Inzichten in cybertolerantie

Onderzoek naar hiaten in de cybertolerantie, veranderende dreigingen, AI-gestuurde verdedigingsmechanismen en herstelstrategieën in APJ

Uitdagingen op het gebied van cybertolerantie nemen toe naarmate cyberaanvallen en hiaten in databescherming leiden tot verhoogde risico's op onderbrekingen. Organisaties met een volledig ontwikkelde strategie voor cybertolerantie* hebben bijna drie keer meer kans om goed te herstellen. Door strategieën voor cybertolerantie te moderniseren, detectiemogelijkheden te verbeteren en prioriteit te geven aan continue optimalisatie, kunnen IT-leiders de risico's minimaliseren en het vertrouwen versterken in hun vermogen om zich aan te passen aan veranderende dreigingen.

Overmoedige leidinggevenden

74% van de IT-professionals is van mening dat hun leidinggevenden overschatten hoe goed ze zijn voorbereid op cyberincidenten. Overmoed creëert gevaarlijke blinde vlekken die cruciale investeringen vertragen en kwetsbaarheden laten bestaan.

De kloof tussen vertrouwen en vermogen

99,3% van de organisaties heeft strategieën voor cybertolerantie

Maar slechts **55%** is niet goed hersteld na hun laatste test of incident

Preventie versus herstel: een onevenwichtige aanpak

87%
is van mening dat hun organisatie zich meer richt op het voorkomen van aanvallen dan op het voorbereiden op het herstellen ervan

Maar slechts
30%
beschikt over een uitgebreid platform voor dreigingsdetectie in de primaire storage, back-upstorage en netwerkinfrastructuur

En maar
41%
heeft een aanval of cyberincident succesvol ingeperkt met minimale gevolgen en is hiervan hersteld

Wanneer er onvermijdelijk een inbreuk plaatsvindt, zijn veel organisaties daarom niet voorbereid op de herstelfase, die bepalend kan zijn voor hun voortbestaan.

De weg vooruit:
Volwassen organisaties leveren resultaten

Organisaties met een volledig ontwikkelde strategie voor cybertolerantie hebben bijna 2,8 keer meer kans om goed te herstellen

Strategische volwassenheid op drie essentiële vlakken zorgt voor een ongekende veerkracht.

BEVEILIGEN:
Uw vertrouwensbasis opbouwen

Organisaties met een volledig ontwikkelde strategie voor cybertolerantie zijn:

1,8 keer meer geneigd om apparaten te beschermen met behulp van beveiligingscontroles op firmware-/BIOS-niveau

meer geneigd om versleuteling te gebruiken voor data die is opgeslagen of wordt overgedragen

meer geneigd om cyberkluizen te gebruiken voor de bescherming van cruciale data tegen steeds veranderende dreigingen

Maar beveiliging is slechts het begin. Het echte voordeel is dat intelligente detectie dreigingen herkent voordat ze uw waardevolste assets in gevaar brengen.

DETECTEREN:
Intelligentie die nooit slaapt

De uitdaging op het gebied van zichtbaarheid:
Slechts 30% van de organisaties beschikt over robuuste dreigingsdetectie voor back-upstorage, primaire datastorage en netwerkinfrastructuur

De AI-gestuurde oplossing:

57% geeft prioriteit aan investeringen in door AI/ML aangedreven dreigingsdetectie

52% scant back-updata uitgebreid met AI/ML op inbreukindicatoren

Organisaties met volwassen strategieën maken **2,3 keer vaker** gebruik van AI/ML-tools met proactieve playbooks voor risicobeperking en -respons

HERSTELLEN:
Waar voorbereiding en prestaties samenkomen

Het voordeel van testen:

61% van de organisaties die maandelijks of vaker gesimuleerde cyberaanvallen uitvoeren, herstelde succesvol na incidenten

59% van de organisaties die minder dan eens per maand testen, herstelde niet goed van incidenten

Het resultaat:
Organisaties die regelmatig tests uitvoeren, behalen aanzienlijk vaker hun doelstellingen op het gebied van hersteltijd en herstelpunten dan organisaties die sporadisch tests uitvoeren.

Uw weg naar uitstekende cybertolerantie

Organisaties met een volledig ontwikkelde strategie voor cybertolerantie hebben 2,3 keer meer kans om consequent aan hun SLA's te voldoen

Een robuuste basis opbouwen
Geef prioriteit aan preventie en snel herstel.

- **Beveiligen:** verminder risico's met beveiligingscontroles op BIOS-niveau, dataversleuteling en cyberkluizen voor essentiële data.
- **Detecteren:** gebruik realtime AI/ML om dreigingen te detecteren en erop te reageren in alle soorten storage, inclusief primaire en beschermende storage.
- **Herstellen:** test het herstel regelmatig. Organisaties die dit maandelijks doen, behalen veel vaker hun hersteldoelstellingen.

Wilt u uw cybertolerantie verbeteren?

Wilt u uw cybertolerantie verbeteren? Lees alle belangrijkste conclusies uit het *Dell Cyber Resilience Insights onderzoek van 2026.*

DELL Technologies

Bron: Vanson Bourne en Dell Technologies Cyber Resilience Survey 2025.

*Organisaties met een volledig ontwikkelde strategie voor cybertolerantie worden gedefinieerd als organisaties met een strategie die volledig is geïmplementeerd en continu wordt geoptimaliseerd met behulp van voorspellende analyse, automatisering en realtime inzichten (bijv. feeds met dreigingsinformatie, ML-aangedreven aanpassingen, KPI's die verbeteringen ondersteunen)