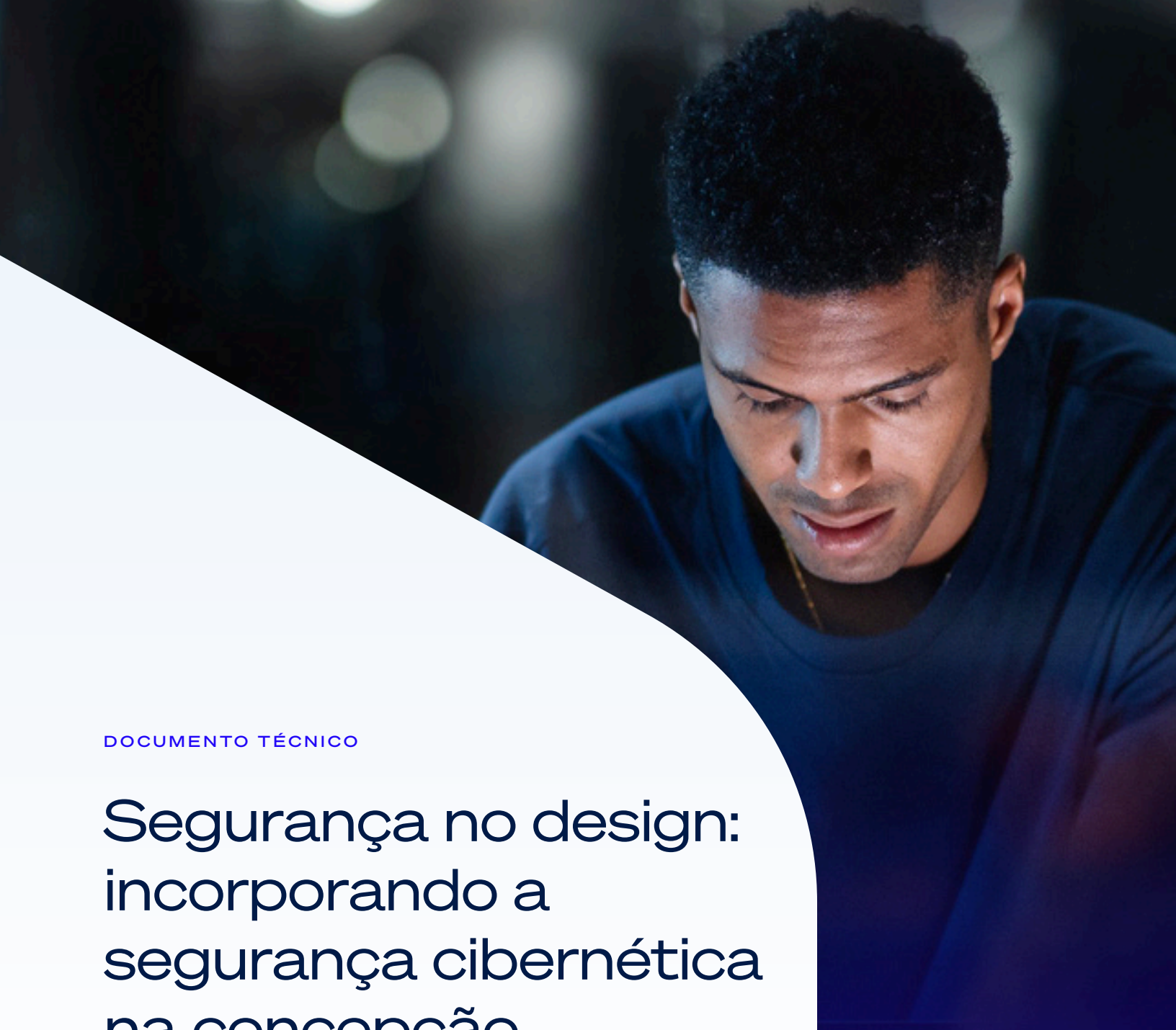

DOCUMENTO TÉCNICO

Segurança no design: incorporando a segurança cibernética na concepção

Por que essa filosofia é importante e como ela reduz sua superfície de ataque partindo de dentro

SOPHOS

Sumário executivo

Secure by Design é um princípio da filosofia de desenvolvimento de software que trata a segurança como um requisito fundamental, não como algo secundário.

Em vez de criar um produto primeiro e adicionar correções de segurança posteriormente, o princípio Secure by Design exige que as considerações de segurança sejam incorporadas em todas as etapas do ciclo de vida de desenvolvimento, desde a arquitetura e projeto e passando pela codificação, teste, implantação e manutenção.

A ideia central é simples: se você criar algo de forma segura desde o início, seus usuários estarão sempre protegidos, em vez de apenas depois de aprender a definir as configurações corretas ou sanar as falhas de segurança após o fato consumado.

Na prática, isso significa adotar medidas como o princípio do privilégio mínimo (conceder aos usuários e processos apenas o acesso mínimo necessário), padrões de segurança predefinidos (lançar produtos com a configuração mais segura já pronta para uso), defesa em profundidade (sobrepor várias camadas de controles de segurança para que nenhuma falha isolada seja catastrófica), além de eliminar categorias inteiras de vulnerabilidades por meio de linguagens, estruturas e padrões de design mais seguros.

A ideia central é simples:

Se você criar algo de forma segura desde o início, seus usuários estarão sempre protegidos, em vez de apenas depois de aprender a ativar as configurações corretas ou sanar as falhas de segurança após o fato consumado.

Por que foi introduzida a abordagem Secure by Design?

Durante décadas, o setor de tecnologia operou sob o modelo “lançar rápido, corrigir depois”. Uma consequência desse legado é que a segurança cibernética acaba sendo vista como um centro de custos, além de algo que atrasa o lançamento no mercado e frustra os desenvolvedores. Os impactos estão se manifestando em tempo real: divulgações constantes de vulnerabilidades, patches de emergência e violações que custam bilhões às organizações, além da exposição de dados pessoais de centenas de milhões de pessoas.

As vulnerabilidades do Ivanti Connect Secure, a exploração de Log4Shell em uma biblioteca de código aberto amplamente utilizada e as vulnerabilidades de MOVEit Transfer demonstraram que a segurança reativa simplesmente não consegue acompanhar o ritmo de adversários determinados.

Em reconhecimento a esse desequilíbrio, em 2023 a CISA (Cybersecurity and Infrastructure Security Agency), em colaboração com parceiros internacionais, formalizou orientações do Secure by Design, instando os fabricantes de tecnologia a assumirem a responsabilidade pelos resultados de segurança de seus clientes.

Os princípios Secure by Design estabelecem que a responsabilidade pela segurança deve recair sobre os fornecedores que desenvolvem os produtos, não sobre os usuários finais que os implantam. Isso mudou a forma como os fornecedores abordavam a segurança dos produtos tecnológicos, mudando o foco da responsabilidade individual ("os usuários devem instalar as correções imediatamente") para a responsabilidade do fabricante ("os fornecedores devem comercializar produtos que sejam seguros desde o primeiro dia").

Por que o princípio Secure by Design é fundamental para as soluções de segurança cibernética

Ele serve como um forte lembrete de que, às vezes, até mesmo as ferramentas de segurança podem se tornar o ponto de entrada de um ataque. No entanto, isso ocorre com uma frequência alarmante.

Ele evidencia uma deficiência crítica para muitas organizações: assim que um dispositivo no perímetro for comprometido, os invasores continuarão atacando-o repetidamente até que esteja totalmente protegido. Os firewalls e outros sistemas de borda podem continuar vulneráveis mesmo após a disponibilização de uma correção. Em todas as vulnerabilidades exploradas confirmadas em uma recente análise de incidentes realizada pela Sophos, o tempo médio entre a publicação de um aviso ou patch pelo fornecedor e a exploração da falha por um invasor foi de 322 dias — quase um ano inteiro de oportunidade para os adversários. Os fornecedores de segurança cibernética não têm como saber se os usuários instalarão os patches imediatamente.

O problema da posição privilegiada

As ferramentas de segurança cibernética ocupam os pontos mais sensíveis da infraestrutura de uma organização. Os agentes de detecção de endpoint são executados com acesso no nível do kernel. As plataformas SIEM consomem logs de todos os sistemas. Os provedores de identidade detêm a chave de todas as contas. Os firewalls ficam na fronteira entre redes confiáveis e não confiáveis.

Quando os produtos de segurança constituem o núcleo de defesa de uma organização, eles assumem a responsabilidade ainda maior de seguir os princípios Secure by Design. Os fornecedores do nosso setor desempenham um papel fundamental na proteção dos clientes, e essa confiança vem acompanhada de expectativas quanto à forma como os produtos são projetados.

Essa posição privilegiada significa que uma vulnerabilidade em um produto de segurança não expõe apenas a si, mas também expõe tudo o que foi projetado para proteger. Um invasor que compromete um agente de detecção e resposta de endpoint (EDR) não controla apenas uma ferramenta — ele controla o endpoint com os privilégios mais elevados. Uma falha em um dispositivo VPN não apenas interrompe o acesso remoto, mas, sim, proporciona ao invasor um caminho direto que contorna todos os controles de perímetro.

O que acontece quando se ignora a segurança no design?

As consequências de negligenciar os princípios Secure by Design estão bem documentadas, mas se esses princípios não forem devidamente seguidos, isso deixará as empresas, os usuários e a Internet, como um todo, menos seguros.

- **Custos crescentes das violações.** Quando vulnerabilidades são descobertas após o lançamento, corrigi-las é exponencialmente mais caro do que resolvê-las durante o desenvolvimento.

- **Perda de confiança.** Clientes, órgãos reguladores e parceiros perdem a confiança em organizações que passam por incidentes de segurança repetidamente. Os danos à reputação podem perdurar por anos após a remediação técnica.

- **Riscos regulatórios e legais.** Governos em todo o mundo estão tornando as regulamentações de segurança cibernética mais rigorosas. A Cyber Resilience Act (CRA) da União Europeia, por exemplo, é uma lei que imporá requisitos de segurança obrigatórios aos produtos com componentes digitais vendidos na Europa. As organizações que ignoram os princípios Secure by Design correm o risco de incorrer em não conformidade, multas e exclusão do mercado.

- **Riscos à segurança nacional.** As infraestruturas críticas, tais como redes elétricas, estações de tratamento de água e sistemas de saúde, dependem cada vez mais de dispositivos e sistemas conectados à Internet. Os produtos nesses ambientes que não são seguros abrem brechas para adversários patrocinados pelo Estado e operadores de ransomware, com a possibilidade de consequências que podem conturbar a vida cotidiana de uma pessoa.

- **Fadiga perpétua de patches.** Sem bases sólidas, as organizações ficam presas em um ciclo reativo: procurando vulnerabilidades, priorizando patches, testando atualizações e implantando correções — repetidamente. Isso consome recursos que poderiam ser destinados a investigações mais aprofundadas em segurança cibernética.

Como escolher um firewall Secure by Design

Ao avaliar seu próximo firewall, garantir que ele seja verdadeiramente seguro desde a concepção deve ser uma prioridade máxima. No entanto, pode ser difícil destrinchar o discurso de marketing dos fornecedores para saber quais recursos a solução realmente oferece. Os critérios a seguir o ajudarão a identificar as principais características a serem consideradas ao selecionar um firewall desenvolvido genuinamente com base nos princípios Secure by Design:

1. Arquitetura reforçada

Como vimos, é de extrema importância que a arquitetura do firewall seja projetada, do código até o núcleo do sistema, sob o princípio Secure by Design. Mas, é claro, é muito difícil saber o que um determinado fabricante de firewall fez para reforçar a segurança do seu produto. A maioria dos fornecedores afirma que seus produtos são seguros, mas são os resultados concretos o que realmente conta.

Estes são alguns pontos óbvios que devem ser verificados:

- Suporte à autenticação multifator (MFA) em todas as áreas do firewall (administração, VPN, portais).
- Suporte integrado para Zero Trust Network Access (ZTNA), para que você possa eliminar a necessidade de acesso remoto por VPN.
- Gerenciamento remoto seguro que NÃO requer SSH nem login remoto no dispositivo pela Internet.
- Portais do usuário reforçados e conteinerizados, caso estejam expostos à Internet.
- Atualizações recentes em suas notas de versão que indicam que estão adotando os princípios Secure by Design.

2. Aplicação automática de patches contra vulnerabilidades sem tempo de inatividade

Um dos principais vetores de ataque contra a infraestrutura de rede são as vulnerabilidades sem patches. Uma vez que uma vulnerabilidade é descoberta, podem se passar semanas até que ela seja efetivamente corrigida. Muitos usuários sofrem com o constante lançamento de novos patches que são obrigados a aplicar, tendo de aceitar o tempo de inatividade associado a eles como algo regular.

Facilite a sua vida e garanta que o seu sistema receba patches rapidamente trabalhando com um fornecedor que ofereça atualizações OTA, que não exigem tempo de inatividade. Não se deixe enganar pelas chamadas de marketing de "atualizações automáticas" — verifique o que realmente querem dizer com isso. Se uma atualização exige reinicialização e tempo de inatividade, ela não é "automática".

3. Auditoria automática de riscos de configuração

Outro fator comum que contribui para um incidente de segurança é a configuração incorreta do firewall. Infelizmente, a maioria dos firewalls não lhe dirá que está mal-configurada, deixando possíveis brechas que podem ser exploradas. Exija que seu próximo firewall faça auditorias de forma automática e contínua das configurações importantes e o informe sobre as definições de alto risco, para que você possa resolvê-las facilmente.

4. Monitoramento proativo pelo fornecedor

Quando a maioria dos firewalls for alvo de um ataque, é provável que você só descubra quando já for tarde demais. Felizmente, isso não acontece com todos os firewalls. Escolha um fornecedor de firewall que monitore seus próprios produtos remotamente, coletando dados de telemetria para detectar sinais de comprometimento logo no início de um ataque. Os fornecedores devem estar dispostos e aptos a agir rapidamente caso seja detecta alguma atividade anormal, entrando em contato imediatamente com você ou com o seu parceiro de segurança cibernética para ajudar a identificar e remediar o ataque.

5. Um fornecedor comprometido com a segurança no design

Nem precisaria ser dito, mas se você chegou até aqui, provavelmente já tem em mente um fornecedor que está claramente comprometido com os princípios Secure by Design. Mas não se baseie apenas no que dizem. Analise o histórico recente da empresa, os relatórios de progresso e suas notas de versão para compreender exatamente o quanto ele está comprometido com a sua segurança.

O compromisso da Sophos com o Secure by Design

Em 8 de maio de 2024, a Sophos tornou-se uma das primeiras organizações a comprometer-se com a iniciativa Secure by Design da agência CISA de segurança cibernética, que se concentra nos sete pilares fundamentais da segurança tecnológica e de produtos:

1. Autenticação multifator.
2. Senhas padrão.
3. Redução de classes inteiras de vulnerabilidade.
4. Patches de segurança.
5. Política de divulgação de vulnerabilidade.
6. CVEs.
7. Evidência de invasões.

Em consonância com nossos valores organizacionais fundamentais em torno da transparência, o princípio Secure by Design tem sido uma força orientadora à medida que avaliamos e aprimoramos continuamente nossas práticas de segurança.

Publicamos nossos compromissos de melhoria e divulgamos o progresso que estamos alcançando em relação aos sete pilares fundamentais da estrutura Secure by Design. É claro que a segurança cibernética está em constante evolução e o trabalho nunca está "concluído". Continuar a aperfeiçoar e aprimorar a aplicação dos princípios Secure by Design em todo o nosso portfólio é uma parte constante e fundamental da nossa filosofia.

A Sophos se destaca por oferecer vários elementos importantes do Secure by Design que melhoram significativamente a postura de segurança do Sophos Firewall e que facilitam muito a sua vida. O Sophos Firewall é o único firewall do mercado que oferece patches de segurança realmente automáticos, sem qualquer tempo de inatividade. Somos também o único fornecedor que monitora ativamente toda a nossa base de firewalls instalados em busca de quaisquer sinais de ataque, o que nos permite responder rapidamente para ajudar você e seu parceiro de segurança cibernética na remediação de problemas e garantir imediatamente que todos os outros clientes estejam protegidos contra ataques semelhantes.

Conclusões

Em consonância com nossos valores organizacionais fundamentais em torno da transparência, o princípio Secure by Design tem sido uma força orientadora à medida que avaliamos e aprimoramos continuamente nossas práticas de segurança.

A versão mais recente (v22) do Sophos Firewall amplia os elementos Secure by Design ainda mais, reforçando significativamente a postura de segurança do firewall. Esses elementos incluem:

- Um novo recurso de verificação de status de integridade para reduzir o risco de uma configuração incorreta que possa levar a um possível ataque.
- Um painel de controle totalmente novo, redesenhado para oferecer segurança e escalabilidade máximas, o que elimina toda uma classe de vulnerabilidades.
- A inclusão do Sophos XDR Linux Sensor, que aprimora o monitoramento em tempo real da integridade dos sistemas de toda a nossa base de clientes por nossas próprias equipes de segurança, permitindo que identifiquem e respondam a ataques com maior rapidez.
- As atualizações de firmware agora são criptografadas e têm certificados vinculados para garantir a autenticidade.
- Uma atualização para o mais recente mecanismo antimalware da Sophos com detecção aprimorada de dia zero em tempo real de ameaças emergentes.

Nosso trabalho na campanha Pacific Rim nos proporcionou uma visão privilegiada de como atuam os agentes de ameaça mais determinados e bem-equipados e o que é realmente necessário para nos defendermos contra eles. A campanha reafirmou que os adversários não ficam esperando que os pontos fracos surjam — eles procuram, ativamente, por falhas em projetos, lacunas de configuração e sistemas sem patches na infraestrutura global.
Essa experiência moldou diretamente nossa abordagem Secure by Design.

Ela destacou que as defesas modernas devem começar por reduzir a superfície de ataque no nível do produto, desenvolvendo padrões robustos, restringindo processos de autenticação e eliminando oportunidades de uso indevido muito antes que uma vulnerabilidade chegue a ser explorada.

O caminho a seguir

O Secure by Design não elimina todas as vulnerabilidades nem isenta as organizações da necessidade de vigilância contínua. Mas ele se tornou um pilar fundamental da segurança cibernética para reduzir a superfície de ataque. A questão não é mais se o princípio Secure by Design é uma boa ideia. O que importa agora é a rapidez com que ele é adotado.

SOPHOS

Pronto para avaliar seu programa de segurança cibernética?

Fale com um especialista da Sophos ainda hoje.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com