DELL Technologies

# Skadlig insiderattack: Stärk cybersäkerheten och motståndskraften med Dell Technologies

## Det ökande hotet från skadliga insiderattacker

Skadliga insiderattacker har blivit ett av de mest akuta cybersäkerhetshoten i dagens företagslandskap. Till skillnad från externa hot har skadliga insiders redan en viss grad av förtroende och åtkomst inom en organisation. Det gör deras handlingar särskilt skadliga och svårare att upptäcka. Insiderattacker som att få åtkomst till känsliga data eller sabotera system kan lamslå viktig verksamhet i företaget, skada företagets rykte och få allvarliga ekonomiska konsekvenser.

Dell Technologies inser den växande fara som dessa attacker utgör och utvecklar därför innovativa, skalbara lösningar som hjälper företag att identifiera, förebygga och minska riskerna för skadliga insiderattacker. Genom att kombinera toppmodern teknik med expertledda tjänster hjälper Dell företag att ligga steget före dessa interna hot.

## Vad är skadliga insiderattacker?

En skadlig insiderattack inträffar när en person inom ett företag missbrukar sin åtkomst för att kompromettera data, störa driften eller extrahera känslig information för personliga, ekonomiska eller konkurrensmässiga mål. Den här personen kan vara en anställd, entreprenör, partner eller någon annan med legitim åtkomst till företagets system och nätverk.

## Så här fungerar skadliga insiderattacker

Skadliga insiders utnyttjar sin betrodda position för att kringgå traditionella säkerhetsförsvar. Exempel på vanliga attacker:

1. **Datastöld:** Exfiltrering av konfidentiella kunddata, immateriell egendom eller ekonomiska register.
2. **Sabotage:** Avsiktligt skada IT-system för att störa affärsverksamheten eller skada företagets anseende.
3. **Missbruk av inloggningsuppgifter:** Använda stulna eller missbrukade inloggningsuppgifter för att eskalera åtkomstbehörigheter eller skapa dummykonton.
4. **Samarbete med externa angripare:** Dela åtkomst eller känslig information med externa cyberbrottslingar i utbyte mot ekonomisk vinning.

Denna dubbla fördel med förtroende och intern kunskap gör skadliga insiders exceptionellt farliga jämfört med externa angripare.

## Påverkan på företag

Antalet skadliga insiderattacker är omfattande och orsakar skador som sträcker sig bortom ekonomiska förluster. Företag kan drabbas av konsekvenser som:

### Ekonomisk förlust

Stöld av känslig information, bedrägeri eller sabotage leder till förlust av intäkter och återställningskostnader som kan uppgå till miljontals dollar.

### Driftstörningar

Systemsabotage eller datadestruktion kan stoppa driften, något som resulterar i förseningar, missade möjligheter och minskad produktivitet.

### Skadat anseende

Intrång eller angrepp från insiders urholkar kundernas och intressenternas förtroende. Det i sin tur påverkar kundernas lojalitet och marknadens uppfattning av företaget.

### Bristande regelefterlevnad

Beroende på bransch kan insiderattacker leda till höga böter och påföljder för känsliga data som hälso- och sjukvård eller ekonomi.

## Verkliga exempel

En IT-entreprenör som år 2020 arbetade för ett stort finansbolag raderade avsiktligt kritiska systemkonfigurationer, något som orsakade nätverksavbrott i över **10 timmar**. Sabotaget ledde till **miljontals** dollar i ekonomiska förluster, omfattande återställningskostnader och ett skadat anseende. Sådana incidenter illustrerar den destruktiva potentialen hos insiderhot och understryker hur brådskande det är med robusta åtgärder för detektering och förebyggande.

## Beräknad kostnad

Den genomsnittliga kostnaden för en insiderrelaterad incident uppskattas till **4,99 miljoner USD** och utgör nästan **55 %** av alla intrång, enligt en studie utförd av Ponemon Institute 2024. Den här siffran tar hänsyn till kostnader för detektering, återställning och reducering. Den visar också det akuta behovet företag har att investera i förebyggande försvar mot insiderrisker.

**83%**

av företagen rapporterade minst en insiderattack under det senaste året

Källa: 2024: Cybersecurity Insiders' Report

## Bekämpa skadliga insiderattacker med Dell Technologies

Dell Technologies erbjuder ett omfattande ekosystem av verktyg och tjänster för att bekämpa skadliga insiderhot. Det säkerställer att ditt företag är förberett på det oväntade.

### Säkra slutpunkter med Dell Trusted Devices

Slutpunkter fungerar ofta som ingångspunkter för insiderhot. Dell Trusted Devices integrerar banbrytande säkerhetsfunktioner i hårdvaran för att stärka slutpunkter och skydda känsliga data.

- **Dell SafeBIOS** säkerställer integriteten för fast mjukvara och förhindrar försök att manipulera systemåtgärder på maskinvarunivå.
- **SafeID** skyddar inloggningsuppgifter, förhindrar obehörig åtkomst och missbruk av inloggningsuppgifter.
- **SafeData** krypterar känsliga data från början till slut och säkerställer att upphämtad eller extraherad information förblir oläsbar för skadliga insiders.

Genom att driftsätta dessa lösningar kan företag säkerställa att deras slutpunkter är skyddade, oavsett om hotet är internt eller externt.

### Proaktiv hotidentifiering med CrowdStrike

För att identifiera insiderhot krävs synlighet och övervakning av användarbeteenden. CrowdStrike är integrerat i Dells lösningar och använder artificiell intelligens och beteendeanalys för att upptäcka avvikelser som tyder på insiderhot.

Onormala dataöverföringar utanför kontorstid eller obehörig åtkomst till kritiska områden i nätverket flaggas omedelbart, något som underlättar snabba åtgärder. En hälso- och sjukvårdsorganisation i USA drog nyligen nytta av proaktiv hotdetektering för att identifiera och stoppa en medarbetares försök att utvinna patientdata, vilket förhindrade ett kostsamt intrång.

### Förbättrat dataskydd med Dell PowerProtect

Dell PowerProtect ger en robust försvarslinje genom säker säkerhetskopiering, lagring med luftgap och oföränderliga kopior av kritiska data. Genom att säkerställa att känslig information skyddas från ändring eller radering kan insiderattacker som riktar sig mot dataintegritet bli verkningslösa.

Ett exempel är ett tillverkningsföretag som upptäckte att de hade en missnöjd anställd som försökte sabotera designfiler. Dell PowerProtects återställningsvalv gjorde det möjligt för företaget att återställa driften inom några timmar, undvika störningar och upprätthålla affärskontinuitet.

### Snabb incidentåterställning med Dell Professional Services

När ett insiderhot eskalerar till en incident är snabb återställning avgörande. Dell Professional Services, inklusive fjärrdataåterställning och incidentsvar, säkerställer att företag snabbt kan återställa data och system. Dells experter leder processen för att minimera driftavbrott och minska påverkan.

Det här är bara några exempel i Dells portfölj med lösningar som kan hjälpa till med skadliga insiderhot.

### 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

Ett effektivt försvar mot insiderrisker kräver mer än ett skyddslager. Implementering av en säkerhetsstrategi i flera lager säkerställer att ingen sårbarhet blir en svag punkt. Viktiga steg omfattar:

### Viktiga steg för att förbättra försvaret

- **Nollförtroendeprinciper:** Verifiera kontinuerligt alla åtkomstförfrågningar och anta att ingen enhet är betrodd, inte ens inom perimetern.
- **Rollbaserade åtkomstkontroller (RBAC):** Begränsa medarbetarnas åtkomst till endast de system och data som krävs för deras roller.
- **Avancerade krypteringslösningar:** Kryptera data i vila och under överföring, något som effektivt neutraliserar datastöld.
- **Medarbetarnas medvetenhet och utbildning:** Inför frekventa program för säkerhetsmedvetenhet för att förhindra oavsiktlig medverkan i skadlig aktivitet.
- **Regelbundna systemtester:** Utför intrångstester och sårbarhetsgenomsökningar för att säkerställa att försvaret förblir tillförlitligt.

Dessa metoder, förstärkta av Dells lösningar, skapar ett enastående och heltäckande skyddsramverk mot skadliga insiders.

## Stärk försvaret genom strategiska partnerskap

Dell samarbetar med branschledande cybersäkerhetsleverantörer som **CrowdStrike** och **Secureworks** för att ytterligare stärka deras lösningar. CrowdStrike förbättrar slutpunktssäkerheten och ger värdefull hotinformation om indikatorer på intrång, medan Secureworks erbjuder avancerade hotdetekterings- och svarstjänster. Dessa samarbeten säkerställer att Dells kunder drar nytta av ett ekosystem av integrerad och banbrytande teknik.

## Därför bör du välja Dell Technologies för cybersäkerhet

Dell Technologies fortsätter att vara den gyllene standarden för cybersäkerhetslösningar i flera lager. Företag drar nytta av Dells branschledande expertis, djupa partnerskap och innovativa produktutbud som anpassar sig till dagens föränderliga hotlandskap. Dell erbjuder ett komplett ramverk för motståndskraft som skapar förtroende och möjliggör tillväxt, med slutpunktssäkerhet, insiderdetektering och incidentåterställning.

## Bygg en motståndskraftig framtid med Dell Technologies

Skydda ditt företag mot skadliga insiderhot med Dell Technologies omfattande och skalbara lösningar. Genom att samarbeta med Dell säkrar du inte bara din verksamhet utan säkerställer även affärskontinuitet, främjar kundernas förtroende och framtidssäkrar din organisation. Kontakta oss om du vill veta mer om hur du implementerar proaktivt försvar idag.

Dell Technologies är din betrodda bundsförvant när det gäller att bekämpa insiderhot, skydda dina kritiska tillgångar och hjälpa ditt företag att blomstra i en dynamisk digital miljö. En framtid med säkerhet är en framtid med framgång, och den börjar med Dell.

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