

Praktijkcase - Microsoft Defender

De manager van een bedrijf van 50 werknemers, ziet de jaarlijkse factuur voor de derde partij licentiesoftware van bijna € 3.000,00. Hij vraagt jou als beheerder of deze extra software nog wel nodig is, en zo ja, of er een goed en goedkoper alternatief is. Hij vraagt je expliciet ook te kijken naar Microsoft Defender in Windows 10 en 11. Omdat de strategie binnen het bedrijf nu richting Microsoft 365 gaat, is de antivirussoftware immers “gratis”.

Opdracht 1 Aanvallen van hackers

Diverse fabrikanten van anti-malware hebben een live overzicht van aanvallen. Dat geeft een aardig beeld van de problematiek in de wereld.

Zoek eens een dergelijke site en toon aan dat het in de wereld wemelt van de virussen en aanvallen.

Opdracht 2 De markt

- Onderzoek welke anti-virusproducten er zijn en welke veel gebruikt worden. Maak in een tabel een globale vergelijking met vijf van de belangrijkste componenten, tussen twee van die producten.
- Hebben de producten een centrale beheermogelijkheid?
- Wat kost een anti-virusproduct voor een bedrijf van 50 medewerkers?
- Wat zeggen de twee fabrikanten van die producten over Microsoft Defender?
- Hoe positioneren ze hun product?

Opdracht 3 Defender op je pc

- Controleer eens of op je eigen pc of een pc van de school Microsoft Defender AntiVirus is ingeschakeld.
- Is er op de pc tevens een ander antivirusproduct geïnstalleerd?
- Is het slim twee anti-malware producten tegelijkertijd/parallel te gebruiken, kan dit wel?
- Onderzoek de opties van Defender Antivirus op een pc, en maak een overzichtje.
- Wat is bijvoorbeeld Security Intelligence?

Opdracht 4 Terminologie

- Wat kun je instellen bij Defender Exploit Protection in Windows 10?
- Wat zijn de mogelijkheden van Defender SmartScreen?
- Wat is Defender Application Guard?
- Wat is Dynamische vergrendeling op Windows 10/Windows 11?
- Waarvoor gebruikt Windows de Trusted Platform Module (TPM)?
- Wat zijn de mogelijkheden van Windows Hello?

Opdracht 5 Netwerk

- Als Defender op alle pc's ingeschakeld is, heb je dan voldoende bescherming op een bedrijfsnetwerk?
- Heeft Microsoft ook een Defender-product voor macOS, iOS, Android of Linux?
- Er bestaat ook een Windows Defender op Windows server. Wat zijn de verschillen met de client versie?

Opdracht 6 Microsoft 365

- a. Onderzoek welke componenten of producten Microsoft onder de naam Defender aanbiedt, en probeer een overzicht te maken welke componenten in welke licenties inbegrepen zijn.
- b. Wat is Microsoft Defender for Endpoint, welke versies zijn er en welke mogelijkheden zijn erbij inbegrepen?
- c. Wat is Defender voor Office 365? Wat is Defender for Identity?

Opdracht 7 Je advies

Microsoft 365 Defender is dé beveiligings-suite van Microsoft. De mogelijkheden zijn zo uitgebreid, dat je hier met gemak een apart dik boek aan zou kunnen wijden. Lang niet alle Defender onderdelen zijn “gratis” maar maken deel uit van betaalde licenties.

Wat wordt je advies aan de manager?