DELL Technologies

Ransomware: Versterking van cyberbeveiliging en veerkracht met Dell Technologies

Wat is ransomware?

Ransomware is een type schadelijke software (malware) die de toegang tot een computersysteem of data blokkeert totdat er losgeld wordt betaald. Het is een van de meest verstorende soorten cyberaanvallen. Vijftig procent van de organisaties wereldwijd is in het afgelopen jaar ten minste één keer getroffen door ransomware en de gemiddelde downtime na een ransomware-aanval is drie weken, wat leidt tot aanzienlijke operationele onderbrekingen

Toenemende dreiging van ransomware

Ransomware is een type schadelijke software (malware) die de toegang tot een computersysteem of data blokkeert totdat er losgeld wordt betaald. Het is een van de meest verstorende soorten cyberaanvallen. Vijftig procent van de organisaties wereldwijd is in het afgelopen jaar ten minste één keer getroffen door ransomware en de gemiddelde downtime na een ransomware-aanval is drie weken, wat leidt tot aanzienlijke operationele onderbrekingen.

Hoe ransomware werkt

Ransomware infecteert organisaties meestal wanneer iemand op een schadelijke link klikt, een geïnfecteerde bijlage opent of een gecompromitteerde website bezoekt. Vervolgens gaat het naar systemen om bestanden te versleutelen, waardoor ze onleesbaar worden. Vervolgens verschijnt er meestal een bericht van het ransomware-programma waarin betaling wordt geëist (vaak in cryptocurrency) in ruil voor een decryptiesleutel. Als het losgeld niet wordt betaald, kan de aanvaller dreigen data te verwijderen of openbaar te maken. Een veelvoorkomend voorbeeld van een ransomware-aanval die in 2017 uitkwam, was de WannaCry-aanval die zich snel over de hele wereld verspreidde, waardoor ziekenhuizen, bedrijven en overheidsinstanties werden getroffen en een enorme financiële impact had. De wereldwijde economische impact van het WannaCry-virus lag tussen de $ 4 miljard en $ 8 miljard volgens Cyber Risk Management (CyRiM) en Lloyd's of London, met meer dan 200.000 systemen die binnen enkele dagen in 150 landen werden getroffen.

Tot de globale bedrijven die werden getroffen, behoren FedEx en Renault-Nissan. De eerste meldde een verlies van 300 miljoen dollar als gevolg van serviceonderbreking en opschoning en de tweede moest de productie in verschillende fabrieken tijdelijk stopzetten. De verborgen kosten van een ransomware-aanval kunnen talrijk zijn, waaronder dingen zoals:

- Bedrijfsstilstand en productiviteitsverlies
- Reputatieschade
- Kosten van systeemherstel en -patches
- Wettelijke en regelgevende boetes

Wanneer bedrijven worden geconfronteerd met een ransomware-aanval, moeten ze de volgende stappen ondernemen:

- Betaal niet tenzij dit absoluut noodzakelijk is. Er is geen garantie dat de aanvallers de toegang zullen herstellen.
- Herstel vanaf back-up, indien beschikbaar.
- Meld de aanval aan de autoriteiten.
- Versterk de verdediging om toekomstige infecties te voorkomen (bijv. software up-to-date houden, personeel trainen, eindpuntprotectie gebruikken).

Ransomware-aanvallen bestrijden met Dell Technologies

Dell Technologies voorziet organisaties van uitgebreide, vooruitstrevende tools die zijn ontworpen om ransomware-risico's te voorkomen voordat ze schade aanrichten.

Verbeterde eindpuntbeveiliging met Dell Trusted Devices

Eindpunten zijn vaak de primaire toegangspunten voor ransomware-aanvallen, waardoor eindpuntbeveiliging een cruciaal aandachtsgebied is. Dell Trusted Devices integreren hardwarebeveiligingsfuncties die systemen beschermen zonder in te leveren op prestaties. Oplossingen zoals Dell SafeBIOS en SafeID versterken eindpuntapparaten tegen onbevoegde toegang, terwijl Dell SafeData gevoelige data versleutelt om deze te beschermen, zelfs buiten de firewall van het bedrijf. Door beveiliging rechtstreeks te integreren in apparaten, zorgen bedrijven voor bescherming op hardwareniveau, waardoor aanvallers minder kans krijgen om binnen te dringen.

Proactieve detectie met CrowdStrike

Ransomware-aanvallen zijn niet onvermijdelijk als organisaties de juiste tools gebruiken om bedreigingen in realtime te detecteren en erop te reageren. CrowdStrike, aangeboden als onderdeel van het oplossingenportfolio van Dell, biedt een next-generation eindpuntbeschermingsplatform dat wordt aangedreven door AI en gedragsanalyses. Deze technologie identificeert en neutraliseert verdachte activiteiten voordat deze zich ontwikkelen tot een aanval. Door naadloos te integreren met de infrastructuur van Dell, kunnen IT-teams met CrowdStrike de zichtbaarheid in hun hele omgeving behouden, zodat ze onmiddellijk en effectief kunnen reageren op bedreigingen.

Uitgebreide databescherming met Dell PowerProtect

Dell PowerProtect oplossingen vormen de ruggengraat van ransomwareveerkracht. Deze geavanceerde tools voor databescherming zijn ontworpen om bedrijfsdata te beveiligen tegen zowel interne als externe bedreigingen. Functies zoals onveranderlijke back-ups zorgen ervoor dat uw data niet kunnen worden gewijzigd, verwijderd of versleuteld door ransomware, waardoor u zelfs bij geavanceerde aanvallen verzekerd bent van een betrouwbaar vangnet. Dell PowerProtect Cyber Recovery Vault soleert essentiële data bijvoorbeeld van het netwerk met behulp van air-gapped technologie, zodat deze zelfs tijdens de meest geavanceerde inbreuken niet aangetast worden. Met geautomatiseerde anomaliedetectie en intelligente workflows krijgen organisaties de mogelijkheid om kwaadaardige activiteiten vroegtijdig te detecteren en te reageren voordat ransomware zich verspreidt.

Geavanceerde netwerkbeveiliging en microsegmentatie met Dell PowerSwitch Networking en SmartFabric OS

Versterkt de bescherming tegen zero-day-aanvallen door geavanceerde netwerksegmentatie, strikte toegangscontroles en realtime verkeersanalyse te leveren in uw hele infrastructuur.

Grootschalig herstel met Dell Data Protection Services

Dell erkent dat, hoewel preventie essentieel is, herstel een even belangrijke rol speelt in de voorbereiding op ransomware. Dell Data Protection Services bieden niet alleen geautomatiseerde back-up- en hersteloplossingen, maar ook deskundig advies om ervoor te zorgen dat bedrijven snel kunnen herstellen en downtime tot een minimum kunnen beperken. Services zoals Remote Data Recovery en incident Response zorgen ervoor dat organisaties de support krijgen die ze nodig hebben tijdens piekmomenten in crisissituaties. Deze uitgebreide aanpak garandeert dat de data-integriteit behouden blijft en de hersteltijden worden verkort, waardoor operationele onderbrekingen worden voorkomen.

Dit zijn slechts een paar voorbeelden binnen het Dell portfolio van oplossingen die kunnen helpen bij kwaadaardige bedreigingen van binnenuit.

Kracht door partnerschappen

De gezamenlijke aanpak van Dell breidt de bescherming uit tot meer dan alleen Dell technologie. Door middel van partnerschappen met toonaangevende cyberbeveiligingsbedrijven zoals CrowdStrike en Secureworks, biedt Dell een ecosysteem van geïntegreerde oplossingen die elke mogelijke aanvalsvector aanpakken. Samen bieden deze oplossingen end-to-end beveiligingsdekking, zodat bedrijven meerlaagse bescherming kunnen creëren die is afgestemd op hun unieke risicoprofielen.

Waarom kiezen voor Dell?

Dell Technologies is meer dan een technologieleverancier: het is een vertrouwde partner in de strijd tegen ransomware. Door innovatie, expertise en een streven naar meer mogelijkheden voor bedrijven te combineren, voorziet Dell organisaties van de tools en het vertrouwen dat nodig is om veranderende bedreigingen het hoofd te bieden. Of het nu gaat om het beveiligen van eindpunten, het beschermen van kritieke data of het mogelijk maken van snel herstel, de producten en services van Dell zorgen voor operationele continuïteit en gemoedsrust.

Een veerkrachtige toekomst bouwen

Ransomware-aanvallen blijven evolueren, maar met Dell Technologies kunnen bedrijven een stap voor blijven. Door gebruik te maken van geavanceerde hardware, software en services, kunnen organisaties een cyberbeveiligingsframework bouwen dat veerkrachtig, aanpasbaar en betrouwbaar is. Bescherm uw data, bescherm uw activiteiten en maak uw bedrijf vandaag nog toekomstbestendig met de uitgebreide oplossingen van Dell tegen ransomware.

Om de veerkracht van uw bedrijf te garanderen, is het van cruciaal belang om inzicht te krijgen in het huidige bedreigingslandschap en op de hoogte te blijven van opkomende bedreigingen. De cyberbeveiligingsexperts van Dell Technologies controleren voortdurend op nieuwe aanvalsvectoren (wat bedoelen we hiermee?) en werken aan het proactief aanpakken van potentiële kwetsbaarheden in onze producten en services. Hierdoor kunnen we u de meest actuele bescherming bieden tegen steeds veranderende ransomware-bedreigingen.

Bedrijven moeten niet alleen op de hoogte blijven, maar ook een meerlaagse beveiligingsaanpak starten. Dit betekent het implementeren van een reeks beveiligingsmaatregelen, zoals firewalls, anti-malwaresoftware, inbraakdetectiesystemen en databack-ups. Door uw verdedigingsstrategieën te diversifiëren, kunt u de impact van één aanval minimaliseren en ervoor zorgen dat uw bedrijf operationeel blijft, zelfs bij een succesvolle ransomware-poging.

Het is ook belangrijk om uw beveiligingsmaatregelen regelmatig te testen en bij te werken (zowel uw systemen patchen als uw beleid bijwerken). Hackers vinden voortdurend nieuwe manieren om traditionele beveiligingsmaatregelen te omzeilen, dus het is cruciaal dat bedrijven de concurrentie voor blijven door hun verdediging regelmatig te testen en indien nodig bij te werken. Dit omvat het uitvoeren van regelmatige kwetsbaarheidsbeoordelingen, penetratietests en patchbeheer.

Een ander belangrijk aspect bij de bescherming van uw bedrijf tegen ransomware is het informeren van uw werknemers over best practices voor cyberbeveiliging. Veel ransomware-aanvallen worden gestart via social engineering-tactieken, zoals phishing-e-mails of schadelijke koppelingen. Door uw werknemers te informeren over hoe u deze bedreigingen kunt herkennen en voorkomen, kunt u de kans op een succesvolle aanval aanzienlijk verkleinen.

Bovendien kan een herstelplan na noodgeval de impact van een ransomware-aanval aanzienlijk beperken. Dit plan moet regelmatige back-ups van belangrijke data en systemen omvatten, evenals een duidelijke procedure voor het reageren op een aanval en herstel.

Naast deze proactieve maatregelen is het ook belangrijk om een goed incidentresponsplan te hebben. Dit omvat duidelijk gedefinieerde rollen en verantwoordelijkheden voor het omgaan met een ransomware-aanval, evenals communicatieprotocollen voor het melden van belanghebbenden en het beperken van schade.

Tot slot kunt u door op de hoogte te blijven van de nieuwste trends en ontwikkelingen op het gebied van ransomware-aanvallen, potentiële bedreigingen een stap voor blijven. Door regelmatig rapporten en updates van beveiligingsexperts te bekijken, kunt u proactief nieuwe beveiligingsmaatregelen implementeren om uw bedrijf te beschermen.

Onthoud dat geen enkel bedrijf immuun is voor ransomware-aanvallen, maar met de juiste strategieën en tools kunt u het risico en de impact van dergelijke aanvallen minimaliseren. Door een proactieve aanpak van cyberbeveiliging te hanteren, beschermt u niet alleen uw bedrijf, maar bouwt u ook vertrouwen op bij uw klanten en belanghebbenden.

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

Meer informatie over oplossingen van Dell

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies