DELL Technologies

Försvar mot cyberattacker i leverantörskedjan med Dell Technologies

Sammanfattning

Affärsverksamheters alltmer globala och sammankopplade natur har gjort att organisationer utsätts för ökande hot från cyberattacker i leverantörskedjan. De här sofistikerade attackerna utnyttjar sårbarheter i hårdvarans livscykel, från tillverkning till driftsättning samt tredjepartsmjukvara, och gör det möjligt för skadliga aktörer att kompromettera hela system genom betrodda program eller uppdateringar. Sådana incidenter är inte bara katastrofala ur ett ekonomiskt perspektiv utan kan även försämra företags anseende och störa driften i stor skala.

Konsekvenserna av dessa hot är allvarliga. Attacker i leverantörskedjan upptäcks ofta inte förrän stora skador redan har uppstått, vilket gör proaktiva försvarsstrategier avgörande. Med avancerat slutpunktsskydd, proaktiv övervakning och omfattande server- och datasäkerhetslösningar gör Dell det möjligt för företag att skydda sina leverantörskedjor från början till slut. Genom teknik, partnerskap och expertis kan organisationer bygga motståndskraft och skydda sig mot sårbarheter i sina ekosystem.

Det ökande hotet från cyberattacker i leverantörskedjan

Attacker i leverantörskedjan har ökat avsevärt under de senaste åren. Genom att manipulera fysiska enheter under produktion, leverans eller distribution eller hitta svagheter hos mjukvaruleverantörer får angripare möjlighet att injicera skadliga komponenter eller kod, skada system eller exfiltrera känsliga data. Offren sträcker sig från småföretag till globala företag, med resultat som allvarliga ekonomiska förluster, komprometterat kundförtroende och juridiska konsekvenser. Dell Technologies inser denna tilltagande fara och förespråkar förebyggande åtgärder för att mildra de katastrofala effekterna av sådana attacker.

Förstå cyberattacker i leverantörskedjan

Så här fungerar hårdvaruattacker i leverantörskedjan

1. **Tillverkningsfas:** Angripare introducerar skadliga komponenter under hårdvarumonteringen och utnyttjar ofta komprometterade leverantörer.
2. **Leveransfas:** Enheter fångas upp under transport och ändras för att inkludera skadliga modifieringar av fast mjukvara eller hårdvara.
3. **Driftsättning och aktivering:** När den komprometterade hårdvaran kommer in i organisationens nätverk får angriparna åtkomst till känsliga data eller får möjlighet till åtgärder via bakdörrar.

Så här fungerar mjukvaruattacker i leverantörskedjan

1. **Inledande intrång:** En tredjepartsleverantör av mjukvara kompromitteras, ofta genom nätfiske, sårbarheter som inte har korrigerats eller insiderhot.
2. **Kodmanipulering:** Skadliga aktörer injicerar skadliga element, som skadliga program eller bakdörrar i mjukvara som är avsedd för driftsättning.

3. **Spridning till slutanvändare:** Företag som installerar eller uppdaterar kompromitterad mjukvara laddar oavsiktligt ner skadliga komponenter.

Vanliga tekniker – hårdvara

- **Manipulering av fast mjukvara:** Inbäddning av skadlig kod som aktiveras efter driftsättning.
- **Hårdvaruimplantering:** Integrering av dolda komponenter för att övervaka eller exfiltrera data.
- **Utnyttjande av betrodda leverantörer:** Utnyttjande av tredjepartsleverantörer med mindre säkra processer.

Vanliga tekniker – mjukvara

- **Komponentkapning:** Infektering av tredjepartsbibliotek eller -ramverk med skadlig kod.
- **Uppdateringsinjektion:** Ändring av officiella mjukvaruuppdateringar så att de inkluderar sårbarheter.
- **Beroendeförvirring:** Utnyttjande av organisationers beroende av osäkra paketberoenden.

Påverkan på företag

Ekonomiska konsekvenser

Attacker som riktar sig mot leverantörskedjor leder ofta till kostnader som omfattar böter, utgifter för systemåterställning och kompensation till kunder. En uppmärksammad incident som involverade ett globalt IT-förvaltningsföretag ledde till förluster på över 70 miljoner USD, vilket illustrerar den ekonomiska katastrof som dessa intrång kan orsaka.

Driftstörningar

Skadade eller inaktiverade system p.g.a. skadliga program leder ofta till omfattande driftavbrott, vilket leder till att organisationens produktivitet minskar och projektleveranser försenas.

Skadat anseende

Förtroende för mjukvarupartner är avgörande för moderna företag. Ett intrång i leverantörskedjan som är kopplat till en organisations mjukvaruutbud kan skada dess anseende och urholka kundlojaliteten.

Verkliga exempel – hårdvara/mjukvara

En global elektroniktillverkare upptäckte kompromitterade komponenter i leverantörskedjan, vilket ledde till omfattande systemfel. Attacken kostade över **45 miljoner USD** i återställningskostnader och juridiska avgifter, tillsammans med irreparabla skador på leverantörsrelationer.

SolarWinds-intrånget är bland de mest ökända mjukvaruattackerna i leverantörskedjan. Intrånget i deras Orion-produkt infekterade organisationer över hela världen, inklusive myndigheter och Fortune 500-företag. Skadorna uppskattas till mer än **90 miljoner USD** och intrånget satte de långtgående konsekvenserna av sårbarheter i leverantörskedjan i fokus.

Dell Technologies expertis när det gäller att bekämpa attacker i leverantörskedjan

Dell Technologies breda portfölj med säkerhetslösningar gör det möjligt för företag att ligga steget före föränderliga cyberrisker.

Dells säkra komponentverifiering (SCV)

Säker komponentverifiering (SCV) är en integrerad del av Dell Technologies säkerhetsstrategi för leverantörskedjan som utformats för att säkerställa äktheten och integriteten hos hårdvarukomponenter i olika Dell-lösningar. SCV tillhandahåller kryptografisk validering av systemkomponenter från tillverkningstillfället till leverans och driftsättning. Dell Technologies tillhandahåller robust säkerhet i leverantörskedjan, och säkerställer att systemen är manipuleringsfria och säkra från fabrik till driftsättning. Detta förbättrar den övergripande säkerheten, tillförlitligheten och prestandan för Dells kunder.

Säkra slutpunkter med Dell Trusted Devices

Dell Trusted Devices integrerar säkerhet på hårdvaru- och fast mjukvarunivå för att skapa manipuleringssäkra system.

- **SafeBIOS** säkerställer den fasta mjukvarans integritet vid start, förhindrar obehöriga konfigurationsändringar och verifierar den fasta mjukvarans integritet vid start, vilket hindrar komprometterade system från att starta.
- **SafeID** säkrar autentiseringsuppgifter på hårdvarunivå, förhindrar obehörig åtkomst och skyddar inloggningsuppgifter genom att säkra autentiseringsnycklar, och på så sätt utelåsa obehöriga användare.
- **SafeData** möjliggör heltäckande kryptering för känsliga företagsfiler, vilket blockerar försök till exfiltrering av data.

Proaktiv hotidentifiering med CrowdStrike

CrowdStrike integreras med Dells teknik och levererar insikter i realtid om beteende hos skadlig programvara.

- **Analys av beteende och hotdetektering:** Övervakar hårdvaras och fast mjukvaras beteende för tecken på manipulering och upptäcker ovanlig mjukvaruaktivitet för att förhindra driftsättning av skadliga program.
- **Verktyg för omedelbar respons:** AI isolerar komprometterade system och förhindrar lateral förflyttning inom nätverket.
- **AI-baserad hotsanering:** Identifierar och isolerar hot aktivt, och förhindrar lateral spridning inom företagssystem.
- **Integreringsfunktioner:** Hybrid- och flermolnsmiljöer skyddas holistiskt med Dell- och CrowdStrike-verktyg.

Stärkt säkerhet via Dells server- och lagringslösningar

Dell PowerEdge-serverserien innehåller avancerat skydd för att skydda verksamhetskritiska mjukvaruplattformar. Lagringssystem som Dell PowerStore erbjuder branschledande kryptering för program och data.

- **Säker fast servermjukvara:** Övervakar och blockerar obehöriga ändringar på hårdvarunivå.
- **Isolerad nätverksövervakning:** Upptäcker avvikelser som tyder på manipulering av leverantörskedjan.
- **Oföränderliga säkerhetskopior:** Skyddar återställningspunkter även när den primära lagringen komprometteras.
- **Återställningsvalv:** Isolerade miljöer skyddar mot kaskadfel som initieras från komprometterade system.

Metoder i flera lager för att minska riskerna

Dell uppmuntrar företag att implementera omfattande strategier som kombinerar teknik, personalrutiner och uppdaterade processer.

Strategiska steg

- **Förbättra leverantörskedjans synlighet:** Kräv att alla leverantörer följer rigorösa säkerhetsstandarder och certifierar hårdvaran i varje steg.
- **Implementera avancerad kryptering:** Säkra data på alla nivåer med hjälp av avancerade protokoll, vilket begränsar tillgängligheten även i komprometterad hårdvara.
- **Anta nollförtroendepolicyer:** Ingen enhet, inget program och ingen användare får automatiskt förtroende utan verifiering.
- **Säkra kodningsstandarder:** Samarbeta med mjukvarupartner som tillämpar rigorösa riktlinjer för insticksprogram, API:er och integreringar.
- **Övervaka aktivitet och granska regelbundet:** Frekventa insynsgranskningar säkerställer integriteten hos tredjepartstjänster.
- **Utför regelbundna tester:** Driftsätt intrångstester och bedömningar av fast mjukvara för att validera enhetens integritet kontinuerligt.
- **Utbilda medarbetarna:** Utbilda teamen i att känna igen komponenter eller paket som uppvisar misstänkt beteende.

Så här säkerställer Dell Professional Services företags motståndskraft

Dell Professional Services vägleder företag vid implementering av robusta försvar i leverantörskedjan. Team med erfarna cybersäkerhetsexperter tillhandahåller bedömningar, utbildning och hothanteringsstrategier som är skräddarsydda för unika organisationsbehov.

- **Implementeringsvägledning:** Anpassa nollförtroende och reviderade leverantörsmetoder strategiskt i leverantörsmiljöer.
- **Incidentrespons:** Se till att företag snabbt återställs efter skadliga incidenter.

Framtidssäkra företagssystem med Dell

Cyberattacker i leverantörskedjan är exempel på sofistikerade moderna hot. Företag behöver skydd som inte bara förhindrar intrång utan även säkerställer snabb återställning när incidenter inträffar. Genom samarbete med Dell Technologies får du tillgång till banbrytande verktyg, strategisk expertis och ett nätverk av betrodda samarbetspartner.

Ta nästa steg

Skydda känsliga tillgångar och effektivisera verksamhetens tillförlitlighet genom att implementera bästa praxis med teknik från Dell Technologies. Kontakta oss idag för en skräddarsydd konsultation medan du förbereder dig för att säkra dina företagssystems livlina.

Dell Technologies representerar förtroende, anpassningsförmåga och innovation i takt med att cybersäkerheten i leverantörskedjan utvecklas. Dagens engagemang säkrar morgondagens framgång.

En säkrare framtid börjar med Dell Technologies. Lita på oss för att skydda det som är viktigast.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **Dell.com/SecuritySolutions**

Mer information om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

DELL Technologies