Beveiliging en de rol ervan in digitale transformatie

Versterk en bescherm uw IT-infrastructuur
met Dell Technologies

DELL Technologies

intel

Inhoudsopgave

1

Samenvatting

Beveiliging is een belangrijke drijfveren voor kleine bedrijven die een digitale transformatiestrategie implementeren. Naarmate ondernemers, start-ups en kleine organisaties hun bedrijf laten groeien, groeit ook het risico dat zij lopen op een beveiligingsaanval of gegevensinbreuk.

De snelheid waarmee cyberaanvallen plaatsvinden neemt toe, waardoor bedrijven en hun beveiligingsteams voor de uitdaging staan om gelijke tred te houden met een steeds groeiende lijst van bedreigingen.

Er zijn vele soorten bedreigingen voor de digitale infrastructuur die verwoestend kunnen zijn voor de activiteiten en de reputatie van een klein bedrijf. Met een gemiddelde kostprijs van 13 miljoen dollars moeten kleine bedrijven alle mogelijke maatregelen nemen om een cyberaanval te voorkomen.

Gegevens vormen de kern van digitale transformatie en zelfs kleine bedrijven verwerken een grote hoeveelheid persoonlijke en zakelijke gegevens. Indien die in de handen komen van de verkeerde personen kan de schade aanzienlijk zijn.

Er zijn stappen die organisaties kunnen nemen om zich te beschermen tegen bedreigingen. Dell Technologies biedt ondernemers, starters en kleine bedrijven de ondersteuning die nodig is om hun digitale infrastructuur veilig uit te breiden.

2

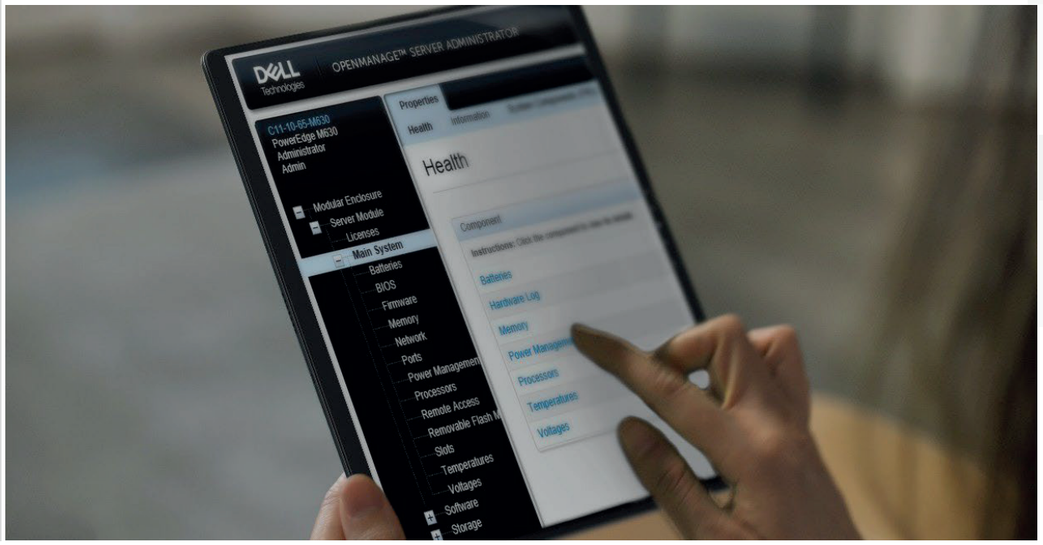
Inleiding

Digitale transformatie is geen nieuwe trend, maar is de afgelopen jaren wel vooruitgestuwd waarbij de Covid pandemie als aanjager heeft gefunctioneerd. Naarmate bedrijven hun technologie en digitale strategieën blijven ontwikkelen, is het van groot belang om de beveiliging bovenaan de agenda te houden.

Naarmate kleine bedrijven hun IT-netwerk uitbreiden, neemt hun kwetsbaarheid voor een inbreuk op de beveiliging toe. Van gegevensbescherming tot integriteit van de toeleveringsketen en ransomware-aanvallen, beveiliging moet centraal staan bij digitale transformatie om ervoor te zorgen dat een bedrijf kan blijven navigeren en reageren op bedreigingen en zijn gegevens kan beschermen.

Een belangrijk element van digitale transformatie is een meer datagedreven organisatie te worden. Dit houdt in dat gegevens uit het hele bedrijf worden gecentraliseerd, waarbij zelfs de kleinste bedrijven vertrouwen op bedrijfs-, werknemers- en klantgegevens om nieuwe inzichten te verkrijgen.

Dit soort gegevens zijn zeer waardevol, wat betekent dat naarmate bedrijven meer gegevens verzamelen, verplaatsen, verbinden en opslaan, zij op hun beurt kwetsbaarder worden voor aanvallen van hackers.



Bovendien heeft de pandemie geleid tot de behoefte aan hybride werkomgevingen, en hoewel deze flexibiliteit enorm gunstig is voor werknemers, creëert ze een beveiligingsuitdaging. IT-beveiligingsteams moeten nu enorme infrastructuren beheren met pc's die vanaf meerdere en mogelijk wereldwijde locaties verbinding maken. Dit versterkt de noodzaak voor elke werknemer om zijn persoonlijke verantwoordelijkheid te nemen en correcte cyberbeveiligingsrichtlijnen te volgen.

Cyberaanvallen nemen toe; gemiddeld vindt er elke 11 seconden één plaats[1]. Met een gemiddelde kostprijs van 13 miljoen dollar[2] bedreigt een aanval niet alleen de reputatie van een bedrijf, maar ook zijn vermogen om zijn activiteiten voort te zetten. Kleine bedrijven kunnen het zich niet veroorloven deze risico's te nemen als het gaat om de beveiliging van hun IT-netwerk.

Met de evolutie van Kunstmatige Intelligentie en Machine Learning worden aanvallen steeds geraffineerder. Desondanks beschikken veel organisaties niet over strenge maatregelen om met deze risico's om te gaan. Dit geldt met name voor ondernemers, kleinere bedrijven en start-ups, omdat zij vaak niet over de middelen beschikken om met risico's om te gaan, waardoor zij kwetsbaarder zijn voor een inbreuk op de beveiliging.

Naarmate de aanvallen complexer worden, wordt cyberbeveiliging niet langer uitsluitend als een IT-kwestie beschouwd, maar eerder als een bedrijfsrisico. Een bedrijf is slechts zo sterk als zijn IT-infrastructuur, wat betekent dat het zijn bedrijfsstrategie moet afstemmen op IT-beveiliging.

Medewerkers spelen een belangrijke rol bij het handhaven van de veiligheid van hun systemen en moeten de risico's die het bedrijf kan lopen volledig begrijpen. Gartner voorspelt dat het steeds gebruikelijker zal worden dat werknemers op leidinggevend niveau in hun arbeidscontracten verantwoordelijkheid krijgen voor de behandeling van cyberbeveiligingsrisico's en dat eventuele risicobetalingen (bijvoorbeeld bonussen) worden gekoppeld aan hun vermogen om de risico's tot een aanvaardbaar niveau te beperken[3].

AI en ML
hebben cyberaanvallen geavanceerder gemaakt

Hoe vaak
een cyberaanval plaatsvindt
11 seconden

De gemiddelde
kosten van een aanval
13 miljoen dollar

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[2] https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
[3] Gartner. (2022). Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem.

3

Soorten veiligheidsbedreigingen

- Beveiligingsbedreigingen voor IT-infrastructuur komen in verschillende vormen voor. Aanvallen kunnen worden geclassificeerd als passief of actief en kunnen zowel besturingssystemen als hardware treffen.

- Passieve bedreigingen zijn aanvallen waarbij de systemen van een bedrijf niet rechtstreeks worden beschadigd, maar waarbij informatie wordt verkregen die gevoelige gegevens kan zijn. Een voorbeeld hiervan is afluisteren.

Actieve aanvallen omvatten een brede waaier van verschillende technieken die de systemen van een organisatie beschadigen of wijzigen, de werking ervan beïnvloeden en een bedreiging vormen voor zowel de organisatie als individuele personen. Dergelijke aanvallen omvatten virussen, malware of ransomware.

Veel voorkomende veiligheidsbedreigingen zijn onder meer:

Phishing

Een veel voorkomende, maar effectieve vorm van aanval die meestal via e-mail wordt uitgevoerd en bedoeld is om de inloggegevens van gebruikers te stelen en hen ertoe te verleiden schadelijke software op hun apparaat te installeren. Phishing-aanvallen zijn effectiever en geraffineerder geworden omdat de referenties van de aanvallers vaak legitiem lijken.

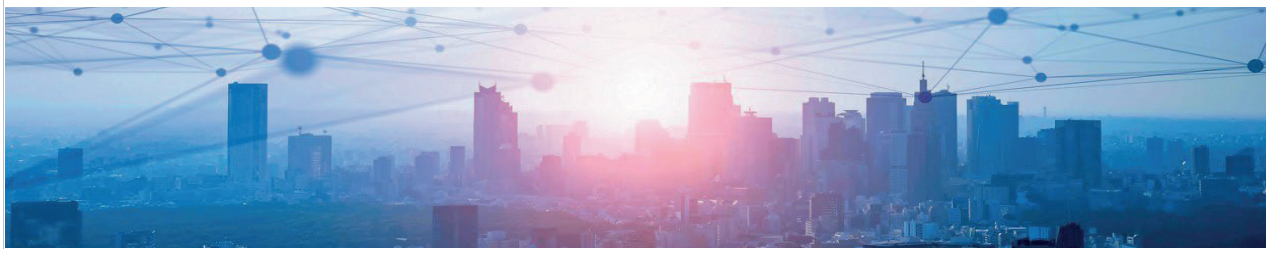
Malware

Alle kwaadaardige software die bedoeld is om een computer, server of computernetwerk te beschadigen of te verstoren om privégegevens te lekken, ongeoorloofde toegang te krijgen en de beveiliging en privacy te verstoren.

Denial of Service (DoS)

Een aanval uitgevoerd door bots die zijn ontworpen om een systeem van een organisatie te overspoelen met valse verzoeken, waardoor legitieme verzoeken worden geblokkeerd. Dit type aanval tast niet alleen de middelen van een systeem aan, maar kan ook de infrastructuur beschadigen.

Cyberaanvallen kunnen zowel besturingssystemen als hardware aantasten, wat een uitdaging vormt voor kleine bedrijven die hun infrastructuur met beperkte middelen willen versterken.



4

Uitdagingen

Aangezien digitale transformatie nieuwe en steeds evoluerende technologie introduceert in de IT-infrastructuur van kleine bedrijven, is het onvermijdelijk dat het potentiële aanvalsoppervlak van een organisatie groeit.

Terwijl ze proberen te navigeren door een breed scala aan potentiële bedreigingen, kunnen kleine bedrijven moeite hebben om de juiste middelen te verdelen om ervoor te zorgen dat ze veilig blijven, waardoor ze kwetsbaar zijn voor verschillende beveiligingsuitdagingen zoals:

Veilige back-up en herstel van gegevens

Bedrijven moeten ervoor zorgen dat ze over adequate systemen beschikken om veilig een back-up te maken en hun gegevens te herstellen, mochten deze beschadigd raken. Met name gegevensgestuurde bedrijven moeten hun informatie beschermen tegen geavanceerde ransomware-aanvallen. Aangezien kleine bedrijven steeds vaker multi-cloud en on-premise opslag van gegevens in hun IT-infrastructuur opnemen, is cyberweerbaarheid essentieel om de bedrijfscontinuïteit te waarborgen in geval van gegevensverlies.

Detectie en reactie op bedreigingen en kwetsbaarheden

Naarmate kleine bedrijven groeien en meer apparaten aan hun netwerk toevoegen, groeien ook de mogelijkheden van een inbreuk, zowel boven als onder het besturingssysteem. Bedreigingen zijn er in verschillende vormen met als doel het verkrijgen, wijzigen, vernietigen of verwijderen van informatie zonder geautoriseerde toegang. Kleine bedrijven kunnen moeite hebben om efficiënte systemen te implementeren die deze bedreigingen tijdig kunnen identificeren.

Integriteit van de toeleveringsketen

Bedrijven vertrouwen op geavanceerde technologie om connectiviteit en geavanceerde logistieke netwerken te ondersteunen. Deze technologie is echter ook kwetsbaar voor aanvallen, waardoor de integriteit van de supply chain-systemen in gevaar komt. Het is van vitaal belang de veiligheid van de ecosystemen van de toeleveringsketen te handhaven om operationele onderbrekingen, inkomstenverlies, in gevaar gebrachte gegevens, verminderde productiviteit en mogelijke schade aan merk en reputatie te voorkomen.

Toeleveringsketens van technologie kunnen ook worden geïnfiltreerd met nagemaakte apparaten waarmee is geknoeid. Bedrijven moeten ervoor zorgen dat apparaten en hun componenten veilig kunnen worden ingezet met behulp van veilige verificatie.

Beveiligingsactiviteiten 24/7 beheren

Cyberaanvallen kunnen op elk moment van de dag toeslaan, wat betekent dat bedrijven 24/7 op hun hoede moeten zijn. Kleine bedrijven hebben hier vaak moeite mee, omdat ze niet de middelen hebben om hun netwerken 24 uur per dag fysiek te bewaken. Aangezien bedreigingen steeds vaker voorkomen, is een efficiënt systeem voor bedreigingsdetectie nodig om bedreigingen te detecteren en aanvallen te stoppen voordat de schade is aangericht.

Beveiligingsuitdagingen voor kleine bedrijven

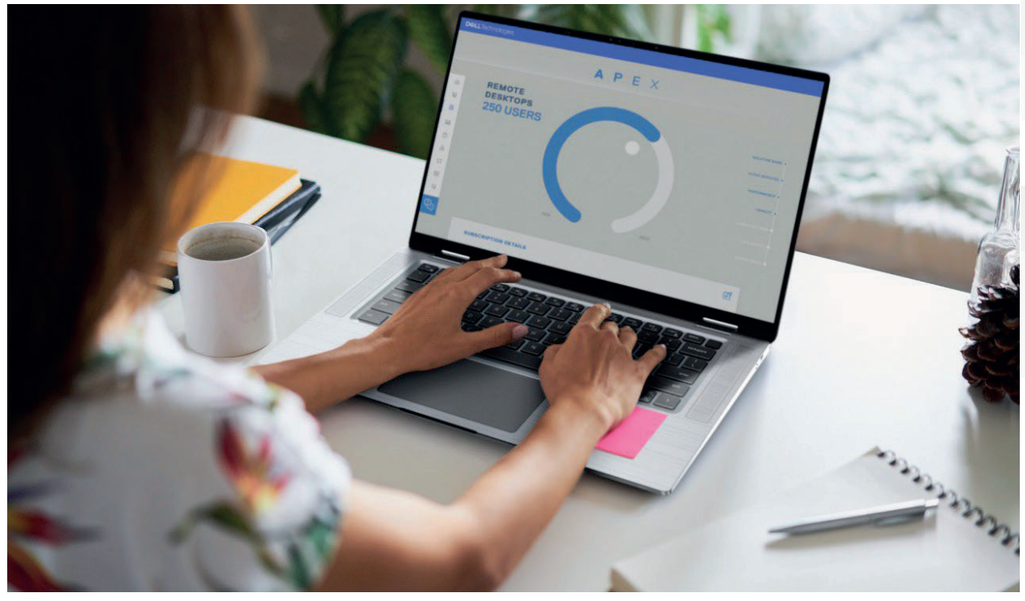
- Veilige back-up en herstel van gegevens
- Detectie en reactie op bedreigingen en kwetsbaarheden
- Integriteit van de toeleveringsketen
- 24/7 bewaking

5

Hoe u uw beveiligingspraktijken kunt verbeteren?

Inbreuken op de beveiliging kunnen een ravage aanrichten bij kleine bedrijven en onherstelbare schade veroorzaken. Het is noodzakelijk om een offensieve aanpak te hanteren door maatregelen en technologie in te voeren die beveiligingsrisico's voor hun infrastructuur en organisatie kunnen beperken.

Het kan ontmoedigend lijken om u voor te bereiden op een mogelijke inbreuk, maar er zijn veel stappen die u kunt nemen om uw beveiligingsmaatregelen binnen uw organisatie te verbeteren, zoals:



Maak een back-up van uw gegevens in de cloud

Kiezen voor de cloud om een back-up van uw gegevens te maken vereenvoudigt het proces en elimineert het risico van verlies van toegang tot belangrijke gegevens in het geval van een hardwarestoring of corruptie. Harde schijven en andere fysieke apparaten op locatie zijn gevoeliger voor diefstal of beschadiging. Zowel de publieke als de private cloud bieden firewallbescherming, waardoor beide opties een veilige keuze zijn voor gegevensopslag.

Implementeer toegangscontroles

Beleid voor toegangscontrole beperkt de toegang tot de kritieke bedrijfsmiddelen. Vermijd het delen van gebruikers-ID's voor toegang tot systemen en gegevens. Het gebruik van unieke ID's en aanmeldingsgegevens maakt het gemakkelijker om na te gaan wie toegang heeft tot uw bronnen. De implementatie van geautomatiseerde systemen voor Identity Access Management (IAM) helpt bij het stroomlijnen van deze taak, terwijl ook een groot deel van het risico wordt weggenomen.

Gebruikersauthenticatie

Multi-factor authenticatie creëert een gelaagd beveiligingssysteem waarbij uw werknemers naast hun wachtwoord een willekeurig gegenereerde, via SMS of e-mail verzonden code moeten gebruiken om hun identiteit te verifiëren. Dit type beveiligingssysteem beschermt uw gegevens omdat het voorkomt dat onbevoegde gebruikers van derden toegang krijgen tot bedrijfssystemen en websites.

Implementeer een Managed Detection and Response (MDR)-dienst

Kleine bedrijven en hun IT-beveiligingsteams kunnen moeite hebben om de groeiende hoeveelheid technologie en bedreigingen bij te houden. Een MDR is een cyberbeveiligingsdienst die geavanceerde technologie combineert met menselijke expertise om de impact van cyberbedreigingen snel te identificeren en te beperken zonder dat er extra personeel moet worden aangenomen.

6

Hoe kan Dell Technologies uw kleine onderneming helpen met beveiliging?

Cyberaanvallen kunnen op elk moment plaatsvinden, maar Dell Technologies is er om ervoor te zorgen dat uw bedrijf optimaal is voorbereid op mogelijke incidenten en uw organisatie beschermt terwijl deze groeit.

Door samen te werken met Dell kunt u er zeker van zijn dat uw IT-infrastructuur en gegevens veilig zijn. Wij zetten ons in om technologie van de hoogste kwaliteit te leveren om aanvallen te verijdelen en bieden uitgebreide detectie en reactie op bedreigingen, gegevensbescherming en cyberherstel.

Versterk uw cyberbeveiligingstools met Dell Technologies, krijg controle en versnel digitale innovatie met een gerust hart.

Van recovery-diensten, cyberbescherming en endpointbeveiliging, de adviseurs van Dell Technologies begeleiden u bij elke stap om u te adviseren over het beste systeem voor de beveiligingsbehoeften van uw bedrijf.

Praat vandaag nog met een Dell Technologies Advisor en ontdek hoe u uw IT-beveiligingsstrategie kunt versterken en uw bedrijf veilig kunt houden terwijl u groeit.

Bouw cyberweerbaarheid op met Dell Technologies

- Bescherm uw gegevens
- Beveilig endpoints
- Valideer hardware
- Detecteer en reageer op bedreigingen

Beveiliging en de rol ervan in digitale transformatie

DELL Technologies

intel