DELL Technologies

Infiltration i säkerhetskopior: Stärk cybersäkerheten och motståndskraften med Dell Technologies

Sammanfattning

Infiltration i säkerhetskopior utgör ett växande hot mot företag inom alla sektorer – sårbarheter i just de system som är utformade för att skydda kritisk information utnyttjas. Dessa attacker äventyrar dataåterställningssystem, underminerar förtroendet och äventyrar driften. Konsekvenserna kan vara allvarliga, från betydande ekonomiska förluster till längre driftavbrott och skadat anseende.

Dell Technologies tillhandahåller ett heltäckande försvar för att skydda känsliga data och förhindra sådana attacker, inklusive Dell Trusted Devices, Dell Trusted Infrastructure och omfattande säkerhetsfunktioner som är integrerade i alla våra lösningar. Med tillägg av strategiska partnerskap och professionella tjänster hjälper Dell organisationer att etablera ett motståndskraftigt säkerhetsramverk i flera lager för att upptäcka och förhindra incidenter med infiltration i säkerhetskopior samt för effektiv återställning.

Genom att implementera Dells innovativa lösningar och expertsupport är företagen bättre förberedda för att säkra sin infrastruktur och upprätthålla driftskontinuitet.

Ökande hot om infiltration i säkerhetskopior

Säkerhetskopieringssystem är avgörande för verksamhetskontinuitet och av största vikt för återställning efter cyberincidenter, som efter utpressningsvirusattacker eller hårdvarufel. Tyvärr har dessa livlinor alltmer blivit måltavlor för cyberbrottslingar. Infiltration i säkerhetskopior skadar eller raderar säkerhetskopierade data, och gör dem otillgängliga när de behövs som mest.

Mot dessa föränderliga hot krävs proaktiva åtgärder. Underlåtenhet att skydda säkerhetskopieringssystemen äventyrar driften och exponerar känsliga data. Företag i alla storlekar, från små företag till multinationella företag, är potentiella mål, och branscher som hälso- och sjukvård, finans och tillverkning är särskilt utsatta.

Dell Technologies inser hur brådskande det är att stärka säkerhetskopieringsmiljöer och erbjuder avancerade verktyg och vägledning för att motverka sådana sofistikerade attacker.

Attacker mot säkerhetskopior

Infiltration av säkerhetskopior sker när cyberbrottslingar utnyttjar sårbarheter i säkerhetskopieringssystem för att kompromettera, förstöra eller kryptera kritiska återställningsdata. Sådana sofistikerade attacker kan sammanfalla med eller följa efter andra incidenter, t.ex. utpressningsvirus eller installation av skadliga program, vilket förstärker de operativa och ekonomiska konsekvenserna.

Så här fungerar attacker mot säkerhetskopior

1. **Inledande intrång:** Angripare får obehörig åtkomst till nätverket, ofta genom nätfiske, svaga inloggningsuppgifter eller sårbarheter som inte har korrigerats.
2. **Lateral förflyttning:** Väl inne i nätverket använder angriparna verktyg för att förflytta sig utan att bli upptäckta och riktar in sig på lagringen av säkerhetskopior och kritiska datauppsättningar.
3. **Kompromettering av säkerhetskopior:** Viktiga taktiker omfattar kryptering av filer med säkerhetskopior, radering av återställningspunkter eller förvanskning av data.

Vanliga tekniker

- **Stöld av inloggningsuppgifter** för intrång i adminkonton som ger fullständig åtkomst till säkerhetskopieringssystem.
- **Installation av utpressningsvirus** som krypterar både livedata och säkerhetskopior, och betalning för dekryptering krävs.
- **Styrd förstörelse** komprometterar säkerhetskopior gradvis för att undgå upptäckt samtidigt som företag blir exponerade när återställning krävs.

Sådana tekniker lyfter fram hur sofistikerade och allvarliga dessa hot är – och att förebyggande åtgärder krävs.

Påverkan på företag

Ekonomisk förlust

Infiltration i säkerhetskopior leder till ökade återställningskostnader och driftavbrott, och fördubblar eller tredubblar ofta svarskostnaderna. Återställning från krypterade eller komprometterade säkerhetskopior kan kräva att angripare betalas, ny infrastruktur eller dyra konsulter.

Driftstörningar

Utan fungerande säkerhetskopior står organisationer inför långa återställningstider som stör tjänster, försenar projekt och stoppar kritiska funktioner.

Skadat anseende

Permanent dataförlust eller längre driftavbrott urholkar intressenternas förtroende, vilket kan skada företagets långsiktiga lönsamhet.

Verkliga exempel

En global hälso- och sjukvårdsleverantör upptäckte att dess säkerhetskopior hade skadats under en utpressningsvirusattack. Trots att man betalade lösensumman förlorade man tre veckors patientdata permanent, vilket ledde till försenade operationer och stämningar. De totala återställningskostnaderna översteg **50 miljoner USD.**

Skrämmande statistik

Enligt en ny studie uppskattas den genomsnittliga ekonomiska förlusten från ett komprometterat säkerhetskopieringssystem till över **4,45 miljoner USD**[1], vilket inkluderar böter, driftstopp och återställningskostnader. Särskilt oroande är den ökande frekvensen av sådana incidenter, med globala rapporter som visar en ökning av säkerhetskopieringsrelaterade hot med **39 %** från år till år.

57 %
av alla attacker mot säkerhetskopior lyckas infiltrera lagringen av säkerhetskopior

Källa: 2024: Index Engines

Bekämpa infiltration i säkerhetskopior med Dell Technologies

Dell Technologies tillhandahåller en robust uppsättning verktyg och tjänster som hanterar de unika utmaningar som attacker mot säkerhetskopior utgör, och gör det möjligt för företag att effektivt förebygga, upptäcka och återställa.

Säkerhetslösningar för servrar och lagring

Dells server- och lagringslösningar ger oöverträffad motståndskraft mot säkerhetskopieringsinriktade attacker. Inbyggda funktioner säkerställer att säkerhetskopior förblir säkra och att snapshots inte äventyras.

- **Oföränderliga säkerhetskopior/snapshots** skapar manipuleringssäkra återställningspunkter.
- **Återställning med luftgap** isolerar data från aktiva nätverk för att förhindra skador.

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

Stärk Dell Data Protection-enheter

Dell Data Protection-enheter har funktioner som Dell SafeBIOS för integritet för fast mjukvara och SafeData för säker kryptering för att skydda mot attacker mot säkerhetskopior. Dessutom har dessa lösningar funktioner som multifaktorautentisering (MFA), rollbaserade åtkomstkontroller (RBAC) och dubbel autentisering för att hålla hotaktörer borta.

Avancerad hotidentifiering med CrowdStrike

Integreringen mellan CrowdStrike och Dell Data Protection fokuserar på att förbättra säkerheten och övervakningen av dataskyddsmiljöer genom en uppsättning avancerade funktioner.

1. **Slutpunkts- och dataskydd:** Dell integrerar CrowdStrikes slutpunktssäkerhet och utökade identifiering och svar (EDR/XDR) i sina dataskyddslösningar. Detta inkluderar telemetrisamling från Dells PowerProtect Data Manager och PowerProtect Data Domain, tillsammans med säkerhetsinsikter från CrowdStrike Falcon-konsolen och nästa generations SIEM-mjukvara
2. **Övervaka och svara:** Dells Managed Detection and Response (MDR) hanterar CrowdStrike-mjukvaran på uppdrag av kunder, samlar in loggar och undersöker eventuella angreppsindikatorer (IOC) eller upptäckta avvikelser. Tack vare den här integreringen kan Dell tillhandahålla kontinuerlig övervakning och samarbeta med kundens SOC för att säkerställa snabba och effektiva åtgärder vid hot
3. **Insyn och kontroll av dataflytt i realtid:** CrowdStrike Falcon Data Protection-plattformen ger insyn i dataflytt i realtid över olika källor och kanaler, med klassificering av data efter både innehåll och kontext. Detta hjälper till att förhindra datastöld och säkerställa att dataskyddspolicyer tillämpas effektivt genom att kombinera innehåll med kontextuell analys
4. **Enhetlig hantering och förenklad distribution:** Integreringen gör det möjligt för en enda plattform och agent att hantera både slutpunkts- och dataskydd, vilket minskar komplexiteten och driftkostnaderna. Detta underlättas av CrowdStrike Falcon-plattformens lätta och molnbaserade metod, vilket möjliggör snabb distribution och minimala störningar

Integreringen mellan CrowdStrike och Dell Data Protection drar nytta av avancerade EDR/XDR-funktioner, realtidsövervakning och omfattande datahantering för att förbättra den övergripande säkerheten och motståndskraften i dataskyddsmiljöer.

En ledande finansinstitution driftsatte nyligen PowerProtect Cyber Recovery, som hindrar angripare från att komma åt 90 % av alla kritiska säkerhetskopior under ett intrång, och möjliggör smidig återställning utan lösenbetalningar.

Dell PowerProtect-lösningar för integritet i säkerhetskopior

Dell PowerProtect ger omfattande säkerhetskopieringsskydd genom att utnyttja oföränderlighet, isolering och komprimering för att förhindra hot mot säkerhetskopieringssystemet. Genom integrering med verktyg för detektering av utpressningsvirus säkerställer PowerProtect att suspekta förändringar utlöser varningar för omedelbar åtgärd.

Säkerhetsmetod i flera lager

För att skydda data krävs samordnade och mångfacetterade säkerhetsstrategier. Dell hjälper företag att implementera branschens bästa rutiner för att skapa en motståndskraftig säkerhetskopieringsmiljö.

Viktiga steg för att förbättra försvaret

- **Anta nollförtroendeprinciper:** Validera kontinuerligt alla användare, enheter och processer, för att minska risken för obehörig åtkomst.
- **Kryptera alla säkerhetskopior:** Se till att data förblir oläsliga om de äventyras, både under flytt och i vila.
- **Utbilda medarbetarna:** Lär medarbetare att känna igen nätfiskeförsök och andra taktiker för social manipulering som leder till inledande intrång.
- **Regelbundna sårbarhetstester:** Frekventa tester hjälper organisationer att identifiera och korrigera svaga områden innan angripare kan utnyttja dem.

Dell kombinerar dessa metoder med banbrytande lösningar och bygger en robust och responsiv infrastruktur som är redo att möta nya utmaningar.

Strategiska partnerskap som förbättrar säkerheten

Dell samarbetar med cybersäkerhetsledare som Microsoft, CrowdStrike och Secureworks. Varje partnerskap förbättrar Dells lösningar och erbjuder kunderna oöverträffade skyddsfunktioner som avancerad hotinformation, slutpunktsövervakning och omfattande svarsstrategier.

Dra nytta av Dell Professional Services

Dell Technologies Professional Services tillhandahåller expertis och vägledning för att hjälpa företag att hantera komplexa cybersäkerhetsutmaningar på ett effektivt sätt. Dells specialister ser till att kundmiljöer förblir motståndskraftiga mot moderna hot som infiltration i säkerhetskopior, med allt från att skapa incidentresponsplaner till att implementera nollförtroendearkitekturer.

Bygg upp företagets motståndskraft med Dell

Företag som väljer Dell Technologies har större chans att utmanövrera sofistikerade angripare samtidigt som de upprätthåller driftskontinuitet. Genom innovation, samarbete och expertis säkerställer Dell att organisationer kan förhindra, upptäcka och återställa även de mest allvarliga attackerna mot säkerhetskopior.

Ta nästa steg

Kontakta Dell Technologies idag för att skydda ditt företag. Tillsammans skyddar vi dina kritiska tillgångar och ditt anseende och bygger en motståndskraftig framtid.

Dell är fast beslutna att främja förtroende för den digitala eran och ge organisationer de verktyg, den kunskap och det stöd de behöver för att fungera på ett säkert sätt och frodas.

Motståndskraft i säkerhetskopiering börjar med Dell Technologies. Agera nu för att framtidssäkra din verksamhet och skapa förtroende för din cybersäkerhetsställning.

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

Läs mer om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

DELL Technologies