Microsoft

Security in het MKB: Windows 10

De security uitdagingen en behoeften in het MKB

De security uitdagingen en behoeften in het MKB

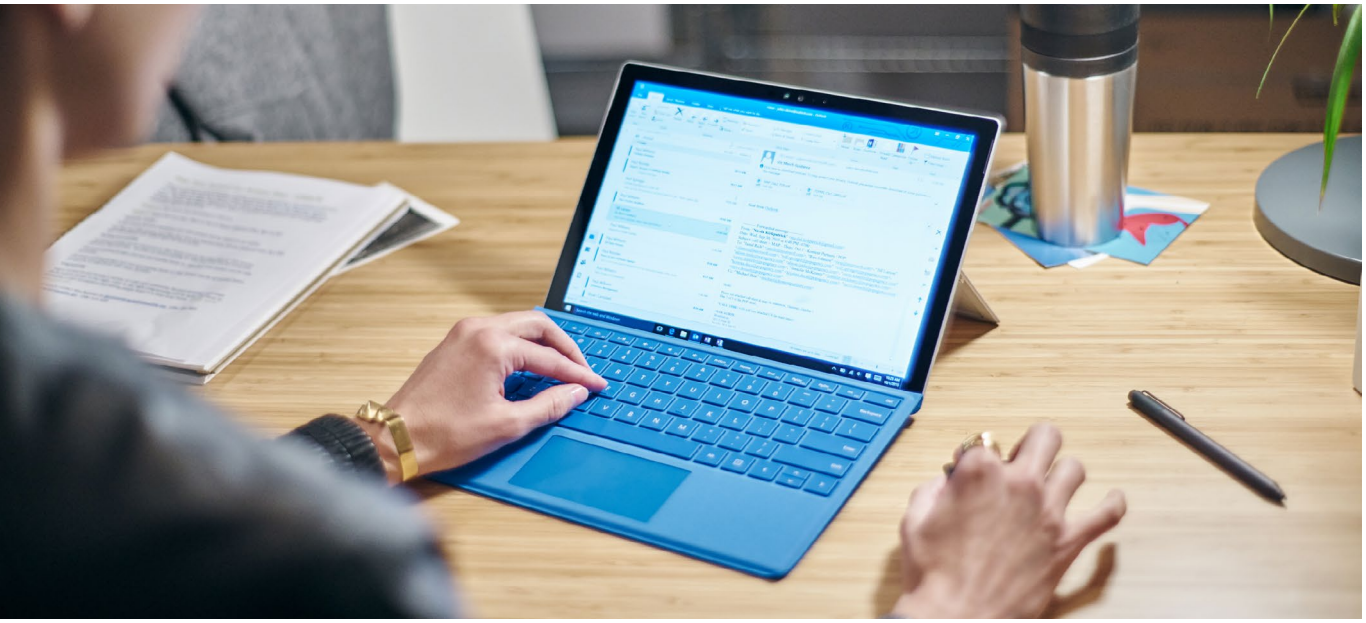
Bedrijven zijn zich inmiddels bewust van de noodzaak om hun bedrijfsgegevens veilig op te slaan en te verwerken. Ze kennen de risico's van diefstal of verlies van gegevens, maar zijn vaak nog niet op de hoogte van de mogelijkheden om de beveiliging in de eigen organisatie te verbeteren.

Hoe Windows 10 het MKB ondersteunt

Windows 10 Pro helpt je organisatie om overal veilig te kunnen werken en biedt de flexibiliteit om met je organisatie mee te groeien.

Door over te stappen naar Windows 10 Pro, bespaar je tijd en kosten. Windows 10 Pro ondersteunt je bij het beheren en beveiligen van systemen. Je beschikt met Windows 10 Pro over geavanceerde beveiligingsmogelijkheden om gegevens te beschermen. Je kunt de beveiliging eenvoudig voor meerdere gebruikers instellen en beheren, met beheeroplossingen zoals Microsoft Enterprise Mobility & Security.

Windows werkt op verschillende apparaten en integreert perfect met Office 365 en Enterprise Mobility Security (EMS), zodat jij en collega's altijd en overal productief kunnen zijn. In combinatie met een Windows 10-apparaat – die beschikbaar zijn in verschillende uitvoeringen – halen jij en je collega's het meeste uit de dag.



Windows 10 veiligheid

Windows is veilig vanuit de kern en beschikt over functies waarmee bedrijven veilig zaken kunnen doen. Met onder meer de volgende functies zijn je gebruikers, data en apparaten goed beschermd.

Windows Hello

Met Windows Hello kunnen gebruikers zich op basis van biometrische kenmerken (zoals vingerafdruk en iris) bij Windows en andere diensten aanmelden. Hierdoor is je apparaat en netwerk beter beveiligd dan alleen met een gebruikersnaam-wachtwoord combinatie.

BitLocker en BitLocker to Go

BitLocker en BitLocker to Go zorgen ervoor dat gegevens versleuteld worden opgeslagen en alleen beschikbaar zijn voor gebruikers die hiervoor de juiste rechten hebben.
Mocht je onverhoopt je apparaat verliezen dan weet je zeker dat niemand toegang zal krijgen tot jouw persoonlijke data.

Windows Information Protection

Windows Information Protection voorkomt dat gegevens in verkeerde handen terechtkomen. De technologie kan onderscheid maken tussen zakelijke en persoonlijke gegevens, en geeft een melding als een gebruiker per ongeluk zakelijke data dreigt te lekken, bijvoorbeeld bij het kopiëren van een zakelijk document naar een USB-stick.

Device Guard

Device Guard* beschermt uw apparaten tegen malware, niet-vertrouwde apps en programma's (o.a. .exe-bestanden). Trusted Boot en Secure Boot zorgen er samen voor dat de computer altijd beveiligd wordt opgestart en dat er alleen vertrouwde programma's tijdens het opstarten mogen worden geladen: een onmisbare beveiliging in deze tijd.

Credential Guard

Gestolen of illegaal bemachtigde gebruikersgegevens is een veel toegepaste vorm om in te breken op een pc en/of netwerk. Met credential guard voorkom en beperk je de impact een dergelijke identiteitsdiefstal. Credential guard beschermd tegen Pass the Hash-aanvallen, een tactiek die vaak wordt gebruikt bij beveiligingslekken. Het biedt aanvullende bescherming tegen malware in het besturingssysteem.

AppLocker management

AppLocker management beschermt tegen het uitvoeren van ongewenste en onbekende programma's in het netwerk, door alleen vertrouwde apps en websites op apparaten toe te staan. Het werkt samen met bestaande infrastructuur.

App-V

Vereenvoudig applicatiebeheer met App-Virtualisatie. Apps worden niet direct op het apparaat geïnstalleerd, waardoor er geen conflicten of compatibiliteitsproblemen ontstaan en alle apps actueel en beschermd blijven.

Managed User Experience

Verbeterde beveiliging door de gebruikerservaring op slot te zetten, bijvoorbeeld door kiosk mode voor apparaten in een publieke ruimte, zodat alleen specifieke taken mogelijk zijn.

Windows Defender

Windows Defender is een programma waarmee spyware, virussen en andere malware tegengehouden en verwijderd worden. Windows Defender draait op de achtergrond en geeft automatisch een notificatie op het moment dat er actie ondernomen moet worden. Ook kun je het op ieder moment gebruiken om je apparaat te scannen op malware als deze niet goed werkt of als je op een verdachte link hebt geklikt.

Er bestaan verschillende redenen om een nieuw apparaat te overwegen.

De afgelopen jaren is de wereld op het gebied van veiligheidsrisico's sterk veranderd. Dat stelt niet alleen eisen aan de software, maar ook aan apparaten. Bijvoorbeeld tijdens het opstartproces, dat steeds vaker wordt gebruikt om als eerste kwaadaardige programma's te starten en daarna pas het officiële operating system. Bedrijven die nieuwe Windows 10-apparaten aanschaffen krijgen daarmee de beschikking over hardwarematige beveiliging, waarover oudere apparaten niet beschikken, maar die inmiddels nodig is om de organisatie goed te beschermen.

Benieuwd hoeveel jij weet over beveiliging voor je bedrijf?

Doe nu de Digital Security Test

* Voor Windows Hello, Credential Guard en Device Guard heeft u hardware nodig dat deze functionaliteiten ondersteunt.