Infiltratie van back-ups: versterking van cyberbeveiliging en veerkracht met Dell Technologies

Beknopt overzicht

Infiltratie van back-ups vormt een groeiende bedreiging voor bedrijven in elke sector. Er wordt hierbij gebruik gemaakt van beveiligingslekken in systemen die juist zijn ontworpen om kritieke informatie te beschermen. Deze aanvallen compromitteren dataherstelsystemen, ondermijnen het vertrouwen en brengen activiteiten in gevaar. De gevolgen kunnen ernstig zijn - van aanzienlijke financiële verliezen tot langdurige downtime en reputatieschade.

Dell Technologies biedt een uitgebreide reeks beveiligingsmaatregelen om gevoelige data te beschermen en dergelijke aanvallen te voorkomen. Deze maatregelen bestaan uit Dell Trusted Devices, Dell Trusted Infrastructure en uitgebreide beveiligingsmogelijkheden die in al onze oplossingen zijn geïntegreerd. Door strategische partnerschappen en professionele diensten te combineren kunnen organisaties dankzij Dell een robuust beveiligingsframework opzetten dat uit meerdere lagen bestaat. Dit framework is ontworpen om incidenten waarbij back-ups worden geïnfiltreerd efficiënt te detecteren, voorkomen en herstellen.

Door de innovatieve oplossingen en deskundige support van Dell te implementeren, is de infrastructuur van bedrijven beter beveiligd en blijft de operationele continuïteit behouden.

Toenemende dreiging van geïnfiltreerde back-ups

Back-upsystemen zijn essentieel voor de bedrijfscontinuïteit en het herstel na een cybergebeurtenis, zoals ransomware of hardwarestoringen. Helaas zijn deze reddingsboeien steeds meer het doelwit geworden van cybercriminelen. Bij de infiltratie van back-ups worden back-updata beschadigd of verwijderd, waardoor deze ontoegankelijk worden juist wanneer ze nodig zijn.

Voor deze evoluerende bedreigingen zijn proactieve maatregelen vereist. Het niet beschermen van back-upsystemen brengt activiteiten in gevaar en stelt gevoelige data bloot. Bedrijven van elke omvang, van kleine ondernemingen tot multinationals, vormen een potentieel doel, waarbij sectoren zoals gezondheidszorg, de financiële sector en productiefaciliteiten in het bijzonder in gevaar komen.

Dell Technologies erkent de urgentie van het versterken van back-upomgevingen, heeft geavanceerde tools en biedt begeleiding om deze geavanceerde aanvallen tegen te gaan.

Infiltratieaanvallen van back-ups

Infiltratie van back-ups vindt plaats wanneer cybercriminelen beveiligingslekken in back-upsystemen misbruiken om kritieke hersteldata in gevaar te brengen, te vernietigen of te versleutelen. Deze geavanceerde aanvallen kunnen samenvallen met of volgen op andere incidenten, zoals ransomware- of malware-implementatie, waardoor de operationele en financiële gevolgen worden versterkt.

Hoe back-upaanvallen werken

1. **Eerste inbraak:** aanvallers krijgen ongeautoriseerde toegang tot het netwerk, vaak door middel van phishing, zwakke inloggegevens of niet-gerepareerde beveiligingslekken.
2. **Laterale verplaatsing:** als aanvallers zich eenmaal binnen het netwerk bevinden, gebruiken ze tools om zich ongemerkt te verplaatsen, waarbij ze zich richten op storagelocaties voor back-updata en essentiële datasets.
3. **Schending van back-ups:** belangrijke tactieken zijn het versleutelen van back-upbestanden, het verwijderen van herstelpunten of het beschadigen van data.

Veelvoorkomende technieken

- **Bij diefstal van inloggegevens** worden beheeraccounts gehackt om volledige toegang tot back-upsystemen te krijgen.
- **Bij een ransomware-implementatie** worden zowel live data als back-ups versleuteld, waarna betaling voor ontsleuteling wordt geëist.
- **Bij getimede beschadiging worden** back-ups geleidelijk aan aangetast om aan detectie te ontsnappen, waardoor bedrijven kwetsbaar zijn wanneer herstel nodig is.

Dergelijke technieken benadrukken de verfijning en ernst van deze bedreigingen, waardoor preventieve actie nodig is.

De impact op bedrijven

Financieel verlies

Infiltratie van back-ups verhoogt de herstelkosten en verlengt de downtime, waardoor de responskosten vaak worden verdubbeld of verdrievoudigd. Voor het herstel van versleutelde of gecompromitteerde back-ups kunnen aanvallers betaling eisen, en mogelijk is er een nieuwe infrastructuur nodig of zijn er dure consultants nodig.

Operationele storing

Zonder bruikbare back-ups worden organisaties geconfronteerd met langdurige hersteltijden die services verstoren, projecten vertragen en kritieke functies stopzetten.

Gevolgen voor de reputatie

Definitief dataverlies of langdurige downtime gaat ten koste van het vertrouwen van belanghebbenden, wat de levensvatbaarheid van een bedrijf op de lange termijn kan schaden.

Praktijkvoorbeeld

Een wereldwijde zorgverlener ontdekte dat zijn back-ups tijdens een ransomware-aanval beschadigd waren geraakt. Ondanks het betalen van het losgeld gingen er drie weken aan patiëntgegevens definitief verloren, waardoor operaties werden vertraagd en rechtszaken moesten worden aangespannen. De totale herstelkosten bedroegen meer dan **$ 50 miljoen.**

Alarmerende statistieken

Recente onderzoeken schatten dat de gemiddelde financiële schade van een gecompromitteerd back-upsysteem meer dan **4,45 miljoen dollar**[1] bedraagt, en dat is inclusief boetes, downtime en herstelkosten. Bijzonder alarmerend is het toenemende aantal dergelijke incidenten, waarbij wereldwijde rapporten een jaarlijkse toename van **39% aan** back-upgerelateerde bedreigingen laten zien.

Bij 57%
van de aanvallen gericht op back-ups slaagt men erin om back-upstoragelocaties binnen te dringen

Bron: 2024: Index Engines

Bestrijding van de infiltratie van back-ups, met Dell Technologies

Dell Technologies biedt een robuuste suite van tools en services die de unieke uitdagingen van infiltratie-aanvallen bij back-ups aanpakken, zodat bedrijven deze kunnen voorkomen, detecteren en ervan kunnen herstellen.

Beveiligingsoplossingen voor servers en storage

De server- en storageoplossingen van Dell bieden een ongeëvenaarde weerstand tegen pogingen om back-ups als doelwit te kiezen. Geïntegreerde functies zorgen ervoor dat back-ups beschermd zijn en dat snapshots niet worden gecompromitteerd.

- **Onveranderlijke back-ups/snapshots** zorgen voor herstelpunten die bestand zijn tegen sabotage.
- **Bij air-gapped herstel** worden data geïsoleerd van live netwerken om beschadiging te voorkomen.

[1] Ponemon - Cost of a Data Breach Report 2024

Fortify Dell Data Protection apparaten

In Dell Data Protection apparaten zijn functies opgenomen zoals Dell SafeBIOS voor firmware-integriteit en SafeData voor veilige versleuteling om bescherming te bieden tegen aanvallen die zijn gericht op back-ups. Bovendien bieden deze oplossingen mogelijkheden zoals multi-factor authenticatie (MFA), op rollen gebaseerde toegangscontroles (RBAC) en dubbele verificatie om dreigingsactoren buiten de deur te houden.

Geavanceerde bedreigingsdetectie met CrowdStrike

De integratie tussen CrowdStrike en Dell Data Protection richt zich op het verbeteren van de beveiliging en bewaking van databeschermingsomgevingen door middel van een reeks geavanceerde mogelijkheden.

1. **Eindpunt- en databescherming:** Dell integreert de eindpuntbeveiliging en uitgebreide detectie en respons (EDR/XDR) van CrowdStrike met de oplossingen om data te beschermen. Deze bestaan uit telemetrieverzameling vanuit Dell PowerProtect Data Manager en PowerProtect Data Domain, naast beveiligingsinzichten vanuit de CrowdStrike Falcon console en next-generation SIEM software
2. **Bewaken en reageren:** de MDR-service (Managed Detection and Response) van Dell beheert de CrowdStrike-software namens klanten, verzamelt logboeken en onderzoekt eventuele detecties van een indicator van inbreuk (IOC) of afwijkingen. Met deze integratie kan Dell continu bewaking bieden en samenwerken met de SOC van de klant om te garanderen dat bedreigingen snel en effectief worden opgelost
3. **Realtime zichtbaarheid en controle over dataverplaatsing:** het CrowdStrike Falcon Data Protection platform biedt realtime inzicht in dataverplaatsing tussen verschillende bronnen en kanalen, waarbij data worden geclassificeerd op basis van zowel content als context. Dit draagt bij aan het voorkomen van datadiefstal en het effectief afdwingen van databeschermingsbeleid door content te combineren met contextuele analyses
4. **Uniform beheer en vereenvoudigde implementatie:** dankzij de integratie kan één platform en agent zowel eindpunten als databescherming beheren, waardoor complexiteit en operationele overhead worden verminderd. Dit wordt mogelijk gemaakt door de lichtgewicht en cloud-native aanpak van het CrowdStrike Falcon platform, waardoor snelle implementatie en minimale onderbrekingen mogelijk zijn

De integratie tussen CrowdStrike en Dell Data Protection maakt gebruik van geavanceerde EDR/XDR-mogelijkheden, realtime bewaking en uitgebreid databeheer om de algehele beveiliging en veerkracht van databeschermingsomgevingen te verbeteren.

Een toonaangevende financiële instelling heeft onlangs PowerProtect Cyber Recovery geïmplementeerd, waardoor aanvallers geen toegang hebben tot 90% van de kritieke back-ups tijdens een inbreuk, en naadloos herstel mogelijk is zonder dat er losgeld hoeft te worden betaald.

Dell PowerProtect oplossingen voor back-upintegriteit

Dell PowerProtect biedt uitgebreide back-upbescherming, waarbij gebruik wordt gemaakt van onveranderlijkheid, isolatie en compressie om schending van het back-upsysteem te voorkomen. Door te integreren met ransomware-detectietools zorgt PowerProtect ervoor dat verdachte wijzigingen waarschuwingen activeren zodat onmiddellijk actie kan worden ondernomen.

De meerlaagse beveiligingsaanpak

Voor de bescherming van data zijn gecoördineerde, veelzijdige beveiligingsstrategieën vereist. Dell helpt bedrijven best practices in de sector te implementeren om een veerkrachtige back-upomgeving op te bouwen.

Belangrijke stappen om uw verdediging te verbeteren

- **Implementeer Zero Trust-principes:** valideer voortdurend alle gebruikers, apparaten en processen, zodat het risico op onbevoegde toegang wordt verminderd.
- **Versleutel alle back-ups:** zorg ervoor dat data onleesbaar blijven adat ze zijn gecompromitteerd, zowel tijdens overdracht als in rust.
- **Informeer werknemers:** leer werknemers om phishing-pogingen en andere social engineering-tactieken te herkennen die tot een eerste inbreuk kunnen leiden.
- **Test regelmatig op beveiligingslekken:** met frequente tests kunnen organisaties zwakke gebieden identificeren en repareren voordat aanvallers er misbruik van maken.

Dell combineert deze praktijken met geavanceerde oplossingen en bouwt een robuuste en responsieve infrastructuur die klaar is voor opkomende uitdagingen.

Strategische partnerschappen die de beveiliging verbeteren

Dell werkt samen met cyberbeveiligingsleiders zoals Microsoft, CrowdStrike en Secureworks. Elk partnerschap verbetert de oplossingen van Dell en biedt klanten ongeëvenaarde beschermingsmogelijkheden, zoals informatie over geavanceerde bedreigingen, bewaking van eindpunten en uitgebreide responsstrategieën.

Dell Professional Services inzetten

Dell Professional Services van Dell Technologies biedt expertise en begeleiding om bedrijven te helpen complexe uitdagingen op het gebied van cyberbeveiliging effectief aan te pakken. Specialisten van Dell zorgen er met het opstellen van incidentresponsplannen tot het implementeren van zero-trust architecturen voor dat de omgeving van de klant bestand is tegen moderne bedreigingen, zoals de infiltratie van back-ups.

Bouw bedrijfstolerantie op met Dell

Door Dell Technologies te kiezen, kunnen bedrijven geavanceerde aanvallers beter weren en tegelijkertijd hun operationele continuïteit behouden. Door innovatie, partnerschap en expertise zorgt Dell ervoor dat organisaties zelfs de ernstigste infiltratieaanvallen bij back-ups kunnen voorkomen, detecteren en ervan kunnen herstellen.

Zet de volgende stap

Neem vandaag nog contact op met Dell Technologies om uw bedrijf te beschermen. Samen beveiligen we uw kritieke assets, beschermen we uw reputatie en bouwen we aan een veerkrachtige toekomst.

Dell blijft zich inzetten om het vertrouwen in het digitale tijdperk te bevorderen en organisaties de tools, kennis en support te bieden die ze nodig hebben om veilig te werken en succesvol te zijn.

Degelijke back-ups beginnen bij Dell Technologies. Reageer nu om uw activiteiten toekomstbestendig te maken en vertrouwen op te bouwen in uw cyberbeveiligingsmentaliteit.

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

Meer informatie over Dell oplossingen

Neem contact op met een Dell Technologies Expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies