Överlevnadsguide för cybersäkerhet:

Att reagera på moderna cyberhot

Den digitala världen har blivit en riskfylld djungel där varje klick, nedladdning och inloggning kan utlösa en dold cyberfälla.

Dagens cyberlandskap är mer farligt än någonsin tidigare, med hot som utpressningsvirus, DDoS-attacker, nätfiskebedrägerier och säkerhetskopieringsintrång som blir allt mer avancerade. Hackare använder nu AI för att överlista traditionella försvar och omvandlar det som en gång var opportunistiska attacker till beräknade och permanents hot som kan orsaka omfattande skador.

Dell-kunder har rapporterat oroväckande AI-drivna attacker där hackare genomsöker sociala medier för att skapa övertygande meddelanden som kan lura även de mest cybermedvetna medarbetarna.

Dessa berättelser utgör en viktig påminnelse om hur angripare nyttjar avancerade tekniker för att manipulera, lura och infiltrera företag med oöverträffad precision.

För att navigera i denna fientliga miljö behöver företag tillämpa en omfattande cybersäkerhetsstrategi – ett överlevnadspaket som kombinerar banbrytande verktyg, proaktiva strategier och en vaksamhetskultur. Den här guiden utforskar komponenterna i en sådan strategi och hjälper företag att bygga upp motståndskraften mot dagens mest akuta cyberhot.

Planen för att skydda ditt företag: ett ramverk med nollförtroende

I dagens AI-drivna hotlandskap är det inte längre valfritt att införa ett ramverk med nollförtroende. Angripare använder AI för att automatisera spaning, stjäla inloggningsuppgifter och anpassa sina tekniker snabbt, vilket gör traditionella försvar mindre effektiva. Nollförtroende utgår från att alla åtkomstbegäranden kontinuerligt verifieras och strikta autentiseringsprocesser implementeras för att minimera riskerna.

Genom proaktiv övervakning av användare, enheter och program minskar nollförtroende risken för obehörig åtkomst och dataläckor. Det är en modern, enhetlig metod för identitetshantering.

Håll datormiljön säker genom att minska attackytan

Att minska attackytan är avgörande för att försvara sig mot AI-drivna hot, eftersom slutpunkter, API:er och sårbarheter i leverantörskedjan ofta utnyttjas av angripare. Slutpunkter och API:er fungerar som ingångspunkter till nätverk och används ofta för att distribuera skadliga program och stjäla känsliga data.

För att skydda dessa områden krävs en försvarsstrategi i flera lager, inklusive stark autentisering, krypterade data under överföring, regelbunden sårbarhetstestning, slutpunktsdetektering och respons, korrigeringshantering och enhetshärdning. Lösningar för slutpunktsövervakning och kontinuerlig hotdetektering bidrar till att identifiera och blockera skadliga aktiviteter i realtid.

Företag måste införa proaktiva strategier för att skydda sina mjukvaruleverantörskedjor och sin utvecklingslivscykel. Genom att upprätthålla åtkomst med minsta behörighet säkerställer man att endast auktoriserade användare och program kan interagera med viktiga system, medan automatiserad hotdetektering och respons snabbt kan åtgärda sårbarheter när de uppstår.

Ta hjälp av en erfaren guide i den digitala djungeln med proaktiv hotdetektering och respons

AI-drivna attacker utnyttjar sårbarheter, härmar legitima beteenden och anpassar sig dynamiskt för att kringgå säkerhetsåtgärder, vilket gör dem svåra att upptäcka. För att bekämpa dessa sofistikerade hot behöver företag mer än reaktiva åtgärder – de behöver avancerade hotdetekteringssystem i kombination med kapacitet för snabb respons. Genom att utnyttja AI och maskininlärning kan säkerhetsteamen analysera beteendemönster, upptäcka avvikelser, reagera på hot i realtid och åtgärda problem innan betydande skador uppstår.

Ett effektivt detekterings- och svarssystem måste ta in enorma mängder driftdata så att det kan identifiera risker och utlösa automatiserade åtgärder. Hotinformation bygger också på sig själv, vilket gör systemet smartare så att det proaktivt kan identifiera och motverka angriparens nya taktiker.

Öva på att bygga upp skyddet i förväg med incidentrespons och återställning

Att förebygga attacker är det första steget, men företag måste agera som om en attack är oundviklig. Målet är att överleva attacken med minimala skador, och en effektiv strategi består av två delar:

- En kraftfull plan för respons och återställning.
- Tekniska åtgärder inriktade på att säkerhetskopiera kritiska data och program.

En incidentåterställningsplan bör vara omfattande. Eftersom en kraftfull attack sannolikt skulle påverka större delen av företagets verksamhet negativt, kanske till och med hela verksamheten, bör planen omfatta vad varje avdelning inom företaget skulle göra i händelse av en cyberincident. Planen bör också ange hur företaget ska kommunicera både internt och externt, med färdiga kommunikationsmallar redo att användas. Planen måste också uppdateras och underhållas regelbundet. Planen behöver också tillämpas på ett adekvat sätt. När ett angrepp kommer måste alla vara instinktivt redo att agera.

Ur ett tekniskt perspektiv bör företag börja med att fastställa hur **den minsta livskraftiga verksamheten** ser ut: Vilka system MÅSTE förbli i drift, även om det innebär att man behöver använda papper och penna? Är det viktigt att försäljningen fortsätter att fungera? Hur är det med kundtjänsten då?

När dessa beslut har tagits bör säkerhetskopierings- och återställningsmekanismerna byggas runtom dem. Att ha möjlighet att återgå till kända fungerande data gör det inte bara möjligt för företag att återuppta verksamheten snabbt, utan det eliminerar även mycket av inflytande från skadliga aktörer som försöker använda data för utpressning. Dessutom måste moderna responsstrategier gå längre än traditionella metoder och behandla AI/LLM-system som chattrobotar och virtuella agenter som nivå 1-tillgångar med samma återställningsprioritet som betalningssystem och kunddata.

Responsplanerna bör balansera automatisering med manuella kontroller för att bekämpa avancerade hot. Det är viktigt att veta hur ditt företag kommer att fungera i händelse av ett totalt systemhaveri. Vad händer om man måste återgå till penna och papper?

Alla behöver bidra – skapa medvetenhet bland medarbetarna

Medarbetarna utgör den främsta försvarslinjen mot cyberhot, ungefär som ett överlevnadsteam som upptäcker faror i naturen. Varje medlem har en nyckelroll när det gäller att identifiera risker och skydda resurserna. För att stärka detta försvar behöver företag robusta medvetenhetsprogram som attacksimuleringar som inkluderar AI-specifika hot som avancerat nätfiske och deepfake-bedrägerier.

De bästa programmen kombinerar löpande utbildning, öppen kommunikation, verkliga simuleringar och en kultur av delat ansvar. När alla, från personal i frontlinjen till cheferna, förstår både traditionella och AI-drivna hot blir företaget en vaksam och välinformerad enhet. Genom att uppmuntra lagarbete och förberedelser kan ditt företag ligga steget före föränderliga cyberrisker och bygga upp ett motståndskraftigt försvar mot potentiella attacker.

Bästa praxis för att upprätthålla motståndskraften mot AI-drivna attacker

För att förbli motståndskraftiga mot AI-drivna attacker måste företag anta en proaktiv och strategisk strategi. Här är tio rekommenderade rutiner:

Arkitektur som bygger på nollförtroende

Kräver kontinuerlig verifiering, strikta åtkomstkontroller och nätverkssegmentering för att säkerställa att varje användare och enhet autentiseras innan åtkomst beviljas, vilket hjälper till att blockera och begränsa snabba, AI-drivna attacker.

Stärka identitets- och åtkomsthanteringen:

Driftsätt robust autentisering (MFA, RBAC) och upprätthåll starka policyer för inloggningsuppgifter för att minska antalet lyckade nätfiskeförsök och användning av stulna inloggningsuppgifter.

Automatiserad tillgångsidentifiering och -inventering:

Identifiera och övervaka alla tillgångar fortlöpande, inklusive moln, IoT och skugg-IT, för att undvika dolda exponeringar.

Mikrosegmentering och nätverksåtkomstkontroller:

Segmentera och isolera nätverk och arbetsbelastningar för att förhindra laterala attackrörelser och begränsa hot.

Slutpunkts- och API-härdning:

Använd ett avancerat slutpunktsskydd (EDR/XDR) och säkra API-gatewayer, stark autentisering, hastighetsbegränsning, indatavalidering och kryptering.

Rigorös sårbarhets- och korrigeringshantering:

Automatisera genomsökning och snabb korrigering för operativsystem, fast mjukvara, appar, API:er och programvara från tredje part.

AI-driven detektering och övervakning av hot:

Dra nytta av beteende- och avvikelsedetektering som drivs av AI/ML för att fånga upp subtila och automatiserade hot i realtid.

Automatiserad incidentrespons:

Använd automatiserade playbooks för att snabbt isolera, begränsa och åtgärda hot, vilket minimerar angriparens kvardröjningstid.

Regelbundna realistiska simuleringar och kontinuerliga förbättringar:

Genomför scenariobaserade övningar, simulerade attacker från ett rött team och nätfiskesimuleringar och uppdatera sedan responsplaner och detekteringsmodeller baserat på utfallen.

Oföränderliga säkerhetskopior och återställning med luftfickor:

Skapa manipuleringssäkra säkerhetskopior – helst med luftgap och regelbundet testade – för att säkerställa en ren och snabb återställning.

DELL Technologies

Dell Technologies: Din guide genom okänt territorium

För att skydda ditt företag från avancerade cyberhot krävs rätt verktyg och expertkunskaper för att ligga steget före risker som ständigt förändras. I dagens komplexa cybersäkerhetslandskap är en robust strategi avgörande för att skydda företagets data, system och rykte. Det är där Dell Technologies hjälper till genom att erbjuda en omfattande svit av lösningar som är anpassade för att tillgodose behoven hos företag av alla storlekar.

Dell utrustar ditt företag med den teknik som behövs för att försvara sig mot moderna cyberattacker, från en säker leverantörskedja, avancerad hotdetektering och slutpunktsskydd till säker datahantering. Dells team har stöd av branschledande experter och arbetar nära tillsammans med er för att ta fram en anpassad säkerhetsstrategi. Med funktioner som realtidsövervakning, automatiserad hotrespons och nollförtroendearkitektur bidrar Dell till att säkerställa att ditt företag förblir proaktivt och har hög motståndskraft.

Oavsett om du hanterar utpressningsprogram, nätfiskeattacker eller regelefterlevnad hjälper Dell Technologies till med att tryggt navigera bland aktuella hot. Samarbeta med Dell för att skydda ditt företag och lyckas i den digitala eran. Se till att verksamheten är säker, effektiv och redo vad som än dyker upp.

> Incidenthanteringsplanen måste skrivas ut på papper eftersom systemen kan vara otillgängliga under en attack.”
>
> ***Rachel Tyler***
> *Cybersecurity Advisory Consultant, Dell Services*

Dell-produkter och -lösningar som kan hjälpa dig

Dells utvalda lösning	Beskrivning
Dells betrodda infrastruktur	En kombination av Dells servrar, nätverk, lagring och lösningar för cyberelasticitet som tillsammans skapar en modern, säker och stabil grund för innovationer.
Cyberelasticitet	En omfattande portfölj med lösningar som utformats för att skydda dina data och garantera en säker återställning. Omfattar enheter, mjukvara och erbjudanden som levereras som tjänster.
Cybersäkerhetstjänster	En svit med tjänster som kan hjälpa dig att utveckla och implementera en omfattande säkerhetsstrategi för arbetsbelastningar. Erbjudandena omfattar rådgivningstjänster, vCISO, Managed Detection and Response, intrångs- och sårbarhetstester samt incidentrespons och återställning.
Dell Trusted Workspace (slutpunktssäkerhet)	En kombination av inbyggda och valfria tilläggsfunktioner som utformats för att skydda kommersiella datorer. Inbyggda funktioner är byggda med metoder för en säker leverantörskedja och inkluderar SafeBIOS och SafeID med TPM. Valfria tillägg inkluderar säker komponentverifiering, SafeID med ControlVault och partnermjukvaran CrowdStrike och Absolute för att maximera säkerheten över arbetsytan.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **dell.com/cybersecuritymonth**