# Verdediging tegen cyberaanvallen in de leveringsketen met Dell Technologies

## Beknopt overzicht

De steeds meer wereldwijde en onderling verbonden aard van bedrijfsactiviteiten heeft organisaties blootgesteld aan toenemende bedreigingen van cyberaanvallen in de leveringsketen. Deze geavanceerde aanvallen maken gebruik van kwetsbaarheden in de hardwarelevenscyclus, van productie tot implementatie, evenals software van derden, waardoor kwaadwillenden volledige systemen kunnen compromitteren via vertrouwde applicaties of updates. Dergelijke incidenten zijn niet alleen financieel rampzalig, maar kunnen ook reputaties aantasten en activiteiten op grote schaal verstoren.

De gevolgen van deze bedreigingen zijn diepgaand. Aanvallen in de leveringsketen worden vaak niet gedetecteerd totdat er aanzienlijke schade is opgetreden, waardoor proactieve verdedigingsstrategieën essentieel zijn. Met geavanceerde eindpuntbescherming, proactieve bewaking en uitgebreide oplossingen voor server- en databeveiliging stelt Dell bedrijven in staat hun leveringsketens van end tot end te beveiligen. Via technologie, partnerschappen en expertise kunnen organisaties veerkracht opbouwen en zichzelf beschermen tegen kwetsbaarheden die inherent zijn aan hun ecosystemen.

## De toenemende dreiging van cyberaanvallen in de leveringsketen

Aanvallen op de leveringsketen zijn de afgelopen jaren aanzienlijk toegenomen. Door fysieke apparaten te manipuleren tijdens productie, verzending of implementatie of door zwakke plekken in softwareleveranciers te vinden, krijgen aanvallers de middelen om kwaadaardige componenten of code in te voegen, systemen te corrumperen of gevoelige data te exfiltreren. Slachtoffers variëren van kleine bedrijven tot wereldwijde ondernemingen, met gevolgen zoals ernstige financiële verliezen, verminderd vertrouwen van klanten en juridische gevolgen. Dell Technologies erkent dit groeiende gevaar en pleit voor preventieve maatregelen om de catastrofale gevolgen van dergelijke aanvallen te beperken.

## Inzicht in cyberaanvallen in de leveringsketen

### Hoe hardware-aanvallen in de leveringsketen werken

1. **Productiefase:** Aanvallers introduceren schadelijke componenten tijdens de productie van hardware, waarbij vaak gebruik wordt gemaakt van gecompromitteerde leveranciers.
2. **Verzendfase:** apparaten worden tijdens het transport onderschept en aangepast om schadelijke firmware- of hardwarewijzigingen toe te passen.
3. **Implementatie en activering:** Zodra de gecompromitteerde hardware het netwerk van de organisatie binnenkomt, krijgen aanvallers toegang tot gevoelige data of kunnen ze backdoor-activiteiten inschakelen.

### Hoe software-aanvallen in de leveringsketen werken

1. **Eerste inbraak:** Een softwareleverancier van derden wordt gecompromitteerd, vaak door phishing, niet-gerepareerde beveiligingslekken of interne bedreigingen.
2. **Codemanipulatie:** Kwaadwillenden injecteren schadelijke elementen zoals malware of backdoors in software die bedoeld is voor distributie.

3. **Verspreiding naar eindgebruikers:** Bedrijven die gecompromitteerde software installeren of bijwerken, downloaden per ongeluk schadelijke componenten.

### Algemene technieken - Hardware

- **Firmwaremanipulatie:** Het insluiten van schadelijke code die na de implementatie wordt geactiveerd.
- **Hardware-implantatie:** Integratie van verborgen componenten om data te controleren of te exfiltreren.
- **Misbruik van vertrouwde leveranciers:** Gebruikmaken van externe leveranciers met minder veilige processen.

### Algemene technieken - Software

- **Component kapen:** Het infecteren van bibliotheken of frameworks van derden met schadelijke code.
- **Update-injectie:** Officiële software-updates wijzigen om exploits op te nemen.
- **Afhankelijkheidsverwarring:** Profiteren van het vertrouwen van organisaties in onveilige pakketafhankelijkheden.

## De impact op bedrijven

### Financiële gevolgen

Aanvallen op leveringsketens leiden vaak tot kosten door juridische boetes, kosten voor systeemherstel en compensatie voor klanten. Eén belangrijk incident waarbij een wereldwijd IT-beheerbedrijf betrokken was, leidde tot verliezen van meer dan $ 70 miljoen, wat illustreert hoe groot de financiële schade van deze inbreuken kan zijn.

### Operationele storing

Beschadigde of uitgeschakelde systemen die worden veroorzaakt door malware-infiltratie leiden vaak tot langdurige downtime, waardoor de productiviteit van de organisatie wordt verstoord en projectleveringen worden vertraagd.

### Gevolgen voor de reputatie

Vertrouwen in softwarepartners is van cruciaal belang voor moderne bedrijven. Een inbreuk in de leveringsketen die is gekoppeld aan het softwareaanbod van een organisatie kan reputaties aantasten en de loyaliteit van klanten verminderen.

## Voorbeelden uit de praktijk - Hardware/software

Een wereldwijde elektronicafabrikant ontdekte gecompromitteerde componenten in zijn leveringsketen, wat leidde tot wijdverbreide systeemstoringen. De aanval kostte meer dan **$ 45 miljoen** aan herstelkosten en juridische kosten, samen met onherstelbare schade aan leveranciersrelaties.

De SolarWinds-inbreuk is een van de meest beruchte software-aanvallen op de leveringsketen. Deze inbreuk op hun Orion-product infecteerde organisaties wereldwijd, waaronder overheidsinstanties en Fortune 500-bedrijven. De geschatte schade bedroeg meer dan **$ 90 miljoen** en de inbreuk benadrukte de verstrekkende gevolgen van kwetsbaarheden in de leveringsketen.

## De expertise van Dell Technologies in het bestrijden van aanvallen in de leveringsketen

Het brede portfolio van beveiligingsoplossingen van Dell Technologies stelt bedrijven in staat om veranderende cyberrisico's voor te blijven.

### Dell Secure Component Verification (SCV)

Secure Component Verification (SCV) is een integraal onderdeel van de beveiligingsstrategie van de leveringsketen van Dell Technologies die is ontworpen om de authenticiteit en integriteit van hardwarecomponenten in verschillende Dell oplossingen te garanderen. SCV biedt cryptografische validatie van systeemcomponenten vanaf het moment van productie tot levering en implementatie. Dell Technologies biedt robuuste beveiliging van de leveringsketen, zodat systemen vrij zijn van sabotage en veilig zijn vanaf de fabriek tot aan de implementatie. Dit verbetert de algehele beveiliging, betrouwbaarheid en prestaties voor Dell klanten.

### Eindpunten beveiligen met Dell Trusted Devices

Dell Trusted Devices integreert beveiliging op hardware- en firmwareniveau om systemen te beveiligen tegen sabotage.

- **SafeBIOS** zorgt voor firmware-integriteit bij het opstarten, voorkomt ongeautoriseerde configuratiewijzigingen en verifieert firmware-integriteit bij het opstarten, waardoor gecompromitteerde systemen niet kunnen worden gestart.
- **SafeID** beveiligt verificatiereferenties op hardwareniveau, voorkomt ongeautoriseerde toegang en beschermt inloggegevens door verificatiesleutels te beveiligen, waardoor onbevoegde gebruikers worden geblokkeerd.
- **SafeData** maakt end-to-endversleuteling mogelijk voor gevoelige bedrijfsbestanden, waardoor pogingen tot misbruik van data-exfiltratie worden geblokkeerd.

### Proactieve bedreigingsdetectie met CrowdStrike

CrowdStrike integreert met de technologieën van Dell om realtime inzichten te leveren in schadelijk softwaregedrag.

- **Gedragsanalyse voor bedreigingsdetectie:** Bewaakt hardware- en firmwaregedrag op tekenen van sabotage en detecteert ongebruikelijke softwareactiviteit om malware-implementatie te voorkomen.
- **Tools voor onmiddellijke respons:** AI isoleert gecompromitteerde systemen, waardoor laterale verplaatsing binnen het netwerk wordt voorkomen.
- **Op AI gebaseerd herstel van dreigingen:** Identificeert en isoleert bedreigingen actief, waardoor laterale verspreiding binnen bedrijfssystemen wordt voorkomen.
- **Integratiemogelijkheden:** Hybride en multicloudomgevingen worden holistisch beschermd met tools van Dell en CrowdStrike.

### Krachtige beveiliging via de server- en storageoplossingen van Dell

De Dell PowerEdge serverreeks bevat geavanceerde bescherming om bedrijfskritieke softwareplatforms te beveiligen. Storagesystemen zoals Dell PowerStore bieden toonaangevende versleuteling voor applicaties en data.

- **Firmware voor beveiligde servers:** Bewaakt en blokkeert ongeautoriseerde wijzigingen op hardwareniveau.
- **Geïsoleerde netwerkbewaking:** Detecteert afwijkingen die wijzen op sabotage in de leveringsketen.
- **Onveranderlijke back-ups:** Bescherm herstelpunten, zelfs wanneer de primaire storage in gevaar komt.
- **Herstelkluizen:** Geïsoleerde omgevingen beschermen tegen trapsgewijze storingen die worden veroorzaakt door gecompromitteerde systemen.

## Meerlaagse benaderingen om risico's te beperken

Dell moedigt bedrijven aan om uitgebreide strategieën te implementeren waarin technologie, personeelspraktijken en bijgewerkte processen worden gecombineerd.

### Strategische stappen

- **Verbeter de zichtbaarheid van de leveringsketen:** Eis dat alle leveranciers zich houden aan strenge beveiligingsnormen en hardware in elke fase certificeren.
- **Geavanceerde versleuteling implementeren:** Beveilig data op elk niveau met behulp van geavanceerde protocollen, waardoor de toegankelijkheid zelfs in gecompromitteerde hardware wordt beperkt.
- **Implementeer Zero-Trust-beleid:** Geen apparaat, applicatie of gebruiker krijgt automatisch vertrouwen zonder verificatie.
- **Standaarden voor veilige codering:** Werk samen met softwarepartners die rigoureuze richtlijnen afdwingen voor plug-ins, API's en integraties.
- **Controleer regelmatig activiteiten en audits:** Frequente zichtbaarheidsaudits zorgen voor integriteit bij services van derden.
- **Regelmatig testen uitvoeren:** Implementeer tests voor indringingsrisico en firmwarebeoordelingen om de integriteit van het apparaat continu te valideren.
- **Informeer werknemers:** Train teams om componenten of pakketten te herkennen die verdacht gedrag vertonen.

## Hoe Dell Professional Services bedrijfsveerkracht garandeert

De Professional Services van Dell begeleiden bedrijven bij het implementeren van robuuste bescherming van de leveringsketen. Teams van ervaren cyberbeveiligingsexperts bieden beoordelingen, training en strategieën voor dreigingsrespons die zijn afgestemd op unieke organisatorische behoeften.

- **Implementatierichtlijnen:** stem zero-trust en gecontroleerde werkwijzen van leveranciers strategisch op elkaar af in alle leveranciersomgevingen.
- **Incidentrespons:** Zorg ervoor dat bedrijven snel herstellen na schadelijke incidenten.

## Toekomstbestendige Enterprise-systemen met Dell

Cyberaanvallen in de leveringsketen illustreren de verfijning van moderne bedreigingen. Bedrijven hebben bescherming nodig die niet alleen inbreuken voorkomt, maar ook zorgt voor snel herstel wanneer er incidenten optreden. Samenwerken met Dell Technologies betekent toegang krijgen tot geavanceerde tools, strategische expertise en een netwerk van vertrouwde medewerkers.

## Zet de volgende stap

Bescherm gevoelige assets en stroomlijn de operationele betrouwbaarheid door best practices te implementeren die worden aangedreven door Dell Technologies. Neem vandaag nog contact op voor advies op maat terwijl u zich voorbereidt om de kern van uw bedrijfssystemen te beveiligen.

Dell Technologies staat voor vertrouwen, aanpasbaarheid en innovatie in de ontwikkeling van cyberbeveiliging van de leveringsketen. De inzet van vandaag garandeert het succes van morgen.

Een veiligere en zekerdere toekomst begint bij Dell Technologies. Vertrouw op ons om te beschermen wat het belangrijkst is.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van dit moment kunt aanpakken op **Dell.com/SecuritySolutions**

Meer informatie over oplossingen van Dell

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag



DELL Technologies