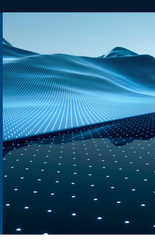
10 aanbevelingen voor cyberbeveiliging

Technologie ontwikkelt zich razendsnel en terwijl we nieuwe tools en systemen omarmen die onze mogelijkheden vergroten, creëren we tegelijkertijd nieuwe mogelijkheden voor cyberdreigingen die kwetsbaarheden proberen uit te buiten. In dit landschap is het cruciaal om robuuste cyberbeveiligingsmaatregelen te implementeren om bescherming te bieden tegen deze opkomende bedreigingen, zodat innovatie kan gedijen in een veilige omgeving. Terwijl organisaties zich aanpassen aan de nieuwe risico's, bevelen cyberbeveiligingsexperts van Dell Technologies 10 fundamentele acties aan om uw cyberbeveiliging te ontwikkelen.



1 Krijg inzicht in uw dreigingsrisicolandschap.

Ervaren cyberbeveiligingspartners kunnen waardevolle expertise en bronnen bieden om te helpen bij het navigeren door het snel veranderende dreigingslandschap.

- Voer grondige kwetsbaarheidsbeoordelingen en penetratietests uit om mogelijke zwakke punten te identificeren die moeten worden aangepakt en om eventuele hiaten in uw strategie te identificeren.
- Profiteer van gespecialiseerde vaardigheden en kennis die mogelijk niet intern beschikbaar zijn, zoals inzicht in opkomende risico's, geavanceerde aanvalstechnieken en de allernieuwste beveiligingsstrategieën en best practices.
- Definieer toegangsrechten en beweegredenen, zodat u het juiste beveiligingskader kunt opzetten voor het implementeren van uw bedrijfscontroles en governance.

2 Vorm een uitgebreide cyberbeveiligingsstrategie.

Om cybertolerantie te waarborgen, is een gecoördineerde inspanning nodig van IT-teams, professionals op het gebied van cyberbeveiliging, management en soms externe experts.

- Bevorder de inzetbaarheid van het hele bedrijf: veiligheid is ieders verantwoordelijkheid.
- Maak waar mogelijk gebruik van automatisering.
- Zorg ervoor dat u een goed geoefend IRR-plan hebt dat alle juiste mensen laat weten wanneer er een cyberaanval plaatsvindt.

3 Werk samen met leveranciers die een veilige leveringsketen hebben.

Beveiliging begint eerder dan u denkt. Zorg voor een vertrouwde basis door samen te werken met leveranciers die prioriteit geven aan beveiliging bij het ontwerp, de productie en de levering van apparaten en infrastructuur. Leveranciers die een veilige toeleveringsketen, een veilige ontwikkelingscyclus en rigoureuze bedreigingsmodellen bieden, kunnen helpen om bedreigingsactoren voor te blijven.

- Bied de vertrouwelijkheid, integriteit en beschikbaarheid van informatie die de IT-leveringsketen beschrijft of de IT-leveringsketen doorloopt, evenals informatie over de partijen die deelnemen aan de IT-leveringsketen.
- Zorg ervoor dat IT-producten en -services in de leveringsketen legitiem en ongewijzigd zijn en voldoen aan de specificaties van de inkoper zonder aanvullende ongewenste functionaliteit.
- Verminder beveiligingslekken die de beoogde functie van een component kunnen beperken, kunnen leiden tot defecte onderdelen of mogelijkheden bieden voor misbruik.

4 Omarm Zero Trust-principes.

Zero Trust is een beveiligingsconcept dat is gebaseerd op de overtuiging dat organisaties niet automatisch alles binnen of buiten hun grenzen moeten vertrouwen, maar in plaats daarvan alles moeten verifiëren wat verbinding probeert te maken met hun systemen voordat ze toegang verlenen.

- Stap over van een beveiligingsmodel op basis van grenzen en implementeer Zero Trust-principes.
- Implementeer het principe van de minste bevoegdheden, waardoor gebruikers- en systeemaccounts alleen de minimale toegangsrechten hebben die nodig zijn voor hun taken. Deze aanpak verkleint het aanvalsoppervlak en de potentiële impact van onbevoegde toegang door aanvallers.
- Integreer oplossingen zoals microsegmentatie, identiteits- en toegangsbeheer (IAM), multifactorauthenticatie (MFA) en beveiligingsanalyses, om er maar een paar te noemen.

5 Beperk het aanvalsoppervlak.

Het aanvalsoppervlak vertegenwoordigt potentiële beveiligingslekken en toegangspunten die kunnen worden uitgebuit door kwaadwillende partijen. Om hun beveiligingsmentaliteit te verbeteren, moeten organisaties het aanvalsoppervlak minimaliseren, risico's beperken en de algehele cyberverdediging tegen nieuwe en opkomende bedreigingen verbeteren.

- Train werknemers en gebruikers in het herkennen en melden van potentiële beveiligingsrisico's, phishing-pogingen en social-engineeringtactieken. Zo minimaliseert u het risico op succesvolle aanvallen die misbruik maken van menselijke kwetsbaarheden.
- Implementeer preventieve maatregelen, zoals uitgebreide netwerksegmentatie, isolatie van kritieke data, het afdwingen van strikte toegangscontroles en het regelmatig bijwerken van en patches uitbrengen voor systemen en applicaties.
- Zorg ervoor dat systemen, netwerken en apparaten correct zijn geconfigureerd met best practices voor beveiliging, zoals het uitschakelen van onnodige services, het gebruik van sterke wachtwoorden en het afdwingen van toegangscontroles.

6 Detecteer en reageer op cyberdreigingen.

Met geavanceerde dreigingen zijn traditionele beveiligingsmaatregelen niet langer voldoende. Organisaties moeten gebruikmaken van geavanceerde technologieën en methodieken voor bedreigingsdetectie om zowel bekende als onbekende bedreigingen effectief te identificeren en erop te reageren.

- Monitor en analyseer netwerkverkeer, systeemlogboeken en andere gebieden, evenals beveiligingsdata om proactief tekenen van onbevoegde toegang, inbraken, malware-infecties, datalekken of andere cyberdreigingen te identificeren.
- Implementeer een responsplan om bevestigde beveiligingsincidenten te onderzoeken en te beperken. Dit houdt in dat de impact moet worden ingeperkt, de hoofdoorzaak moet worden vastgesteld en de noodzakelijke acties moeten worden ondernomen om systemen te herstellen en verdere schade te voorkomen.
- Maak gebruik van AI/ML om cyberdreigingen snel te detecteren door middel van realtime analyse van ongebruikelijke datapatronen of gedragingen. Deze technologieën maken ook een snelle respons mogelijk door de ernst van bedreigingen te beoordelen, gevolgen te voorspellen, bepaalde verdedigingsacties te automatiseren en beveiligingspraktijken op te schalen, waardoor potentiële schade tot een minimum wordt beperkt.

7 Herstel na een cyberaanval.

Zelfs met kritieke proactieve maatregelen moeten organisaties er altijd van uitgaan dat deze zijn geschonden en moeten ze beschikken over veerkrachtige capaciteiten die regelmatig worden getest om effectief herstel na een succesvolle cyberaanval te garanderen.

- Onderneem onmiddellijk actie om de schade veroorzaakt door een cyberaanval te beperken door de impact te isoleren en in te dammen.
- Koppel de getroffen systemen los van het netwerk, schakel gecompromitteerde accounts uit en neem maatregelen om verdere verspreiding of schade te voorkomen.
- Met AI/ML kunt u het herstel versnellen door snel de getroffen systemen en data te identificeren en het herstelproces vanaf back-ups te automatiseren.

8 Maak gebruik van ervaren partners.

Er is geen enkele leverancier die alle benodigde capaciteiten heeft om end-to-end beveiliging te leveren, inclusief mensen, processen en technologie. Daar is een heel team voor nodig. Daarom is het essentieel om samen te werken met een netwerk van ervaren partners.

- Neem contact op met ervaren cyberbeveiligingspartners die waardevolle expertise en middelen bieden om u te helpen navigeren door het snel veranderende dreigingslandschap.
- Profiteer van gespecialiseerde vaardigheden en kennis die mogelijk niet intern beschikbaar zijn, waaronder inzicht in opkomende risico's, geavanceerde aanvalstechnieken en de nieuwste beveiligingsstrategieën en best practices.
- Maak gebruik van de expertise van ervaren professionele services en bouw samenwerkingsrelaties op met vertrouwde zakenpartners om een allesomvattende beveiligingsmentaliteit te ontwikkelen die effectief beschermt tegen evoluerende cyberdreigingen.

9 Breid cyberbeveiliging uit naar edge- en cloudomgevingen.

Naarmate netwerken zich uitbreiden van de core naar de edge en naar de cloud, zijn ze allemaal cruciale kwetsbare plekken geworden. Ongeacht de manier waarop applicaties worden geïmplementeerd, vereisen ze hetzelfde beveiligingsniveau en afstemming op het bedrijfsbeleid om consistentie te garanderen voor zowel gebruikers als beheer van applicaties.

- Zorg ervoor dat de Zero Trust-principes worden uitgebreid naar edge- en cloudomgevingen, met robuuste toegangscontroles, continue authenticatie en uitgebreide zichtbaarheid en controle over netwerkverkeer.
- Implementeer beveiligingsmaatregelen, zoals netwerksegmentatie, versleuteling en continue bewaking, in zowel het corenetwerk als cloudomgevingen om bescherming te bieden tegen potentiële bedreigingen.
- Werk samen met ervaren professionele dienstverleners die gespecialiseerd zijn in edge-, core- en cloudbeveiliging. Hun expertise kunt u inzetten bij het implementeren van effectieve maatregelen die uw organisatie van alle kanten beschermen.

10 Beheer proactief en verhoog de end-to-end tolerantie.

Het beheren van informatie over bedreigingen, incidenten en respons en beveiligingsactiviteiten kan de mogelijkheden van een organisatie verbeteren bij het detecteren van en reageren op cyberdreigingen.

- Stel proactieve protocollen op voor incidentrespons en herstel waarin rollen en verantwoordelijkheden duidelijk worden beschreven, zodat naadloze communicatie en coördinatie tussen teamleden wordt gewaarborgd.
- Verbeter de zichtbaarheid van de omgeving zodat organisaties proactief toezicht kunnen houden op bedreigingen binnen hun netwerken en hierop kunnen reageren. Tegelijkertijd worden er indien nodig waarschuwingen voor herstel gegenereerd.
- Versterk uw vermogen om cyberdreigingen proactief te detecteren en erop te reageren door gebruik te maken van geavanceerde bedreigingsinformatie, Security Information and Event Management (SIEM), oplossingen voor eindpuntbeveiliging en gedragsanalyses.

Laat beveiliging uw innovatie niet belemmeren.
Ontdek hoe u uw cyberbeveiliging en Zero Trust-ontwikkeling kunt verbeteren op dell.com/SecuritySolutions

DELL Technologies