DELL Technologies

Nolldagsattacker: Stärk cybersäkerheten och motståndskraften med Dell Technologies

Det ökande hotet från nolldagsattacker

Nolldagsattacker har snabbt blivit en av de mest allvarliga utmaningarna i dagens cybersäkerhetslandskap. Dessa attacker utnyttjar sårbarheter som är okända för mjukvaruleverantörer och säkerhetsexperter. Resultatet är att företag blir oförberedda och exponerade. Företag i alla branscher, från hälso- och sjukvård till finanssektorn, är sårbara för dessa intrång och de leder ofta till allvarliga ekonomiska och driftsmässiga konsekvenser.

Takten i den digitala omvandlingen ökar och nolldagsattacker har blivit vanligare och mer sofistikerade. Behovet av starkt och robust skydd har aldrig varit större. Dell Technologies inser det här hotets allvarliga natur och ger företag innovativa och skalbara försvar för att effektivt bekämpa och återhämta sig från nolldagsattacker.

Vad är en nolldagsattack?

En nolldagsattack innebär att en hemlig säkerhetsrisk i mjukvara eller hårdvara utnyttjas innan en korrigeringsfil eller korrigering blir tillgänglig. Angripare utnyttjar den här möjlighetens fönster, något som ofta orsakar omfattande störningar innan sårbarheten upptäcks och åtgärdas.

Så här fungerar nolldagsattacker

1. **Upptäckt av sårbarhet:** Hackare identifierar kodningsbrister eller dolda bakdörrar i program eller system.
2. **Utveckling av sårbarheter:** Skadliga program skapas för att utnyttja sårbarheten. Angripare kan använda riktade nätfiskekampanjer eller webbplatser med skadliga program för att genomföra dessa attacker.
3. **Utförande av attack:** Sårbarheten i systemet skapas och hela systemet blir komprometterat. Resultatet är att detta potentiellt möjliggör datastöld eller driftstörningar.

Vanliga tekniker

- Drive-by downloads gör att användare oavsiktligt installerar skadliga program.
- Nätfiskemejl innehåller skadliga länkar eller nyttolaster som utnyttjar sårbarheter.
- Fillösa attacker undviker upptäckt genom att de utför åtgärder i systemets minne.

Dessa otroligt avancerade attackvektorer gör nolldagsattacker extra farliga eftersom traditionella signaturbaserade detekteringsverktyg ofta inte känner igen dem.

Påverkan på företag

Nolldagsattacker medför betydande risker på grund av oförutsägbarheten och att de inte upptäcks i tid. Konsekvenserna kan bli katastrofala på flera fronter.

Ekonomisk förlust

En lyckad nolldagarsattack kan leda till höga kostnader, från böter till förlorade intäkter under driftavbrott. Till exempel kan en oidentifierad sårbarhet som utnyttjas i en e-handelsplattform inaktivera kassaprocessen och direkt påverka försäljningen.

Skadat anseende

Allmänhetens uppfattning om ett företag kan skadas oåterkalleligt. Kunder tappar förtroendet för ett företag när känslig information exponeras eller tjänster slutar fungera.

Driftstörningar

Sårbarheter som inte åtgärdas förlamar ofta system. Det leder till minskad produktivitet, försenade projekt och missade affärsmöjligheter.

Verkliga exempel

En stor hälso- och sjukvårdsleverantör blev utsatt för en nolldagsattack som riktade sig mot mjukvara för medicinsk utrustning, mjukvara som inte hade korrigerats. Attacken störde viktig verksamhet, exponerade patientdata och kostade företaget **miljoner** i återställningsavgifter samtidigt som patienternas förtroende urholkades.

Skrämmande statistik

Enligt en Ponemon-studie från 2023 visar forskning att andelen intrång som involverar nolldagsattacker ligger på cirka 80 %

Nolldagsattacker representerar **70 %** av de sårbarheter som utnyttjas

Källa: 2024: IMandiant ”M-Trends”

Bekämpa nolldagsattacker med Dell Technologies

Dell Technologies levererar branschledande lösningar för att hjälpa företag att aktivt skydda sig mot nolldagsattacker samtidigt som de främjar snabb återställning i efterdyningarna av sådana intrång.

Säkerhetslösningar för servrar och lagring

Dells säkerhetslösningar för servrar och lagring ger ytterligare skyddslager:

- Säkra servrar övervakar och blockerar obehöriga åtkomstförsök.
- System för säkerhetskopiering och återställning av data säkerställer att viktig information förblir tillgänglig och intakt även i värsta fall.

Förstärkta slutpunkter med Dell Trusted Devices

Slutpunkter är en viktig ingångspunkt för angripare. Dell Trusted Devices integrerar avancerade säkerhetsåtgärder och säkerställer att slutpunkter förblir skyddade mot oupptäckta hot.

- **SafeBIOS** skyddar fast mjukvara från manipulering och säkerställer systemets integritet från grunden.
- **SafeID** skyddar användaruppgifter genom att säkra autentiseringsprocesser.
- **SafeData** krypterar känsliga data vid vila och under överföring, och gör dem värdelösa i händelse av avlyssning eller utnyttjande.

Proaktiv hotdetektering med CrowdStrike

CrowdStrike använder avancerad analys och AI för att övervaka slutpunktsaktivitet och upptäcka ovanligt beteende som kan tyda på nolldagsattacker. Denna proaktiva hotdetektering säkerställer snabb respons innan sårbarheter kan leda till omfattande skador.

Till exempel upptäckte telekommunikationsleverantör som använde CrowdStrike avvikelser i nätverkstrafiken tidigt. Det här mildrade en potentiell nolldagsattack på kundservrar.

Dell PowerProtect-lösningar

Dell PowerProtect levererar robusta, oföränderliga säkerhetskopieringar och isolerade återställningsalternativ. Företag kan snabbt och effektivt återställa driften efter en nolldagarsattack, upprätthålla affärskontinuitet och skydda viktiga kunddata.

Till exempel använde en stor detaljhandelskedja PowerProtect för att återställa krypterade filer som komprometterats av en nätfiskeattack som berodde på en sårbarhet inför nolldagsattacker, och undviker därmed långa driftavbrott.

Avancerad nätverkssäkerhet och mikrosegmentering med Dell PowerSwitch Networking och SmartFabric OS

Stärker försvaret mot nolldagsattacker genom att leverera avancerad nätverkssegmentering, strikta åtkomstkontroller och trafikanalys i realtid i hela infrastrukturen.

Betydelsen av en säkerhetsmetod i flera lager

Hög säkerhet kräver mer än en lösning. En strategi i flera lager kombinerar teknik, processer och människor för att skapa ett omfattande skyddsramverk.

Viktiga åtgärder för att stärka försvaret

- **Anta nollförtroendeprinciper:** Verifiera varje individ och enhet som försöker få åtkomst till nätverket.
- **Implementera avancerad kryptering:** Använd krypteringsprotokoll för att skydda både data i rörelse och vid vila.
- **Utbilda medarbetarna:** Erbjud detaljerade utbildningssessioner för att lära medarbetarna hur de känner igen nätfiskeförsök och taktiker för social manipulering.
- **Testa system regelbundet:** Utför konsekventa intrångstester och sårbarhetsgenomsökningar för att säkerställa att försvaret anpassar sig till nya hot.

Dell Technologies kombinerar dessa metoder med sina avancerade säkerhetslösningar och säkerställer att företag är redo att effektivt bekämpa sårbarheter med nolldagsproblem.

Partnerskap som stärker cybersäkerheten

Dells samarbete med branschledarna **Microsoft**, **CrowdStrike** och **Secureworks** ger kunderna tillgång till banbrytande säkerhetsinformation och verktyg.

- **Microsoft** integreras smidigt med Dells lösningar för att säkerställa kompatibilitet i hela systemet och proaktiva skyddsmekanismer
- **CrowdStrike** erbjuder avancerad hotinformation gällande slutpunkter för att upptäcka potentiella kryphål för nolldagsattacker.
- **Secureworks** levererar kontinuerlig övervakning och expertåtgärder för attacksvar i realtid.

Dra nytta av Dell Professional Services

Dells professionella tjänster erbjuder ett omfattande utbud av rådgivning, implementering och återställningshjälp för att hjälpa företag att hantera och minska riskerna förknippade med hot från nolldagsattacker. Dell hjälper företag att uppnå långsiktig motståndskraft: från incidentåtgärder till planering av cybersäkerhetsplaner.

Bygg en motståndskraftig framtid

Att investera i Dell Technologies innebär att ha en partner som inte bara erbjuder överlägsen teknik utan även sinnesro. Genom banbrytande lösningar, strategiska partnerskap och oöverträffad expertis gör Dell det möjligt för företag att förutse, upptäcka och återställa även från de mest avancerade nolldagsattackerna.

Kontakta Dell Technologies idag för att skydda ditt företag och ditt rykte – låt istället ditt företag stärkas i ett oförutsägbart digitalt landskap. Lita på att Dell skyddar dig mot morgondagens hot.

Dell Technologies ger förtroende och gör det möjligt för företag att ligga steget före nya nolldagsattacker genom säkerhetslösningar och tjänster som utformats för att skydda det som är allra 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