DELL Technologies

Öka cybersäkerheten och stärk nollförtroendeprinciperna

Låt inte säkerhetsrisker kväva innovationen

Ta reda på hur ni ligger till med er cybersäkerhet

Ta reda på var ni behöver vara

I dagens komplexa och snabbt föränderliga hotlandskap står organisationer ofta inför resurs- och kunskapsbegränsningar när det gäller att upprätthålla robusta cybersäkerhetsrutiner. Att öka cybersäkerheten och stärka nollförtroendeprinciperna är avgörande för att bekämpa nya cyberhot för att skydda din miljö utan att kväva innovation.

Du kan använda de här checklistorna för att bedöma er aktuella cybersäkerhetsberedskap. Att känna till din organisations styrkor och sårbarheter gör att du kan ta de rätta stegen för att öka er cybersäkerhetsberedskap.

Innehåll

Mer information

Mer information om att öka cybersäkerheten och stärka nollförtroendeprinciperna

Checklista

Minska angreppsytan

Angreppsytan avser alla möjliga punkter eller områden i en miljö som en cyberangripare kan rikta in sig på eller utnyttja. Dessa punkter kan inkludera sårbarheter i programvara, felkonfigurationer, svaga autentiseringsmekanismer, okorrigerade system, överdrivna användarprivilegier, öppna nätverksportar, dålig fysisk säkerhet med mera. De här frågorna kan hjälpa dig att avgöra hur du kan minimera sårbarheter och startpunkter som en illvillig aktör kan utnyttja.

Ja	Nej	
☐	☐	Utför ditt företag regelbundna bedömningar, intrångstester eller intrångsattacksimuleringar för att identifiera sårbarheter och svagheter i system och nätverk, och möjliggöra åtgärder och förbättringar i tid?
☐	☐	Har din organisation säkerhetsutbildning för medarbetarna regelbundet?
☐	☐	Använder din organisation flerfaktorsautentisering (MFA) och rollbaserade åtkomstkontroller (RBAC)?
☐	☐	Har din organisation implementerat nätverkssegmentering i syfte att isolera viktiga tillgångar och begränsa åtkomsten mellan olika delar av nätverket?
☐	☐	Implementerar din organisation säkra kodningsrutiner, genomför regelbundna säkerhetstester och kodgranskningar, och använder brandväggar för webbprogram (WAF) för att skydda mot vanliga angrepp på programnivå och minska angreppsytan på webbprogram?
☐	☐	Väljer din organisation IT-leverantörer som kan intyga att deras processer och rutiner säkrar leverantörskedjan?
☐	☐	Implementerar din organisation nollförtroendeprinciper i stället för traditionell perimeterbaserad säkerhet?
☐	☐	Använder din organisation principen om lägst privilegier för att begränsa användare och systemkonton så att de endast har den lägsta åtkomstbehörighet som krävs för att utföra sina uppgifter?
☐	☐	Korrigerar din organisation regelbundet era system och programvaror?
☐	☐	Används AI/ML-funktioner i din organisations säkerhetsverktyg för att proaktivt identifiera sårbarheter?

Checklista

Upptäck och hantera hot

Att upptäcka och reagera på cyberhot är en viktig komponent i alla säkerhetsstrategier. Det handlar om att övervaka och analysera nätverkstrafik, systemloggar och andra områden, samt säkerhetsdata för att identifiera tecken på obehörig åtkomst, intrång, infektioner med skadliga program, dataläckor och andra cyberhot. De här frågorna kan hjälpa dig att avgöra hur din organisation proaktivt identifierar och aktivt hanterar potentiella säkerhetsincidenter och skadliga aktiviteter inom ett datornätverk, ett system eller en organisation.

Ja	Nej	
☐	☐	Övervakar din organisation kontinuerligt nätverks- och systemaktiviteter med hjälp av säkerhetsverktyg och -teknik som XDR (Extended Detection and Response), IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), SIEM samt logganalys?
☐	☐	Analyserar din organisation insamlade data för att identifiera mönster, avvikelser och indikatorer på hot (IoC) eller attackindikatorer (IOA) som kan tyda på ett potentiellt cyberhot?
☐	☐	Har din organisation driftsatt de senaste synlighets- och övervakningsverktygen för att snabbt upptäcka och varna om potentiella risker?
☐	☐	Övervakar din organisation nätverkstrafiken avseende ovanliga mönster eller misstänkt aktivitet som kan tyda på en pågående cyberattack?
☐	☐	Har din organisation implementerat några AI/ML-verktyg som hjälper till att detektera cyberhot genom realtidsanalys av ovanliga datamönster eller beteenden?
☐	☐	Har din organisation övervägt att implementera nästa generations SIEM-lösning för att bättre kunna hantera säkerhetsvarningar och börja korrelera säkerhetshändelsedata från hela IT-ekosystemet?
☐	☐	Använder din organisation sårbarhetstestning och -hantering för att prioritera och åtgärda befintliga sårbarheter samt för att effektivt kunna reagera på nya sårbarheter?
☐	☐	Har din organisation en incidentresponsplan för att undersöka och åtgärda bekräftade säkerhetsincidenter?
☐	☐	Använder din organisation SOAR-verktyg (Security Orchestration, Automation and Response) för att snabba upp incidentåtgärder som kan bidra till att minska spridningen av en cyberattack?
☐	☐	Tar din organisations incidentresponsplan upp inneslutningsprinciper, kommunikationsplaner, efterlevnadskrav, kriminalteknisk analys och återställningsprocesser?

Checklista

Återställning efter en cyberattack

Återställning efter en cyberattack handlar om att återställa påverkade system, nätverk och data till ett säkert drifttillstånd efter en säkerhetsincident. Det handlar om att vidta åtgärder för att mildra skadan som orsakats av attacken, bygga om komprometterade eller störda tjänster och enheter, analysera incidenten för att förhindra framtida attacker och återställa organisationens verksamhet till det normala. De här frågorna kan hjälpa dig att avgöra om din organisation kan återhämta sig effektivt från cyberattacker.

Ja	Nej	
☐	☐	Har din organisation implementerat några incidentinneslutningsåtgärder i syfte att isolera och begränsa spridningen av en cyberattack?
☐	☐	Har din organisation processer på plats för system- eller enhetsåterställning efter att en incident har inneslutits?
☐	☐	Använder din organisation dataisolering, oföränderlighet eller ett cybervalv när ni skyddar era data?
☐	☐	Har din organisation etablerat rutiner för att återställa data korrekt i händelse av komprometterade, krypterade eller raderade data?
☐	☐	Använder din organisation AI/ML-teknik för att automatisera eller påskynda återställningen efter en cyberattack?
☐	☐	Utvärderar din organisation incidenten kontinuerligt och identifierar förbättringsområden efter en attack och återställning?
☐	☐	Har din organisation genomfört en kriminalteknisk analys i syfte att förstå angreppsmetoden, fastställa intrångets utsträckning, identifiera berörda system och data samt samla bevis för att skydda er och vidta rättsliga eller disciplinära åtgärder?
☐	☐	Vet din organisation om att relevanta parter, till exempel kunder, partner och leverantörer, ska meddelas om en cyberattack och eventuell påverkan på deras data eller verksamhet?
☐	☐	Övar din organisation på återställningsstrategierna flera gånger per år för att ni ska känna er trygga med att återställa verksamheten och uppfylla era SLA:er?
☐	☐	Samarbetar din organisation med tjänsteleverantörer för att hjälpa till med organisationens återställning?

Öka cybersäkerheten och stärk nollförtroendeprinciperna

Det är viktigt för IT-organisationer att planera för det värsta tänkbara scenariot när det gäller cybersäkerhet och att ha ett försvar i flera lager. I det ständigt föränderliga hotlandskapet inom cybersäkerhet är det viktigt att hela tiden förbättra säkerhetsrutinerna och anamma nollförtroendeprinciper. Detta omfattar följande:

Minska angreppsytan

Minimera sårbarheter och startpunkter som kan utnyttjas för att göra intrång i miljön.

Upptäcka och åtgärda cyberhot

Identifiera och åtgärda aktivt potentiella säkerhetsincidenter och skadliga aktiviteter.

Återställning efter cyberattacker

Återställa organisationen till ett säkert och aktivt tillstånd efter en säkerhetsincident.

Genom att utnyttja expertisen hos professionella tjänster och samarbeta med tillförlitliga affärspartner kan Dell hjälpa organisationer att etablera en heltäckande säkerhetsställning som skyddar mot nya cyberhot. I takt med att tekniken utvecklas måste även vår strategi för cybersäkerhet göra det för att skydda vår digitala infrastruktur och upprätthålla förtroendet för den digitala världen.

DELL Technologies

Om Dell Technologies

Dell Technologies hjälper organisationer och individer att skapa sin digitala framtid samt förändra hur de arbetar, lever och leker. Företaget ger kunderna åtkomst till branschens mest omfattande och innovativa teknik- och serviceportfölj, utformad för dataeran.

Det finns mer information på
www.dell.com/securitysolutions