Acronis

Schließen Sie Sicherheitslücken in der Lieferkette: Checkliste für SSDLC-Bewertungen

Angriffe auf Lieferketten zählen zu den gefährlichsten und schwersten Bedrohungen für die Cybersicherheit. Wie die Angriffe auf SolarWinds, Polyfill.io, 3CX und MOVEit deutlich gemacht haben, können Cyberkriminelle durch gezielte Angriffe auf Softwareanbieter ganze Branchen erheblich kompromittieren.

30 %

aller Datenschutzverletzungen in 2024 involvierten einen Drittanbieter – 15 % mehr als im Vorjahr[1]

Bei traditionellen Lieferantenbewertungen stehen die wirtschaftliche Stabilität und die Sicherheit der Infrastruktur im Fokus. Der Bereich, in dem die meisten Schwachstellen entstehen – der Softwareentwicklungsprozess – bleibt dabei jedoch außen vor.

Der Softwareentwicklungsprozess – eine unsichtbare Schwachstelle

Lieferkettenangriffe mit großen Auswirkungen

Unternehmen	Branche	Datum	Folgen
Polyfill.io	Content Delivery Network (CDN)	2024	Tausende Websites waren betroffen
3CX	VoIP-Services	2023	Tausende von großen Unternehmen waren betroffen
MOVEit	Dateiübertragung	2023	Über 2.000 Unternehmen waren betroffen
SolarWinds	IT-Software	2020	Mehr als 18.000 Unternehmen waren betroffen

Sicherheitschecks zur Ausführungszeit können unsicheren Code nicht nachträglich unschädlich machen. Wenn während der Entwicklung oder Programmierung Schwachstellen entstehen, sind Kund:innen so lange gefährdet, bis der Anbieter einen Patch bereitstellt.

Der Secure Software Development Life Cycle (SSDLC) integriert Sicherheit in alle Phasen der Softwareentwicklung – von der Konzeption bis hin zu Updates nach der Veröffentlichung.

Bewertungskriterien für den Softwareentwicklungsprozess

Für eine evidenzbasierte Qualitätssicherung ist eine Bewertung in sechs Dimensionen erforderlich.

Governance und Richtlinien:

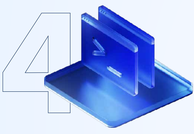
Dokumentierte Richtlinien, formelle Sicherheitsrollen und Aufsicht durch die Geschäftsleitung.

Risikomanagement und Design:

Bedrohungsmodellierung, Sicherheitsanforderungen und Designbewertungen.

Implementierungspraktiken:

Schulungen für Entwickler:innen, Standards für sicheres Programmieren und Codeüberprüfung.



Verifizierung und Validierung:

Automatisierte Tests, Penetrationstests und Validierung durch Dritte.

Veröffentlichung und Bereitstellung:

Abgesicherte Pipelines, Codesignierung und getrennte Umgebungen.

Wartung und Monitoring:

Veröffentlichung von Schwachstellen, Zeitpläne für Patches und Kundenbenachrichtigungen.

Acronis: Zertifizierte SSDLC-Exzellenz

Die von unabhängiger Seite verifizierten Zertifizierungen belegen die Führungsrolle von Acronis im Bereich SSDLC:

IEC 62443-4-1
Sichere Produktentwicklung für OT-Umgebungen

ISO/IEC 27001
Informationssicherheitsmanagement

ISO/IEC 27017/27018
Sicherheit und Datenschutz bei Cloud-Services

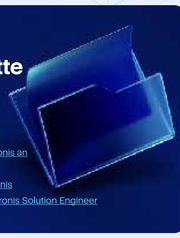
CSA STAR Level 2
Unabhängige Cloud-Sicherheitsbewertung

Diese Zertifizierungen sind selten und nur schwer zu erlangen.

IEC 62443-4-1 gilt als Goldstandard für die sichere Produktentwicklung in industriellen Umgebungen. Die Zertifizierung bestätigt, dass bei der Entwicklung von Acronis Produkten die Sicherheit im Vordergrund steht. Unternehmen und Partner im OT-Bereich können sich darauf verlassen, dass Acronis Lösungen ihre Lieferkettenrisiken reduzieren und die Einhaltung von NIS 2, DORA und anderen Vorschriften erleichtern.

Mehr erfahren

Verbessern Sie die Sicherheit Ihrer Lieferkette mit dem zertifizierten Ansatz von Acronis:



- Sehen Sie sich die IEC 62443-4-1-Zertifizierung von Acronis an
- Lesen Sie das gesamte SSDLC-Whitepaper
- Entdecken Sie die Cyber Protection-Lösungen von Acronis
- Vereinbaren Sie eine individuelle Beratung mit einem Acronis Solution Engineer

Über Acronis

Acronis ist ein globales Unternehmen für Cyber Protection, das direkt integrierte Cyber Security, Data Protection und Endpunkt-Verwaltung für Managed Service Provider (MSPs), kleine und mittelständische Unternehmen (KMU) sowie IT-Abteilungen von Großunternehmen bereitstellt. Die Lösungen von Acronis sind hocheffizient und darauf ausgelegt, moderne Cyberbedrohungen zu identifizieren, zu verhindern, zu erkennen, darauf zu reagieren, sie zu beseitigen und sich mit minimalen Ausfallzeiten von ihnen zu erholen. Dank diesem vollständigen Ansatz werden die Datenintegrität und Kontinuität des Geschäftsbetriebs gewährleistet. Acronis bietet die umfassendste Sicherheitslösung auf dem Markt für MSPs mit seiner speziellen Fähigkeit, die Anforderungen von diversifizierten und dezentralen IT-Umgebungen zu bedienen.

Acronis ist ein Schweizer Unternehmen, das 2003 in Singapur gegründet wurde und weltweit 15 Niederlassungen und Mitarbeiter in über 45 Ländern hat. Acronis Cyber Protect ist in 26 Sprachen in 150 Ländern verfügbar und wird von über 20.000 Service Providern zum Schutz von über 750.000 Unternehmen eingesetzt. Erfahren Sie mehr unter www.acronis.com.

[1] „Data Breach Investigations Report", Verizon, 2025

Acronis Erfahren Sie mehr auf acronis.com