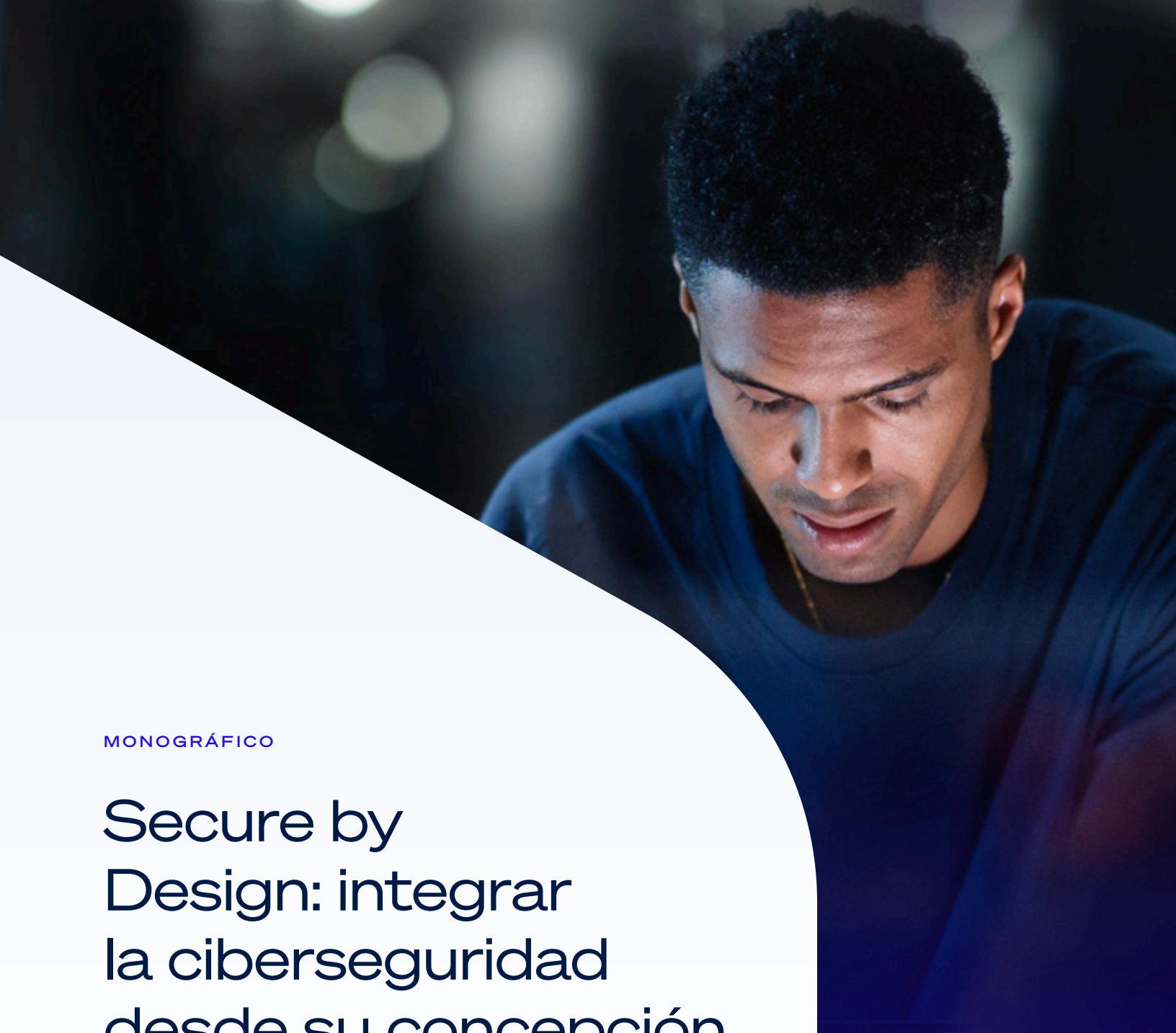

MONOGRÁFICO

Secure by Design: integrar la ciberseguridad desde su concepción

Por qué es importante esta filosofía y cómo reduce su superficie de ataque desde el interior

SOPHOS

Resumen ejecutivo

«Secure by Design» es una filosofía de desarrollo de software que considera la seguridad como un requisito fundamental, en lugar de un elemento añadido a posteriori.

En lugar de crear primero un producto y añadirle posteriormente medidas de seguridad, el enfoque Secure by Design exige que las consideraciones de seguridad se integren en todas las fases del ciclo de vida del desarrollo, desde la arquitectura y el diseño hasta la programación, las pruebas, el despliegue y el mantenimiento.

La premisa central es sencilla: si se diseña algo de forma segura desde cero, los usuarios estarán protegidos de forma predeterminada, en lugar de estarlo solo cuando sepan cómo configurar los parámetros adecuados o cuando se subsanen las brechas de seguridad a posteriori.

En la práctica, esto implica adoptar principios como el del privilegio mínimo (que consiste en conceder a los usuarios y a los procesos solo el acceso mínimo que necesitan), valores predeterminados seguros (que consisten en suministrar los productos con la configuración más segura lista para usar), una defensa en profundidad (que consiste en superponer varios controles de seguridad para que ningún fallo aislado resulte catastrófico), así como la eliminación de categorías enteras de vulnerabilidades gracias a lenguajes, marcos y modelos de diseño más seguros.

La premisa central es sencilla:

si se diseña algo de forma segura desde cero, los usuarios estarán protegidos de forma predeterminada, en lugar de estarlo solo cuando sepan cómo activar los parámetros adecuados o cuando se subsanen las brechas de seguridad a posteriori.

¿Por qué se introdujo el enfoque Secure by Design?

Durante décadas, muchas empresas del sector tecnológico han funcionado según el modelo de «lanzar rápido, parchear después». Una de las consecuencias de ese legado es que la ciberseguridad puede considerarse simplemente como un centro de costes, algo que ralentiza los lanzamientos y frustra a los desarrolladores. Las repercusiones se están manifestando en tiempo real: vulnerabilidades que se dan a conocer con frecuencia, parches de emergencia elaborados a toda prisa y filtraciones que suponen pérdidas de miles de millones a las organizaciones, al tiempo que exponen los datos personales de cientos de millones de personas.

Las vulnerabilidades de Ivanti Connect Secure, el exploit Log4Shell en una biblioteca de código abierto de uso generalizado y las vulnerabilidades de MOVEit Transfer han demostrado que la seguridad reactiva es incapaz de seguir el ritmo de unos adversarios decididos.

Consciente de este desequilibrio, la CISA (Cybersecurity and Infrastructure Security Agency) de EE. UU., junto con sus Partners internacionales, publicó en 2023 unas directrices oficiales de Secure by Design, en las que instaba a los fabricantes de tecnología a asumir la responsabilidad de los resultados en materia de seguridad de sus clientes.

Los principios de Secure by Design establecen que la responsabilidad en materia de seguridad debe recaer en los proveedores que fabrican los productos, y no en los usuarios finales que los despliegan. Esto ha cambiado la forma en que los proveedores abordan la seguridad de los productos tecnológicos, desplazando el debate de la responsabilidad individual («los usuarios deben instalar las actualizaciones sin demora») a la responsabilidad del fabricante («los proveedores deben comercializar productos que sean seguros desde el primer día»).

Por qué el enfoque Secure by Design es fundamental para las soluciones de ciberseguridad

Nos hace tomar conciencia de una forma contundente: en ocasiones, incluso las herramientas de seguridad pueden convertirse en el punto de entrada de un ataque. Y, sin embargo, esto ocurre con una frecuencia preocupante.

Esto pone de manifiesto una debilidad crítica para muchas organizaciones: una vez que un dispositivo perimetral queda expuesto, los atacantes seguirán atacándolo repetidamente hasta que se haya protegido por completo. Los firewalls y otros sistemas perimetrales pueden seguir siendo vulnerables, incluso aunque haya una corrección disponible. Según un análisis reciente de los incidentes remediados por Sophos, que abarca todas las vulnerabilidades confirmadas que han sido explotadas, el tiempo medio transcurrido entre la publicación de un aviso o un parche por parte del proveedor y la explotación de dicha vulnerabilidad por parte de un atacante ascendió a 322 días, lo que supone casi un año entero de oportunidades para los ciberdelincuentes. Los proveedores de ciberseguridad no pueden dar por sentado que los usuarios van a aplicar los parches de inmediato.

El problema de la posición privilegiada

Las herramientas de ciberseguridad ocupan los puntos más sensibles de la infraestructura de una organización. Los agentes de detección de las soluciones para endpoints se ejecutan con acceso a nivel del kernel. Las plataformas SIEM recopilan registros de todos los sistemas. Los proveedores de identidad custodian las claves de todas las cuentas. Los firewalls se sitúan en la frontera entre las redes de confianza y las que no lo son.

Cuando los productos de seguridad constituyen el núcleo de las defensas de una organización, asumen una mayor responsabilidad a la hora de cumplir los principios de Secure by Design. Los proveedores de nuestro sector desempeñan un papel fundamental a la hora de proteger a los clientes, y esa confianza conlleva unas expectativas en cuanto al diseño de los productos.

Esta posición privilegiada implica que una vulnerabilidad en un producto de seguridad no solo pone en peligro al propio producto, sino también a todo aquello que se supone que debe proteger. Un atacante que compromete un agente de detección y respuesta para endpoints (EDR) no solo se hace con el control de una herramienta, sino que se hace con el control del endpoint con los privilegios más elevados. Una vulnerabilidad en un dispositivo VPN no solo impide el acceso remoto, sino que ofrece al adversario un acceso directo que elude todos los controles perimetrales.

Qué pasa cuando no se respeta el principio de Secure by Design

Las consecuencias de no seguir los principios de Secure by Design están bien documentadas y, si no se aplican correctamente, reducen la seguridad de las empresas, los usuarios e Internet en su conjunto.

- **Aumento de los costes derivados de las filtraciones de seguridad.** Cuando se detectan vulnerabilidades tras el lanzamiento, subsanarlas resulta exponencialmente más costoso que abordarlas durante la fase de desarrollo.

- **Pérdida de confianza.** Los clientes, los organismos reguladores y los Partners pierden la confianza en las organizaciones que sufren incidentes de seguridad de forma reiterada. Los daños a la reputación pueden prolongarse durante años después de que se hayan remediado los problemas técnicos.

- **Riesgos normativos y legales.** Los gobiernos de todo el mundo están endureciendo la normativa en materia de ciberseguridad. La Ley de Ciberresiliencia de la Unión Europea, por ejemplo, impondrá requisitos de seguridad obligatorios a los productos con componentes digitales que se comercialicen en Europa. Las organizaciones que no respeten los principios de Secure by Design se exponen a incurrir en incumplimientos, a multas y a la exclusión del mercado.

- **Riesgos para la seguridad nacional.** Las infraestructuras críticas, como las redes eléctricas, las plantas de tratamiento de agua y los sistemas sanitarios, dependen cada vez más de dispositivos y sistemas conectados a Internet. En estos entornos, los productos que no están protegidos de forma predeterminada constituyen una puerta abierta para los ciberdelincuentes patrocinados por Estados y para los autores de ransomware, con las consiguientes consecuencias que pueden alterar la vida cotidiana de las personas afectadas.

- **Saturación por la gestión de parches** Sin unos cimientos sólidos, las organizaciones se ven atrapadas en un círculo vicioso: deben detectar vulnerabilidades, priorizar los parches, probar las actualizaciones e implementar los parches, una y otra vez. Esto consume recursos que podrían destinarse a investigaciones más exhaustivas en materia de ciberseguridad.

Cómo elegir un firewall Secure by Design

A la hora de evaluar su próximo firewall, debe asegurarse ante todo que siga el principio Secure by Design. Sin embargo, puede resultar difícil dejar de lado los argumentos de marketing de los proveedores para comprender qué funcionalidades ofrece realmente una solución. Los siguientes criterios le ayudarán a identificar las características clave que debe tener en cuenta a la hora de elegir un firewall diseñado según los auténticos principios de Secure by Design:

1. Arquitectura reforzada

Como hemos visto, es de vital importancia que la arquitectura del firewall esté diseñada, desde el código hasta el núcleo del sistema, según el principio de Secure by Design. Pero, por supuesto, es muy difícil saber qué medidas concretas ha tomado un proveedor de firewalls concreto para reforzar la seguridad de su producto. La mayoría de los proveedores afirman que sus productos son seguros, pero, en última instancia, su historial reciente revelará la verdad.

He aquí algunos aspectos básicos que debe comprobar:

- Compatibilidad con la autenticación multifactor en todas las áreas del firewall (administración, VPN, portales).
- Compatibilidad integrada con Zero Trust Network Access (ZTNA), lo que le permite prescindir de una VPN de acceso remoto.
- Gestión remota segura que NO requiera SSH ni el inicio de sesión remoto en el dispositivo desde Internet.
- Portales de usuario reforzados y en contenedores, en caso de que estén expuestos a Internet.
- La mención, en las notas de la edición más recientes, de que aplican los principios de Secure by Design.

2. Aplicación automática de parches sin interrupciones del servicio

Uno de los principales vectores de ataque contra la infraestructura de red son las vulnerabilidades sin parchear. Cuando se detecta una vulnerabilidad, pueden pasar semanas hasta que se corrige. Muchos usuarios sufren de saturación por la gestión de parches, ya que tienen que instalar constantemente nuevos parches y soportar con regularidad los tiempos de inactividad que ello conlleva.

Gane en tranquilidad y asegúrese de que su sistema se parchee rápidamente colaborando con un proveedor que ofrezca actualizaciones OTA que no requieran tiempo de inactividad. No se deje engañar por las promesas de marketing de las llamadas «actualizaciones automáticas»: compruebe qué significa realmente «automática». Las actualizaciones que siguen requiriendo un reinicio y un tiempo de inactividad no son «automáticas».

3. Auditoría automática de los riesgos de configuración

Otro factor habitual que contribuye a los incidentes de seguridad es la configuración incorrecta del firewall. Por desgracia, la mayoría de los firewalls no le avisan de que están mal configurados, con lo que dejan una posible brecha que podría ser explotada. Exija que su próximo firewall audite de forma automática y continua las configuraciones importantes y le avise de los parámetros de alto riesgo para que pueda abordarlos fácilmente.

4. Supervisión proactiva por parte del proveedor

Cuando la mayoría de los firewalls sufren un ataque, es probable que usted no se entere hasta que sea demasiado tarde. Por suerte, no ocurre así con todos los firewalls. Elija un proveedor de firewalls que monitorice sus propios productos de forma remota y recopile datos de telemetría para detectar a tiempo cualquier indicio de vulneración. Los proveedores deben estar dispuestos y ser capaces de actuar con rapidez si se detecta una actividad anómala, poniéndose en contacto rápidamente con usted o con su Partner de ciberseguridad para ayudar a identificar y remediar el ataque.

5. Un proveedor comprometido con el enfoque Secure by Design

No hace falta decirlo, pero si ha llegado hasta aquí, probablemente ya tenga en mente un proveedor que apueste claramente por los principios del enfoque Secure by Design. Pero no se fíe solo de su palabra. Indague en su historial reciente, sus informes de progreso y sus notas de la edición para comprender exactamente hasta qué punto se toman en serio su seguridad.

El compromiso de Sophos con Secure by Design

El 8 de mayo de 2024, Sophos se convirtió en una de las primeras organizaciones en adherirse a la iniciativa «Secure by Design» de la CISA (Cybersecurity and Infrastructure Security Agency) de EE. UU., que se centra en siete pilares fundamentales de la seguridad tecnológica y de los productos:

1. Autenticación multifactor.
2. Contraseñas por defecto.
3. Reducción de categorías enteras de vulnerabilidades.
4. Parches de seguridad.
5. Política de divulgación de vulnerabilidades.
6. Vulnerabilidades y exposiciones comunes (CVE).
7. Indicios de intrusiones.

En consonancia con nuestros valores organizativos centrales en torno a la transparencia, el enfoque Secure by Design ha sido el principio rector a la hora de evaluar y mejorar continuamente nuestras prácticas de seguridad.

Hemos publicado nuestros compromisos de mejora y compartimos públicamente los avances que vamos logrando en relación con los siete pilares fundamentales del marco Secure by Design. Por supuesto, la ciberseguridad está en constante evolución y esta labor nunca «termina». Seguir perfeccionando y mejorando la aplicación de los principios de Secure by Design en toda nuestra cartera de productos es un elemento fundamental y central de nuestra filosofía.

Sophos destaca por ofrecer varias funcionalidades importantes de Secure by Design que mejoran significativamente la postura de seguridad de Sophos Firewall, al tiempo que le facilitan enormemente el trabajo. Sophos Firewall es el único firewall del mercado que ofrece parches de seguridad OTA realmente automáticos que requieren una interrupción del servicio nula. También somos el único proveedor que supervisa de forma activa toda nuestra base de firewalls instalados en busca de cualquier indicio de ataque, lo que nos permite responder rápidamente para ayudarle a usted y a su Partner de ciberseguridad a remediarlo, y garantizar de inmediato que todos los demás clientes estén protegidos frente a ataques similares.

Conclusiones

En consonancia con nuestros valores organizativos centrales en torno a la transparencia, el enfoque Secure by Design ha sido el principio rector a la hora de evaluar y mejorar continuamente nuestras prácticas de seguridad.

La última versión (v22) de Sophos Firewall amplía aún más sus capacidades Secure by Design, lo que refuerza considerablemente la postura de seguridad del firewall. Entre estas capacidades se incluyen:

- Una nueva función de comprobación del estado de seguridad para reducir el riesgo de que un error de configuración dé lugar a un posible ataque.
- Un plano de control totalmente nuevo, rediseñado para ofrecer la máxima seguridad y escalabilidad, que elimina una categoría entera de vulnerabilidades.
- La incorporación de Sophos XDR Linux Sensor, que mejora la supervisión en tiempo real de la integridad de los sistemas de toda nuestra base de clientes por parte de nuestros propios equipos de seguridad, lo que les permite identificar los ataques y responder a ellos con mayor rapidez.
- Las actualizaciones de firmware ahora están cifradas y cuentan con un certificado fijado para garantizar su autenticidad.
- Una actualización al motor antimalware más reciente de Sophos, con detección mejorada en tiempo real de amenazas emergentes y de día cero.

El trabajo que realizamos en la campaña Pacific Rim nos permitió observar de primera mano cómo operan los ciberdelincuentes decididos y con recursos suficientes, y lo que realmente se necesita para defenderse de ellos. La campaña nos confirmó que los adversarios no se limitan a esperar a que surjan vulnerabilidades, sino que buscan activamente fallos de diseño, carencias en la configuración y sistemas sin parchear en toda la infraestructura global. Esa experiencia influyó directamente en nuestro enfoque Secure by Design.

Subrayó que las defensas modernas deben partir de la reducción de la superficie de ataque a nivel del producto, incorporando configuraciones predeterminadas robustas, reforzando los procesos de autenticación y eliminando posibles usos indebidos mucho antes de que una vulnerabilidad salga a la luz.

El camino a seguir

El enfoque Secure by Design no elimina todas las vulnerabilidades, ni exime a las organizaciones de mantener una vigilancia constante. Sin embargo, se ha convertido en un pilar fundamental de la ciberseguridad para reducir la superficie de ataque. La cuestión ya no es si el principio de Secure by Design es una buena idea, sino la rapidez con la que se adopta.

SOPHOS

¿Listo para evaluar su programa de ciberseguridad?

Póngase en contacto con un experto de Sophos hoy mismo.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com