TLP:CLEAR

Cambio del equilibrio de los riesgos de ciberseguridad: principios y enfoques para el software seguro desde el diseño

Publicación: 13 de abril de 2023

Agencia de Seguridad Cibernética y de Infraestructura (Cybersecurity and Infrastructure Security Agency)

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Índice

DESCRIPCIÓN GENERAL: VULNERABLE DESDE EL DISEÑO

La tecnología está integrada en casi todas las facetas de la vida diaria. Los sistemas orientados a Internet están conectados a sistemas críticos que repercuten de forma directa en nuestra prosperidad económica, nuestros medios de vida e incluso nuestra salud, desde la gestión de la identidad personal hasta la atención médica. Solo a modo de ejemplo, infracciones cibernéticas han provocado que hospitales cancelen cirugías y desvíen la atención de pacientes a nivel mundial. La tecnología insegura y las vulnerabilidades de los sistemas críticos pueden ser propensas a intrusiones cibernéticas malintencionadas, lo que conlleva graves riesgos potenciales para la[1] seguridad.

Ahora más que nunca, es crucial que los fabricantes de tecnología coloquen a la seguridad desde el diseño y a la seguridad por defecto en el centro de los procesos de diseño y desarrollo de productos. Algunos proveedores han dado grandes pasos para hacer avanzar a la industria en el protección del software, mientras que otros se han quedado rezagados. Las agencias autoras alientan enfáticamente a todos los fabricantes de tecnología a que construyan sus productos de forma que eviten que los clientes tengan que realizar constantemente tareas de supervisión, actualizaciones rutinarias y control de daños en sus sistemas para mitigar las intrusiones cibernéticas. Se anima a los fabricantes a asumir la responsabilidad de mejorar los resultados de seguridad de sus clientes. Históricamente, los fabricantes de tecnología han confiado en solucionar las vulnerabilidades detectadas después de que los clientes hayan utilizado los productos, lo que les obliga a aplicar esos parches por su cuenta. Solo mediante la incorporación de prácticas de seguridad desde el diseño romperemos el círculo vicioso de crear y aplicar correcciones.

Para alcanzar este elevado nivel de seguridad del software, las agencias autoras animan a los fabricantes a dar prioridad a la integración de la seguridad de los productos como requisito previo fundamental para las prestaciones y la rapidez de comercialización. Con el tiempo, los equipos de ingeniería podrán establecer un nuevo ritmo estable en el que la seguridad esté realmente integrada y requiera menos esfuerzo para mantenerla. Como reflejo de esta perspectiva, la Unión Europea refuerza la importancia de la seguridad de los productos en la Ley de Resiliencia Cibernética, que enfatiza que los fabricantes deben implementar medidas de seguridad durante todo el ciclo de vida de un producto para evitar que los fabricantes introduzcan productos vulnerables en el mercado.

Para crear un futuro en el que la tecnología y los productos asociados sean más seguros para los clientes, las agencias autoras instan a los fabricantes a renovar sus programas de diseño y desarrollo para permitir que solo se envíen a los clientes productos seguros desde el diseño y seguros por defecto. Los productos seguros desde el diseño son aquellos en los que la seguridad de los clientes es un objetivo empresarial fundamental, no solo una característica técnica. Los productos seguros desde el diseño empiezan con ese objetivo antes de iniciar el desarrollo. Los productos seguros por defecto son aquellos que son seguros para usar "desde el primer momento", con pocos o ningún cambio de configuración necesario, y cuyas características de seguridad están disponibles sin costo adicional. Juntos, estos dos principios

[1] Las agencias autoras reconocen que el término "seguridad" tiene múltiples significados según el contexto en que se utilice. A los efectos de esta guía, "seguridad" se referirá a elevar los estándares de seguridad tecnológica para proteger a los clientes de actividades cibernéticas maliciosas.

trasladan gran parte de la carga de mantener la seguridad a los fabricantes y reducen las posibilidades de que los clientes sean víctimas de incidentes de seguridad derivados de configuraciones erróneas, parches insuficientemente rápidos o muchos otros problemas comunes.

La Agencia de Seguridad Cibernética y de Infraestructura (CISA, por sus siglas en inglés), la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), la Oficina Federal de Investigación (FBI, por sus siglas en inglés) y los siguientes socios[2] internacionales ofrecen las recomendaciones de esta guía como hoja de ruta para que los fabricantes de tecnología garanticen la seguridad de sus productos:

- Centro Australiano de Seguridad Cibernética (ACSC, por sus siglas en inglés)
- Centro Canadiense de Seguridad Cibernética (CCCS, por sus siglas en inglés)
- Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC-UK, por sus siglas en inglés)
- Oficina Federal de Seguridad de la Información (BSI, por sus siglas en inglés) de Alemania
- Centro Nacional de Seguridad Cibernética de los Países Bajos (NCSC-NL, por sus siglas en inglés)
- Equipo de Respuesta a Emergencias Informáticas de Nueva Zelanda (CERT NZ, por sus siglas en inglés) y Centro Nacional de Seguridad Cibernética de Nueva Zelanda (NCSC-NZ, por sus siglas en inglés)

Las agencias autoras reconocen las contribuciones de muchos socios del sector privado para promover la seguridad desde el diseño y la seguridad por defecto. Este producto tiene como objetivo promover una conversación internacional sobre prioridades, inversiones y decisiones clave necesarias para lograr un futuro donde la tecnología sea segura y resistente desde el diseño y por defecto. Para ello, las agencias autoras solicitan comentarios sobre este producto a las partes interesadas y tienen la intención de convocar una serie de sesiones de escucha para perfeccionar, especificar y avanzar en nuestra orientación para lograr nuestros objetivos comunes.

Para obtener más información sobre la importancia de la seguridad de los productos, consulte el artículo de la Agencia de Seguridad Cibernética y de Infraestructura (CISA), El costo de la tecnología insegura y qué podemos hacer al respecto.

Seguridad desde el diseño

"Seguridad desde el diseño" significa que los productos tecnológicos se construyen de una manera que les permita protegerse razonablemente contra ciberataques maliciosos que logran acceder a dispositivos, datos e infraestructura conectada. Los fabricantes de software deben realizar una evaluación de riesgos para identificar y enumerar las amenazas cibernéticas prevalentes de los sistemas críticos y luego incluir protecciones en los modelos de productos que tengan en cuenta el panorama en evolución de las amenazas cibernéticas.

También se recomiendan prácticas seguras de desarrollo de tecnología de la información (IT, por sus siglas en inglés) y múltiples capas de defensa, conocidas como "defensa en profundidad", para evitar que actividades de adversarios comprometan los sistemas u obtengan acceso no autorizado a datos confidenciales. Las agencias autoras recomiendan que los fabricantes utilicen un modelo de amenaza personalizado durante la etapa de desarrollo del producto para abordar todas las amenazas potenciales de un sistema y tener en cuenta el

[2] En adelante, denominadas "agencias autoras".

proceso de implementación de cada sistema.

Las agencias autoras instan a los fabricantes a adoptar un enfoque de seguridad integral para sus productos y plataformas. El desarrollo de seguridad desde el diseño requiere la inversión de recursos significativos por parte de los fabricantes de software en cada capa del proceso de diseño y desarrollo del producto que no se pueden "integrar" más adelante. Se requiere un fuerte liderazgo por parte de los principales ejecutivos del fabricante para hacer de la seguridad una prioridad empresarial, no solo una característica técnica. Esta colaboración entre líderes empresariales y equipos técnicos se extiende desde las etapas iniciales de diseño y desarrollo hasta la implementación y el mantenimiento una vez que el producto está en manos del cliente. Se alienta a los fabricantes a hacer concesiones e inversiones difíciles, incluidas aquellas que serán "invisibles" para los clientes, como migrar a lenguajes de programación que eliminen vulnerabilidades generalizadas. Deberían priorizar las características, los mecanismos y la implementación de herramientas que protejan a los clientes en lugar de las características del producto que parecen atractivas, pero amplían la superficie de ataque.

No existe una solución única para poner fin a la amenaza persistente de los actores cibernéticos maliciosos que explotan las vulnerabilidades tecnológicas, y los productos que son "seguros desde el diseño" seguirán sufriendo vulnerabilidades; sin embargo, un gran conjunto de vulnerabilidades se debe a un subconjunto relativamente pequeño de causas fundamentales. Los fabricantes deben desarrollar hojas de ruta escritas para alinear sus carteras de productos existentes con prácticas de diseño más seguras, asegurándose de desviarse solo en situaciones excepcionales.

Las agencias autoras reconocen que apropiarse de los resultados de seguridad para los clientes y garantizar este nivel de seguridad del cliente puede aumentar los costos de desarrollo. Sin embargo, invertir en prácticas de "seguridad desde el diseño" mientras se desarrollan nuevos productos tecnológicos y se mantienen los existentes puede mejorar sustancialmente la situación de seguridad de los clientes y reducir la probabilidad de que esta se vea comprometida. Los principios de "seguridad desde el diseño" no solo fortalecen la situación de seguridad para los clientes y la reputación de la marca para los desarrolladores, sino que también reduce los costos de mantenimiento y parches para los fabricantes a largo plazo.

La sección "Recomendaciones para fabricantes de software" que aparece más abajo proporciona una lista de prácticas y políticas de desarrollo de productos recomendadas que los fabricantes deben considerar.

Seguridad por defecto

"Seguridad por defecto" significa que los productos son resistentes a las técnicas de explotación predominantes desde el primer momento y sin cargo adicional. Estos productos protegen contra las amenazas y vulnerabilidades más frecuentes sin que los usuarios finales tengan que tomar medidas adicionales para protegerse. Los productos seguros por defecto están diseñados para que los clientes sean plenamente conscientes de que cuando se desvían de los valores predeterminados seguros, aumentan la probabilidad de ataques, a menos que implementen controles compensatorios adicionales.

- Una configuración segura debe ser la base predeterminada. Los productos seguros por defecto habilitan automáticamente los controles de seguridad más importantes necesarios para proteger a las empresas de actores cibernéticos maliciosos, además de brindar la capacidad de usar y configurar controles de seguridad adicionales sin costo extra.
- La complejidad de la configuración de seguridad no debería ser un problema para el cliente. El personal de IT de la organización con frecuencia está sobrecargado con responsabilidades operativas y de seguridad, lo que genera un tiempo limitado para comprender e implementar las implicaciones de seguridad y las mitigaciones necesarias para una postura sólida de ciberseguridad. Al optimizar la configuración segura de sus productos (es decir, asegurar la "ruta predeterminada"), los fabricantes pueden ayudar a sus clientes garantizando que sus productos se fabrican, distribuyen y utilizan de forma segura de acuerdo con los estándares de "seguridad por defecto".

Los fabricantes de productos que son "seguros por defecto" no cobran más por implementar configuraciones de seguridad adicionales. En cambio, las incluyen en el producto base, como se incluyen los cinturones de seguridad en todos los automóviles nuevos. La seguridad no es una opción de lujo, sino que se acerca más al estándar que todo cliente debería esperar sin negociaciones ni pagos adicionales.

RECOMENDACIONES PARA FABRICANTES DE SOFTWARE

Esta guía conjunta proporciona recomendaciones a los fabricantes para desarrollar una hoja de ruta escrita para implementar y garantizar la seguridad de IT. Las agencias autoras recomiendan que los fabricantes de software implementen las estrategias descritas en las secciones siguientes para apropiarse de los resultados de seguridad de sus clientes a través de principios de seguridad desde el diseño y por defecto.

Principios de seguridad para productos de software

Se anima a los fabricantes de tecnología a adoptar un enfoque estratégico que priorice la seguridad del software. Las agencias autoras desarrollaron los tres principios básicos siguientes para guiar a los fabricantes de software en la incorporación de la seguridad del software en sus procesos de diseño antes de desarrollar, configurar y enviar sus productos.

1. La carga de la seguridad no debe recaer únicamente en el cliente. Los fabricantes de software deberían responsabilizarse de los resultados de seguridad de las compras de sus clientes y desarrollar sus productos en consecuencia.

2. Adoptar métodos radicales de transparencia y rendición de cuentas. Los fabricantes de software deben enorgullecerse de ofrecer productos seguros, además de diferenciarse del resto de la comunidad de fabricantes en función de su capacidad para hacerlo. Esto puede incluir compartir información que aprenden de las implementaciones de sus clientes, como la adopción de mecanismos de autenticación sólidos de forma predeterminada. También incluye un fuerte compromiso para garantizar que los asesoramientos de vulnerabilidad y los registros de exposiciones y vulnerabilidades comunes (CVE, por sus siglas en inglés) asociados sean completos y precisos. Sin embargo, se debe tener cuidado con la tentación de considerar los CVE como una

métrica negativa, ya que dichos números también son una señal de una comunidad saludable de análisis y pruebas de código.

3. Construir estructura organizacional y liderazgo para lograr estos objetivos. Si bien la experiencia técnica en la materia es fundamental para la seguridad del producto, los ejecutivos sénior son los principales tomadores de decisiones para implementar cambios en una organización. El compromiso a nivel ejecutivo de los fabricantes de software de priorizar la seguridad como un elemento crítico del desarrollo de productos requiere el desarrollo de asociaciones con los clientes de una organización para comprender lo siguiente:
    a. Guía del escenario de implementación del producto junto con un modelo de amenazas personalizado.
    b. Implementación propuesta para que los controles de seguridad se alineen con los principios de seguridad por defecto.
    c. Estrategias de asignación de recursos adaptadas al tamaño de la empresa y la capacidad de reemplazar prácticas de desarrollo heredadas por prácticas de seguridad desde el diseño.
    d. La necesidad de mantener una línea de comunicación abierta para recibir comentarios interno y externos (por ejemplo, comentarios de empleados y clientes) respecto de cuestiones de seguridad del producto. La seguridad del software debe enfatizarse en foros internos (por ejemplo, reuniones generales o reuniones informales), así como en el marketing externo de productos y la interacción con los clientes.
    e. Mediciones de efectividad dentro de las implementaciones de clientes Los altos ejecutivos querrán saber cómo las inversiones en seguridad desde el diseño y por defecto están ayudando a los clientes a través de la disminución del ritmo de los parches de seguridad, la reducción de los errores de configuración y de la superficie de ataque.

Para habilitar estos tres principios, los fabricantes deberían considerar varias tácticas operativas para hacer evolucionar sus procesos de desarrollo.

Convoque reuniones de rutina con el liderazgo ejecutivo de la empresa para impulsar la importancia de la seguridad desde el diseño y la seguridad por defecto dentro de la organización. Se deben establecer políticas y procedimientos para recompensar a los equipos de producción que desarrollen productos que cumplan con estos principios, lo que podría incluir premios por implementar prácticas sobresalientes de seguridad de software o incentivos para escalar puestos y criterios de promoción.

Opere en torno a la importancia de la seguridad del software para el éxito empresarial. Por ejemplo, considere asignar un “líder de seguridad de software” o un “equipo de seguridad de software” que defienda las prácticas comerciales y de IT para vincular directamente los estándares de seguridad del software y la responsabilidad del fabricante. Los fabricantes deben asegurarse de contar con programas sólidos e independientes de evaluación y evaluación de la seguridad de sus productos.

Utilice un modelo de amenazas adaptado durante el desarrollo para priorizar los productos más críticos y de mayor impacto. Los modelos de amenazas consideran el caso de uso específico de un producto y permiten a los equipos de desarrollo fortalecer los productos. Finalmente, los líderes sénior deben responsabilizar a los equipos por la entrega de productos seguros como elemento clave de la excelencia y la calidad del producto.

Tácticas de seguridad desde el diseño

El Marco de desarrollo de software seguro (SSDF, por sus siglas en inglés), también conocido como SP 800-218, del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), es un conjunto central de prácticas de desarrollo de software seguro de alto nivel que se pueden integrar en cada etapa del ciclo de vida del desarrollo de software (SDLC, por sus siglas en inglés). Seguir estas prácticas puede ayudar a los productores de software a ser más eficaces a la hora de encontrar y eliminar vulnerabilidades en el software presentado, mitigar el impacto potencial de la explotación de vulnerabilidades y abordar las causas fundamentales de las vulnerabilidades para evitar que se repitan en el futuro.

Las agencias autoras fomentan el uso de tácticas seguras desde el diseño, incluidos principios que hacen referencia a las prácticas SSDF. Los fabricantes de software deben desarrollar una hoja de ruta escrita para adoptar prácticas de desarrollo de software más seguras desde el diseño en toda su cartera. La siguiente es una lista ilustrativa no exhaustiva de las prácticas recomendadas de la hoja de ruta:

- Lenguajes de programación seguros para la memoria (SSDF PW.6.1): Priorice el uso de lenguajes seguros para la memoria siempre que sea posible. Las agencias autoras reconocen que otras mitigaciones específicas de la memoria, como la aleatorización del diseño del espacio de direcciones (ASLR, por sus siglas en inglés), la integridad del flujo de control (CFI, por sus siglas en inglés) y la pruebas de exploración de vulnerabilidades mediante datos aleatorios son útiles para las bases de código heredadas, pero no son suficientes para considerarse seguras desde el diseño, ya que no previenen adecuadamente la explotación. Algunos ejemplos de lenguajes modernos seguros para la memoria incluyen C#, Rust, Ruby, Java, Go y Swift. Lea la hoja de información de seguridad de la memoria de la Agencia de Seguridad Nacional (NSA) para obtener más información.
- Base de hardware segura: Incorpore características arquitectónicas que permitan una protección de memoria detallada, como las descritas en el proyecto Instrucciones RISC Mejoradas de Hardware de Capacidad (CHERI, por sus siglas en inglés), que pueden ampliar las arquitecturas de conjunto de instrucciones (ISA, por sus siglas en inglés) de hardware convencional, al igual que otras características, como módulos de plataforma confiable y módulos de seguridad de hardware. Para obtener más información, visite la página web CHERI de la Universidad de Cambridge.
- Componentes de software seguros (SSDF PW 4.1): Adquiera y mantenga componentes de software bien protegidos (por ejemplo, bibliotecas de software, módulos, middleware, marcos) de desarrolladores externos, de código abierto y comerciales verificados para garantizar una seguridad sólida en los productos de software de consumo.

- Marcos de plantillas web (SSDF PW 5.1): Utilice marcos de plantillas web que implementen el escape automático de la entrada del usuario para evitar ataques web como secuencias de comandos entre sitios.
- Consultas parametrizadas (SSDF PW 5.1): Utilice consultas parametrizadas en lugar de incluir entradas del usuario en las consultas para evitar ataques de inyección SQL.
- Pruebas de seguridad de aplicaciones estáticas y dinámicas (SAST/DAST, por sus siglas en inglés) (SSDF PW.7.2, PW.8.2): Utilice estas herramientas para analizar el código fuente del producto y el comportamiento de las aplicaciones a fin de detectar prácticas propensas a errores. Estas herramientas cubren problemas que van desde la gestión inadecuada de la memoria hasta la construcción de consultas de bases de datos propensas a errores (por ejemplo, entradas de usuario sin escape que conducen a una inyección de SQL). Las herramientas SAST y DAST se pueden incorporar a los procesos de desarrollo y ejecutarse automáticamente como parte del desarrollo de software. SAST y DAST deben complementar otros tipos de pruebas, como pruebas unitarias y pruebas de integración, para garantizar que los productos cumplan con los requisitos de seguridad esperados. Cuando se identifican problemas, los fabricantes deben realizar un análisis de la causa raíz para abordar las vulnerabilidades de manera sistémica.
- Revisión de código (SSDF PW.7.1, PW.7.2): Procure que el código enviado a los productos pase por una revisión por pares realizada por otros desarrolladores para garantizar una mayor calidad.
- Lista de materiales de software (SBOM, por sus siglas en inglés) (SSDF PS.3.2, PW.4.1): Incorpore la creación de SBOM[3] para brindar visibilidad del conjunto de software que incluyen los productos.
- Programas de divulgación de vulnerabilidades (SSDF RV. 1.3): Establezca programas de divulgación de vulnerabilidades que permitan a los investigadores de seguridad informar sobre vulnerabilidades y recibir protección legal al hacerlo. Como parte de esto, los proveedores deben establecer procesos para determinar las causas fundamentales de las vulnerabilidades descubiertas. Dichos procesos deben determinar si la adopción de alguna de las prácticas de seguridad desde el diseño incluidas en este documento (u otras prácticas similares) habría evitado la introducción de la vulnerabilidad.
- Completitud de los puntos vulnerables y las exposiciones comunes (CVE, por sus siglas en inglés): Asegúrese de que los CVE publicados incluyan la causa raíz o la enumeración de debilidades comunes (CWE, por sus siglas en inglés) para permitir el análisis de las fallas de diseño de seguridad del software en toda la industria. Si bien garantizar que cada CVE sea correcto y completo puede llevar más tiempo, permite a entidades dispares detectar tendencias de la industria que benefician a todos los fabricantes y clientes. Para obtener más información sobre la gestión de vulnerabilidades, consulte la guía Categorización de vulnerabilidades específicas de las partes interesadas (SSVC, por sus siglas en inglés) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA).

[3] Algunas de las agencias autoras están explorando enfoques alternativos para obtener garantías de seguridad en toda la cadena de suministro de software.

- Defensa en profundidad: Diseñe la infraestructura de modo que el compromiso de un único control de seguridad no genere el compromiso de todo el sistema. Por ejemplo, garantizar que los privilegios de usuario se proporcionen de manera estricta y que se empleen listas de control de acceso puede reducir el impacto de una cuenta comprometida. Además, las técnicas de zona de pruebas de software pueden poner en cuarentena una vulnerabilidad para limitar el riesgo de una aplicación completa.
- Cumplimiento de los objetivos de desempeño de ciberseguridad (CPG, por sus siglas en inglés): Diseñe productos que cumplan con las prácticas de seguridad básicas. Los objetivos de desempeño de ciberseguridad (CPG) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) describen medidas básicas y fundamentales de ciberseguridad que las organizaciones deben implementar. Además, para conocer más formas de fortalecer la posición de su organización, consulte el Marco de evaluación cibernética del Reino Unido, que comparte similitudes con los objetivos de desempeño de ciberseguridad (CPG) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA). Si un fabricante no cumple con los objetivos de desempeño de ciberseguridad (CPG), como no exigir autenticación multifactor resistente a la suplantación de identidad para todos los empleados, entonces no se puede considerar que ofrece productos seguros desde el diseño.

Las agencias autoras reconocen que estos cambios son cambios significativos en la postura de una organización. Como tal, se debe priorizar su introducción en función de su criticidad, la complejidad y el impacto comercial. Estas prácticas pueden introducirse para software nuevo y ampliarse gradualmente para cubrir casos de uso y productos adicionales. En algunos casos, la criticidad y la postura de riesgo de un determinado producto pueden ameritar un cronograma acelerado para adoptar estas prácticas. En otros, las prácticas pueden introducirse en un código base heredado y corregirse con el tiempo.

Tácticas de seguridad por defecto

Además de adoptar prácticas de desarrollo seguras desde el diseño, las agencias autoras recomiendan que los fabricantes de software den prioridad a las configuraciones seguras por defecto en sus productos. Estos deberían esforzarse por actualizar los productos para que se ajusten a estas prácticas a medida que se actualizan. Por ejemplo:

- Eliminar las contraseñas por defecto: Los productos no deben venir con contraseñas predeterminadas que se compartan universalmente. Para eliminar las contraseñas por defecto, las agencias autoras recomiendan que los productos exijan a los administradores que establezcan una contraseña segura durante la instalación y la configuración.
    - Exigir la autenticación multifactor (MFA, por sus siglas en inglés) para usuarios privilegiados. Observamos que la administración de muchas implementaciones empresariales está a cargo de administradores que no han protegido sus cuentas con MFA. Dado que los administradores son objetivos de alto valor, los productos deberían hacer que la MFA sea una función para desactivar en lugar de habilitar. Además, el sistema debería solicitar periódicamente al administrador que se inscriba en MFA hasta que lo haya habilitado

correctamente en su cuenta. El NCSC de los Países Bajos tiene una guía paralela a la de la CISA; visite su hoja informativa sobre autenticación madura para obtener más información.

- Inicio de sesión único (SSO, por sus siglas en inglés): Las aplicaciones de IT deben implementar tecnología de inicio de sesión único a través de estándares abiertos modernos. Los ejemplos incluyen Security Assertion Markup Language (SAML) u OpenID Connect (OIDC). Esta capacidad debería estar disponible de forma predeterminada sin costo adicional.
- Registro seguro: Proporcione registros de auditoría de alta calidad a los clientes sin costo adicional. Los registros de auditoría son cruciales para detectar y escalar posibles incidentes de seguridad. También son cruciales durante la investigación de un incidente de seguridad sospechoso o confirmado. Considere las mejores prácticas, como proporcionar una integración sencilla con sistemas de gestión de eventos e información de seguridad (SIEM) con acceso a la interfaz de programación de aplicaciones (API, por sus siglas en inglés) que utiliza hora universal coordinada (UTC, por sus siglas en inglés), formato de zona horaria estándar y técnicas de documentación sólidas.
- Perfil de autorización de software: Los proveedores de software deben proporcionar recomendaciones sobre roles de perfil autorizados y su caso de uso designado. Los fabricantes deben incluir una advertencia visible que notifique a los clientes sobre un mayor riesgo si se desvían de la autorización del perfil recomendado. Por ejemplo, los médicos pueden ver todos los registros de los pacientes, pero un programador médico tiene acceso limitado a cierta información necesaria para programar citas.
- Seguridad orientada al futuro por encima de la compatibilidad con versiones anteriores: Con demasiada frecuencia, se incluyen funciones heredadas compatibles con versiones anteriores en los productos, y a menudo se habilitan, a pesar de causar riesgos para la seguridad del producto. Priorice la seguridad sobre la compatibilidad con versiones anteriores, lo que permitirá a los equipos de seguridad eliminar funciones inseguras incluso si eso significa provocar cambios importantes.
- Rastrear y reducir el tamaño de la “guía de refuerzo”: Reduzca el tamaño de las “guías de refuerzo” que se incluyen con los productos y esfuércese por garantizar que el tamaño se reduzca con el tiempo a medida que se lanzan nuevas versiones del software. Integre componentes de la “guía de refuerzo” como configuración predeterminada del producto. Las agencias autoras reconocen que las guías de refuerzo abreviadas son el resultado de una asociación continua con los clientes existentes e incluyen esfuerzos de muchos equipos de productos, incluida la experiencia del usuario (UX, por sus siglas en inglés).
- Considere las consecuencias de la configuración de seguridad para la experiencia del usuario: Cada nueva configuración aumenta la carga cognitiva de los usuarios finales, y debe evaluarse junto con el beneficio empresarial que deriva. Idealmente, no debería existir una configuración; en cambio, la configuración más segura debería integrarse en el producto de forma predeterminada. Cuando es necesaria la configuración, la opción predeterminada debe ser ampliamente segura contra amenazas comunes.

Las agencias autoras reconocen que estos cambios pueden tener efectos operativos en la forma en que se emplea el software. Por lo tanto, la opinión de los clientes es fundamental para equilibrar las consideraciones operativas y de seguridad. Las agencias autoras creen que desarrollar hojas de ruta escritas y apoyo ejecutivo que prioricen estas ideas en los productos más críticos de una organización es el primer paso para avanzar hacia prácticas de desarrollo de software seguras. Si bien la opinión de los clientes es importante, las agencias autoras han observado casos importantes en los que los clientes no han querido o no han podido adoptar estándares mejorados, a menudo protocolos de red. Es importante que los fabricantes creen incentivos significativos para que los clientes se mantengan actualizados y no les permitan permanecer vulnerables indefinidamente.

GUÍAS DE REFUERZO FRENTE A LAS DE FLEXIBILIZACIÓN

Las guías de refuerzo pueden resultar de la falta de controles de seguridad del producto integrados en la arquitectura de un producto desde el inicio del desarrollo. En consecuencia, las guías de refuerzo también pueden ser una hoja de ruta para que los adversarios identifiquen y exploten características inseguras. Es común que muchas organizaciones desconozcan las guías de refuerzo, por lo que dejan los ajustes de configuración de sus dispositivos en una postura insegura. Un modelo invertido conocido como guía de alivio debería reemplazar dichas guías de refuerzo y explicar qué cambios deben realizar los usuarios y al mismo tiempo enumerar los riesgos de seguridad resultantes.

En lugar de desarrollar guías de refuerzo que enumeren métodos para proteger los productos, las agencias autoras recomiendan que los fabricantes de software adopten un enfoque seguro por defecto y proporcionen guías de flexibilización. Estas guías explican el riesgo empresarial de las decisiones en un lenguaje sencillo y comprensible y pueden aumentar la conciencia organizacional sobre los riesgos de intrusiones cibernéticas maliciosas. Los ejecutivos sénior de los clientes deben determinar las compensaciones en materia de seguridad, equilibrando la seguridad con otros requisitos comerciales.

RECOMENDACIONES PARA CLIENTES

Las agencias autoras recomiendan que las organizaciones responsabilicen a los fabricantes de tecnología proveedores de los resultados de seguridad de sus productos. Como parte de esto, las agencias autoras recomiendan que los ejecutivos de las organizaciones prioricen la importancia de comprar productos seguros desde el diseño y seguros por defecto. Esto puede manifestarse mediante el establecimiento de políticas que exijan que los departamentos de IT evalúen la seguridad del software del fabricante antes de comprarlo, y que también empoderen a los departamentos de IT para que retrocedan si es necesario. Los departamentos de IT deben estar facultados para desarrollar criterios de compra que enfaticen la importancia de las prácticas seguras desde el diseño y seguras por defecto (tanto las descritas en este documento como otras desarrolladas por la organización). Además, los departamentos de IT deben contar con el apoyo de la dirección ejecutiva a la hora de hacer cumplir estos criterios en las decisiones de compra. Las decisiones organizacionales para aceptar los riesgos asociados con productos tecnológicos específicos deben documentarse formalmente, aprobarse por un alto ejecutivo comercial y presentarse periódicamente a la Junta Directiva.

Los servicios clave de IT empresarial que respaldan la postura de seguridad de la organización, como la red empresarial, la gestión de acceso e identidad empresarial, y las operaciones de seguridad y capacidades de respuesta, deben verse como funciones comerciales críticas que se financian para alinearse con su importancia para el éxito de la misión de la organización. Las organizaciones deben desarrollar un plan para actualizar estas capacidades para aprovechar los fabricantes que adoptan prácticas seguras desde el diseño y seguras por defecto.

Siempre que sea posible, las organizaciones deben esforzarse por forjar relaciones de asociaciones estratégicas con sus proveedores clave de IT. Dichas relaciones incluyen confianza en múltiples niveles de la organización y brindan vehículos para resolver problemas e identificar prioridades compartidas. La seguridad debe ser un elemento crítico de tales relaciones, y las organizaciones deben esforzarse por reforzar la importancia de las prácticas seguras desde el diseño y seguras por defecto tanto en la dimensión formal (por ejemplo, contratos o acuerdos con proveedores) como en la informal de la relación. Las organizaciones deben esperar transparencia de sus proveedores de tecnología sobre su postura de control interno, así como su hoja de ruta para adoptar prácticas seguras desde el diseño y seguras por defecto.

Además de hacer de la seguridad una prioridad dentro de una organización, los líderes de IT deben colaborar con sus pares de la industria para comprender qué productos y servicios incorporan mejor estos principios de diseño. Estos líderes deberían coordinar sus solicitudes para ayudar a los fabricantes a priorizar sus próximas iniciativas de seguridad. Al trabajar juntos, los clientes pueden ayudar a brindar información significativa a los fabricantes y crear incentivos para que prioricen la seguridad.

Al aprovechar los sistemas en la nube, las organizaciones deben asegurarse de comprender el modelo de responsabilidad compartida con su proveedor de tecnología. Es decir, las organizaciones deben tener claras las responsabilidades de seguridad del proveedor y no solo las del cliente. Las organizaciones deben priorizar a los proveedores de nube que sean transparentes en cuanto a su postura de seguridad, controles internos y capacidad para cumplir con sus obligaciones bajo el modelo de responsabilidad compartida.

DESCARGO DE RESPONSABILIDAD

La información contenida en este informe se proporciona “tal cual” solo con fines informativos. La Agencia de Seguridad Cibernética y de Infraestructura (CISA) y las agencias autoras no respaldan ningún producto ni servicio comercial, incluido ningún tema de análisis. Cualquier referencia a entidades comerciales específicas o productos, procesos o servicios comerciales mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo no constituye ni implica respaldo, recomendación ni favoritismo por parte de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) ni las agencias autoras. Este documento es una iniciativa conjunta de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) que no sirve automáticamente como documento regulatorio.

RECURSOS

Agencia de Seguridad Cibernética y de Infraestructura (CISA)

- Orientación sobre listas de materiales de software (SBOM, por sus siglas en inglés) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA)
- Objetivos de Desempeño de Ciberseguridad Intersectoriales de la Agencia de Seguridad Cibernética y de Infraestructura (CISA)
- Directrices sobre interoperabilidad tecnológica
- Defensa contra ataques a la cadena de suministro de software de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) y el Instituto Nacional de Estándares y Tecnología (NIST)
- El costo de la tecnología insegura y qué podemos hacer al respecto | Agencia de Seguridad Cibernética y de Infraestructura (CISA)
- Dejemos de pasar la pelota en ciberseguridad: por qué las empresas deben incorporar la seguridad en los productos tecnológicos (foreignaffairs.com)
- Guía de categorización de vulnerabilidades específicas (SSVC) de las partes interesadas de la Agencia de Seguridad Cibernética y de Infraestructura (CISA)
- Hojas informativas de MFA resistente a la suplantación de identidad de la Agencia de Seguridad Cibernética y de Infraestructura (CISA)
- Guía cibernética para pequeñas empresas | Agencia de Seguridad Cibernética y de Infraestructura (CISA)

NSA

- Hoja de información de ciberseguridad de la Agencia de Seguridad Nacional (NSA) sobre seguridad de la memoria
- El Marco de seguridad duradero (ESF, por sus siglas en inglés) de la Agencia de Seguridad Nacional (NSA) asegura la cadena de suministro de software: prácticas recomendadas para proveedores

FBI

- Comprender y responder al ataque a la cadena de suministro de SolarWinds: la perspectiva federal
- La amenaza cibernética: respuesta e informes
- La estrategia cibernética del FBI

Instituto Nacional de Estándares y Tecnología (NIST)

- Pautas de identidad digital del Instituto Nacional de Estándares y Tecnología (NIST)
- Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST)

- Marco de desarrollo de software seguro (SSDF) del Instituto Nacional de Estándares y Tecnología (NIST)

Centro Australiano de Seguridad Cibernética (ACSC)

- Guía del Código de Prácticas para Fabricantes de IoT del Centro Australiano de Seguridad Cibernética (ACSC)

Centro Nacional de Seguridad Cibernética del Reino Unido (UK)

- Marco de evaluación cibernética del Reino Unido
- Guía de implementación y desarrollo seguro del Centro Nacional de Seguridad Cibernética del Reino Unido (UK NCSC, por sus siglas en inglés)
- Guía de gestión de vulnerabilidades del Centro Nacional de Seguridad Cibernética del Reino Unido (UK NCSC)
- Conjunto de herramientas de divulgación de vulnerabilidades del UK NCSC
- CHERI de la Universidad de Cambridge
- Hasta luego y gracias por todos los detalles - NCSC.GOV.UK

Centro Canadiense de Seguridad Cibernética (CCCS)

- Orientación del CCCS sobre cómo protegerse contra ataques a la cadena de suministro de software
- Cadena de suministro cibernética: enfoque para evaluar los riesgos
- Guía sobre ransomware CONTI del Centro Canadiense de Seguridad Cibernética

Oficina Federal de Seguridad de la Información (BSI) de Alemania

- El compendio BSI Grundschutz (módulo CON.8)
- La norma internacional IEC 62443, parte 4-1
- Estado de la seguridad informática en Alemania en 2022
- Prácticas de BSI sobre seguridad de aplicaciones web

Centro Nacional de Seguridad Cibernética de los Países Bajos

- Hoja informativa sobre autenticación madura del NCSC-NL

Otro

- Cómo fallan los sistemas complejos
- La nueva mirada en fallas de sistemas complejos