WHITEPAPER

In één klap 5 keer veiliger werken

Beveilig al jouw digitale werkplekken en devices

Slaat een cybercrimineel toe, dan staat je zaak stil. Dat mag jou natuurlijk niet overkomen, maar heb je cybersecurity wel goed geregeld? Is dit goed ingesteld voor alle werkplekken en alle mobiele apparaten? Dat is in het mkb meestal niet het geval. Het is daarom de hoogste tijd om je security te verbeteren, voor ál je werkplekken.

Hoe is de cybersecurity bij jouw bedrijf geregeld? Waarschijnlijk draait er een antiviruspakket op de computers van je medewerkers. Dat is niet meer voldoende. Onderzoek wijst uit dat bij kleine en middelgrote bedrijven dataveiligheid nog altijd onder de maat is. Dit is gevaarlijk omdat mkb-bedrijven juist nu vaker het doelwit zijn van cybercriminelen. Bij veel ondernemers is het niet de vraag of, maar wanneer ze gehackt worden.

Daarom hebben veel ondernemers ook een extra beveiliging bovenop de basisbescherming. Dit is al een stuk veiliger, maar kost op maandbasis een redelijke duit. En zijn hiermee ook alle laptops, telefoons en tablets beschermd? Het is de hoogste tijd voor echt goede security, daarmee houd je jouw bedrijf altijd in beweging. Maar wat moet je doen? Allereerst is Microsoft Defender een veilige keuze. Het hoort standaard bij Windows 10 en is beschikbaar voor alle andere computers, maar ook smartphones. Maar het kan en moet nóg beter. 5 keer beter om precies te zijn.

1. Al je computers en smartphones wél goed beveiligd

We werkten al steeds vaker buiten de kantoormuren, maar vanwege de COVID-19 uitbraak is thuiswerken gemeengoed. Waarschijnlijk werken ook veel collega's met een eigen laptop of smartphone. Maar zijn die apparaten wel goed beveiligd? Je wil zorgeloos kunnen werken en vertrouwen op een systeem dat geavanceerde bedreigingen detecteert, onderzoekt en uitschakelt.
Het liefst zou je één systeem hebben wat een oogje in het zeil houdt op alle computers, laptops, smartphones en tablets. Met de upgrade **Microsoft Defender for Endpoint** (voorheen Microsoft Defender ATP) krijg je centraal grip op alle apparaten waarmee je collega's werken, ook op Apple- en Android-apparaten. Met een upgrade naar **Microsoft Defender for Endpoint** neem je afscheid van losse virusscanners die bovendien niet meer afdoende zijn en bescherm je alle werkplekken van je bedrijf tegen virussen, spyware en andere schadelijke software.

2. Blokkeer phishingmail

Van alle soorten cybercrime is phishing de grootste plaag. Je kent ze wel, uitnodigende mails van bijvoorbeeld banken of andere bedrijven met een link richting een valse inlogpagina. Probeer je hier in te loggen, dan hebben de criminelen beet en gijzelen ze bijvoorbeeld je computer of zelfs je hele

netwerk. Jij checkt natuurlijk altijd de echtheid van mails voordat je op een link klikt... Het probleem is dat iedereen wel eens een foutje maakt, en dan kunnen de gevolgen desastreus zijn omdat je gewoonweg niet meer kunt werken.

Je kunt dit voorkomen met een systeem dat alle verbindingen checkt. Klik je op een link die je naar een gevaarlijke site stuurt, dan checkt **Microsoft Defender for Endpoint** of de link waarnaar je gaat wel te vertrouwen is. Blijkt dat niet het geval te zijn, dan krijg je een melding dat de site gevaarlijk is. Via deze netwerkbeveiliging monitort het systeem al je verkeer. Microsoft put hierbij onder andere uit al het e-mailverkeer wat via Outlook wordt verstuurd.

3. Bescherm je kroonjuwelen

Is er wel eens bij je ingebroken? Inbrekers in de fysieke wereld gaan zo snel mogelijk met de buit ervandoor, cybercriminelen gaan vaak heel anders te werk. Neem bijvoorbeeld de digitale inbraak bij de Universiteit van Maastricht. Eenmaal binnen via een gewiekste phishingmail, hielden ze zich ruim twee maanden stil. Ze namen ruim de tijd om rond te snuffelen en maakten ondertussen op de achtergrond onder andere de back-ups ontoegankelijk. Hierna sloegen de hackers toe en versleutelden ze alle belangrijke bestanden. De universiteit kon niet terugvallen op back-ups en ging akkoord met € 200.000 losgeld.

Had de Universiteit van Maastricht een controle op toegang tot de documenten gehad, dan waren de bestanden helemaal niet versleuteld. **Microsoft Defender for Endpoint** checkt altijd de toegang tot je belangrijkste gegevens. Zo zet je een slot op belangrijke mappen op je SharePoint, maar ook op alle computers, smartphones en tablets.

4. Zoek de zwakste schakel

Waar zit in jouw cybersecurity de zwakste schakel? Is het de server? De smartphone van Klaas of is de configuratie van de pc van Marlies niet helemaal goed? Of heeft John zijn virusscanner uitgezet? Het probleem is duidelijk: je weet niet of alle werkplekken geen zwakke plekken vertonen. Vertelt je basis virusscanner dat? En je premiumversie die je deze extra zekerheid belooft te geven?

Het zou mooi zijn als een team van knappe koppen en AI continu alle instellingen en statussen van alle computers van je medewerkers in de gaten houden. **Microsoft Defender for Endpoint** checkt het voor je en geeft bovendien aan wat je moet doen. Zo zet je bijvoorbeeld op afstand Johns virusscanner weer aan, of zie je dat de pc van Marlies een update nodig heeft.

5. Stop met allerlei virusscanners

De kans is groot dat je al een virusscanner hebt, of zelfs meerdere: elk apparaat heeft zijn eigen beveiliging. Het is vanuit kosten- en veiligheidsoverwegingen handig om één systeem te nemen. Een goede stap is om op alle werkplekken het gratis Microsoft Defender Antivirus te installeren. Maar daarmee ben je er nog niet. Met het geld dat je uitspaart voor deze virusscanners kun je een extra stap zetten en meteen alle werkplekken goed en centraal beveiligen. Upgrade daarom naar **Microsoft Defender for Endpoint**, daarmee verbind je alle veiligheidsmaatregelen en zet je de deur voor cybercriminelen pas echt op slot.

Besteed je security uit

Cybersecurity vraagt om specialistische IT-kennis. Dat is voor mkb'ers zelf niet altijd optimaal te regelen. Natuurlijk kun je met de upgrade naar **Microsoft Defender for Endpoint** zelf de security regelen en computers op afstand beheren. Maar misschien leidt dit je te veel af van het ondernemen zelf. Daarom kiezen steeds meer ondernemers ervoor om cybersecurity uit handen te geven. Hierdoor ben je ook buiten kantooruren optimaal beschermd doordat het netwerk continu in de gaten wordt gehouden. Je hoeft niet meer te denken aan back-ups, updates, beveiligingspatches, trainingen en regelmatige netwerktesten want onze specialisten nemen je dit werk uit handen. Zo kun jij je volledig focussen op de zaak en is jouw bedrijf optimaal beschermd tegen cybercrime.