Is Microsoft 365 veilig voor MKB bedrijven?

https://aucuba.nl/kennisbank/uncategorized/is-microsoft-365-veilig-voor-mkb-bedrijven/

Microsoft 365 is over het algemeen veilig voor MKB-bedrijven, maar alleen als het platform goed is geconfigureerd en actief wordt beheerd. Microsoft biedt een robuuste beveiligingsinfrastructuur, maar de eindverantwoordelijkheid voor een veilige inrichting ligt grotendeels bij het bedrijf zelf. In dit artikel beantwoorden we de meest gestelde vragen over Microsoft 365-beveiliging voor het MKB.

Welke beveiligingsrisico's zijn er bij Microsoft 365?

De grootste beveiligingsrisico's bij Microsoft 365 zijn geen zwakheden in het platform zelf, maar ontstaan door onjuist gebruik, slechte configuratie en menselijk gedrag. Denk aan phishingaanvallen via e-mail, zwakke of hergebruikte wachtwoorden, onbeveiligde accounts zonder meervoudige verificatie, en het onbedoeld delen van gevoelige bestanden via SharePoint of OneDrive.

Concreet zijn dit de meest voorkomende risico's voor MKB-bedrijven:

- **Phishing en social engineering:** Aanvallers sturen nep-e-mails die lijken op officiële Microsoft-berichten om inloggegevens te stelen.
- **Gecompromitteerde accounts:** Als een medewerker zijn wachtwoord hergebruikt of op een phishinglink klikt, kan een aanvaller volledige toegang krijgen tot e-mail, bestanden en contacten.
- **Onbeveiligd extern delen:** Bestanden in SharePoint of OneDrive kunnen per ongeluk openbaar worden gemaakt als de instellingen niet correct zijn geconfigureerd.
- **Onbeheerde apparaten:** Medewerkers die Microsoft 365 gebruiken op privéapparaten zonder beveiligingsbeleid vormen een kwetsbaar toegangspunt.
- **Ransomware via e-mailbijlagen:** Kwaadaardige bestanden die via Outlook worden geopend, kunnen een heel netwerk infecteren.

Voor MKB-bedrijven is het risico extra relevant omdat er vaak geen dedicated IT-afdeling is die dreigingen actief monitort. Daardoor blijven aanvallen soms lang onopgemerkt.

Welke beveiligingsfuncties zitten standaard in Microsoft 365?

Microsoft 365 bevat standaard een aantal krachtige beveiligingsfuncties die direct beschikbaar zijn voor alle gebruikers. De meest essentiële zijn meervoudige verificatie (MFA), spamfiltering via Exchange Online Protection, versleuteling van data in transit en in rust, en basale toegangscontrole via Azure Active Directory.

Hieronder een overzicht van de ingebouwde beveiligingsfuncties:

- **Meervoudige verificatie (MFA):** Een extra verificatiestap bij het inloggen, die het risico op accountovername drastisch vermindert.
- **Exchange Online Protection (EOP):** Filtert spam, malware en phishingmails automatisch uit de inbox van medewerkers.
- **Versleuteling:** Alle data die via Microsoft 365 wordt verstuurd of opgeslagen, is versleuteld volgens industriestandaarden.
- **Beveiligde aanmelding via Azure AD:** Centraal identiteitsbeheer voor alle gebruikers en toegangsrechten.
- **Auditlogboeken:** Activiteiten van gebruikers worden bijgehouden, wat helpt bij het opsporen van verdacht gedrag.

Hoewel deze functies waardevol zijn, zijn ze lang niet altijd standaard ingeschakeld. MFA, bijvoorbeeld, moet actief worden geconfigureerd. Wie dit vergeet, laat een van de meest effectieve beveiligingslagen onbenut.

Wat is het verschil tussen Microsoft 365 Business Basic, Standard en Premium op het gebied van beveiliging?

Op het gebied van beveiliging zijn er duidelijke verschillen tussen de drie abonnementsvormen. Business Basic biedt basale bescherming, Standard voegt daar iets aan toe, maar het is Premium dat de meest uitgebreide beveiligingsfuncties biedt en daarmee het meest geschikt is voor MKB-bedrijven met hogere beveiligingseisen.

Microsoft 365 Business Basic en Standard

Business Basic bevat de kernfuncties zoals Exchange Online Protection, MFA en Azure AD. Business Standard voegt hier de volledige Office-applicaties aan toe, maar de extra

beveiligingsfuncties ten opzichte van Basic zijn beperkt. Beide abonnementen missen geavanceerde dreigingsbeveiliging en uitgebreid apparaatbeheer.

Microsoft 365 Business Premium

Business Premium is de meest complete keuze voor cloudbeveiliging in het MKB. Dit abonnement bevat onder andere Microsoft Defender for Business, waarmee endpoints actief worden bewaakt en bedreigingen automatisch worden geblokkeerd. Daarnaast biedt Premium Intune voor apparaatbeheer, Azure AD Premium voor voorwaardelijke toegang, en geavanceerde anti-phishingbeveiliging via Defender for Office 365. Voor MKB-bedrijven die serieus omgaan met Microsoft 365-veiligheid, is Premium de aanbevolen keuze.

Hoe stel je Microsoft 365 veilig in voor een MKB-bedrijf?

Een veilige inrichting van Microsoft 365 voor een MKB-bedrijf begint met het activeren van meervoudige verificatie voor alle gebruikers, gevolgd door het instellen van een sterk wachtwoordbeleid, het beperken van externe deelrechten en het configureren van beveiligingswaarschuwingen. Dit zijn geen optionele stappen, maar de minimale basis voor verantwoord gebruik.

Een praktische aanpak bestaat uit de volgende stappen:

1. **Activeer MFA voor alle accounts:** Zonder meervoudige verificatie is elk account kwetsbaar, ongeacht de wachtwoordsterkte.
2. **Stel een sterk wachtwoordbeleid in:** Verplicht complexe wachtwoorden en voorkom hergebruik.
3. **Beperk externe deelrechten:** Zorg dat medewerkers bestanden niet standaard openbaar kunnen delen via OneDrive of SharePoint.
4. **Configureer beveiligingswaarschuwingen:** Stel meldingen in bij verdachte aanmeldpogingen of ongewone activiteiten.
5. **Beheer apparaten centraal:** Gebruik Intune (beschikbaar in Premium) om te controleren welke apparaten toegang hebben tot bedrijfsdata.
6. **Train medewerkers:** Technische maatregelen zijn nutteloos als medewerkers niet weten hoe ze phishingmails herkennen.

Een goede basisinrichting kost tijd en technische kennis. Veel MKB-bedrijven laten dit over aan een externe IT-partner om zeker te zijn dat niets over het hoofd wordt gezien.

Wat zijn de verantwoordelijkheden van Microsoft versus die van het bedrijf zelf?

Microsoft en het bedrijf dat Microsoft 365 gebruikt, delen de verantwoordelijkheid voor beveiliging. Dit wordt het **gedeelde verantwoordelijkheidsmodel** genoemd. Microsoft is verantwoordelijk voor de beveiliging van de infrastructuur, datacenters en het platform zelf. Het bedrijf is verantwoordelijk voor de configuratie, de gebruikers, de apparaten en de data.

In de praktijk betekent dit:

- **Microsoft zorgt voor:** Fysieke beveiliging van datacenters, platformupdates, encryptie van de infrastructuur en beschikbaarheid van de dienst.
- **Het bedrijf is zelf verantwoordelijk voor:** Het activeren van beveiligingsfuncties, het beheer van gebruikersaccounts, het instellen van toegangsrechten, de beveiliging van endpoints en de naleving van privacywetgeving zoals de AVG.

Een veelgemaakte misvatting is dat Microsoft 365 veilig is zodra je het aanschaft. Dat klopt niet. Microsoft levert een veilig platform, maar de inrichting en het dagelijks beheer vallen volledig onder de verantwoordelijkheid van het bedrijf zelf. Wie dit negeert, neemt onnodig risico.

Heeft een MKB-bedrijf een externe IT-partner nodig voor veilig gebruik van Microsoft 365?

Een externe IT-partner is niet strikt verplicht, maar voor de meeste MKB-bedrijven zonder interne IT-afdeling is het sterk aan te raden. De configuratie van Microsoft 365-veiligheid is technisch complex, verandert regelmatig door updates en vereist actieve monitoring om dreigingen tijdig te signaleren.

Een IT-partner biedt toegevoegde waarde op drie vlakken:

- **Initiële inrichting:** Een correcte en volledige configuratie van alle beveiligingsinstellingen vanaf het begin, zodat er geen gaten in de beveiliging ontstaan.
- **Proactief beheer en monitoring:** Actief toezicht op verdachte activiteiten, updates en kwetsbaarheden, zodat problemen worden opgelost voordat ze schade veroorzaken.
- **Ondersteuning bij incidenten:** Snelle hulp als er toch iets misgaat, van een gecompromitteerd account tot een ransomware-aanval.

De kosten van een IT-partner wegen in de meeste gevallen ruimschoots op tegen de potentiële schade van een beveiligingsincident, zowel financieel als reputatieschade. Voor MKB-bedrijven die

zich willen concentreren op hun kernactiviteiten zonder ICT-zorgen, is volledige ontzorging door een betrouwbare partner de meest verstandige keuze. Wil je weten hoe wij jouw Microsoft 365-omgeving veilig kunnen inrichten en beheren? Neem dan contact met ons op voor een vrijblijvend gesprek.