Praktische cyberbeveiligingsgids:

# Reageren op moderne cyberdreigingen

## De digitale wereld is een verraderlijke wildernis geworden waar elke klik, download of aanmelding een verborgen cyberval kan activeren.

Het cyberlandschap van nu is gevaarlijker dan ooit, met bedreigingen zoals ransomware, DDoS-aanvallen, phishingscams en infiltraties van back-ups die steeds geavanceerder worden. Hackers maken nu gebruik van AI om traditionele beveiliging te slim af te zijn. Dat betekent dat de ooit opportunistische aanvallen nu berekende en persistente bedreigingen zijn die enorme schade kunnen veroorzaken.

Klanten van Dell hebben melding gemaakt van alarmerende door AI aangedreven aanvallen waarbij hackers sociale media gebruiken om overtuigende berichten te maken die zelfs de meest cyberbewuste werknemers kunnen misleiden.

Deze verhalen zijn een reminder van hoe aanvallers gebruikmaken van geavanceerde technologieën om organisaties met ongekende nauwkeurigheid te manipuleren, te bedriegen en te infiltreren.

Om door deze vijandige omgeving te navigeren, hebben organisaties een uitgebreide cyberbeveiligingsstrategie nodig. Een overlevingspakket met geavanceerde tools, proactieve strategieën en een cultuur van waakzaamheid. Deze gids onderzoekt de onderdelen van zo'n strategie, waarmee organisaties veerkracht kunnen opbouwen tegen de meest urgente cyberdreigingen van nu.

## De kaart voor een beschermde organisatie: een Zero Trust-framework

In het huidige door AI gestuurde bedreigingslandschap is het implementeren van een Zero Trust-framework niet langer optioneel. Aanvallers gebruiken AI voor geautomatiseerde verkenning, om inlogdata te stelen en hun technieken snel aan te passen, waardoor traditionele verdediging minder effectief is. Zero Trust werkt op basis van de mentaliteit 'aanname van inbreuk', waarbij elke toegangsaanvraag continu wordt gecontroleerd en strikte verificatieprocessen worden geïmplementeerd om risico's te minimaliseren.

Door proactief gebruikers, apparaten en applicaties te monitoren, vermindert Zero Trust de kans op ongeautoriseerde toegang en datalekken. Het is een moderne, uniforme aanpak van identiteitsbeheer.

## Houd de omgeving veilig: beperk het aanvalsoppervlak

Het aanvalsoppervlak beperken is essentieel voor de verdediging tegen met AI aangedreven bedreigingen, waarbij eindpunten, API's en kwetsbaarheden in de leveringsketen vaak worden misbruikt door aanvallers. Eindpunten en API's dienen als access points voor netwerken en zijn vaak gericht op het implementeren van malware of het stelen van gevoelige data.

Voor het beveiligen van deze gebieden is een gelaagde verdedigingsstrategie vereist, waaronder sterke verificatie, versleutelde stromende data, regelmatige kwetsbaarheidstests, EDR-tools (eindpuntdetectie en -respons), patchbeheer en verscherping van de apparaatbeveiliging. Oplossingen voor eindpuntmonitoring en continue bedreigingsdetectie helpen schadelijke activiteiten in real time te identificeren en te blokkeren.

Organisaties moeten proactieve strategieën implementeren om hun leveringsketens en ontwikkelingscyclus van software te beveiligen. Het afdwingen van toegang met minimale bevoegdheden zorgt ervoor dat alleen geautoriseerde gebruikers en applicaties kunnen communiceren met kritieke systemen. Geautomatiseerde bedreigingsdetectie en -respons kunnen kwetsbaarheden snel aanpakken zodra ze zich voordoen.

## Handel als doorgewinterde jagers: proactieve dreigingsdetectie en -respons

Door AI ondersteunde aanvallen misbruiken kwetsbaarheden, imiteren legitiem gedrag en passen zich dynamisch aan om beveiligingsmaatregelen te omzeilen, waardoor ze moeilijk te detecteren zijn. Om deze geavanceerde bedreigingen te bestrijden, hebben organisaties meer nodig dan reactieve maatregelen: ze hebben geavanceerde systemen voor bedreigingsdetectie nodig in combinatie met snelle responsmogelijkheden. Door gebruik te maken van AI en machine learning kunnen beveiligingsteams gedragspatronen analyseren, afwijkingen detecteren en in real time op bedreigingen reageren, en problemen aanpakken voordat er aanzienlijke schade optreedt.

Een effectief detectie- en responssysteem moet enorme hoeveelheden operationele data verwerken, zodat het risico's kan herkennen en geautomatiseerde reacties in gang kan zetten. Deze dreigingsinformatie bouwt ook voort op de eigen kennis, waardoor het systeem slimmer wordt en proactief nieuwe tactieken van kwaadwillenden kan identificeren en tegengaan.

## Oefen met een schuilplaats bouwen voor de storm: incidentrespons en -herstel

Hoewel aanvallen voorkomen de eerste stap is, moeten organisaties werken alsof een aanval onvermijdelijk is. Het doel is om de aanval met minimale schade te overleven en een effectieve strategie is tweeledig:

- Een robuust incidentrespons en -herstelplan (IRR, Incident Response and Recovery).
- Technologische maatregelen die gericht zijn op back-ups maken van kritieke data en applicaties.

Een incidentherstelplan moet uitgebreid zijn. Aangezien een krachtige aanval waarschijnlijk de meeste, zo niet alle activiteiten van het bedrijf platlegt, moet in het plan staan wat elke afdeling in het bedrijf zou doen in het geval van een cyberincident. Het plan moet ook ingaan op hoe de organisatie zowel intern als extern zal communiceren, met vooraf geschreven communicatiesjablonen die klaar zijn om verstuurd te worden. Het plan moet ook regelmatig worden bijgewerkt en onderhouden. Tot slot werkt het plan alleen goed als er regelmatig mee wordt geoefend. Wanneer de aanval plaatsvindt, moet iedereen op instinct kunnen handelen.

Vanuit technologisch perspectief moeten organisaties beginnen met bepalen welke activiteiten nodig zijn voor **minimale bedrijfsvoering**. Welke systemen MOETEN operationeel blijven, zelfs als dat met pen en papier moet? Is het belangrijk dat de sales doorgaan? Hoe zit het met de klantenservice?

Zodra dit is bepaald, moeten de back-up- en herstelmechanismen eromheen worden gebouwd. De mogelijkheid om terug te keren naar bekende goede data, betekent niet alleen dat de organisatie de activiteiten snel kan hervatten, maar ook dat de aanvallers die proberen uw data in gijzeling te houden een minder sterke onderhandelingspositie hebben. Bovendien moeten moderne IR-strategieën verder gaan dan traditionele benaderingen, waarbij AI/LLM-systemen zoals chatbots en virtuele agents worden behandeld als Tier 1-assets met dezelfde herstelprioriteit als betalingssystemen of klantdata.

Om geavanceerde bedreigingen tegen te gaan, moet er in IR-plannen een balans zijn tussen automatisering en handmatige controles. Het is van cruciaal belang om te weten hoe uw organisatie zal functioneren in het geval van een totale systeemstoring. Wat als je moet terugvallen op pen en papier?

## Iedereen moet meedoen: bewustzijn onder werknemers

Werknemers zijn uw eerste verdedigingslinie tegen cyberdreigingen, net als een overlevingsteam dat gevaren in de wildernis overwint. Elk lid speelt een belangrijke rol bij het identificeren van risico's en het beschermen van resources. Om deze verdediging te versterken, hebben organisaties robuuste bewustwordingsprogramma's nodig, zoals aanvalssimulaties met AI-specifieke bedreigingen. Denk hierbij aan geavanceerde phishing en deepfakes.

De beste programma's combineren doorlopende training, open communicatie, realistische simulaties en een cultuur van gedeelde verantwoordelijkheid. Wanneer iedereen, van eerstelijns personeel tot leidinggevenden, inzicht heeft in zowel traditionele als door AI gestuurde bedreigingen, wordt de organisatie een waakzame, goed geïnformeerde eenheid. Door teamwork en voorbereiding te stimuleren, kan uw organisatie evoluerende cyberrisico's voor blijven en een veerkrachtige verdediging opbouwen tegen potentiële aanvallen.

## Best practices om AI-aanvallen het hoofd te blijven bieden

**Om door AI gestuurde aanvallen het hoofd te blijven bieden, moeten organisaties een proactieve en strategische aanpak hanteren. Hier volgen 10 best practices:**

**Zero Trust-architectuur**

Vereist continue verificatie, strikte toegangscontroles en netwerksegmentatie om ervoor te zorgen dat elke gebruiker en elk apparaat worden geverifieerd voordat toegang wordt verleend, zodat snel bewegende, door AI gestuurde aanvallen worden geblokkeerd en ingeperkt.

**Verbeterd identiteits- en toegangsbeheer:**

Implementeer solide verificatie (MFA, RBAC) en dwing een sterk aanmeldbeleid af om de kans op succes van phishing en credential stuffing te verkleinen.

**Geautomatiseerde detectie en inventarisatie van assets:**

Ontdek en monitor voortdurend alle assets, inclusief cloud, IoT en schaduw-IT, om verborgen blootstelling te voorkomen.

**Microsegmentatie en netwerktoegangscontroles:**

Segmenteer en isoleer netwerken en workloads om laterale bewegingen van aanvallers te voorkomen en bedreigingen te beperken.

**Verscherping van de eindpunt- en API-beveiliging:**

Gebruik geavanceerde eindpuntbescherming (EDR/XDR) en beveiligde API-gateways; sterke verificatie, snelheidsbeperking, invoervalidatie en versleuteling.

**Rigoureus kwetsbaarheids- en patchbeheer:**

Automatiseer scans en snelle patches voor besturingssysteem, firmware, apps, API's en software van derden.

**Door AI aangestuurde bedreigingsdetectie en -monitoring:**

Maak gebruik van gedrags- en anomaliedetectie aangedreven door AI/ML om subtiele of geautomatiseerde bedreigingen in real time te detecteren.

**Geautomatiseerde incidentrespons:**

Gebruik geautomatiseerde playbooks om bedreigingen snel te isoleren, te beperken en te herstellen, waardoor de verblijfstijd van de aanvaller tot een minimum wordt beperkt.

**Regelmatige realistische simulaties en continue verbetering:**

Voer table-topoefeningen, red teaming en phishing-simulaties uit en werk IR-plannen en detectiemodellen bij op basis van de resultaten.

**Onveranderlijke, air-gapped back-ups en herstel:**

Maak back-ups die bestand zijn tegen manipulatie, zoals air-gapped back-ups en back-ups die regelmatig worden getest om een snel herstel te garanderen.



DELL Technologies

## Dell Technologies: uw gids voor onbekend terrein

Om uw organisatie te beschermen tegen geavanceerde cyberdreigingen, hebt u de juiste tools en expertise nodig om evoluerende risico's voor te blijven. In het huidige complexe landschap van cyberbeveiliging is een robuuste strategie essentieel om uw data, systemen en reputatie te beschermen. Daar komt Dell Technologies om de hoek kijken met een uitgebreid pakket oplossingen die zijn afgestemd op de behoeften van organisaties van elke omvang.

Dell voorziet uw bedrijf van de technologie die nodig is om u te beschermen tegen moderne cyberaanvallen, van een beveiligde leveringsketen, geavanceerde bedreigingsdetectie en eindpuntbescherming tot beveiligd databeheer. Het team van Dell kan bogen op toonaangevende expertise en werkt nauw met u samen om een aangepaste beveiligingsstrategie te ontwikkelen. Met functies zoals realtime monitoring, geautomatiseerde respons op bedreigingen en Zero Trust-architectuur helpt Dell ervoor te zorgen dat uw organisatie proactief en veerkrachtig blijft.

Of u nu te maken hebt met ransomware, phishingaanvallen of wettelijke naleving, Dell Technologies helpt u vol vertrouwen door het huidige bedreigingslandschap te navigeren. Werk samen met Dell om uw bedrijf te beschermen en te groeien in het digitale tijdperk, zodat uw activiteiten beveiligd, efficiënt en klaar zijn voor wat er gaat komen.

> Uw incidentresponsplan moet worden afgedrukt, omdat uw systemen mogelijk niet toegankelijk zijn tijdens een aanval."
>
> ***Rachel Tyler***
> *Cybersecurity Advisory Consultant, Dell Services*

## Dell producten en oplossingen die kunnen helpen

| Aanbevolen Dell oplossing | Omschrijving |
|---|---|
| Dell Trusted Infrastructure | Een combinatie van Dell server-, netwerk-, storage- en cybertolerantie-oplossingen die samen een moderne, beveiligde en veerkrachtige basis voor innovatie creëren. |
| Cybertolerantie | Een uitgebreid portfolio van oplossingen die zijn ontworpen om uw data te beschermen en veilig herstel te garanderen. Bevat apparaten, software en as-a-service-oplossingen. |
| Cybersecurity Services | Een reeks services die u kunnen helpen bij het ontwikkelen en implementeren van een uitgebreide beveiligingsstrategie voor verschillende workloads. Het aanbod omvat adviesdiensten, vCISO, Managed Detection and Response, penetratie- en kwetsbaarheidstests, en incidentrespons en -herstel. |
| Dell Trusted Workspace (eindpuntbeveiliging) | Een combinatie van geïntegreerde en optionele add-on-mogelijkheden die zijn ontworpen om zakelijke pc's te beveiligen. Ontwikkeld met veilige werkwijzen voor de leveringsketen en ingebouwde mogelijkheden zoals SafeBIOS en SafeID met TPM. Tot optionele add-ons behoren Secured Component Verification, SafeID met ControlVault en de partnersoftware CrowdStrike en Absolute voor maximale beveiliging van de werkruimte. |

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van vandaag kunt aanpakken op **dell.com/cybersecuritymonth**