Acronis

Cerrando la brecha de seguridad en la cadena de suministro: lista de verificación de evaluación de SSDLC

Los ataques de cadena de suministro se encuentran entre las amenazas de ciberseguridad más críticas y difíciles de defender. Los ataques de SolarWinds, Polyfill.io, 3CX y MOVEit demostraron cómo atacar a los proveedores de software permitió a los atacantes comprometer industrias enteras a gran escala.

30 % de todas las brechas en 2024 involucran ahora a un tercero, un aumento del 15 % desde 2023[1]

Las evaluaciones tradicionales de proveedores se enfocan en la salud financiera y la seguridad de la infraestructura, pero pasan por alto donde surgen la mayoría de las vulnerabilidades: el proceso de desarrollo de software.

La vulnerabilidad oculta: Proceso de desarrollo de software

Ataques a la cadena de suministro que hicieron historia

Empresa	Sector	Fecha	Impacto
Polyfill.io	Red de entrega de contenido (CDN)	2024	Miles de sitios web afectados
3CX	Servicios VOIP	2023	Miles de empresas afectadas
MOVEit	Transferencia de archivos	2023	Más de 2,000 organizaciones afectadas
SolarWinds	Software de TI	2020	Más de 18,000 organizaciones comprometidas

Los controles de seguridad en tiempo de ejecución no pueden corregir retroactivamente el código inseguro. Si las vulnerabilidades se introducen durante el diseño o la codificación, los clientes esperan a que los proveedores apliquen parches mientras permanecen expuestos.

El ciclo de vida de desarrollo de software seguro (SSDLC) incorpora la seguridad en cada fase del desarrollo de software, desde el diseño hasta el mantenimiento posterior al lanzamiento.

Cómo evaluar el desarrollo de software

La garantía basada en evidencia requiere una evaluación en seis dimensiones:

1 Administración y directiva:

Directivas documentadas, roles formales de seguridad y supervisión ejecutiva.

2 Gestión de riesgos y diseño:

Modelado de amenazas, requisitos de seguridad y evaluaciones de diseño.

3 Prácticas de implementación:

Capacitación de desarrolladores, estándares de codificación segura y revisión de código.

4 Verificación y validación:

Pruebas automatizadas, pruebas de penetración y validación de terceros.

5 Lanzamiento y despliegue:

Canalizaciones reforzadas, firma de código y segregación de entornos.

6 Mantenimiento y supervisión:

Divulgación de vulnerabilidades, plazo de parcheo y notificaciones a los clientes.

Acronis: Excelencia certificada en SSDLC

Acronis demuestra liderazgo en SSDLC a través de certificaciones verificadas de forma independiente:

IEC 62443-4-1
Desarrollo de productos seguros para entornos OT

ISO/IEC 27001
Gestión de seguridad de la información

ISO/IEC 27017/27018
Seguridad y privacidad de servicios en la nube

CSA STAR Nivel 2
Evaluación independiente de seguridad en la nube

Estos certificados son poco comunes y difíciles de obtener.

IEC 62443-4-1 representa el estándar de oro para el desarrollo seguro de productos en entornos industriales, validando que los productos de Acronis están diseñados con la seguridad en su núcleo. Los clientes y partners de OT pueden confiar en que las soluciones de Acronis reducen el riesgo en su cadena de suministro y simplifican el cumplimiento de NIS 2, DORA y otras regulaciones.

IEC 62443-4-1 CERTIFIED

Obtenga más información

Refuerce la seguridad de su cadena de suministro con el enfoque certificado de Acronis:

- Ver el certificado IEC 62443-4-1 de Acronis
- Leer el documento técnico completo sobre SSDLC
- Explorar las soluciones de ciberprotección de Acronis
- Programar una consulta 1 a 1 con un ingeniero de soluciones de Acronis

Acerca de Acronis

Acronis es una empresa global de ciberprotección que ofrece ciberseguridad, protección de datos y gestión de endpoints integrados de forma nativa para proveedores de servicios gestionados (MSP), pequeñas y medianas empresas (pymes) y departamentos de TI empresariales. Las soluciones de Acronis son muy eficaces y están diseñadas para identificar, prevenir, detectar, responder, remediar y recuperarse de las ciberamenazas modernas con un tiempo de inactividad mínimo, garantizando la integridad de los datos y la continuidad de la actividad empresarial. Acronis ofrece la solución de seguridad más completa del mercado para MSP, con su capacidad exclusiva para satisfacer las necesidades de entornos de TI diversos y distribuidos.

Acronis es una empresa suiza fundada en Singapur en 2003, con 15 oficinas en todo el mundo y empleados en más de 45 países. Acronis Cyber Protect está disponible en 26 idiomas en 150 países y es utilizado por más de 20 000 proveedores de servicios para proteger a más de 750 000 empresas. Obtenga más información en www.acronis.com.

[1] Verizon. "2025 Data Breach Investigations Report."

Acronis

Obtenga más información en **acronis.com**