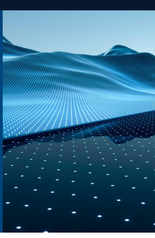
10 rekommendationer för cybersäkerhet

Tekniken utvecklas i en så snabb takt, och när vi anammar nya verktyg och system som förbättrar vår kapacitet skapar vi samtidigt nya möjligheter för cyberhot som försöker utnyttja våra sårbarheter. I det här landskapet är det viktigt att implementera robusta cybersäkerhetsåtgärder som skydd mot dessa nya hot och för att säkerställa att innovationen kan blomstra i en säker miljö. När organisationer anpassar sig till de nya riskerna rekommenderar cybersäkerhetsexperter från Dell Technologies 10 grundläggande åtgärder för att främja din cybersäkerhetsmognad.



1 Förstå ditt hotlandskap.

Erfarna cybersäkerhetspartner kan tillhandahålla värdefull expertis och viktiga resurser för att hjälpa till att navigera i det snabbt föränderliga hotlandskapet.

- Genomför grundliga sårbarhetsbedömningar och intrångstester för att identifiera potentiella svagheter som måste åtgärdas samt eventuella luckor i din strategi.
- Dra nytta av specialiserade färdigheter och kunskaper som kanske inte finns tillgängliga internt, till exempel kunskap om nya risker, avancerade angreppstekniker och de allra senaste säkerhetsstrategierna samt bästa praxis.
- Definiera åtkomstbehörigheter och motiv, så att du kan upprätta lämpliga säkerhetsramverk för att implementera dina affärskontroller och din affärsstyrning.

2 Skapa en omfattande strategi för cybersäkerhet.

IT-teamet, cybersäkerhetspersonalen, ledningen och ibland även externa experter måste samarbeta för att säkerställa cyberhållighet.

- Främja möjliggörandet för hela företaget – säkerheten är allas ansvar.
- Utnyttja automatisering där det är möjligt.
- Se till att du har en väl inövad IRR-plan som gör att rätt personer får veta när en cyberattack inträffar.

3 Arbeta med leverantörer som har en säker leverantörskedja.

Säkerheten börjar tidigare än du tror. Etablera en säker grund genom att samarbeta med leverantörer som prioriterar säkerhet vid utformning, tillverkning och leverans av enheter och infrastruktur. Leverantörer som erbjuder en säker leverantörskedja, en säker utvecklingslivscykel och rigorös hotmodellering kan hjälpa dig att ligga steget före hotaktörer.

- Tillhandahåll sekretess, integritet och tillgänglighet vad gäller den information som beskriver eller hanteras i IT-leverantörskedjan, samt information om de parter som ingår i IT-leverantörskedjan.
- Se till att IT-produkter eller -tjänster i leverantörskedjan är äkta, oförändrade och uppfyller köparens specifikationer utan ytterligare oönskade funktioner.
- Minska sårbarheter som kan begränsa avsedd funktion för en komponent eller leda till komponentfel eller säkerhetsproblem.

4 Använd nollförtroendeprinciper.

Nollförtroende är ett säkerhetskoncept som bygger på uppfattningen att organisationer inte automatiskt ska lita på något inom eller utanför sina gränser, utan i stället måste verifiera allt som försöker ansluta till deras system innan de beviljar åtkomst.

- Rör dig bort från en perimeterbaserad säkerhetsmodell och börja använda nollförtroendeprinciper.
- Implementera principen om lägst privilegier, vilket innebär att begränsa användar- och systemkonton så att de endast har de lägsta åtkomsträttigheterna som krävs för deras uppgifter. Den här metoden minskar angreppsytan och den potentiella effekten av obehörig åtkomst för angripare.
- Införliva lösningar som mikrosegmentering, identitets- och behörighetshantering (IAM), flerfaktorsautentisering (MFA) och säkerhetsanalys, för att nämna några.

5 Minska angreppsytan.

Angreppsytan representerar potentiella sårbarheter och startpunkter som kan utnyttjas av illvilliga aktörer. För att förbättra sin säkerhetsställning måste organisationer minska angreppsytan, minska risker och förbättra det övergripande cyberskyddet mot nya och framväxande hot.

- Utbilda medarbetare och användare så att de kan känna igen och rapportera potentiella säkerhetshot, nätfiskeförsök och försök till socialteknik för att minimera risken för lyckade angrepp som utnyttjar mänskliga sårbarheter.
- Implementera förebyggande åtgärder, som omfattande nätverkssegmentering, isolering av kritiska data, användning av strikta åtkomstkontroller och regelbunden uppdatering och korrigering av system och program.
- Se till att system, nätverk och enheter är korrekt konfigurerade med bästa säkerhetspraxis. till exempel genom att inaktivera onödiga tjänster, använda starka lösenord och tillämpa åtkomstkontroller.

6 Upptäcka och åtgärda cyberhot.

Inför sofistikerade hot är traditionella säkerhetsåtgärder inte längre tillräckliga. Organisationer bör utnyttja avancerad teknik och avancerade metoder för hotidentifiering för att effektivt identifiera och reagera på både kända och okända hot.

- Övervaka och analysera nätverkstrafik, systemloggar och andra områden, samt säkerhetsdata för att proaktivt identifiera tecken på obehörig åtkomst, intrång, infektioner med skadliga program, dataläckor och andra cyberhot.
- Implementera en åtgärdsplan för att snabbt undersöka och minska bekräftade säkerhetsincidenter. Detta inkluderar att begränsa effekterna, identifiera grundorsaken och implementera nödvändiga åtgärder för att återställa system och förhindra ytterligare skador.
- Använd AI/ML för att snabbt upptäcka cyberhot genom realtidsanalys av ovanliga datamönster eller beteenden. Dessa tekniker underlättar också snabb respons genom att bedöma hotets allvarlighetsgrad, förutsäga effekter, automatisera vissa defensiva åtgärder och skala säkerhetsrutiner, vilket minimerar den potentiella skadan.

7 Återställning efter en cyberattack.

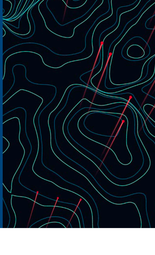
Även med viktiga proaktiva åtgärder på plats bör organisationer alltid förutsätta att de har utsatts för intrång och de måste ha tillgå funktioner på plats, som testas ofta, för att säkerställa effektiv återställning från en genomförd cyberattack.

- Vidta omedelbara åtgärder för att minimera skadan som orsakas av en cyberattack genom att isolera och begränsa effekterna.
- Koppla bort angripna system från nätverket, inaktivera konton som har äventyrats och implementera åtgärder för att förhindra ytterligare spridning eller skador.
- Användning av AI/ML kan påskynda återställningen genom att snabbt identifiera drabbade system och data samt automatisera återställningsprocessen från säkerhetskopior.

8 Dra nytta av erfarna partner.

Ingen enskild leverantör har alla funktioner som behövs för att tillhandahålla heltäckande säkerhet, som personal, processer eller teknik – det krävs samarbete. Därför är det viktigt att samarbeta med ett nätverk av erfarna partner.

- Ha kontakt med erfarna cybersäkerhetspartner som har värdefull expertis och viktiga resurser för att hjälpa till att navigera i det snabbt föränderliga hotlandskapet.
- Dra nytta av specialiserade färdigheter och kunskaper som kanske inte finns tillgängliga internt, till exempel kunskap om nya risker, avancerade angreppstekniker och de senaste säkerhetsstrategierna samt bästa praxis.
- Dra nytta av expertisen hos erfarna professionella tjänster och etablera samarbetsrelationer med tillförlitliga affärspartner för att etablera en heltäckande säkerhetsställning som effektivt skyddar mot nya cyberhot.



9 Utöka cybersäkerheten till kanter och molnmiljöer.

När nätverken sprider sig från kärnan till kanten och till molnet har de alla blivit en viktig sårbarhetspunkt. Oavsett hur program driftsätts kräver de samma säkerhetsnivå och anpassning till affärspolicyer för att säkerställa enhetlighet för både programanvändare och -hantering.

- Se till att nollförtroendeprinciperna utökas till att omfatta kant- och molnmiljöer, och tillhandahåll robusta åtkomstkontroller, kontinuerlig autentisering och omfattande synlighet och kontroll över nätverkstrafik.
- Implementera säkerhetsåtgärder, som nätverkssegmentering, kryptering och kontinuerlig övervakning, i både kärnnätverket och molnmiljöerna för att skydda mot potentiella hot.
- Samarbeta med erfarna professionella tjänster som är specialiserade på kant-, kärn- och molnsäkerhet för att dra nytta av deras expertis vad gäller att implementera effektiva åtgärder som skyddar organisationen från alla håll.

10 Hantera proaktivt och öka motståndskraften heltäckande.

Hantering av hotinformation, incidenter och respons samt säkerhetsåtgärder kan förbättra en organisations förmåga att identifiera och reagera på cyberhot.

- Upprätta proaktiva protokoll för incidentrespons och återställning som tydligt beskriver roller och ansvarsområden, vilket säkerställer smidig kommunikation och samordning mellan teammedlemmarna.
- Förbättra synligheten för miljön så att organisationer proaktivt kan övervaka och reagera på hot i sina nätverk, samtidigt som de tillhandahåller varningar för återställning vid behov.
- Stärk din förmåga att proaktivt upptäcka och reagera på cyberhot genom att utnyttja avancerad hotinformation, säkerhetsinformation och händelsehantering (SIEM), lösningar för slutpunktsskydd samt beteendeanalyser.

Låt inte säkerhetsriskerna kväva innovationen.
Lär dig hur du kan öka cybersäkerheten och stärka nollförtroendeprinciperna på dell.com/SecuritySolutions

DELL Technologies