DELL Technologies

Verbeter uw cyberbeveiliging en de ontwikkeling van Zero Trust.

Laat veiligheidsrisico's uw innovatie niet belemmeren

Weet hoe het staat met uw cyberbeveiliging

Weet wat er nog gedaan moet worden

In het complexe en snel veranderende dreigingslandschap van vandaag hebben organisaties vaak te maken met beperkingen op het gebied van middelen en kennis als het gaat om het handhaven van robuuste cyberbeveiligingspraktijken. Het bevorderen van cyberbeveiliging en de ontwikkeling van Zero Trust is essentieel om veranderende cyberdreigingen te bestrijden om uw omgeving veilig te houden en innovatie niet te belemmeren.

Gebruik deze checklists om de huidige staat van uw cyberbeveiliging te beoordelen. Als u de sterke punten en kwetsbaarheden van uw organisatie kent, kunt u de volgende stappen zetten voor de ontwikkeling van uw cyberbeveiliging.

Inhoud

Meer informatie

Meer informatie over het verbeteren van uw cyberbeveiliging en het ontwikkelen van Zero Trust

Checklist:

Het aanvalsoppervlak beperken

Het aanvalsoppervlak verwijst naar alle mogelijke punten of gebieden in een omgeving die het doelwit kunnen zijn of kunnen worden uitgebuit door een cyberaanvaller. Deze punten kunnen bestaan uit softwarekwetsbaarheden, verkeerde configuraties, zwakke authenticatiemechanismen, niet-gepatchte systemen, buitensporige gebruikersrechten, open netwerkpoorten, slechte fysieke beveiliging en meer. Deze vragen kunnen helpen bepalen hoe u beveiligingslekken en toegangspunten die een kwaadwillende kan compromitteren, kunt minimaliseren.

Ja	Nee	
☐	☐	Voert uw organisatie regelmatig evaluaties, penetratietests of simulaties van inbreukaanvallen uit om beveiligingslekken en zwakke punten in systemen en netwerken te identificeren, zodat deze tijdig kunnen worden hersteld en verbeterd?
☐	☐	Geeft uw organisatie regelmatig beveiligingstrainingen voor uw medewerkers?
☐	☐	Maakt uw organisatie gebruik van meervoudige authenticatie (MFA) en op rollen gebaseerde toegangscontroles (RBAC)?
☐	☐	Heeft uw organisatie netwerksegmentatie geïmplementeerd om essentiële assets te isoleren en de toegang tussen verschillende delen van uw netwerk te beperken?
☐	☐	Implementeert uw organisatie veilige coderingspraktijken, voert u regelmatig beveiligingstests en codebeoordelingen uit en gebruikt u webapplicatiefirewalls (WAF's) om u te beschermen tegen veelvoorkomende aanvallen op applicatieniveau en om het aanvalsoppervlak van webapplicaties te verkleinen?
☐	☐	Kiest uw organisatie voor IT-leveranciers die kunnen aantonen dat zij over de processen en procedures beschikken om hun leveringsketen te beveiligen?
☐	☐	Implementeert uw organisatie Zero Trust-principes ter vervanging van traditionele grensgebaseerde beveiliging?
☐	☐	Maakt uw organisatie gebruik van het principe van de minste bevoegdheden om gebruikers en systeemaccounts te beperken zodat ze alleen de minimale toegangsrechten hebben die nodig zijn om hun taken uit te voeren?
☐	☐	Brengt uw organisatie regelmatig patches uit voor uw systemen en software?
☐	☐	Maken de beveiligingstools van uw organisatie gebruik van AI/ML-mogelijkheden om kwetsbaarheden proactief te identificeren?

Checklist:

Bedreigingen detecteren en erop reageren

Het detecteren van en reageren op cyberdreigingen is een essentieel onderdeel van elke beveiligingsstrategie. Het omvat het bewaken en analyseren van netwerkverkeer, systeemlogboeken en andere gebieden, evenals beveiligingsdata om tekenen van ongeoorloofde toegang, inbraken, malware-infecties, datalekken of andere cyberdreigingen te identificeren. Deze vragen kunnen helpen bepalen hoe uw organisatie proactief potentiële beveiligingsincidenten en schadelijke activiteiten binnen een computernetwerk, systeem of organisatie identificeert en actief aanpakt.

Ja	Nee	
☐	☐	Controleert uw organisatie voortdurend netwerk- en systeemactiviteiten met behulp van beveiligingstools en -technologieën als Extended Detection and Response (XDR), inbraakdetectiesystemen (IDS), inbraakpreventiesystemen (IPS), SIEM en logboekanalyse?
☐	☐	Analyseert uw organisatie de verzamelde data om patronen, afwijkingen en indicatoren of inbreuk (IoC's) en/of indicatoren van aanvallen (IOA) te identificeren die kunnen wijzen op een potentiële cyberdreiging?
☐	☐	Heeft uw organisatie de nieuwste zichtbaarheids- en bewakingstools geïmplementeerd om snel potentieel te detecteren en hierop te waarschuwen?
☐	☐	Controleert uw organisatie het netwerkverkeer op ongebruikelijke patronen of verdachte activiteiten die kunnen duiden op een cyberaanval?
☐	☐	Heeft uw organisatie AI/ML-tools geïmplementeerd om cyberdreigingen te helpen detecteren door middel van realtime analyse van ongebruikelijke datapatronen of gedragingen?
☐	☐	Heeft uw organisatie overwogen een SIEM-oplossing van de volgende generatie te implementeren om beveiligingswaarschuwingen beter te beheren en te beginnen met de correlatie van data over beveiligingsgebeurtenissen uit het hele IT-ecosysteem?
☐	☐	Voert uw organisatie beveiligingstests en -beheer uit om bestaande kwetsbaarheden te prioriteren en aan te pakken, en om efficiënt te reageren op nieuwe kwetsbaarheden?
☐	☐	Heeft uw organisatie een incidentresponsplan om bevestigde beveiligingsincidenten te onderzoeken en te beperken?
☐	☐	Maakt uw organisatie gebruik van SOAR-tools (Security Orchestration, Automation and Response) om acties voor incidentrespons te versnellen die kunnen helpen de verspreiding van een cyberaanval te verminderen?
☐	☐	Houdt het incidentresponsplan van uw organisatie rekening met inperkingsbeleid, communicatieplannen, nalevingsvereisten, forensische analyse en herstelprocessen?

Checklist:

Herstellen van een cyberaanval

Herstellen van een cyberaanval is het proces waarbij de getroffen systemen, netwerken en data na een beveiligingsincident worden hersteld naar een veilige en operationele staat. Het omvat het ondernemen van actie om de schade veroorzaakt door de aanval te beperken, het opnieuw opbouwen van gecompromitteerde of verstoorde services en apparaten, het analyseren van het incident om toekomstige aanvallen te voorkomen en het herstellen van de activiteiten van de organisatie naar normaal. Deze vragen kunnen helpen bepalen of uw organisatie effectief herstelt van cyberaanvallen.

Ja	Nee	
☐	☐	Heeft uw organisatie maatregelen geïmplementeerd om een cyberaanval te isoleren en in te dammen?
☐	☐	Heeft uw organisatie processen voor systeem- en/of apparaatherstel nadat een incident is ingeperkt?
☐	☐	Maakt uw organisatie gebruik van data-isolatie, onveranderlijkheid of een cyberkluis bij het beschermen van uw data?
☐	☐	Heeft uw organisatie procedures opgesteld om data schoon te herstellen in het geval van gecompromitteerde, versleutelde of verwijderde data?
☐	☐	Maakt uw organisatie gebruik van AI/ML-technologieën om het herstel na een cyberaanval te automatiseren of te versnellen?
☐	☐	Evalueert uw organisatie het incident voortdurend en identificeert u verbeterpunten na een aanval en herstel?
☐	☐	Heeft uw organisatie een forensische analyse uitgevoerd om inzicht te krijgen in de aanvalsmethodologie, de omvang van de inbreuk te bepalen, getroffen systemen en data te identificeren en bewijs te verzamelen om u veiliger te maken en juridische of disciplinaire maatregelen te nemen?
☐	☐	Weet uw organisatie dat relevante partijen, zoals klanten, partners en leveranciers, op de hoogte moeten worden gesteld van een cyberaanval en mogelijke gevolgen voor hun data of activiteiten?
☐	☐	Oefent uw organisatie uw herstelstrategieën meerdere keren per jaar om vertrouwen te krijgen in het herstel van uw bedrijf en om uw SLA's te halen?
☐	☐	Werkt uw organisatie samen met serviceproviders om u te helpen bij het herstel van uw organisatie?

Verbeter de cyberbeveiliging en de ontwikkeling van Zero Trust

Het is van cruciaal belang voor IT-organisaties om te plannen voor het ergste scenario als het gaat om cyberbeveiliging en om meerdere beveiligingslagen te hebben. Gezien het voortdurend veranderende dreigingslandschap op het gebied van cyberbeveiliging is het van cruciaal belang om voortdurend beveiligingspraktijken te verbeteren en Zero Trust-principes te omarmen. Dit omvat:

Het beperken van het aanvalsoppervlak

Minimaliseer beveiligingslekken en beperk het aantal toegangspunten die kunnen worden misbruikt om de systeemomgeving in gevaar te brengen.

Het detecteren van en reageren op cyberdreigingen

Actief alle mogelijke beveiligingsincidenten en schadelijke activiteiten identificeren en aanpakken.

Het herstellen van een cyberaanval

Herstel de organisatie naar een veilige, operationele staat na een beveiligingsincident.

Door gebruik te maken van de expertise van professionele dienstverleners en samen te werken met vertrouwde zakenpartners, kan Dell organisaties helpen een uitgebreide beveiligingsmentaliteit op te zetten die bescherming biedt tegen evoluerende cyberdreigingen. Naarmate de technologie zich blijft ontwikkelen, moet ook onze aanpak van cyberbeveiliging toenemen om onze digitale infrastructuur te beschermen en het vertrouwen in de digitale wereld te behouden.

Over Dell Technologies

Dell Technologies helpt organisaties en particulieren hun digitale toekomst vorm te geven en te transformeren hoe ze werken, leven en spelen. Het bedrijf biedt klanten de breedste en meest innovatieve technologieën in de branche en serviceportfolio's voor het datatijdperk.

Meer informatie op www.dell.com/securitysolutions