DELL Technologies

INTERAKTIVA CYBERSÄKERHETSSCENARIER – E-BOK

Verkliga scenarier. Smartare beslut. Starkare försvar.

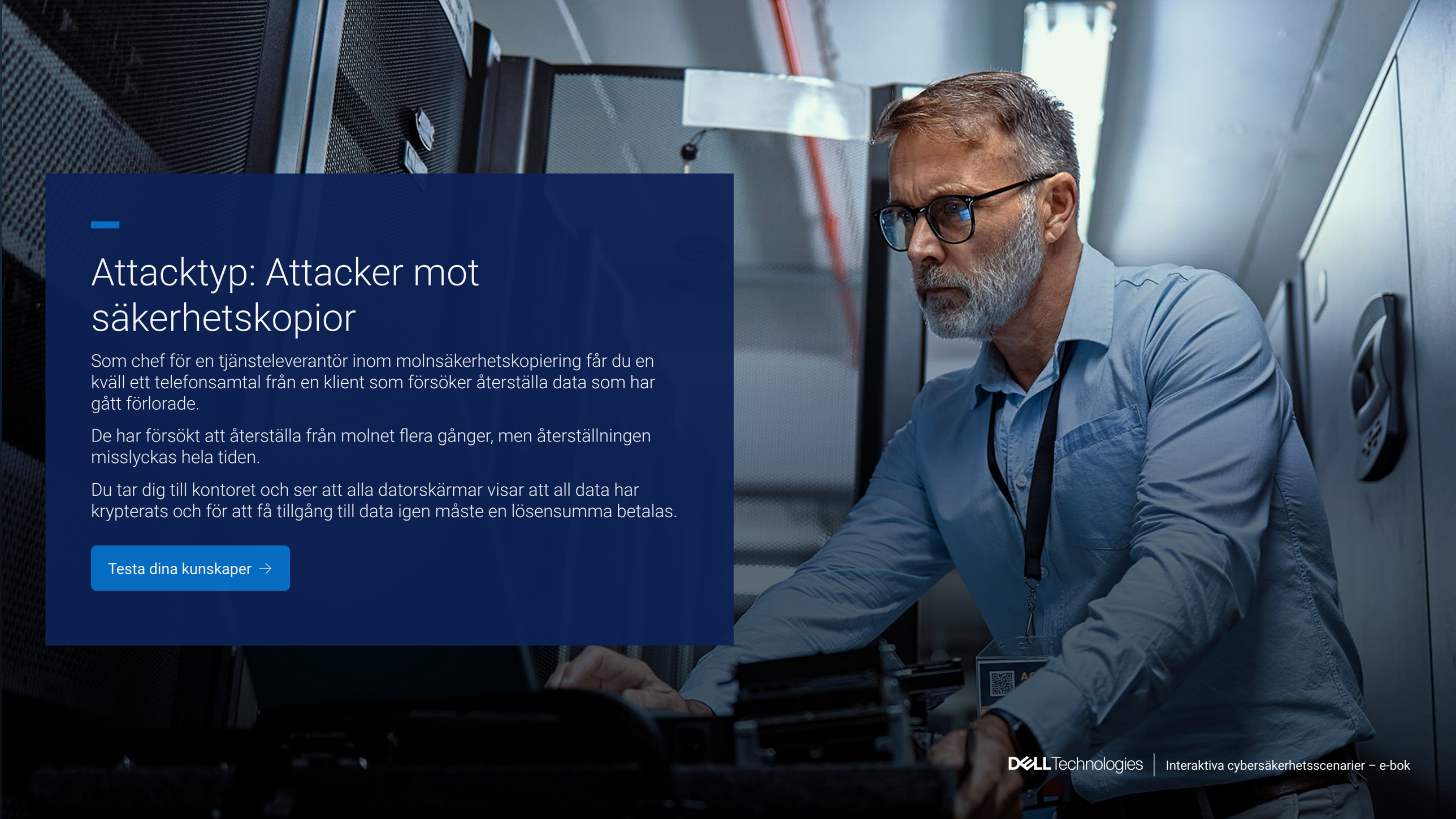
Dells engagemang för säkerhet är grunden för allt vi gör. Denna e-bok delar med sig av insikter, bästa praxis och innovativ teknik med målet att ge dig de verktyg och den kunskap du behöver för att ligga steget före nya cyberrisker.

Välj ett attackscenario

Cybersäkerhetshoten utvecklas hela tiden och organisationer måste hantera dem på ett effektivt sätt för att skydda sina data. Du kan förbereda organisationen på bästa sätt genom att fördjupa dig i simuleringsövningar från verkligheten som hjälper dig att hitta rätt cybersäkerhetsstrategier för att bekämpa cyberattacker.

Utforska många olika attacktyper och branschspecifika utmaningar inom sektorer som nationella, regionala och lokala myndigheter, finansiella tjänster och hälso- och sjukvård. Längs vägen upptäcker du hur Dells integrerade säkerhetslösningar, för allt från bärbara och stationära datorer till företagssystem, har utformats för att skydda mot dessa hot.

- Attacker mot säkerhetskopior →
- Ransomware →
- Distribuerad överbelastningsattack (DDoS) →
- Hårdvara i leverantörskedjan →
- Skadlig insiderattack →
- Mjukvara i leverantörskedjan →
- Man-in-the-Middle-attack (MITM) →
- Nolldagsattack →
- Prompt-/SQL-injektion →



Attacktyp: Attacker mot säkerhetskopior

Som chef för en tjänsteleverantör inom molnsäkerhetskopiering får du en kväll ett telefonsamtal från en klient som försöker återställa data som har gått förlorade.

De har försökt att återställa från molnet flera gånger, men återställningen misslyckas hela tiden.

Du tar dig till kontoret och ser att alla datorskärmar visar att all data har krypterats och för att få tillgång till data igen måste en lösensumma betalas.

Testa dina kunskaper →

Attacktyp: Attacker mot säkerhetskopior

1: Minimera angreppsytan — 2 — 3 — 4

Du är inte säker på vilka säkerhetskopieringssystem eller kunder som har påverkats. Vad bör vara ditt första steg?

- [ ] Underrätta myndigheterna
- [ ] Stäng av alla system
- [ ] Försök att begränsa och isolera hotet
- [ ] Identifiera om du har en ren säkerhetskopia att återställa från

Se rätt svar →

Attacktyp: Attacker mot säkerhetskopior

1: Minimera angreppsytan — 2 — 3 — 4

Du är inte säker på vilka säkerhetskopieringssystem eller kunder som har påverkats. Vad bör vara ditt första steg?

- ✗ Underrätta myndigheterna
- ✗ Stäng av alla system
- ✓ Försök att begränsa och isolera hotet
- ✗ Identifiera om du har en ren säkerhetskopia att återställa från

Genom att omedelbart begränsa och isolera ett hot förhindras ytterligare spridning eller skada och man får tid att bedöma incidentens omfattning, vilket kan minimera påverkan för alla typer av cyberattacker, inklusive sådana som omfattar AI.

Nästa fråga →

Attacktyp: Attacker mot säkerhetskopior

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Din prioritet är att se till att dina kunders data blir tillgängliga för dem snabbt. Hur skulle du åstadkomma det?

- [ ] Betala lösensumman
- [ ] Identifiera typen av utpressningsvirus
- [ ] Underrätta myndigheterna
- [ ] Identifiera vilka data som har utsatts för risk

Se rätt svar →

Attacktyp: Attacker mot säkerhetskopior

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Din prioritet är att se till att dina kunders data blir tillgängliga för dem snabbt. Hur skulle du åstadkomma det?

- ✗ Betala lösensumman
- ✗ Identifiera typen av utpressningsvirus
- ✗ Underrätta myndigheterna
- ✓ Identifiera vilka data som har utsatts för risk

Genom att identifiera vilka data som har utsatts för risk kan du fokusera återställningsinsatserna på att återställa den mest kritiska kundinformationen, vilket säkerställer snabbare datatillgänglighet och förhindrar onödigt arbete på system som inte påverkas.

Nästa fråga →

Attacktyp: Attacker mot säkerhetskopior

1 — 2 — 3: Återställning efter en cyberattack — 4

Du identifierar en säkerhetskopia som det går att återställa från. Vad bör vara det första steget i processen?

- [ ] Prioritera återställning av kritiska system först
- [ ] Använda kriminalteknisk analys för att bekräfta att attacken har inneslutits helt
- [ ] Ändra alla lösenord och återkalla inloggningsuppgifter som utsatts för risk
- [ ] Implementera nollförtroendeprinciper

Se rätt svar →

Attacktyp: Attacker mot säkerhetskopior

1 — 2 — 3: Återställning efter en cyberattack — 4

Du identifierar en säkerhetskopia som det går att återställa från. Vad bör vara det första steget i processen?

- ✗ Prioritera återställning av kritiska system först
- ✓ Använda kriminalteknisk analys för att bekräfta att attacken har inneslutits helt
- ✗ Ändra alla lösenord och återkalla inloggningsuppgifter som utsatts för risk
- ✗ Implementera nollförtroendeprinciper

Innan systemen återställs måste du se till att attacken har inneslutits helt för att förhindra återinfektion och ytterligare skador, så att inte hoten bibehålls eller eskalerar i miljön.

Nästa fråga →

Attacktyp: Attacker mot säkerhetskopior

1 2 3 4: Övergripande bästa praxis

Vilka är potentiella metoder för att minska risken att detta händer i framtiden?

- [ ] Använd nollförtroendeprinciper
- [ ] Aktivera funktioner för Endpoint Detection and Response (EDR)
- [ ] Implementera oföränderliga och frånkopplade säkerhetskopior
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Attacker mot säkerhetskopior

1 2 3 4: Övergripande bästa praxis

Vilka är potentiella metoder för att minska risken att detta händer i framtiden?

- [x] Använd nollförtroendeprinciper
- [x] Aktivera funktioner för Endpoint Detection and Response (EDR)
- [x] Implementera oföränderliga och frånkopplade säkerhetskopior
- [x] Alla ovanstående

Genom att använda en försvarsstrategi i flera lager går det att minska riskerna, minimera skadorna och förbättra organisationens motståndskraft, eftersom ingen enskild åtgärd är tillräcklig på egen hand.

Se lösningar →

ATTACKTYP: ATTACKER MOT SÄKERHETSKOPIOR

Sammanfattning

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.

Vi på Dell vill ge organisationer möjlighet att förbli motståndskraftiga när de möter föränderliga cyberhot. Med våra banbrytande lösningar, experttjänster och betrodda samarbeten finns vi här för att hjälpa dig att skydda det som är viktigast.

Läs mer om våra lösningar och hur vi hanterar dagens svåraste cyberutmaningar.

Utforska översikten om attacker mot säkerhetskopior →

Tillbaka till scenarier

PowerProtect-portföljen ›

Våra oföränderliga, frånkopplade och krypterade säkerhetskopieringsvalv, som drivs av AI-driven CyberSense-analys, säkerställer snabb identifiering och återställning så att du kan behålla motståndskraften.

PowerEdge-servrar ›

Med hjälp av säker start, Root of Trust för hårdvara och systemlåsning erbjuder Dell en infrastruktur som du kan lita på för att skydda dina säkerhetskopior.

Betrodd arbetsyta ›

SafeBIOS- och SafeData-skydd minskar riskerna och säkerställer att säkerhetskopieringssystemen förblir omanipulerade och att de är redo när du behöver dem.

Tjänster för säkerhet och motståndskraft ›

Från säker distribution till proaktiv incidenthantering – våra experter och partner hjälper dig att bygga upp motståndskraft och återställa snabbare.

Nätverkslösningar ›

Med nätverkssegmentering, flerfaktorsautentisering (MFA) och konfigurationer med lägsta behörighet hjälper Dell dig att låsa åtkomsten och skydda kritiska data.

Attacktyp: Distribuerad överbelastningsattack (DDoS)

Det är tisdag eftermiddag på en statlig myndighet och en stor snöstorm är i antågande.

IT-teamet på transportmyndigheten får en mängd samtal från agenter som inte kan komma in i några av sina system för att:

- Förnya körkort
- Skaffa trafiktillstånd
- Betala skatter
- Kontrollera vägförhållanden
- Aktivera nödsystem, vilket gör att det tar längre tid för snöröjarna att hantera snöiga/isiga vägar

och allt beror på att systemens tidsgräns löper ut.

Testa dina kunskaper →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1: Minimera angreppsytan — 2 — 3 — 4

Vilket är det första stället där du bör leta efter vad det kan vara som händer?

- [ ] Kontrollera nätverksenheter för plötsliga oförklarliga toppar i inkommande trafik
- [ ] Kontrollera nätverksenheter för ovanlig trafik från en enda eller ett begränsat antal IP-adresser
- [ ] Kontrollera loggarna för brandväggs- eller nätverkssynlighetsverktyg för att se om det finns för många misslyckade anslutningar eller händelser som blockerar trafik
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1: Minimera angreppsytan — 2 — 3 — 4

Vilket är det första stället där du bör leta efter vad det kan vara som händer?

- [x] Kontrollera nätverksenheter för plötsliga oförklarliga toppar i inkommande trafik
- [x] Kontrollera nätverksenheter för ovanlig trafik från en enda eller ett begränsat antal IP-adresser
- [x] Kontrollera loggarna för brandväggs- eller nätverkssynlighetsverktyg för att se om det finns för många misslyckade anslutningar eller händelser som blockerar trafik
- [x] Alla ovanstående

Om du ska kunna diagnostisera omfattande systemavbrott korrekt måste du samtidigt granska nätverksenhetsaktivitet och loggar för brandväggs- eller synlighetsverktyg för att snabbt kunna upptäcka ovanliga mönster eller blockerande händelser. Det möjliggör snabbare och mer exakt incidentsvar eftersom du kan skilja mellan cyberincidenter och infrastrukturproblem.

Nästa fråga →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Du misstänker att det kan vara en DDoS-attack. Vilket är ditt första steg?

- [ ] Dirigera om all nätverkstrafik via en DDoS-begränsningstjänst
- [ ] Aktivera WAF-regler (Web Application Firewall) för att filtrera bort skadliga mönster
- [ ] Kontrollera om trafikökningen beror på legitima källor
- [ ] Kommunicera internt och externt vad som händer

Se rätt svar →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Du misstänker att det kan vara en DDoS-attack. Vilket är ditt första steg?

- ✗ Dirigera om all nätverkstrafik via en DDoS-begränsningstjänst
- ✗ Aktivera WAF-regler (Web Application Firewall) för att filtrera bort skadliga mönster
- ✓ Kontrollera om trafikökningen beror på legitima källor
- ✗ Kommunicera internt och externt vad som händer

Innan DDoS-motåtgärder aktiveras är det viktigt att verifiera legitimiteten för en trafiktopp. På så sätt undviker du att oavsiktligt blockera äkta användare, förhindrar störningar för kritiska intressenter och säkerställer att eventuella ytterligare skyddsåtgärder är lämpliga och exakt riktade, vilket minimerar den negativa effekten på offentlig verksamhet och övergripande affärskontinuitet.

Nästa fråga →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka åtgärder kan du vidta för att försöka undvika en DDoS-attack i framtiden?

- [ ] Blockera störande IP-adresser
- [ ] Utföra regelbundna intrångstester med DDoS-simuleringar
- [ ] Flytta alla program till molnet eftersom molnleverantörer vanligtvis inte utsätts för DDoS-attacker
- [ ] Implementera nollförtroendeprinciper

Se rätt svar →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka åtgärder kan du vidta för att försöka undvika en DDoS-attack i framtiden?

- ✗ Blockera störande IP-adresser
- ✓ Utföra regelbundna intrångstester med DDoS-simuleringar
- ✗ Flytta alla program till molnet eftersom molnleverantörer vanligtvis inte utsätts för DDoS-attacker
- ✓ Implementera nollförtroendeprinciper

Proaktiva intrångstester med DDoS-simuleringar identifierar och stärker luckor i försvaret, medan nollförtroendeprinciper fokuserar på att minimera riskerna genom att upprätthålla åtkomst med lägsta behörighet hela tiden. Detta bidrar till att minska risken för störningar i viktiga system, till exempel samordning av nödåtgärder eller kontroll av trafiksignaler i realtid, som måste fortsätta att fungera även under en attack.

Nästa fråga →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 2 3 4: Övergripande bästa praxis

Vem ska du meddela som en del av den övergripande incidentrespons- och återställningsplanen (IRR)?

- [ ] Det juridiska teamet
- [ ] Cyberförsäkringsleverantören
- [ ] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Distribuerad överbelastningsattack (DDoS)

1 2 3 4: Övergripande bästa praxis

Vem ska du meddela som en del av den övergripande incidentrespons- och återställningsplanen (IRR)?

- [x] Det juridiska teamet
- [x] Cyberförsäkringsleverantören
- [x] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Alla ovanstående

Under en storskalig cyberincident bör du överväga att samordna med juridiska myndigheter, försäkringsbyråer och myndigheter gällande efterlevnad, anspråk och brottsbekämpning. När du har säkerställt att alla lagstadgade krav är uppfyllda kan organisationen begränsa, lösa och återställa efter incidenten på ett effektivt sätt.

Se lösningar →

ATTACKTYP: DISTRIBUERAD ÖVERBELASTNINGSATTACK (DDOS)

Sammanfattning

En DDoS-attack syftar till att störa den normala funktionen hos ett nätverk, en tjänst eller en server genom att överbelasta den med en enorm trafikvolym från flera källor. Dessa attacker utförs genom att utnyttja botnät, som är nätverk av infekterade enheter som styrs av angripare på distans.

Vi på Dell hjälper organisationer att förbli motståndskraftiga mot DDoS-attacker genom att kombinera avancerad detekterings- och begränsningsteknik med experttjänster och en nollförtroendestrategi, vilket säkerställer snabba svar, minimerade störningar och starkare försvar.

Läs mer om avancerade strategier för cyberelasticitet och hur Dell kan hjälpa dig att skydda din organisation mot DDoS-attacker.

Utforska översikten om DDoS →

Tillbaka till scenarier

Nätverkslösningar ›

Möjliggör nätverkssegmentering, mikrosegmentering och efterlevnad av lägsta behörighet för att isolera kritiska tillgångar, begränsa attackens spridning och säkerställa snabb DDoS-inneslutning.

PowerEdge-servrar ›

Dell levererar tåligt DDoS-skydd med hög prestanda och accelererad återställning med Root of Trust för hårdvara, säker start, systemlåsning och manipuleringsbevis i realtid.

Betrodda enheter ›

Integrerad SafeBIOS, SecureData och automatiserad detektering och respons minskar slutpunktens angreppsytor med upp till 70 %, vilket förhindrar att DDoS-drivna distraktioner blir intrångsvektorer.

PowerProtect-portföljen ›

Krypterade, oföränderliga och frånkopplade miljöer för säkerhetskopior, som drivs av AI-driven hotanalys, säkerställer snabb, validerad återställning och upprätthåller affärskontinuitet under DDoS-störningar.

Tjänster för säkerhet och motståndskraft ›

Managed Detection and Response (MDR), incidentrespons och återställning (IRR), hotidentifiering och vägledning om motståndskraftig arkitektur förbättrar beredskapen mot DDoS och stärker försvarsförmågan.

Attacktyp: Skadlig insiderattack

Klockan är 08.00 på en tisdag. Arbetsdagen har precis börjat för medarbetarna på ett amerikanskt sjukvårdsföretag.

En medarbetare på chefsnivå som arbetar med mycket känsliga patientdata loggar in efter en sen kväll på kontoret.

Hon lägger märke till förändringar i en mapp som hon arbetade med kvällen innan. Hon diskuterar det med sitt team och tar sedan upp frågan med IT.

När de undersöker saken upptäcker de att en IT-medarbetare med kopplingar till ett brottssyndikat har lurat en chef att sätta in ett skadligt USB-minne i sin enhet, vilket nedgraderar BIOS-systemet (Basic Input/Output System) till en sårbar version, vilket utsätter systemet för risk.

Testa dina kunskaper →

Attacktyp: Skadlig insiderattack

1: Minimera angreppsytan — 2 — 3 — 4 — 5

Insidern med skadliga avsikter initierade attacken genom två metoder som spårats av ramverket MITRE Adversarial Tactics, Techniques, and Common Knowledge, eller MITRE ATT&CK. Vilka är de?

- [ ] Betrodd relation + replikering genom löstagbara medier
- [ ] Socialteknik + replikering genom löstagbara medier
- [ ] Socialteknik + externa fjärrtjänster
- [ ] Betrodd relation + hårdvarutillägg

Se rätt svar →

Attacktyp: Skadlig insiderattack

1: Minimera angreppsytan — 2 — 3 — 4 — 5

Insidern med skadliga avsikter initierade attacken genom två metoder som spårats av ramverket MITRE Adversarial Tactics, Techniques, and Common Knowledge, eller MITRE ATT&CK. Vilka är de?

- ✗ Betrodd relation + replikering genom löstagbara medier
- ✓ Socialteknik + replikering genom löstagbara medier
- ✗ Socialteknik + externa fjärrtjänster
- ✗ Betrodd relation + hårdvarutillägg

Genom att följa MITRE ATT&CK-tekniker för både mänsklig manipulering och replikering via bärbar lagring använde angriparen socialteknik för att lura en chef att ansluta ett skadligt USB-minne och leverera skadade data via löstagbara medier.

Nästa fråga →

Attacktyp: Skadlig insiderattack

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4 — 5

Varför behöver angriparen använda båda metoderna?

- [ ] Gå in i nätverket som global administratör för att nedgradera BIOS (Basic Input/Output System)
- [ ] Lura administratören så att hen nedgraderar BIOS
- [ ] Ändra enhetens DNS-leverantör (Domain Name System) för att få de inloggningsuppgifter som behövs för engångsåtkomst till nätverket
- [ ] Installera skadliga program på en enhet för att få de inloggningsuppgifter som behövs för kontinuerlig nätverksåtkomst

Se rätt svar →

Attacktyp: Skadlig insiderattack

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4 — 5

Varför behöver angriparen använda båda metoderna?

- ✗ Gå in i nätverket som global administratör för att nedgradera BIOS (Basic Input/Output System)
- ✗ Lura administratören så att hen nedgraderar BIOS
- ✗ Ändra enhetens DNS-leverantör (Domain Name System) för att få de inloggningsuppgifter som behövs för engångsåtkomst till nätverket
- ✓ Installera skadliga program på en enhet för att få de inloggningsuppgifter som behövs för kontinuerlig nätverksåtkomst

Angriparen behövde använda båda metoderna, dvs. installation av skadliga program via USB-minnet för att kompromettera enheten och inloggningsuppgifterna för att möjliggöra kontinuerlig nätverksåtkomst, för att upprätta beständig obehörig kontroll över målmiljön.

Nästa fråga →

Attacktyp: Skadlig insiderattack

1 2 3: Upptäcka och reagera på cyberhot 4 5

Vilket är ett sätt att upptäcka onormal nätverksaktivitet?

- [ ] Programkontroll
- [ ] Extended Detection and Response (XDR)
- [ ] Nästa generations antivirus (NGAV)
- [ ] Geofencing för slutpunkter

Se rätt svar →

Attacktyp: Skadlig insiderattack

1 2 3: Upptäcka och reagera på cyberhot 4 5

Vilket är ett sätt att upptäcka onormal nätverksaktivitet?

- ✗ Programkontroll
- ✓ Extended Detection and Response (XDR)
- ✗ Nästa generations antivirus (NGAV)
- ✗ Geofencing för slutpunkter

När det gäller att tillhandahålla bred och korrelerad synlighet för snabb identifiering av hot är XDR bäst för att upptäcka misstänkt nätverksaktivitet eftersom det kontinuerligt övervakar och analyserar aktivitet på slutpunkter, nätverk och molnmiljöer.

Nästa fråga →

Attacktyp: Skadlig insiderattack

1 2 3 4: Återställning efter en cyberattack 5

Vilken inbyggd datorsäkerhet kan upptäcka misstänkt aktivitet tidigt i angreppskedjan?

- [ ] SIEM (Security Information and Event Management)
- [ ] Extended Detection and Response (XDR)
- [ ] Indicators of Attach (IOA)
- [ ] Rollbaserad åtkomstkontroll (RBAC, Role-Based Access Control)

Se rätt svar →

Attacktyp: Skadlig insiderattack

1 2 3 4: Återställning efter en cyberattack 5

Vilken inbyggd datorsäkerhet kan upptäcka misstänkt aktivitet tidigt i angreppskedjan?

- ✗ SIEM (Security Information and Event Management)
- ✗ Extended Detection and Response (XDR)
- ✓ Indicators of Attach (IOA)
- ✗ Rollbaserad åtkomstkontroll (RBAC, Role-Based Access Control)

IOA fokuserar på att upptäcka angripares beteenden och misstänkta aktivitetsmönster när de inträffar, vilket gör det möjligt för säkerhetsteam att identifiera hot tidigare än signaturbaserade metoder och ingripa innan betydande skador inträffar.

Nästa fråga →

Attacktyp: Skadlig insiderattack

1 2 3 4 5: Övergripande bästa praxis

Vilken åtgärd kan du vidta för att återställa från och förhindra liknande framtida intrång efter att du har fastställt den initiala åtkomstmetoden?

- [ ] Uppdatera BIOS till senaste versionen
- [ ] Avaktivera BIOS-nedgraderingsalternativet
- [ ] Avaktivera USB-portar
- [ ] Implementera detaljerad kontroll för att möjliggöra säker användning av USB-enheter och förhindra spridning av skadliga program
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Skadlig insiderattack

1 2 3 4 5: Övergripande bästa praxis

Vilken åtgärd kan du vidta för att återställa från och förhindra liknande framtida intrång efter att du har fastställt den initiala åtkomstmetoden?

- [x] Uppdatera BIOS till senaste versionen
- [x] Avaktivera BIOS-nedgraderingsalternativet
- [x] Avaktivera USB-portar
- [x] Implementera detaljerad kontroll för att möjliggöra säker användning av USB-enheter och förhindra spridning av skadliga program
- [x] Alla ovanstående

Genom att hantera olika attackvektorer för att säkerställa att hårdvaran är säker och nedgraderingar blockeras kan USB-baserade hot begränsas och spridningen av skadlig mjukvara stoppas vid flera punkter för att skapa ett omfattande försvar med flera lager som återställer berörda system och skyddar mot framtida intrång.

Se lösningar →

ATTACKTYP: SKADLIG INSIDERATTACK

Sammanfattning

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 syften. Den här personen kan vara en anställd, entreprenör, partner eller någon annan med legitim åtkomst till företagets system och nätverk.

Dell skyddar mot skadliga insiderattacker genom en kombination av avancerad teknik och strikta säkerhetsprotokoll.

Läs mer om avancerade strategier för cyberelasticitet och hur Dell kan hjälpa dig att skydda din organisation mot skadliga insiderattacker.

Utforska översikten om skadliga insiderattacker →

Tillbaka till scenarier

Betrodda enheter och infrastruktur ›

Inbyggd lägsta behörighet, flerfaktorsautentisering (MFA), rollbaserad åtkomstkontroll (RBAC), dubbel autentisering och nollförtroendeskydd skyddar slutpunkter och infrastruktur, vilket minskar riskerna för insiderhot.

PowerEdge-servrar ›

Root of Trust-hårdvara, säker start, dynamisk USB-porthantering och systemlåsning skyddar mot manipulering och stoppar fysiska eller fast mjukvarubaserade insiderattacker.

PowerProtect-portföljen ›

Ej modifierbara och isolerade säkerhetskopior säkerställer dataintegritet, snabb återställning och tidig identifiering av försök till datamanipulation, vilket möjliggör återställning från insiderincidenter.

Tjänster för säkerhet och motståndskraft ›

Utbildning som leds av experter, intrångstestning, hotidentifiering, incidentrespons och tjänster för intrångsåterställning stärker beredskapen och motståndskraften mot insiderdrivna händelser.

Säkerhetspartner ›

Integrerad Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) och automatiserad hotinformation identifierar, begränsar och mildrar komplexa interna hot i realtid.

Attacktyp: Man-in-the-Middle-attack (MITM)

En intet ont anande kund ansluter till ett kostnadsfritt oskyddat Wi-Fi på ett kafé för att göra några uppdateringar av ett delat teamdokument i sista stund.

En stund senare får företagets IT-avdelning meddelanden om ovanliga inloggningsförsök från medarbetarens konto, samt obehörig dataåtkomst från flera platser över hela världen.

När de undersöker saken kan de bekräfta att angriparen har fångat upp och manipulerat den trådlösa anslutningen och fått åtkomst till känslig information.

Testa dina kunskaper →

Attacktyp: Man-in-the-Middle-attack (MITM)

1: Minimera angreppsytan — 2 — 3 — 4

Var bör IT-teamet först undersöka när man upptäcker ovanliga inloggningsförsök?

- [ ] Brandvägg, system för intrångsdetektering (IDS), loggar för intrångsförebyggande system (IPS) och XDR (Extended Detection Response)
- [ ] Den berörda medarbetarens bärbara dator
- [ ] Nätverkstrafik på kaféets oskyddade Wi-Fi
- [ ] Autentiseringsloggar från företagets system

Se rätt svar →

Attacktyp: Man-in-the-Middle-attack (MITM)

1: Minimera angreppsytan — 2 — 3 — 4

Var bör IT-teamet först undersöka när man upptäcker ovanliga inloggningsförsök?

- ✓ Brandvägg, system för intrångsdetektering (IDS), loggar för intrångsförebyggande system (IPS) och XDR (Extended Detection Response)
- ✗ Den berörda medarbetarens bärbara dator
- ✗ Nätverkstrafik på kaféets oskyddade Wi-Fi
- ✓ Autentiseringsloggar från företagets system

Genom att analysera loggarna från brandvägg, IDS/IPS och autentisering kan IT-teamen spåra obehöriga åtkomstförsök, bedöma vilka konton som utsatts för risk och få en bättre förståelse för incidentens omfattning.

Nästa fråga →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Vilka omedelbara åtgärder bör vidtas av IT-teamet efter att MITM-attacken har bekräftats?

- [ ] Koppla omedelbart bort den komprometterade medarbetarens enhet från nätverket och isolera den för analys
- [ ] Uppdatera brandväggsregler och nätverkskonfigurationer för att stoppa ytterligare obehörig åtkomst
- [ ] Återställa lösenorden till alla medarbetarkonton
- [ ] Avaktivera berörda system för att förhindra dataexfiltrering

Se rätt svar →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Vilka omedelbara åtgärder bör vidtas av IT-teamet efter att MITM-attacken har bekräftats?

- ✓ Koppla omedelbart bort den komprometterade medarbetarens enhet från nätverket och isolera den för analys
- ✓ Uppdatera brandväggsregler och nätverkskonfigurationer för att stoppa ytterligare obehörig åtkomst
- ✗ Återställa lösenorden till alla medarbetarkonton
- ✗ Avaktivera berörda system för att förhindra dataexfiltrering

Genom att omedelbart koppla bort och isolera den komprometterade enheten stoppas angriparens åtkomst och bevarar kriminaltekniska bevis, medan uppdatering av brandväggs- och nätverksregler blockerar ytterligare skadliga anslutningar och skyddar nätverket som helhet från pågående risk.

Nästa fråga →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka förebyggande åtgärder hade kunnat minska sårbarheten inför MITM-attacken?

- [ ] Tvinga alla medarbetare att använda virtuella privata nätverk (VPN)
- [ ] Implementera säkerhetsprinciper med nollförtroende, till exempel flerfaktorsautentisering (MFA)
- [ ] Undvika offentliga Wi-Fi-nätverk
- [ ] Kryptera känsliga filer som delas via mejl

Se rätt svar →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka förebyggande åtgärder hade kunnat minska sårbarheten inför MITM-attacken?

- ✓ Tvinga alla medarbetare att använda virtuella privata nätverk (VPN)
- ✓ Implementera säkerhetsprinciper med nollförtroende, till exempel flerfaktorsautentisering (MFA)
- ✗ Undvika offentliga Wi-Fi-nätverk
- ✗ Kryptera känsliga filer som delas via mejl

Genom att tvinga fram VPN-användning vid oskyddade nätverk krypteras medarbetarnas internettrafik för att förhindra avlyssning, medan implementering av nollförtroendesäkerhet och MFA säkerställer att varje åtkomstbegäran verifieras kontinuerligt.

Nästa fråga →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 2 3 4: Övergripande bästa praxis

Vilka långsiktiga strategier bör organisationen implementera efter att ha åtgärdat intrånget?

- [ ] Granska och korrigera system regelbundet
- [ ] Öka nätverkssegmenteringen för att isolera känsliga data och system
- [ ] Driftsätta lösningar för Endpoint Detection and Response (EDR) och Managed Detection and Response (MDR)
- [ ] Implementera robust och regelbunden utbildning för medarbetarna
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Man-in-the-Middle-attack (MITM)

1 2 3 4: Övergripande bästa praxis

Vilka långsiktiga strategier bör organisationen implementera efter att ha åtgärdat intrånget?

- [x] Granska och korrigera system regelbundet
- [x] Öka nätverkssegmenteringen för att isolera känsliga data och system
- [x] Driftsätta lösningar för Endpoint Detection and Response (EDR) och Managed Detection and Response (MDR)
- [x] Implementera robust och regelbunden utbildning för medarbetarna
- [x] Alla ovanstående

Dessa långsiktiga strategier kombineras som ett skydd mot olika hot genom att utgöra en omfattande och motståndskraftig säkerhetsställning som blockerar angripare från att utnyttja luckor och säkerställer snabba och effektiva svar vid intrång.

Se lösningar →

ATTACKTYP: MAN-IN-THE-MIDDLE-ATTACK (MITM)

Sammanfattning

En MITM-attack inträffar när en cyberbrottsling i hemlighet fångar upp kommunikation mellan två parter, till exempel mellan en anställd och en företagsserver eller en kund och en företagswebbplats. Angriparna kan ha olika mål, men resultatet är detsamma: ett brott mot förtroende och säkerhet.

Vi på Dell levererar innovativa och skalbara säkerhetslösningar som gör det möjligt för organisationer att neutralisera MITM-hot, skydda tillgångar och upprätthålla affärsintegriteten med de verktyg och den expertis som behövs för att upptäcka, reagera på och återställa med tillförsikt.

Läs mer om avancerade strategier för cyberelasticitet och se hur Dell kan hjälpa dig att skydda din organisation mot MITM-attacker.

Läs översikten om MITM-attacker →

Tillbaka till scenarier

Betrodda enheter >

Med hjälp av hårdvaruautentisering, skydd för fast mjukvara som SafeBIOS och SafeID, robust kryptering och ramverk med nollförtroende skyddar Dell slutpunkter och data under överföring.

PowerEdge-servrar >

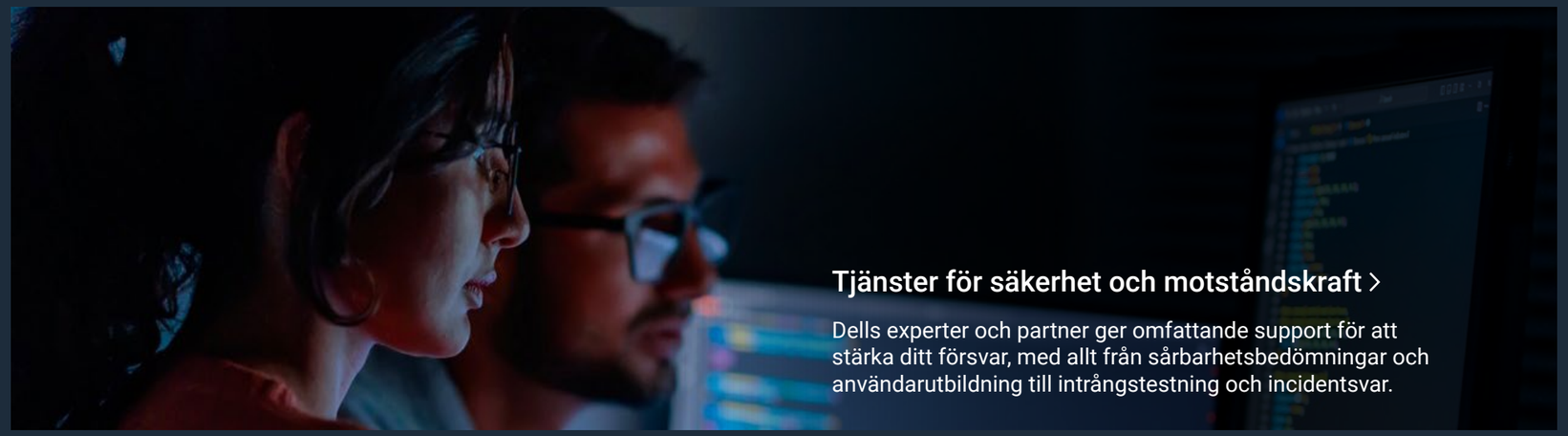
Säker start, Silicon Root of Trust, dynamisk USB-porthantering och systemlåsning säkerställer hårdvaruintegritet och skyddar kritiska arbetsbelastningar från nätverksbaserade hot.

Lagringslösningar >

Krypterade data i vila och under överföring, kombinerat med isolerade ögonblicksbildskopior och funktioner för snabb återställning, säkerställer att filerna förblir säkra och snabbt kan återställas efter en MITM-attack.

PowerProtect-portföljen >

Ej modifierbara och isolerade säkerhetskopior och AI-driven CyberSense-analys möjliggör snabb återställning och betrodd dataåterställning om en MITM-attack skulle inträffa.



Tjänster för säkerhet och motståndskraft >

Dells experter och partner ger omfattande support för att stärka ditt försvar, med allt från sårbarhetsbedömningar och användarutbildning till intrångstestning och incidentsvar.

Attacktyp: Prompt-/SQL-injektion

Du arbetar på kundtjänstavdelningen för ett flygbolag som huvudsakligen levererar sin tjänst via en chattbot.

Du märker att du och dina kollegor börjar få allt fler samtal från kunder som säger att de inte kan komma in på sina flygbonuskonton, och när de gör det ser de att alla deras flygmil är borta.

Testa dina kunskaper →

Attacktyp: Prompt-/SQL-injektion

1: Minimera angreppsytan — 2 — 3 — 4

Du ser några fel i loggarna vid undersökning: *Syntaxfel i SQL-satsen (Structured Query Language) eller Ogiltigt kolumnnamn ”admin”*. Vilken typ av cyberincident är det här?

- [ ] Stulna inloggningsuppgifter
- [ ] Prompt- eller SQL-injektion
- [ ] Man-in-the-Middle-attack
- [ ] Nätfiske

Se rätt svar →

Attacktyp: Prompt-/SQL-injektion

1: Minimera angreppsytan — 2 — 3 — 4

Du ser några fel i loggarna vid undersökning: *Syntaxfel i SQL-satsen (Structured Query Language)* eller *Ogiltigt kolumnnamn ”admin”*. Vilken typ av cyberincident är det här?

- ✗ Stulna inloggningsuppgifter
- ✓ Prompt- eller SQL-injektion
- ✗ Man-in-the-Middle-attack
- ✗ Nätfiske

”Prompt- eller SQL-injektion” är rätt eftersom loggfel som ”Syntaxfel i SQL-satsen” eller ”Ogiltigt kolumnnamn ”admin”” avslöjar att angripare har utnyttjat chattbotens inmatningsfält med skadlig SQL-kod för att komma åt eller ändra kundkontodata, vilket är tydliga tekniska indikatorer på en SQL-injektionsattack som överensstämmer med den misstänkta aktivitet som beskrivs.

Nästa fråga →

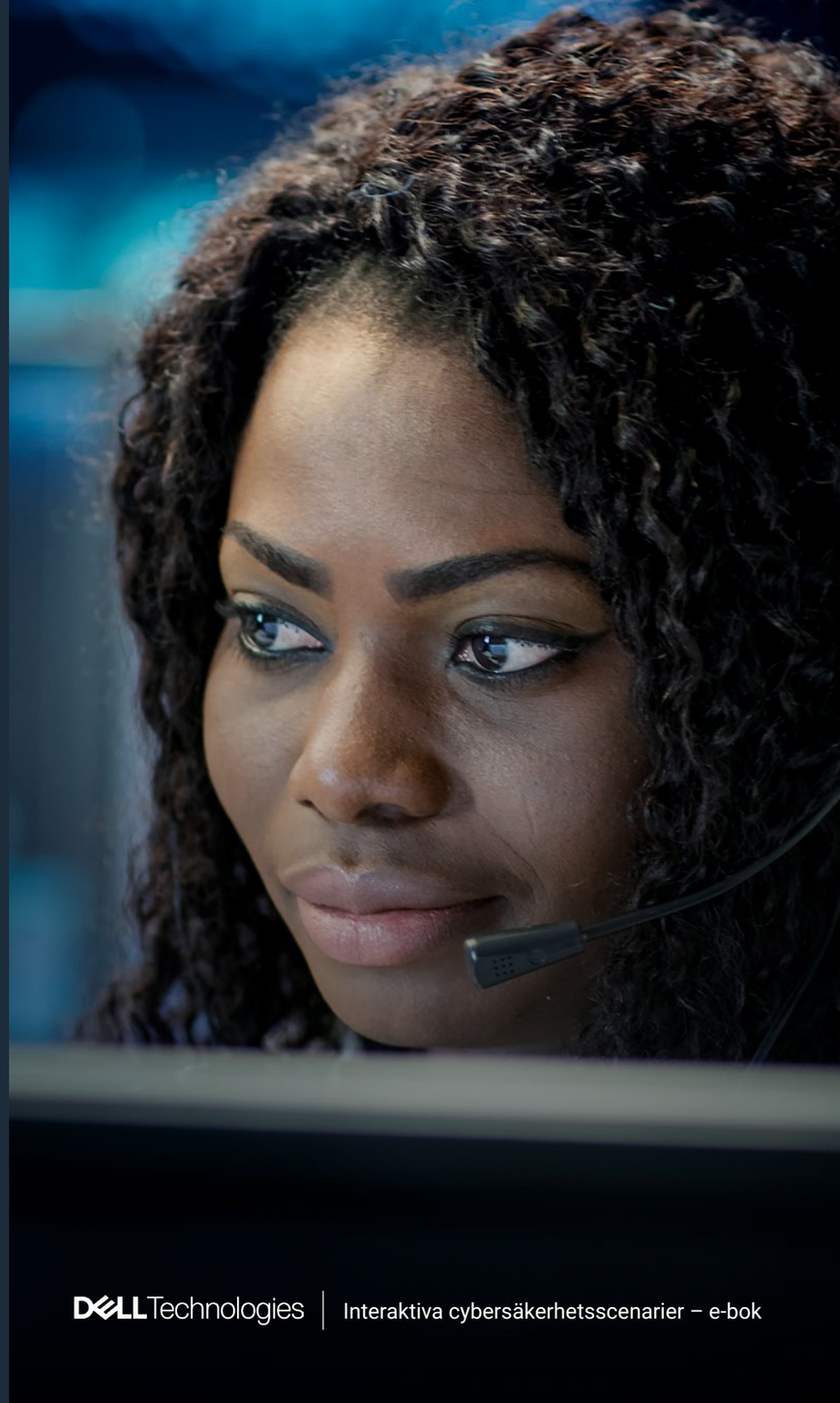
Attacktyp: Prompt-/SQL-injektion

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Du inser att du har drabbats av en prompt-/SQL-injektionsattack via chattboten för kundtjänst. Vad ska du göra?

- [ ] Koppla bort boten så att den är offline
- [ ] Granska databasloggar för att se om det förekommer obehörig åtkomst och stulna, ändrade eller borttagna data
- [ ] Följ alla lagar om avslöjande av dataläckor
- [ ] Alla ovanstående

Se rätt svar →



Attacktyp: Prompt-/SQL-injektion

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Du inser att du har drabbats av en prompt-/SQL-injektionsattack via chattboten för kundtjänst. Vad ska du göra?

- [x] Koppla bort boten så att den är offline
- [x] Granska databasloggar för att se om det förekommer obehörig åtkomst och stulna, ändrade eller borttagna data
- [x] Följ alla lagar om avslöjande av dataläckor
- [x] Alla ovanstående

När du ska hantera en prompt-/SQL-injektionsattack måste du se till att chattboten är offline, granska databasloggar för att se om det förekommer obehörig åtkomst och säkerställa efterlevnad av lagar om avslöjande. Dessa steg är avgörande för att stoppa exploatering, bedöma skadorna och uppfylla lagstadgade och etiska skyldigheter.

Nästa fråga →

Attacktyp: Prompt-/SQL-injektion

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka funktioner bör du införa för att stoppa prompt-/SQL-injektioner?

- [ ] Utbilda utvecklingsteamen i att använda förberedda uttalanden och parametriserade frågor som kodningspraxis
- [ ] Verktyg för Managed Detection and Response (MDR)
- [ ] Implementera åtkomst med lägsta behörighet, till exempel flerfaktorsautentisering (MFA), rollbaserad åtkomstkontroll (RBAC), brandvägg för webbprogram (WAF) osv.
- [ ] Segmentera serverdelsdatabaser/kunskapsdatabaser

Se rätt svar →

Attacktyp: Prompt-/SQL-injektion

1 — 2 — 3: Återställning efter en cyberattack — 4

Vilka funktioner bör du införa för att stoppa prompt-/SQL-injektioner?

- ✓ Utbilda utvecklingsteamen i att använda förberedda uttalanden och parametriserade frågor som kodningspraxis
- ✗ Verktyg för Managed Detection and Response (MDR)
- ✓ Implementera åtkomst med lägsta behörighet, till exempel flerfaktorsautentisering (MFA), rollbaserad åtkomstkontroll (RBAC), brandvägg för webbprogram (WAF) osv.
- ✗ Segmentera serverdelsdatabaser/kunskapsdatabaser

Genom att utbilda utvecklingsteamen i att använda förberedda uttalanden och parametriserade frågor blockeras SQL-injektionsattacker vid källan, medan tvingande åtkomstkontroll med lägsta behörighet, till exempel MFA, RBAC och WAF, begränsar effekten av eventuella försök till injektion genom att förhindra angriparna från att eskalera privilegier eller röra sig lateralt.

Nästa fråga →

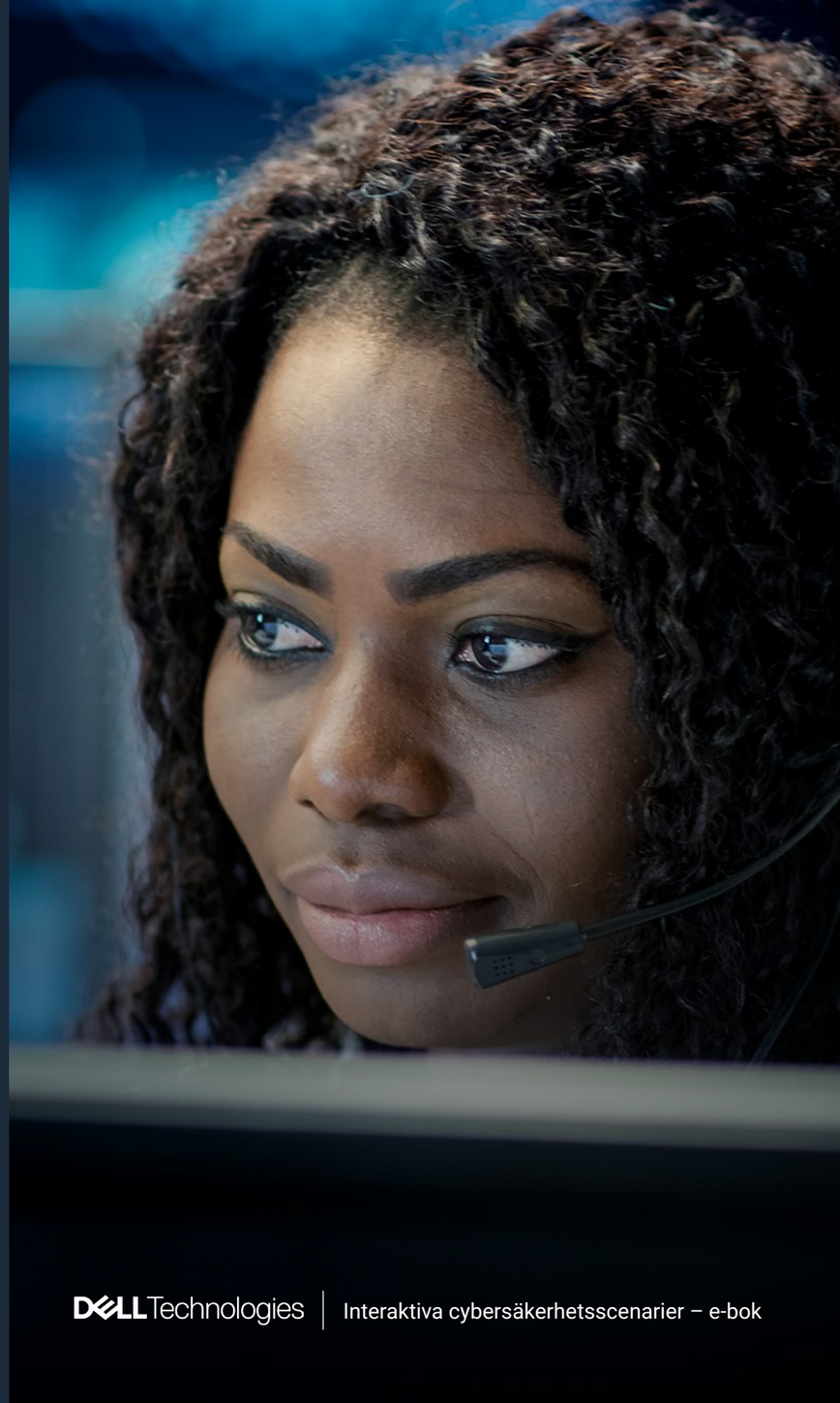
Attacktyp: Prompt-/SQL-injektion

1 2 3 4: Övergripande bästa praxis

Vilka åtgärder skulle du vidta för att få tillbaka kundernas data?

- [ ] Spåra stulna data
- [ ] Låta kunderna återskapa sina profiler
- [ ] Köpa tillbaka data från cyberangriparna
- [ ] Återställa från den senaste säkerhetskopia som inte utsatts för att återställa bonusmilen och meddela kunderna att de bör ändra sina lösenord och kontrollera sina kreditkort

Se rätt svar →



Attacktyp: Prompt-/SQL-injektion

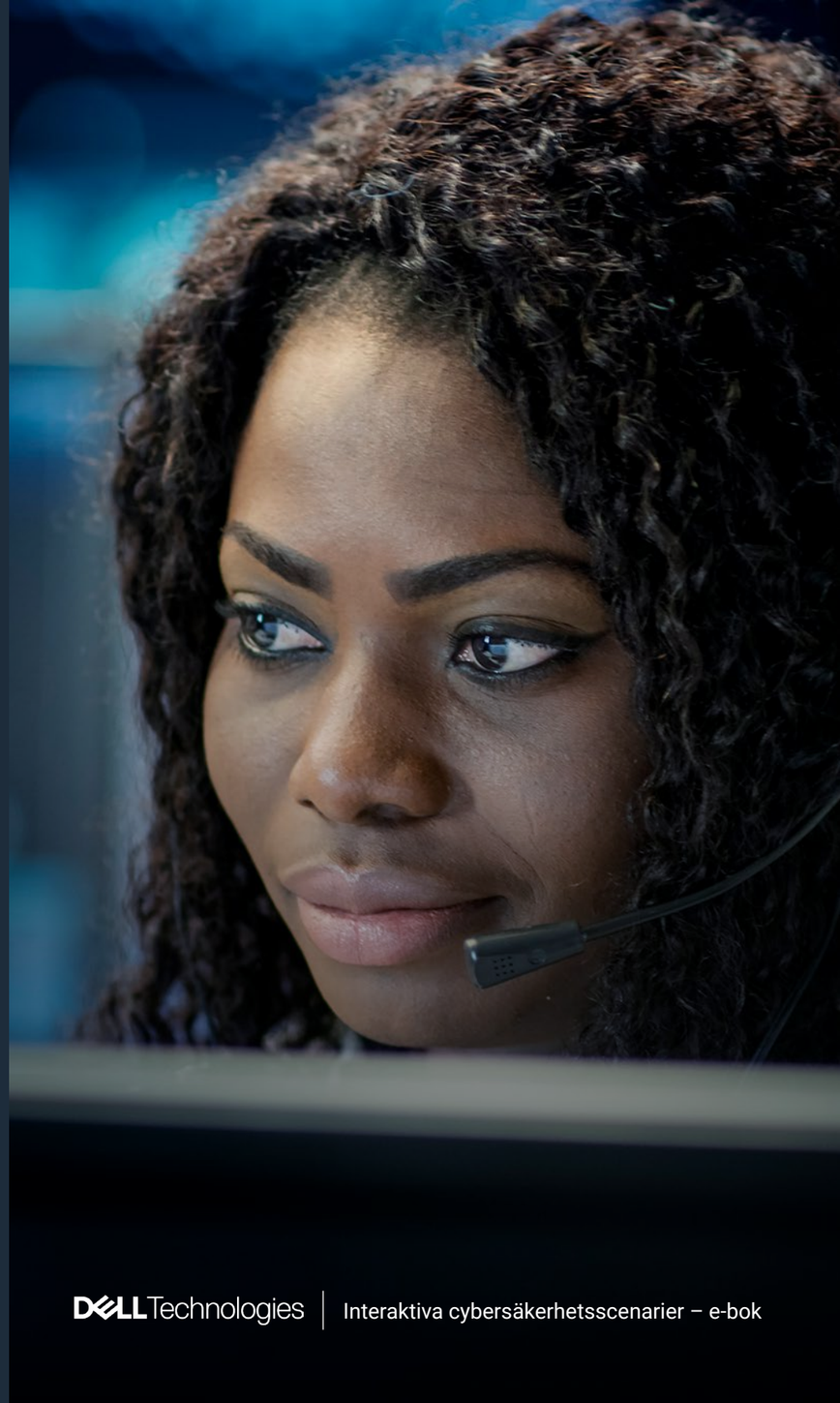
1 2 3 4: Övergripande bästa praxis

Vilka åtgärder skulle du vidta för att få tillbaka kundernas data?

- ✗ Spåra stulna data
- ✗ Låta kunderna återskapa sina profiler
- ✗ Köpa tillbaka data från cyberangriparna
- ✓ Återställa från den senaste säkerhetskopia som inte utsatts för att återställa bonusmilen och meddela kunderna att de bör ändra sina lösenord och kontrollera sina kreditkort

Återställning av förlorade kontodata från den senaste säkerhetskopia som inte utsatts bidrar till att upprätthålla dataintegriteten och förkorta driftavbrottet. Meddela kunderna att återställa sina lösenord och övervaka kreditkortsaktivitet snarast för att ytterligare stödja efterlevnad efter en destruktiv injektionsattack.

Se lösningar →



ATTACKTYP: PROMPT-/SQL-INJEKTION

Sammanfattning

Prompt-och SQL-injektionsattacker har upprepade gånger visat sig vara bland de skadligaste och mest genomgripande metoderna för cyberattacker som används av cyberbrottslingar. Dessa attacker utnyttjar sårbarheter i användarfråge- eller databassystem och gör det möjligt för skadliga aktörer att manipulera servrar, stjäla data eller störa arbetsflöden.

Att skydda organisationen mot nya hot och attacker med prompt-/SQL-injektion är en del av Dells pågående arbete för cybersäkerhet, och vi tillhandahåller de verktyg och de expertkunskaper som behövs för identifiering, svar och återställning.

Upptäck avancerade strategier för cyberelasticitet och se hur Dell kan stärka organisationens försvar mot prompt- och SQL-injektionsattacker.

Utforska översikten om prompt-/SQL-injektionsattacker →

Tillbaka till scenarier

Betrodd arbetsyta och betrodd infrastruktur ›

Skyddar slutpunkter och minskar risken för att komprometterade inloggningsuppgifter utnyttjas i injektionsattacker.

PowerEdge-servrar ›

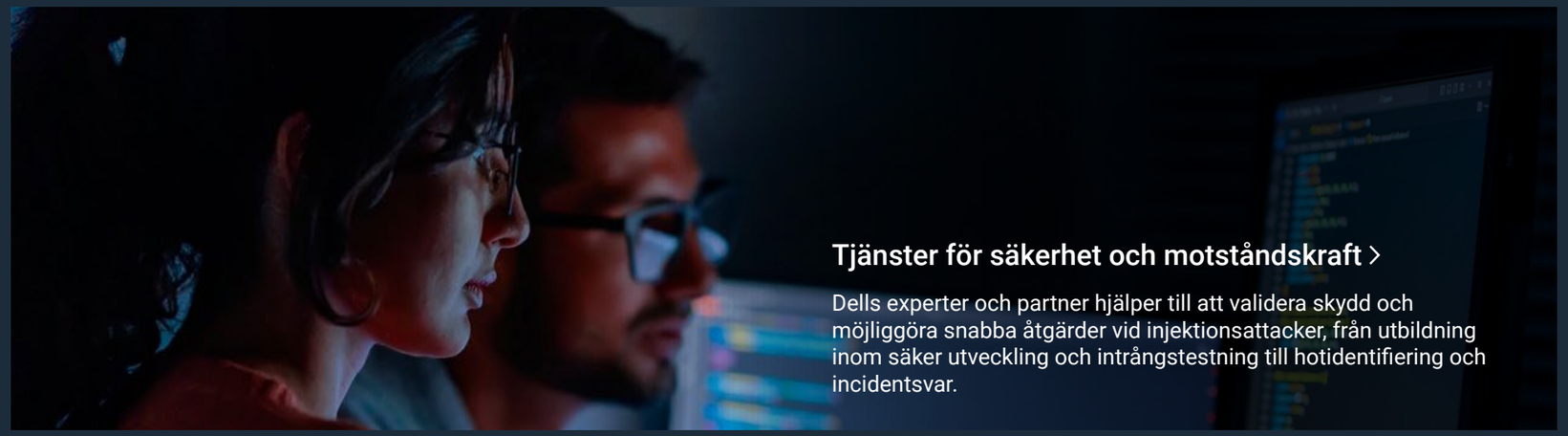
Dell PowerEdge-servrar har en manipuleringssäker infrastruktur som endast kör betrodd kod, med säker start, kiselbaserad säkerhet och konfigurationsvalidering i realtid.

Säkerhetspartner ›

Med detaljerad åtkomstkontroll, avancerad hotinformation och extern detektering och respons hjälper Dells säkerhetspartner till att identifiera och mildra försök till SQL- och promptinjektion.

PowerProtect-portföljen ›

Dells oföränderliga och frånkopplade säkerhetskopior och avancerade cyberåterställningsanalyser ger betrodda återställningspunkter, vilket möjliggör snabb återställning vid skadade data eller exfiltrering.



Tjänster för säkerhet och motståndskraft ›

Dells experter och partner hjälper till att validera skydd och möjliggöra snabba åtgärder vid injektionsattacker, från utbildning inom säker utveckling och intrångstestning till hotidentifiering och incidentsvar.

Attacktyp: Utpressningsvirus

Du är IT-tekniker på ett regionalt sjukhus som är känt för sina uppkopplade medicinska system, inklusive elektroniska patientjournaler (EHR), smarta infusionspumpar och radiologi, som alla är anslutna till ett centraliserat nätverk.

I går kväll började flera system krascha samtidigt. På morgonen rapporterar klinisk personal att de är utelåsta från patientjournaler.

Följande utpressningsmeddelande visas på flera terminaler:

”Era filer är krypterade. Betala 20 bitcoin inom 72 timmar eller så offentliggörs patientdata.”

Testa dina kunskaper →

Attacktyp: Utpressningsvirus

1: Minimera angreppsytan — 2 — 3 — 4

Helpdesken tar emot över 100 rapporter om filkryptering och programfel. Säkerhetsloggarna visar ovanlig namnbytesaktivitet för filer från ett internt domänkonto. Vilket är ditt första steg?

- [ ] Betala lösensumman omedelbart för att återställa kritiska tjänster
- [ ] Kontakta polis och juridiska rådgivare
- [ ] Börja skapa nya avbilder av alla berörda slutpunkter
- [ ] Koppla bort infekterade system från nätverket

Se rätt svar →

Attacktyp: Utpressningsvirus

1: Minimera angreppsytan — 2 — 3 — 4

Helpdesken tar emot över 100 rapporter om filkryptering och programfel. Säkerhetsloggarna visar ovanlig namnbytesaktivitet för filer från ett internt domänkonto. Vilket är ditt första steg?

- ✗ Betala lösensumman omedelbart för att återställa kritiska tjänster
- ✗ Kontakta polis och juridiska rådgivare
- ✗ Börja skapa nya avbilder av alla berörda slutpunkter
- ✓ Koppla bort infekterade system från nätverket

Genom att omedelbart koppla bort och isolera infekterade sjukhussystem hindras utpressningsviruset från att sprida sig, det skyddar kritiska medicinska enheter och känsliga patientdata, bevarar bevis för utredning och ger viktig tid till samordnade åtgärder och återställning.

Nästa fråga →

Attacktyp: Utpressningsvirus

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Incidenthanteringsteamet upptäcker att attacken troligen hade sitt ursprung i ett komprometterat konto som användes för att komma åt en server utan flerfaktorsautentisering (MFA). Vilket av följande bidrog mest direkt till attacken?

- [ ] Gamla antivirusdefinitioner
- [ ] En exponerad databas med elektroniska patientjournaler (EHR)
- [ ] Brist på flerfaktorsautentisering vid fjärråtkomst
- [ ] Bristande mejlfiltrering

Se rätt svar →

Attacktyp: Utpressningsvirus

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Incidenthanteringsteamet upptäcker att attacken troligen hade sitt ursprung i ett kompromitterat konto som användes för att komma åt en server utan flerfaktorsautentisering (MFA). Vilket av följande bidrog mest direkt till attacken?

- ✗ Gamla antivirusdefinitioner
- ✗ En exponerad databas med elektroniska patientjournaler (EHR)
- ✓ Brist på flerfaktorsautentisering vid fjärråtkomst
- ✗ Bristande mejlfiltrering

Brist på flerfaktorsautentisering vid fjärråtkomst möjliggjorde serverintrånget genom att tillåta att angripare loggar in med stulna eller gissade inloggningsuppgifter utan ett extra verifieringssteg. Med MFA skulle även utsatta konton kräva en andra faktor, vilket avsevärt minskar risken för obehörig åtkomst.

Nästa fråga →

Attacktyp: Utpressningsvirus

1 — 2 — 3: Återställning efter en cyberattack — 4

Medicinsk personal förlitar sig nu på pappersbaserade arbetsflöden. Patienter som har planerade operationer i dag kan inte verifieras i systemet. Vilken är den bästa kortsiktiga åtgärden för att underlätta sjukhusets drift?

- [ ] Starta om kärndatabasservern för att försöka utföra ominitiering
- [ ] Aktivera alla gamla säkerhetskopior, även om de är sex månader gamla
- [ ] Aktivera sjukhusets manuella driftstoppsprocesser och eskalera till nödresponsteamet
- [ ] Låt personalen avgöra hur de ska gå vidare utifrån enskilda fall

Se rätt svar →

Attacktyp: Utpressningsvirus

1 — 2 — 3: Återställning efter en cyberattack — 4

Medicinsk personal förlitar sig nu på pappersbaserade arbetsflöden. Patienter som har planerade operationer i dag kan inte verifieras i systemet. Vilken är den bästa kortsiktiga åtgärden för att underlätta sjukhusets drift?

- ✗ Starta om kärndatabasservern för att försöka utföra ominitiering
- ✗ Aktivera alla gamla säkerhetskopior, även om de är sex månader gamla
- ✓ Aktivera sjukhusets manuella driftstoppsprocesser och eskalera till nödresponsteamet
- ✗ Låt personalen avgöra hur de ska gå vidare utifrån enskilda fall

Genom att aktivera manuella driftstoppsprocesser och eskalera till nödresponsteamet säkerställer du omedelbar kontinuitet i kritiska kliniska arbetsflöden, skyddar patientsäkerheten och upprättar en standardiserad process för verifiering och dokumentation av vård. Denna metod minimerar fel, hanterar risker och resurser på ett effektivt sätt och gör det lättare för specialisterna att återställa digitala system på ett säkert sätt.

Nästa fråga →

Attacktyp: Utpressningsvirus

1 2 3 4: Övergripande bästa praxis

Lokala medier har tagit upp händelsen. Ledningen vill veta om de ska utfärda ett offentligt uttalande, och juridikavdelningen frågar om skyldigheter enligt HIPAA (Health Insurance Portability and Accountability Act). Vilket är det lämpligaste efterföljande steget?

- [ ] Förneka incidenten offentligt tills mer information finns tillgänglig
- [ ] Utfärda ett pressmeddelande som lägger skulden på tredjepartsleverantören för IT
- [ ] Meddela tillsynsmyndigheterna och påbörja interna processer för meddelanden om intrång
- [ ] Betala omedelbart lösensumman och undvik uppmärksamhet från allmänheten

Se rätt svar →

Attacktyp: Utpressningsvirus

1 — 2 — 3 — 4: Övergripande bästa praxis

Lokala medier har tagit upp händelsen. Ledningen vill veta om de ska utfärda ett offentligt uttalande, och juridikavdelningen frågar om skyldigheter enligt HIPAA (Health Insurance Portability and Accountability Act). Vilket är det lämpligaste efterföljande steget?

- ✗ Förneka incidenten offentligt tills mer information finns tillgänglig
- ✗ Utfärda ett pressmeddelande som lägger skulden på tredjepartsleverantören för IT
- ✓ Meddela tillsynsmyndigheterna och påbörja interna processer för meddelanden om intrång
- ✗ Betala omedelbart lösensumman och undvik uppmärksamhet från allmänheten

Snabb rapportering till myndigheter och berörda individer vid intrång på skyddad hälsoinformation, enligt HIPAA och regionala lagar, säkerställer regelefterlevnad, rättsligt skydd och transparens enligt bästa praxis för att förhindra juridiska effekter och skador på anseende, uppfylla obligatoriska informationskrav och upprätta korrekt kommunikation med patienter, personal och intressenter.

Se lösningar →

ATTACKTYP: UTPRESSNINGSVIRUS

Sammanfattning

Utpressningsvirus är en typ av skadlig mjukvara som blockerar åtkomst till ett datorsystem eller data tills en lösensumma betalas. Det är en av de cyberattacker som orsakar mest störningar. Hälften av alla företag globalt har under det senaste året drabbats av en utpressningsvirusattack minst en gång, och i genomsnitt varar driftstoppet efter en attack i tre veckor. Resultatet är stora störningar i verksamheten.

Vi på Dell prioriterar att skydda organisationen med nollförtroenderamverk, slutpunktsskydd och nätverkssegmentering för att blockera intrång från utpressningsvirus och begränsa dess spridning. Med incidenthanteringsplanering som leds av experter hjälper vi dig att bibehålla motståndskraften och återhämta dig snabbt från attacker.

Läs mer om avancerade strategier för cyberelasticitet och se hur Dell kan hjälpa dig att skydda din organisation mot utpressningsvirusattacker.

Utforska översikten om utpressningsvirusattacker →

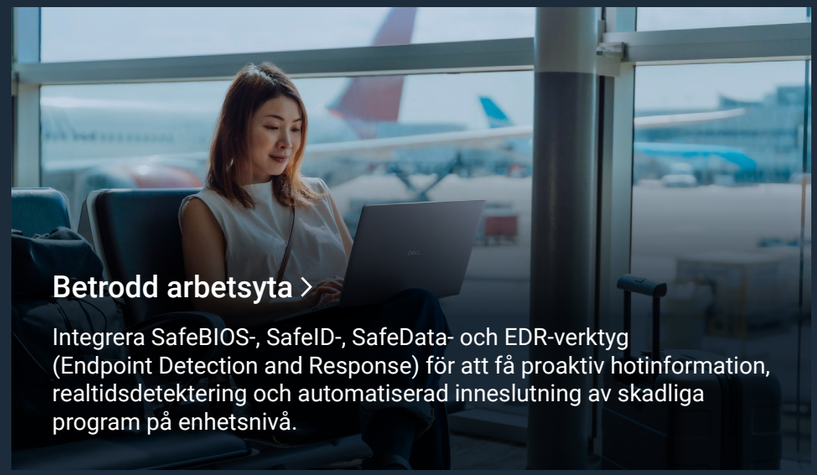
Tillbaka till scenarier

Betrodd infrastruktur ›

Blockera utpressningsvirus på infrastrukturnivå genom hårdvaruautentisering, flerfaktorsautentisering (MFA), rollbaserad åtkomstkontroll (RBAC) och nollförtroenderamverk.

Nätverk och PowerEdge-servrar ›

Begränsa utpressningsvirus. Med nätverkssegmentering, säker start, Silicon Root of Trust, dynamisk USB-porthantering och systemlåsning.



Betrodd arbetsyta ›

Integrera SafeBIOS-, SafeID-, SafeData- och EDR-verktyg (Endpoint Detection and Response) för att få proaktiv hotinformation, realtidsdetektering och automatiserad inneslutning av skadliga program på enhetsnivå.

PowerProtect-portföljen ›

Skydda kritiska data med oföränderliga och frånkopplade säkerhetskopior, intelligent cyberåterställningsanalys och funktioner för snabb återställning för att förhindra utpressning och möjliggöra motståndskraft.

Tjänster för säkerhet och motståndskraft ›

Samarbeta med experter som CrowdStrike för att få hjälp med bedömningar, sårbarhetshantering, utbildning i säkerhetsmedvetenhet, intrångstestning och incidentåtgärder.

Attacktyp: Hårdvara i leverantörskedjan

Ditt företag driftsätter 500 nya bärbara datorer på sina globala kontor. Eftersom du vill att arbetet ska gå snabbare lägger du ut avbildnings- och hårdvaruförberedelserna på en tredjepartsleverantör av IT-logistik. De levererar förkonfigurerade maskiner direkt till medarbetarna.

Det tar bara några dagar innan du får flera samtal från fältet som uppger:

- Begäranden om flerfaktorsautentisering (MFA) kringgås och inte fungerar korrekt.
- Säkerhetsteamet ser ett antal obehöriga administratörsinloggningar på udda tider.
- De ser även trafik från virtuella privata nätverk (VPN) från användare som ska vara offline.

Testa dina kunskaper →

Attacktyp: Hårdvara i leverantörskedjan

1: Minimera angreppsytan 2 3 4

En medarbetare rapporterar att hen får push-meddelanden om flerfaktorsautentisering (MFA) när hen inte försöker logga in. Organisationens säkerhetspanel visar att inloggningen kom från en enhet med en tillgångstagg som utfärdats av företaget. Vilket är det mest logiska första steget för SOC-teamet (Security Operations Center)?

- [ ] Avaktivera användarens konto och rensa personens bärbara dator på distans
- [ ] Jämför inloggnings-IP och enhetens fingeravtryck med andra kända komprometterade användare
- [ ] Eskalera till personalavdelningen, eftersom du antar att användaren har fel
- [ ] Utfärda en varning inom hela företaget om att omedelbart ändra lösenord

Se rätt svar →

Attacktyp: Hårdvara i leverantörskedjan

1: Minimera angreppsytan — 2 — 3 — 4

En medarbetare rapporterar att hen får push-meddelanden om flerfaktorsautentisering (MFA) när hen inte försöker logga in. Organisationens säkerhetspanel visar att inloggningen kom från en enhet med en tillgångstagg som utfärdats av företaget. Vilket är det mest logiska första steget för SOC-teamet (Security Operations Center)?

- ✗ Avaktivera användarens konto och rensa personens bärbara dator på distans
- ✓ Jämför inloggnings-IP och enhetens fingeravtryck med andra kända komprometterade användare
- ✗ Eskalera till personalavdelningen, eftersom du antar att användaren har fel
- ✗ Utfärda en varning inom hela företaget om att omedelbart ändra lösenord

Om SOC-teamet fastställer huruvida misstänkt aktivitet är en del av en större attack eller en isolerad attack för att möjliggöra snabb mönsterigenkänning är riktad incidentrespons och begränsning av ytterligare risker det logiska första steget vid identifiering av en hårdvaruattack i leverantörskedjan.

Nästa fråga →

Attacktyp: Hårdvara i leverantörskedjan

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Incidenthanteringsteamet upptäcker att flera berörda bärbara datorer kör SSD-versioner av fast mjukvara som inte överensstämmer med den officiella versionskommentarer från leverantören. Endpoint Detection Response (EDR) visar inga skadliga processer. Vad tyder detta mest sannolikt på?

- [ ] Ett konfigurationsfel från IT-leverantören
- [ ] En ny typ av utpressningsvirus som raderar sig själv
- [ ] En kompromiss i leverantörskedjan på den fasta mjukvarans nivå
- [ ] Normalt beteende under avbildning

Se rätt svar →

Attacktyp: Hårdvara i leverantörskedjan

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Incidenthanteringsteamet upptäcker att flera berörda bärbara datorer kör SSD-versioner av fast mjukvara som inte överensstämmer med den officiella versionskommentarer från leverantören. Endpoint Detection Response (EDR) visar inga skadliga processer. Vad tyder detta mest sannolikt på?

- ✗ Ett konfigurationsfel från IT-leverantören
- ✗ En ny typ av utpressningsvirus som raderar sig själv
- ✓ En kompromiss i leverantörskedjan på den fasta mjukvarans nivå
- ✗ Normalt beteende under avbildning

Obehörig fast SSD-mjukvara på flera bärbara datorer som inte upptäcks av EDR och som inte stämmer överens med officiella versioner, tyder på avsiktlig manipulering av hårdvara eller fast mjukvara, vilket är kännetecknande för en kompromiss i leverantörskedjan på den fasta mjukvarans nivå.

Nästa fråga →

Attacktyp: Hårdvara i leverantörskedjan

1 — 2 — 3: Återställning efter en cyberattack — 4

Du har isolerat 100 misstänkta enheter med falsk fast SSD-mjukvara. Du måste bestämma dig för hur du ska gå vidare utan att angriparen, som kan ha fjärråtkomst, får nys om det. Vilket är det bästa efterföljande draget?

- [ ] Stäng av alla enheter och skicka dem till forensisk undersökning
- [ ] Utför minnesdumpar live och undersök medan systemen körs
- [ ] Meddela tredjepartsleverantören att intrång har skett
- [ ] Rensa alla enheter och skicka ut nya bärbara datorer till alla användare globalt

Se rätt svar →

Attacktyp: Hårdvara i leverantörskedjan

1 — 2 — 3: Återställning efter en cyberattack — 4

Du har isolerat 100 misstänkta enheter med falsk fast SSD-mjukvara. Du måste bestämma dig för hur du ska gå vidare utan att angriparen, som kan ha fjärråtkomst, får nys om det. Vilket är det bästa efterföljande draget?

- ✗ Stäng av alla enheter och skicka dem till forensisk undersökning
- ✓ Utför minnesdumpar live och undersök medan systemen körs
- ✗ Meddela tredjepartsleverantören att intrång har skett
- ✗ Rensa alla enheter och skicka ut nya bärbara datorer till alla användare globalt

Minnesdumpar live är avgörande för att bevara flyktiga bevis, som aktiva skadliga program och spökprogram, och möjliggör riktade incidentsvar genom att upptäcka dolda hot och åtkomstpunkter innan de går förlorade eller angriparna varnas.

Nästa fråga →

Attacktyp: Hårdvara i leverantörskedjan

1 2 3 4: Övergripande bästa praxis

Din informationssäkerhetschef vill ha en sammanfattning av hur den här attacken tog sig in i miljön. Du måste presentera en kortfattad förklaring för ledningen. Hur ska du förklara attacken?

- [ ] Ett virus laddades ner av misstag från en nätfiskelänk
- [ ] Vi hade en felaktig konfiguration av nätverket som möjliggjorde extern åtkomst
- [ ] Skadlig fast mjukvara fördes in via en kompromitterad hårdvaruleverantör under driftsättning av bärbara datorer
- [ ] En av våra utvecklare skickade kod som inte var säker till produktion

Se rätt svar →

Attacktyp: Hårdvara i leverantörskedjan

1 2 3 4: Övergripande bästa praxis

Din informationssäkerhetschef vill ha en sammanfattning av hur den här attacken tog sig in i miljön. Du måste presentera en kortfattad förklaring för ledningen. Hur ska du förklara attacken?

- ✗ Ett virus laddades ner av misstag från en nätfiskelänk
- ✗ Vi hade en felaktig konfiguration av nätverket som möjliggjorde extern åtkomst
- ✓ Skadlig fast mjukvara fördes in via en komprometterad hårdvaruleverantör under driftsättning av bärbara datorer
- ✗ En av våra utvecklare skickade kod som inte var säker till produktion

De felaktiga versionerna av den fasta mjukvaran och frånvaron av aktiva skadliga program bekräftar att det här var en attack på fast mjukvarunivå från leverantören, inte ett användarfel eller en felaktig konfiguration.

Se lösningar →

ATTACKTYP: HÅRDVARA I LEVERANTÖRSKEDJAN

Sammanfattning

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 kan vara allt från småföretag till globala företag, med resultat som allvarliga ekonomiska förluster, bristande kundförtroende och juridiska konsekvenser.

Dell minskar risken för hårdvaruattacker i leverantörskedjan genom att integrera rigorösa leverantörsriskbedömningar och bädda in nollförtroendeprinciper tillsammans med kontinuerlig enhetsvalidering och oberoende integritetskontroller. Vi stärker hårdvaruintegriteten under hela livscykeln.

Läs mer om avancerade strategier för cyberelasticitet och se hur Dell kan hjälpa dig att skydda din organisation mot hårdvaruattacker i leverantörskedjan.

Utforska översikten om hårdvaruattacker i leverantörskedjan →

Tillbaka till scenarier

Trygghet inom leverantörskedjan ›

Dells leverantörskedja säkerställer att hårdvara, fast mjukvara och leverantörer verifieras noggrant innan de når din organisation genom avancerad ursprungsgranskning, manipuleringssäker logistik och transparenta inköp.

Säker komponentverifiering (SCV) ›

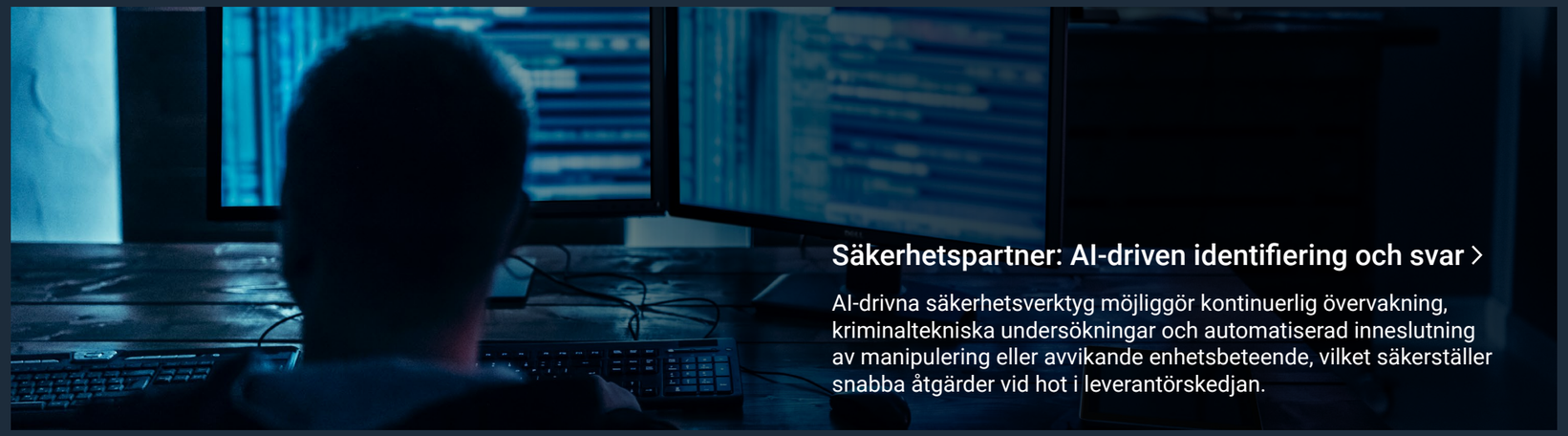
Kryptografisk verifiering av datorkomponenter på fabriken och under installationen säkerställer autenticiteten, identifierar dolda ändringar och minskar manipuleringsriskerna i leverantörskedjan.

Betrodd arbetsyta och betrodd infrastruktur ›

Hårdvarubaserad autentisering och kontinuerliga integritetskontroller av fast mjukvara skyddar slutpunkterna och varnar dig för obehöriga ändringar eller skadliga installationer innan de blir hot.

Spårning av tillgångar och ProSupport Suite med SupportAssist ›

Omfattande spårning av tillgångar, realtidsövervakning av enheternas ursprung och proaktiv integritetsverifiering säkerställer snabb avvikelsedetektering och säkerhet för hela datorflottan.



Säkerhetspartner: AI-driven identifiering och svar ›

AI-drivna säkerhetsverktyg möjliggör kontinuerlig övervakning, kriminaltekniska undersökningar och automatiserad inneslutning av manipulering eller avvikande enhetsbeteende, vilket säkerställer snabba åtgärder vid hot i leverantörskedjan.

Attacktyp: Mjukvara i leverantörskedjan

Ditt företag tillhandahåller molnbaserad analysmjukvara som används av sjukhus. Era serverdelstjänster är beroende av ett allmänt använt loggbibliotek med öppen källkod som underhålls av en betrodd tredjepartsutvecklare på GitHub.

Det utvecklingsteamet inte vet är att angripare har gett sig på GitHub-kontot och infogat en skadlig uppdatering som innehåller dold kod som är utformad för att:

- Exfiltrera miljövariabler, inklusive API-nycklar (Application Programming Interface) och JWT-hemligheter (JavaScript Object Notation Web Tokens)
- Skapa ett omvänt skal när specifika IP-adresser gör förfrågningar
- Förbli vilande så länge den inte utlöses på distans

Testa dina kunskaper →

Attacktyp: Mjukvara i leverantörskedjan

1: Minimera angreppsytan — 2 — 3 — 4

API:t börjar plötsligt returnera 500-fel till viktiga klienter. Molnövervakningen flaggar utgående anslutningar från de behållarbaserade tjänsterna till en domän du inte har sett tidigare. Vilket är ditt första svar?

- [ ] Avaktivera all utgående nätverkstrafik från behållare
- [ ] Starta om berörda tjänster för att rensa eventuella minnesproblem
- [ ] Kontrollera om koden har bekräftats nyligen i GitHub-lagret
- [ ] Kontakta domänens värdleverantör

Se rätt svar →

Attacktyp: Mjukvara i leverantörskedjan

1: Minimera angreppsytan — 2 — 3 — 4

API:t börjar plötsligt returnera 500-fel till viktiga klienter. Molnövervakningen flaggar utgående anslutningar från de behållarbaserade tjänsterna till en domän du inte har sett tidigare. Vilket är ditt första svar?

- ✓ Avaktivera all utgående nätverkstrafik från behållare
- ✗ Starta om berörda tjänster för att rensa eventuella minnesproblem
- ✗ Kontrollera om koden har bekräftats nyligen i GitHub-lagret
- ✗ Kontakta domänens värdleverantör

Om du inaktiverar all utgående nätverkstrafik från behållare blockeras angriparna omedelbart från att extrahera känsliga data eller upprätta fjärråtkomst via det komprometterade loggningsbiblioteket. På så sätt isoleras miljön i realtid och du får tid att undersöka, skydda API-nycklar och hemligheter och förhindra aktivering av vilande attackmekanismer.

Nästa fråga →

Attacktyp: Mjukvara i leverantörskedjan

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Den tekniskt ansvariga bekräftar att applikationen hämtade kod automatiskt från GitHub tre dagar innan problemen började. Den versionen har ännu inte markerats som skadlig i några offentliga databaser. Vilken är den mest ansvarsfulla omedelbara åtgärden?

- [ ] Kontakta biblioteksägaren direkt via GitHub
- [ ] Ta bort alla lokala projektberoenden och återskapa dem
- [ ] Vänta på information om vanliga säkerhetsproblem och exponeringar (Common Vulnerabilities and Exposures) innan du vidtar ytterligare åtgärder
- [ ] Återställa till den senast kända säkra versionen av koden

Se rätt svar →

Attacktyp: Mjukvara i leverantörskedjan

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Den tekniskt ansvariga bekräftar att applikationen hämtade kod automatiskt från GitHub tre dagar innan problemen började. Den versionen har ännu inte markerats som skadlig i några offentliga databaser. Vilken är den mest ansvarsfulla omedelbara åtgärden?

- ✗ Kontakta biblioteksägaren direkt via GitHub
- ✗ Ta bort alla lokala projektberoenden och återskapa dem
- ✗ Vänta på information om vanliga säkerhetsproblem och exponeringar (Common Vulnerabilities and Exposures) innan du vidtar ytterligare åtgärder
- ✓ Återställa till den senast kända säkra versionen av koden

Återställning till den senast kända säkra kodversionen tar bort den komprometterade uppdateringen omedelbart, eliminerar angriparens fotfäste och återställer driftsintegriteten för att proaktivt begränsa risker och skydda känsliga data.

Nästa fråga →

Attacktyp: Mjukvara i leverantörskedjan

1 — 2 — 3: Återställning efter en cyberattack — 4

Analysen bekräftar att biblioteket exfiltrerade API-nycklar och molninloggningsuppgifter. Du har identifierat flera behållare som har byggts med den skadade versionen. Vilket steg är viktigast i inneslutningsstrategin?

- [ ] Återkalla och rotera alla inloggningsuppgifter i berörda miljöer
- [ ] Göra nya avbildningar av behållarna med en uppdaterad operativsystemsavbildning (OS)
- [ ] Rensa utvecklingsteamets bärbara datorer
- [ ] Lämna in en borttagningsnotis för GitHub-lagret

Se rätt svar →

Attacktyp: Mjukvara i leverantörskedjan

1 — 2 — 3: Återställning efter en cyberattack — 4

Analysen bekräftar att biblioteket exfiltrerade API-nycklar och molninloggningsuppgifter. Du har identifierat flera behållare som har byggts med den skadade versionen. Vilket steg är viktigast i inneslutningsstrategin?

- ✓ Återkalla och rotera alla inloggningsuppgifter i berörda miljöer
- ✗ Göra nya avbildningar av behållarna med en uppdaterad operativsystemsavbildning (OS)
- ✗ Rensa utvecklingsteamets bärbara datorer
- ✗ Lämna in en borttagningsnotis för GitHub-lagret

Återkalla och rotera inloggningsuppgifter är det första viktiga steget efter ett intrång i molnet, eftersom det blockerar angriparna från att komma åt tjänster, stoppar datastöld och säkrar system oavsett intrångets omfattning.

Nästa fråga →

Attacktyp: Mjukvara i leverantörskedjan

1 2 3 4: Övergripande bästa praxis

Du ombeds att förklara vad som hände för teknikchefen och juridik-/efterlevnadsteamen. Vilken är den mest exakta och tydliga förklaringen? Hur sammanfattar du incidenten?

- [ ] Vårt interna verktyg för kontinuerlig integrering och kontinuerlig distribution/leverans (CI/CD) misslyckades, vilket gjorde att skadlig kod kunde distribueras
- [ ] Ett beroende för tredjepartsmjukvara komprometterades och vår automatisering tog in det i produktionen
- [ ] En utvecklare inkluderade otestad kod i en version som skyndades fram
- [ ] En angripare använde kraft för att komma in i vårt GitHub-lager

Se rätt svar →

Attacktyp: Mjukvara i leverantörskedjan

1 — 2 — 3 — 4: Övergripande bästa praxis

Du ombeds att förklara vad som hände för teknikchefen och juridik-/efterlevnadsteamen. Vilken är den mest exakta och tydliga förklaringen? Hur sammanfattar du incidenten?

- ✗ Vårt interna verktyg för kontinuerlig integrering och kontinuerlig distribution/leverans (CI/CD) misslyckades, vilket gjorde att skadlig kod kunde distribueras
- ✓ Ett beroende för tredjepartsmjukvara kompromitterades och vår automatisering tog in det i produktionen
- ✗ En utvecklare inkluderade otestad kod i en version som skyndades fram
- ✗ En angripare använde kraft för att komma in i vårt GitHub-lager

Grundorsaken var en attack i leverantörskedjan: angriparna gav sig på ett beroende för tredjepartsmjukvara och den automatiska byggprocessen tog direkt in den skadliga uppdateringen i produktion, vilket påverkade programintegriteten och känsliga miljöer och belyste risken för skadliga uppdateringar i betrodda externa beroenden.

Se lösningar →

ATTACKTYP: MJUKVARA I LEVERANTÖRSKEDJAN

Sammanfattning

Cyberattacker i leverantörskedjans mjukvara utnyttjar sårbarheter i mjukvaruuppdateringar, integreringar från tredje part och utvecklingsmiljöer för att bädda in skadlig kod som sprids i nätverken. Dessa attacker kan orsaka omfattande dataintrång, driftstörningar och äventyra hela ekosystem, vilket påverkar företag av alla storlekar.

Dell strävar efter cyberelasticitet genom att betona transparens, säker utveckling och kontinuerlig övervakning, samtidigt som vi har en robust incidentåtgärdsplan för att säkerställa snabb återställning och kommunikation med intressenter.

Läs mer om avancerade strategier för cyberelasticitet och se hur Dell kan hjälpa dig att skydda din organisation mot mjukvaruattacker i leverantörskedjan.

Utforska översikten om mjukvaruattacker i leverantörskedjan →

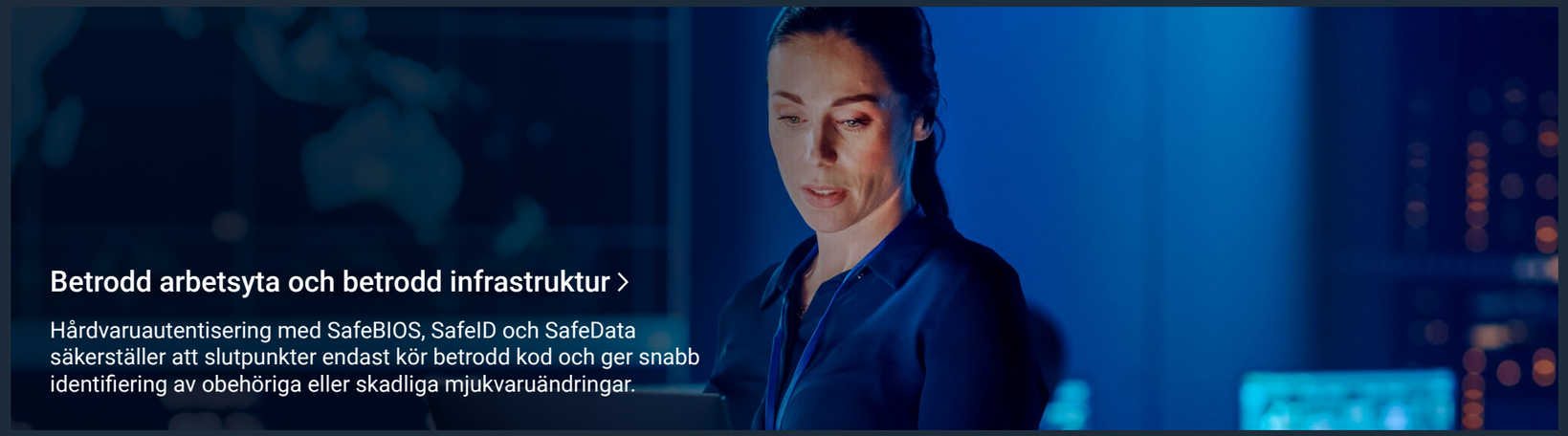
Tillbaka till scenarier

Trygghet inom leverantörskedjan ›

Dells leverantörskedja säkerställer att hårdvara, fast mjukvara och leverantörer verifieras noggrant innan de når din organisation genom avancerad ursprungsgranskning, manipuleringssäker logistik och transparenta inköp.

Livscykel för säkerhetsutveckling (SDL) ›

Implementerar branschledande metoder för säker utveckling för att minska riskerna från tredjepartsberoenden och förhindra mjukvarubaserade attacker i levererade lösningar.



Betrodd arbetsyta och betrodd infrastruktur ›

Hårdvaruautentisering med SafeBIOS, SafeID och SafeData säkerställer att slutpunkter endast kör betrodd kod och ger snabb identifiering av obehöriga eller skadliga mjukvaruändringar.

Spårning av tillgångar och ProSupport Suite med SupportAssist ›

Övervakning i realtid av enheter och mjukvara möjliggör snabb identifiering och svar på avvikelser som kommer in genom leverantörskedjan.

Säkerhetspartner: AI-driven identifiering och inneslutning ›

Upptäck, blockera och åtgärda snabbt mjukvaruattacker i leverantörskedjan, inklusive sådana som kommer in via öppen källkod eller kod från tredje part.

Attacktyp: Nolldag

Du är säkerhetsanalytiker och övervakar ett företags autentiseringsloggar. Användare har på senare tid rapporterat obehörig åtkomst till deras konton, trots att de inte har delat sina inloggningsuppgifter.

När du undersöker loggarna upptäcker du följande aktivitet:

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

Samtidigt identifierar en säkerhetsforskare en sårbarhet i programmeringsgränssnittet (API):

- JWT (JavaScript Object Notation Web Tokens) upphör aldrig att gälla.
- Token lagras i det lokala lagringsutrymmet i stället för HTTP-begränsade cookies.
- Ingen flerfaktorsautentisering (MFA) används.

Testa dina kunskaper →

Attacktyp: Nolldag

1: Minimera angreppsytan — 2 — 3 — 4

Hur skulle du som säkerhetsteam gå tillväga för att bekräfta detta, med tanke på att du misstänker en nolldagsattack eftersom inga varningsklockor ringde?

- [ ] Logga ut alla användare från deras system
- [ ] Identifiera viktiga avvikande autentiseringsbeteenden i loggar
- [ ] Kontakta vänner på andra företag för att se om de har samma problem
- [ ] Prova att korrelera med annan avvikande säkerhetsaktivitet

Se rätt svar →

Attacktyp: Nolldag

1: Minimera angreppsytan — 2 — 3 — 4

Hur skulle du som säkerhetsteam gå tillväga för att bekräfta detta, med tanke på att du misstänker en nolldagsattack eftersom inga varningsklockor ringde?

- ✗ Logga ut alla användare från deras system
- ✓ Identifiera viktiga avvikande autentiseringsbeteenden i loggar
- ✗ Kontakta vänner på andra företag för att se om de har samma problem
- ✓ Prova att korrelera med annan avvikande säkerhetsaktivitet

Du kan bekräfta en samordnad nolldagsattack genom att identifiera avvikande autentiseringsbeteenden, till exempel ovanliga inloggningstider, återanvändning av inloggningsuppgifter eller åtkomst från ovanliga enheter, och korrelera dem med annan avvikande säkerhetsaktivitet som avvikelser i dataåtkomst eller utökning av privilegier.

Nästa fråga →

Attacktyp: Nolldag

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Eftersom sårbarheten är okänd måste säkerhetsteamen begränsa skadan samtidigt som de utreder. Hur skulle du göra det?

- [ ] Ogiltigförklara alla autentiseringssessioner i hela systemet
- [ ] Fokusera alla resurser på angreppets ingångspunkt
- [ ] Tvinga fram inloggning med flerfaktorsautentisering (MFA) enbart
- [ ] Förlita dig på aktuella regler för statiska brandväggar eller WAF (Web Application Firewall)

Se rätt svar →

Attacktyp: Nolldag

1 — 2: Upptäcka och reagera på cyberhot — 3 — 4

Eftersom sårbarheten är okänd måste säkerhetsteamen begränsa skadan samtidigt som de utreder. Hur skulle du göra det?

- ✓ Ogiltigförklara alla autentiseringssessioner i hela systemet
- ✗ Fokusera alla resurser på angreppets ingångspunkt
- ✓ Tvinga fram inloggning med flerfaktorsautentisering (MFA) enbart
- ✗ Förlita dig på aktuella regler för statiska brandväggar eller WAF (Web Application Firewall)

Tillsammans stärker dessa åtgärder säkerheten och minimerar riskerna samtidigt som de stoppar angriparnas åtkomst så att säkerhetsteamen kan undersöka och lösa den underliggande sårbarheten.

Nästa fråga →

Attacktyp: Nolldag

1 — 2 — 3: Återställning efter en cyberattack — 4

Dell-datorer har teknik som Secure Boot, Trusted Platform Module (TPM), Basic Input/Output System (BIOS) Password Protection och SafeBIOS. Hur kan dessa hjälpa till vid en nolldagsattack?

- [ ] Skyddar mot attacker med dumpning av inloggningsuppgifter som stjäl API-token (Application Programming Interface)
- [ ] Förhindrar att en angripare med fysisk åtkomst kan kringgå operativsystemets (OS) säkerhet för att installera skadliga program som stjäl autentiseringstoken
- [ ] Säkerställer att angripare inte kan manipulera BIOS-inställningarna för att försämra operativsystemets säkerhet, vilket kan leda till API-sessionskapning
- [ ] Alla ovanstående

Se rätt svar →

Attacktyp: Nolldag

1 — 2 — 3: Återställning efter en cyberattack — 4

Dell-datorer har teknik som Secure Boot, Trusted Platform Module (TPM), Basic Input/Output System (BIOS) Password Protection och SafeBIOS. Hur kan dessa hjälpa till vid en nolldagsattack?

- [x] Skyddar mot attacker med dumpning av inloggningsuppgifter som stjäl API-token (Application Programming Interface)
- [x] Förhindrar att en angripare med fysisk åtkomst kan kringgå operativsystemets (OS) säkerhet för att installera skadliga program som stjäl autentiseringstoken
- [x] Säkerställer att angripare inte kan manipulera BIOS-inställningarna för att försämra operativsystemets säkerhet, vilket kan leda till API-sessionskapning
- [x] Alla ovanstående

Den här metoden med flera lager ger ett omfattande skydd mot nolldagsattacker som riktar sig mot BIOS, fast mjukvara, inloggningsuppgifter och systemkonfigurationer. Genom att förhindra manipulering, obehörig åtkomst och stöld av inloggningsuppgifter förblir dessa tekniker effektiva även när angripare upptäcker nya sårbarheter.

Nästa fråga →

Attacktyp: Nolldag

1 2 3 4: Övergripande bästa praxis

Vilket är det bästa sättet att försöka förhindra nolldagsattacker?

- [ ] Inte använda mjukvara med öppen källkod
- [ ] Använda nollförtroendeprinciper
- [ ] Se till att alla säkerhetskorrigeringar är installerade, inklusive för operativsystem (OS), fast mjukvara, API:er (Application Programming Interface), bibliotek och behållare
- [ ] Konfigurera en elektrisk grind runt företaget som håller hotfulla aktörer borta

Se rätt svar →

Attacktyp: Nolldag

1 — 2 — 3 — 4: Övergripande bästa praxis

Vilket är det bästa sättet att försöka förhindra nolldagsattacker?

- ✗ Inte använda mjukvara med öppen källkod
- ✓ Använda nollförtroendeprinciper
- ✗ Se till att alla säkerhetskorrigeringar är installerade, inklusive för operativsystem (OS), fast mjukvara, API:er (Application Programming Interface), bibliotek och behållare
- ✗ Konfigurera en elektrisk grind runt företaget som håller hotfulla aktörer borta

Om det finns okända sårbarheter eller system som inte har säkerhetskorrigeringar installerade kan nollförtroendeprinciper förhindra nolldagsattacker genom att ta bort inneboende tillit från användare och enheter, upprätthålla kontinuerlig autentisering, begränsa åtkomsten till endast nödvändig information och begränsa motståndarnas rörelser för att avsevärt minska den risk organisationen utsätts för från oupptäckta hot.

Se lösningar →

ATTACKTYP: NOLLDAG

Sammanfattning

En nolldagsattack innebär att en ej upptäckt 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.

Dell hanterar nolldagsattacker med nollförtroendekontroller, nätverkssegmentering, snabb inneslutning och användarutbildning som ytterligare stärker försvaret mot nya hot.

Läs mer om avancerade strategier för cyberelasticitet och se hur Dell kan hjälpa dig att skydda din organisation mot nolldagsattacker.

Utforska översikten om nolldagsattacker →

Tillbaka till scenarier

Betrodd arbetsyta och betrodd infrastruktur ›

Försvara slutpunkter och infrastruktur. Med SafeBIOS-, SafeID-, SafeData-skydd och nollförtroenderamverk som flerfaktorsautentisering (MFA) och rollbaserad åtkomstkontroll (RBAC) levererar Dell försvar i flera lager för att begränsa sårbarhetsvägar och säkerställa hårdvaruautentisering.

PowerEdge-servrar ›

Säker start, Silicon Root of Trust och nätverkssegmentering med SmartFabric begränsar lateral förflyttning, vilket säkerställer att endast betrodd kod körs på infrastrukturen.

Säkerhetspartner ›

Avancerad hotinformation, Managed Detection and Response (MDR), Extended Detection and Response (XDR) och detaljerade åtkomstkontroller hjälper till att upptäcka, eftersöka och begränsa nolldagsattacker innan de sprids.

PowerProtect-portföljen ›

Oföränderliga säkerhetskopior, isolerade cyberåterställningsvalv och AI-driven CyberSense-analys säkerställer snabb återställning och motståndskraft efter nolldagsintrång.

Tjänster för säkerhet och motståndskraft ›

Dells experter tillhandahåller snabb inneslutning, kriminalteknisk utredning och motståndsplanering för att motverka nolldagshot, genom allt från korrigeringshantering till incidentåtgärder.


DELL Technologies