Acronis

Fechando a lacuna de segurança na cadeia de suprimentos: Lista de verificação de avaliação SSDLC

Os ataques à cadeia de suprimentos estão entre as ameaças de cibersegurança mais críticas e difíceis de defender. Os ataques SolarWinds, Polyfill.io, 3CX e MOVEit demonstraram como atacar fornecedores de software permitiu que os invasores comprometessem indústrias inteiras em grande escala.

30%

De todas as violações de segurança em 2024, 15% envolvem terceiros, um aumento de 15% desde 2023[1]

As avaliações tradicionais de fornecedores focam na saúde financeira e na segurança da infraestrutura, mas deixam de lado onde a maioria das vulnerabilidades se origina: o processo de desenvolvimento de software.

A vulnerabilidade oculta: Processo de desenvolvimento de software

Ataques históricos na cadeia de suprimentos

Função	Indústria	Data	Impacto
Polyfill.io	Rede de entrega de sumário (CDN)	2024	Milhares de sites afetados
3CX	Serviços de VoIP	2023	Milhares de empresas afetadas
MOVEit	Transferência de arquivo	2023	Mais de 2.000 organizações afetadas
SolarWinds	Software de TI	2020	Mais de 18.000 organizações comprometidas

Os controles de segurança em tempo de execução não podem corrigir retroativamente um código inseguro. Se vulnerabilidades forem introduzidas durante o design ou a codificação, os clientes precisam esperar que os fornecedores lancem correções, permanecendo expostos enquanto isso.

O ciclo de vida de desenvolvimento de software seguro (SSDLC) incorpora segurança em cada estágio do desenvolvimento de software, desde o design até a manutenção pós-lançamento.

Como avaliar o desenvolvimento de software

A garantia baseada em evidências requer avaliação em seis dimensões:

Governança e política:

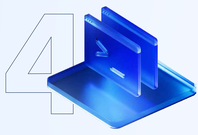
Políticas documentadas, funções formais de segurança e supervisão executiva.

Gestão de riscos e design:

Modelagem de ameaças, requisitos de segurança e avaliações de design.

Práticas de implementação:

Treinamento de desenvolvedores, padrões de codificação segura e revisão de código.



Verificação e validação:

Testes automatizados, testes de penetração e validação por terceiros.

Lançamento e implantação:

Pipelines reforçados, assinatura de código e segregação de ambientes.

Manutenção e monitoramento:

Divulgação de vulnerabilidades, cronogramas para aplicar patches e notificações ao cliente final.

Acronis: Excelência certificada em SSDLC

A Acronis demonstra liderança em SSDLC por meio de certificações verificadas de forma independente:

IEC 62443-4-1
Desenvolvimento seguro de produtos para ambientes OT

ISO/IEC 27001
Informação de gerenciamento da segurança

ISO/IEC 27017/27018
Segurança e privacidade de serviços de nuvem

CSA STAR Level 2
Avaliação independente de segurança em nuvem

Essas certificações são raras e difíceis de obter.

A IEC 62443-4-1 representa o padrão ouro para o desenvolvimento seguro de produtos em ambientes industriais, validando que os produtos da Acronis são projetados com segurança em seu núcleo. Clientes finais e parceiros de OT podem ter confiança de que as soluções da Acronis reduzem o risco em sua cadeia de suprimentos e simplificam a conformidade com NIS 2, DORA e outras regulamentações.

Saiba mais

Fortaleça a segurança da sua cadeia de suprimentos com a abordagem certificada da Acronis:

- Ver certificado IEC 62443-4-1 da Acronis
- Leia o artigo técnico completo sobre SSDLC
- Explore as soluções de ciberproteção da Acronis
- Agende uma consulta individual com um engenheiro de soluções da Acronis

Sobre a Acronis

A Acronis é uma empresa global de proteção cibernética que fornece cibersegurança, proteção de dados e gerenciamento de endpoint nativamente integrados para provedores de serviços gerenciados (MSPs), pequenas e médias empresas (PMEs) e departamentos de TI corporativos. As soluções da Acronis são altamente eficientes e projetadas para identificar, prevenir, detectar, responder, remediar e recuperar-se de ameaças cibernéticas modernas com tempo de inatividade mínimo, garantindo a integridade dos dados e a continuidade dos negócios. A Acronis oferece a solução de segurança mais abrangente do mercado para MSPs com sua capacidade única de atender às necessidades de ambientes de TI diversos e distribuídos.

Uma empresa suíça fundada em Singapura em 2003, a Acronis possui 15 escritórios em todo o mundo e funcionários em mais de 45 países. O Acronis Cyber Protect está disponível em 26 idiomas em 150 países e é usado por mais de 20.000 provedores de serviços para proteger mais de 750.000 empresas.
Saiba mais em www.acronis.com.

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

Acronis

Saiba mais em acronis.com