderia ser devastador para o seu portfólio de clientes.

Provedores de serviços de TI

Provedores de serviços de TI são organizações externas incumbidas da administração da infraestrutura de TI e/ou segurança de TI de uma empresa. Também conhecidos como provedores de serviços gerenciados (MSP) ou provedores de serviços de segurança gerenciados (MSSP), eles estão frequentemente na mira dos ataques à cadeia de suprimentos.

São alvos de ataque particularmente atraentes porque têm as chaves para acessar muitas organizações de diferentes clientes. Com o número de organizações que subcontratam a segurança de TI cogitado a subir para 72% até 2022[3], a postura de segurança desses terceiros é de vital importância para a sua própria postura de segurança.

Como a segurança de TI é entregue: agora e 2022



2,3 Segurança cibernética: o desafio humano – Sophos, 2020

Tipos de ataques à cadeia de suprimentos

Os ataques à cadeia de suprimentos se diferenciam na forma como são entregues, mas os princípios e os objetivos dos criminosos são geralmente os mesmos: infiltrar-se em um fornecedor terceirizado de confiança e usar indevidamente o acesso confiável para implantar malware, roubar propriedade intelectual ou espionar comunicações internas.

Ataques de phishing

Um dos vetores de ataque mais comuns utilizado pelos invasores de cadeias de suprimentos são os e-mails de phishing. Os invasores direcionam seus ataques a terceiros confiáveis com e-mails de phishing para comprometer suas redes e obter acesso, utilizando-as como propulsores à infiltração nos sistemas de seus clientes.

Atualização de software comprometida

Nos ataques mais sofisticados à cadeia de suprimentos, os hackers se infiltram na estrutura de uma empresa de software ou de um distribuidor e inserem um código malicioso nos pacotes de atualização do software. O provedor terceirizado distribui as atualizações a seus clientes, alheio ao fato de que os infectou durante o processo. Como você pode imaginar, as consequências podem ser devastadoras, especialmente se a organização tiver um grande portfólio de clientes. O ataque à SolarWinds, em dezembro de 2020, é um exemplo perfeito desse tipo de ataque.

Estudo de caso do ataque à cadeia de suprimento: SolarWinds

No final de 2020, descobriu-se que a cadeia de suprimentos de uma firma de gerenciamento de TI, a SolarWinds, havia sido comprometida. Acredita-se que esse ataque, cuja descoberta virou manchete pelo mundo todo, colocando em evidência a vulnerabilidade da segurança da cadeia de suprimentos, tenha afetado mais de 18.000 de seus clientes.

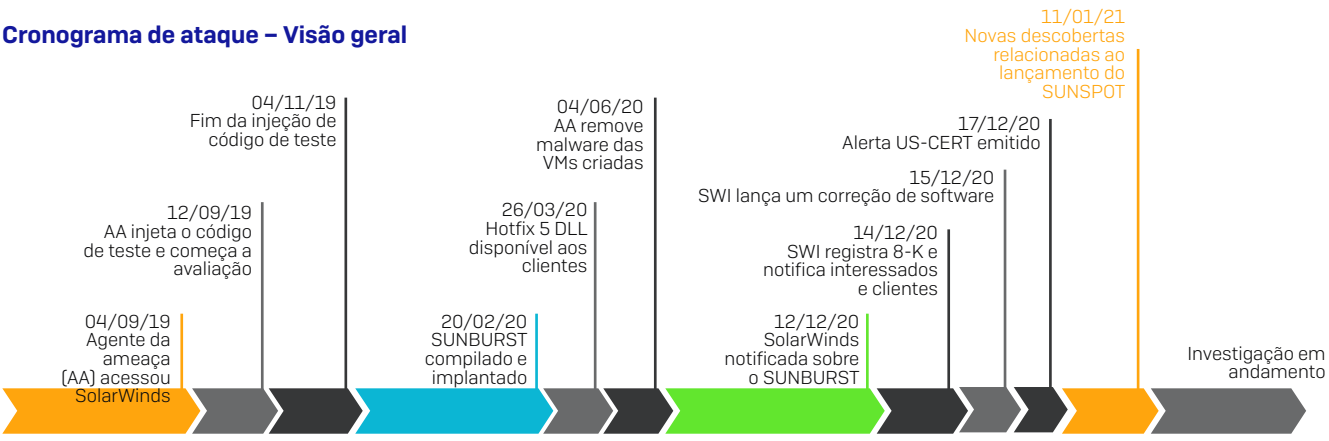
É importante notar que, até a data da publicação, em abril de 2021, a investigação sobre o ataque à SolarWinds ainda estava em andamento e pode ter mudado.

Como os hackers chegaram a isso?

Resumidamente, os hackers conseguiram inserir um código malicioso na plataforma Orion de gerenciamento e monitoramento de infraestrutura da SolarWinds. Esse código malicioso foi enviado inadvertidamente a clientes por meio de atualizações regulares de software. Foi registrado que cerca de 18.000 clientes (incluindo várias empresas da Fortune 500 e agências governamentais dos EUA) instalaram atualizações, deixando-os vulneráveis.

O mais preocupante é que houve indicativos de suspeita de infração pela SolarWinds desde setembro de 2019, como mostra o cronograma abaixo. Isso sugere que o movimento foi calculado e que os invasores se utilizaram de extrema cautela, buscando silenciar o máximo possível de alarmes durante a invasão. Você pode ler uma análise detalhada da Sophos sobre como a variante do malware Sunburst burlou as defesas aqui.

Cronograma de ataque – Visão geral



Todos os eventos, datas e horas aproximados e sujeitos a alterações, aguardando conclusão da investigação SolarWinds - https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Qual foi o impacto do ataque?

O sucesso do ataque, chamado Sunburst, deu aos invasores o acesso amplo a sistemas de informação governamentais e corporativos. Isso já resultou em volumes ainda incalculáveis de dados roubados e levanta considerações preocupantes de que os invasores usaram sua base de operações para inserir outros backdoors em redes empresariais ainda não desvendadas.

Mais importante, a escala global do ataque demonstrou como muitas organizações estão despreparadas quando se trata de se defender contra ataques à cadeia de suprimentos.

Pacotes envenenados

Um tipo menos comum de ataque a cadeias de fornecimento, embora esperemos vê-lo com mais frequência no futuro, é o que nos referimos como "pacotes envenenados". Com o aumento do uso da nuvem, Docker e metodologias de desenvolvimento ágeis, também aumenta o uso de componentes prontos para aplicar visando encurtar o ciclo de vida de desenvolvimento. Agentes maliciosos começaram a esconder armadilhas normalmente usadas em contêineres, bibliotecas e outros recursos na esperança de as verem incorporadas ao seu produto final.

Diretrizes para se defender contra ataques à cadeia de suprimentos

Dada a complexidade e a natureza dos ataques à cadeia de suprimentos, a tecnologia sozinha não é capaz de evitá-los. Pelo contrário, estas diretrizes e práticas recomendadas se destinam a possibilitar que você para minimize o risco associado a um ataque à cadeia de suprimentos.

1. Mude a abordagem à segurança cibernética de reativa para proativa

A SolarWinds foi o toque de alerta para muitas organizações em todo o mundo. Quando um ataque se torna óbvio, geralmente já é tarde demais: no momento em que os criminosos lançam suas cargas, eles já terão roubado dados críticos e, muito provavelmente, já tiveram acesso à sua rede há dias. É preciso mudar a sua forma de pensar: sempre parta do pressuposto de que você está comprometido e saia à caça de ameaças antes que seja tarde demais. Existem tecnologias e serviços que podem dar suporte a esse tipo de abordagem, que explicaremos mais adiante no documento.

2. Monitore os primeiros sinais de comprometimento

Durante as investigações conduzidas pela equipe do Sophos Managed Threat Response (MTR), duas evidências se sobressaíram como indicativos iniciais de comprometimento: uma foi o uso de credenciais para acesso remoto e fins administrativos fora do horário de expediente, a outra foi o uso indevido das ferramentas de administração do sistema para realizar a vigilância e roubar os dados da rede.

O uso de contas legítimas e de suas próprias ferramentas para obter e reter persistência costuma ser chamado de LOL (Living Off the Land, vivendo da terra). Detectar esses tipos de comportamentos requer vigilância e habilidade; entretanto, eles são evidências claras para os olhos treinados de um analista de operações de segurança, que alerta você sobre o ataque antes que os danos tenham sido feitos. Invista na tecnologia e no treinamento necessários para monitorar esses indicadores internamente ou empregar um provedor de serviços de detecção e resposta gerenciadas (MDR) para fazer o monitoramento por você.

3. Faça uma auditoria da sua cadeia de suprimentos

Pode parecer óbvio, mas dedicar um tempo para mapear todas as organizações às quais você está conectado pode ter um valor inestimável – provavelmente você encontrará mais do que pensava existir. Ao realizar esse exercício, você será capaz de identificar rapidamente os pontos fracos (por exemplo, as organizações mais suscetíveis ao crime cibernético) e poderá tomar medidas para mitigar os riscos associados. Espere estar conectado a fornecedores terceirizados como:

- **Provedores de serviços de TI**
  - MSP/MSSP
  - Provedores de nuvem
- **Serviços profissionais**
  - Finanças
  - Legal
  - Segurança
  - Zeladoria
- **Fornecedores**
  - Materiais
  - Serviços
  - Mão de obra
  - Logística

Quando souber com quem está conectado, você poderá avaliar o tipo de acesso à rede que têm e quais informações poderiam ser acessadas usando as credenciais fornecidas. Se o nível estiver acima do mínimo, esse seria o momento de bloquear esse acesso e confiná-lo apenas às informações necessárias. Comece com os provedores que têm o acesso mais desnecessário e siga nessa ordem.

4. Avalie a postura de segurança dos seus fornecedores e parceiros de negócios

Existem várias abordagens para fazer uma avaliação, mas a mais popular para os grandes provedores de serviços, operadores de nuvem e processadoras de pagamento é determinar a que tipos de certificações e auditorias estão sujeitos.

Por exemplo, uma processadora de pagamento estará sujeita à conformidade com PCI DSS. Se estiverem sujeitas à PCI DSS nível 1 ou 2, solicite que apresentem um relatório de conformidade RoC (Report on Compliance) emitido pelo QSA/ISA. Você deve reavaliar esses RoCs trimestralmente para assegurar que atendem às suas expectativas.

Outra certificação popular para confirmar auditorias é a SOC 2/2+/3 dos seus provedores de serviços de nuvem. As auditorias SOC avaliam os controles e mitigações de segurança cobrindo cinco Entidades de Serviço de Confiança: privacidade, segurança, disponibilidade, integridade de processamento e confidencialidade.

Exatamente como acontece com a sua própria segurança, auditorias não são garantia de nada, mas são certamente um indicativo de que o fornecedor leva a segurança e a conformidade a sério. Outros fatores a considerar ou que você pode solicitar incluem relatórios de testes de penetração e conformidade GDPR, ou frequência de falhas ou violações de dados anteriores.

5. Reavalie constantemente a higiene das suas próprias operações de segurança de TI

Ainda que a postura dos seus fornecedores seja crítica para a defesa contra os ataques à cadeia de suprimentos, não negligencie a higiene da sua própria segurança cibernética. Muitas organizações a ignoram porque não sabem por onde começar ou não se acham suficientemente importantes para se tornarem alvo do comprometimento de um parceiro de confiança. As suas práticas de segurança cibernética podem significar a diferença entre um pequeno inconveniente e uma violação de dados catastrófica.

Habilite a autenticação multifator (MFA)

A maneira mais comum de as organizações se tornarem vítimas de ataques à cadeia de suprimentos é pelo uso de acesso roubado, mas autorizado. Os provedores de serviços muito frequentemente recebem credenciais com os mesmos direitos e privilégios que o quadro de funcionários.

Assim sendo, eles não precisam usar MFA, permitindo aos agentes nocivos explorar as credenciais roubadas através de ataques de phishing, bem como a reutilização não autorizada de credenciais pelo próprio pessoal deles. Como a maioria das organizações emprega SSO (logon único), essas credenciais podem ser usadas indevidamente para acessar diferentes tipos de sistemas desnecessários para a tarefa em andamento, aumentando o risco de ataque por funcionários e terceiros mal-intencionados.

Reavalie o acesso de fornecedores e privilégios de aplicativos

Outro erro frequente é oferecer VPN, RDP ou outras tecnologias de acesso remoto irrestrito a terceiros para permitir que gerenciem soluções. Por irrestrito queremos dizer oferecer acesso a toda a rede em vez de segmentar e fortalecer cautelosamente a proteção das ferramentas de acesso remoto necessárias.

Todas as ferramentas voltadas ao público externo devem exigir autenticação multifator, devendo ser limitadas a um único host ou sistema. Para os casos em que se deseja acesso adicional, recomendamos o uso de "jump hosts" para reduzir o risco e oferecer mais oportunidades para monitoramento e log de registro.

Dar permissão por padrão a todos os aplicativos atribuídos pelo certificado de software de um fornecedor também expõe as organizações aos ataques à cadeia de suprimentos. Temos visto repetidamente certificados roubados ou usados indevidamente para assinar malwares. As ferramentas de segurança devem inspecionar tudo o que for possível.

Monitore proativamente boletins de segurança de fornecedores

Monitore todos os boletins de segurança dos fornecedores para poder implantar rapidamente patches e mitigações quando forem descobertas vulnerabilidades, e fique de olho nas manchetes do noticiário sobre seus fornecedores. Nos momentos de crise, o modo de resposta a incidentes da sua organização talvez não esteja entre as prioridades mais altas de notificação do seu provedor. Isso permite que você bloqueie o acesso e comece a investigar se foi afetado pela situação.

Reavalie sua apólice de seguro digital (se tiver uma)

Por último, se você tem uma apólice de seguro digital, determine se ela cobre perdas de terceiros e como combinar a apólice, se necessário. Fale com os seus fornecedores para garantir que a sua cobertura sobreponha qualquer cobertura específica que eles possam ter.

Capacitadores de serviços e tecnologia

Como mencionado anteriormente, a defesa contra ataques à cadeia de suprimentos é complexa por natureza. Ela está mais intrinsecamente relacionada ao tratamento do risco associado e a amenizar o ataque. Felizmente, existem tecnologias e serviços disponíveis ideais para dar suporte à mitigação desse risco.

Caça a ameaças

Mencionamos a necessidade de mudar para uma abordagem proativa à segurança cibernética para se defender contra os ataques à cadeia de suprimentos. A caça a ameaças é uma prática essencial que as organizações precisam adotar para incorporar essa visão.

Endpoint Detection and Response (EDR)

Um capacitador de caça a ameaças essencial é a tecnologia EDR. Normalmente integrada a plataformas de proteção de endpoint, EDR combina dados de endpoints e monitoramento contínuo em tempo real com funcionalidades de análise e resposta automáticas. Isso permite que as equipes de segurança identifiquem e resolvam as ameaças com rapidez.

O Sophos Intercept X para endpoint inclui a poderosa funcionalidade EDR. O Sophos EDR é a primeira solução projetada para analistas de segurança e administradores de TI, fornecendo as ferramentas para que você faça perguntas detalhadas ao caçar ameaças e fortalecer a higiene de suas operações de segurança de TI. Você obtém acesso a consultas SQL avançadas, prontas para usar e personalizáveis que oferecem as informações necessárias para tomar decisões fundamentadas.

Além disso, o recurso de identificação de ameaças automatizada do EDR da Sophos permite que você identifique automaticamente atividades suspeitas, priorize indicadores de ameaças e faça a busca rápida de possíveis ameaças em todos os seus endpoints e servidores.

Saiba mais sobre as habilidades de EDR da Sophos

Serviços de Resposta e Detecção Gerenciadas (MDR)

As ameaças cibernéticas mais devastadoras, como o ataque à SolarWinds, geralmente envolvem uma liderança humana. Embora a tecnologia, em especial as ferramentas de caça a ameaças com EDR, tenha um papel importante a desempenhar, os operadores especializados ainda são necessários. Para deter os ataques conduzidos por humanos precisamos de humanos no encalço dessas ameaças, e os gerentes de TI sabem disso, com 48% deles planejando incorporar essas práticas no decorrer do ano[4].

Uma abordagem de caça a ameaças liderada por humanos seria adquirir um serviço MDR. O premiado serviço MDR da Sophos, o Sophos Managed Threat Response (MTR), vai além da simples notificação de uma ameaça: ele mune a sua equipe de TI com uma equipe dedicada de especialistas em segurança cibernética que trabalha incessantemente para caçar, validar e remediar possíveis ameaças e incidentes por você.

4 Segurança cibernética: o desafio humano – Sophos, 2020

A equipe de caçadores de ameaças e peritos em respostas do Sophos MTR irá:

- Capturar ameaças de forma proativa, validando ameaças e incidentes potenciais
- Usar todas as informações disponíveis para determinar o escopo e a gravidade das ameaças
- Aplicar o contexto comercial apropriado às ameaças validadas
- Iniciar ações para deter, conter e neutralizar as ameaças remotamente
- Oferecer conselhos práticos para tratar da causa primária dos incidentes recorrentes

Saiba mais sobre o Sophos MTR

Siga rumo à segurança cibernética Zero Trust

Anteriormente, falamos sobre a reavaliação da sua própria postura de segurança, especialmente sobre habilitar MFA e reavaliar constantemente os privilégios de acesso e a aplicativos. Tudo isso pode ser obtido mudando para a abordagem de segurança cibernética Zero Trust.

Zero Trust é um conceito baseado no princípio "confie, mas confira", que se concentra na proteção dos recursos, independentemente de onde estão física ou digitalmente. Nenhum fornecedor, produto ou tecnologia lhe dará a confiança plena que o conceito implica. Melhor dizendo, seria necessária uma guinada cultural e muitas soluções diferentes para mudar os paradigmas que formam o arsenal de segurança dos nossos recursos. Porém, um ponto de partida rumo a esse modelo é a adoção de uma solução Zero Trust Network Access (ZTNA).

O conceito por trás do nome ZTNA se baseia no princípio "confie, mas confira". Isso permite que os usuários acessem os dados com segurança de qualquer lugar, fornecendo aos administradores controles supergranulares.

O ZTNA está relacionado à verificação do usuário — geralmente com autenticação multifator e um provedor de identidade — e à validação da integridade e conformidade do dispositivo — verificando se está registrado, atualizado, adequadamente protegido, habilitado para criptografia etc. — e ao uso dessas informações para tomar decisões baseadas em políticas para determinar o acesso e o privilégio a importantes aplicativos na rede. O ZTNA proporciona uma excelente alternativa à VPN de acesso remoto, pois oferece controles supergranulares de quem pode acessar o quê, sendo crítico para proteger contra ataques à cadeia de suprimentos, confiando o acesso de seus sistemas a um fornecedor.

O Sophos ZTNA, a nossa nova solução de acesso à rede gerenciada na nuvem e entregue pela nuvem, está no estágio Early Access Program (EAP) e será disponibilizada a partir do segundo semestre de 2021. A TI oferece proteção para qualquer aplicativo em rede armazenado na sua rede local, na nuvem pública ou em qualquer outro site de hospedagem. Isso abrange tudo, desde acesso RDP a compartilhamentos de arquivos em rede até aplicativos como Jira, Wikis, repositórios de código fonte, aplicativos de suporte e tíquetes e mais.

Saiba mais sobre o Sophos ZTNA

Conclusão

Devido à sua complexidade, é praticamente impossível evitar que um ataque baseado na cadeia de suprimentos ocorra. Entretanto, seguindo as diretrizes neste documento, você pode reduzir os riscos de se tornar vítima de um ataque e evitar que o ataque cause um impacto significativo nos seus negócios. Em resumo:

1. Mude a abordagem à segurança cibernética de reativa para proativa
2. Monitore os primeiros sinais de comprometimento
3. Faça uma auditoria da sua cadeia de suprimentos
4. Avalie a postura de segurança dos seus fornecedores e parceiros de negócios
5. Reavalie constantemente a higiene das suas próprias operações de segurança de TI

Além desses passos, considere a adoção de tecnologias e serviços como EDR, MTR e ZTNA para dar suporte às metas de segurança da sua cadeia de suprimentos.

O cenário das ameaças evoluiu, e o comprometimento da cadeia de fornecimento passou a ser um problema para todas as organizações, grandes e pequenas. Todos nós somos alvos na cadeia de suprimento de alguém; portanto, nunca foi tão importante minimizar o risco da cadeia de fornecimento de terceiros.

Saiba mais sobre as soluções de segurança cibernética líderes do setor da Sophos em 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.

2021-04-14 (PTBR-NP)

SOPHOS