Beheerde eindpuntdetectie en -respons

De beste manier om moderne beveiligingsbedreigingen te beheren

Vroeger was beveiliging zo lekker eenvoudig. U installeerde een antivirusprogramma, trainde uw medewerkers om niet op onbekende koppelingen te klikken en zorgde ervoor dat uw software en websites up-to-date bleven.

Jarenlang waren antivirusprogramma's inderdaad afdoende om het MKB te beveiligen, maar bedreigingspatronen veranderen en het MKB heeft nu een nieuwe manier van beveiligen nodig om deze steeds uitgekiendere en heftigere aanvallen te kunnen bestrijden.
Antivirusprogramma's zijn afhankelijk van handtekeningen om bedreigingen te detecteren, maar de nieuwste bedreigingen gebruiken helemaal geen handtekeningen meer en kunnen dus ongezien de netwerken van uw bedrijf binnendringen.

Hier volgen een aantal voorbeelden van de risico's die we op dit moment tegenkomen op de markt:

- Bewapende documenten die eruitzien als onschuldige PDF-bijlagen in uw e-mailberichten, maar zodra ze in uw netwerk terechtkomen, aanvallen uitvoeren.
- Bestandloze bedreigingen die niet hoeven te worden gedownload maar die vanuit het geheugen worden uitgevoerd, waardoor ze maar moeilijk kunnen worden herkend.
- Zogeheten 'zero-day'-aanvallen die naar onbekende beveiligingsproblemen op de computer zoeken en deze exploiteren voordat software- of hardwareproviders updates kunnen uitgeven.
- En aanvallen met ransomware, waardoor IT-netwerken kunnen worden lamgelegd doordat cybercriminelen enorm veel losgeld eisen om gegevens en services te herstellen, zijn ook nog steeds aan de orde van de dag.

82% van het MKB zegt dat ze weleens te maken hebben gehad met een cyberaanval die niet door hun antivirussystemen is opgepikt.

Bron: Ponemon, 2018.

"De ransomware-aanval was echt de laatste druppel. Het duurde dagen voordat onze systemen weer waren hersteld. We hebben ons beveiligingssysteem nu geüpgraded met beheerde eindpuntdetectie en -respons, zodat ons bedrijf nu is beschermd tegen dit soort bedreigingen".

Bescherm uw bedrijf tegen de nieuwste bedreigingen

Uiteraard wilt u uw bedrijf, medewerkers en alle apparaten beschermen tegen cyberaanvallen. En we weten allemaal dat mobiele apparaten vaak de zwakste schakel in de IT-beveiliging zijn, omdat medewerkers onderweg minder voorzichtig zijn dan op kantoor. Lees hier waarom beheerde eindpuntdetectie en -respons (EDR) op dit moment de beste keuze is voor uw IT-beveiliging en bedrijfscontinuïteit.

Beheerde eindpuntdetectie en -respons	Antivirusoplossingen
Bevrijd u van ransomware en zet apparaten terug naar een tijdstip voordat de infectie plaatsvond.	Kan apparaten niet terugzetten naar een tijdstip vóór de infectie, waardoor u meer risico op ransomware loopt.
Gebruikt kunstmatige intelligentie (AI) om zowel huidige als opkomende bedreigingen te detecteren en te voorkomen, met continue updates voor het platform.	Gebruikt handtekeningen om bedreigingen te identificeren, waardoor ze niet in staat zijn om de nieuwste strategieën van cybercriminelen te detecteren.
Bewaakt processen voor, tijdens en na de uitvoering om te voorkomen dat nieuwe bedreigingen het netwerk infiltreren.	Heeft geen zicht op de situatie wanneer deze wordt uitgevoerd, waardoor nieuwe bedreigingen van slimme criminelen een ingangspunt hebben.
Bewaakt uw systemen in real time.	Is afhankelijk van dagelijkse of wekelijkse scans, waardoor u meer risico loopt.
Zorgt ervoor dat de apparaatprestaties hoog blijven en continu worden bewaakt.	Kan de prestaties van uw apparaat verlagen door lange scanbewerkingen.

Nooit meer zorgen om ransomware met beheerde EDR. Binnen één klik uw apparaten herstellen naar een tijdstip vóór de infectie.

Zo profiteert u van beheerde EDR

- **Bescherm uw bedrijf tegen ransomware-aanvallen –** Laat beheerde EDR al uw apparaten terugzetten naar een tijdstip vóór de bedreiging voor echte gemoedsrust. Herstel geïnfecteerde apparaten met één druk op de knop naar volledige productiviteit, door welke ransomware ze ook worden gegijzeld. U hoeft cybercriminelen geen enorme losgeldbedragen te betalen of dure consultants in te huren om toegang tot het netwerk te herstellen. Beheerde EDR betaalt zichzelf uit omdat het u veilig houdt.
- **Verhoog de productiviteit van medewerkers –** Verwijder bedreigingen die traditionele antivirusprogramma's omzeilen en behoud snellere apparaatprestaties, waardoor er minder afleidingen ontstaan die de productiviteit van uw medewerkers verminderen.
- **Laat beheer doen door de experts –** Besteed uw kostbare tijd niet aan het zelf ondersteunen en beheren van uw systemen en beveiliging. Richt u op het uitvoeren en uitbreiden van uw bedrijf, met de doorlopende ondersteuning van uw Managed Service Provider.

Wilt u meer informatie?

Focusonbusiness

www.focuz.be

info@focuz.be

014 58 04 61