BITSPRAAK

BEVEILIGING IN MICROSOFT 365

EEN STARTPUNT VOOR VEILIG ONLINE WERKEN, SPECIAAL VOOR HET MKB

Wat is belangrijk om veilig online te werken?

Wat kan je zelf doen?

En wat als het mis gaat?

BITSPRAAK

INLEIDING

Je maakt gebruik van Microsoft 365, hebt licenties aangeschaft en je weg gevonden door de initiële instellingen. Als alles goed is gegaan heb je zelf je domein met e-mail gekoppeld aan je Microsoft omgeving. Oftewel, klaar om online los te gaan met alles tools!

Het starten met Microsoft 365 kan in het begin wel als lastig worden ervaren. Maar als het eenmaal draait, dan krijg je er ook veel voor terug. E-mailen, gebruik van Teams en SharePoint. Het maken van formulieren en werkstromen en zelfs je eigen bedrijfsapplicaties in elkaar klikken behoort tot de mogelijkheden.

Zolang je volgens de standaard van Microsoft werkt, lijkt ook alles het te doen. Maar is dat wel de juiste manier voor jouw organisatie? Hoe voorkom je dat jouw data per ongeluk naar externen wordt gestuurd, of dat externen zelf toegang krijgen in jouw omgeving?

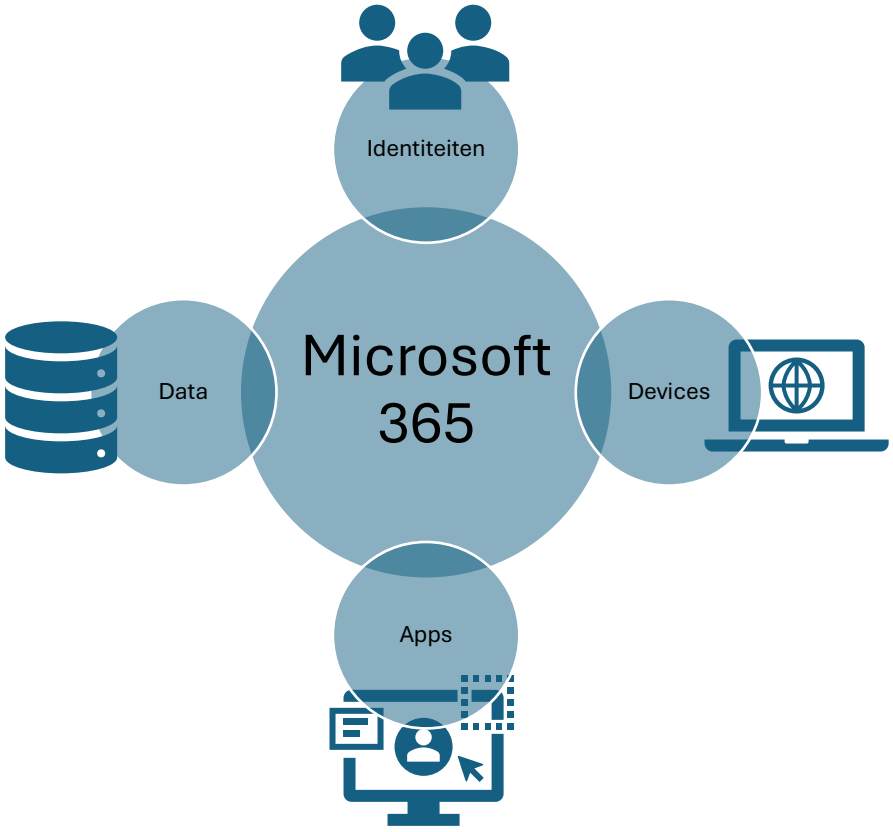
Het is van belang dat je helder hebt, hoe je als bedrijf wil werken met Microsoft 365. En daarop kan je de omgeving laten aansluiten. Dat klink ingewikkeld, en dat is het soms ook. Maar zelf kan je veel doen om in ieder geval in de basis veilig te gaan werken.

In dit document nemen we je mee in de basis van het beveiligen van jouw Microsoft 365 omgeving.

Microsoft 365

WAT MOET IK BEVEILIGEN?

Het is verstandig te kijken naar verschillende elementen waarmee je te maken krijgt als je gebruik maakt van Microsoft 365: Identiteiten (de gebruikers die inloggen), Devices (de apparaten waarmee je werkt), Apps (de applicaties die toegang hebben) en Data (de documenten, chats en e-mails waarmee je werkt). Dit zijn vier elementen waarmee je werkt in Microsoft 365 en die elk hun eigen beveiliging vereisen.



Vaak wordt hierbij ook ‘infrastructuur’ genoemd. Denk hierbij aan je interne netwerk, router of andere netwerkcomponenten. Hoewel ook dit belangrijk is vanuit een beveiligingsperspectief, laten we dit onderdeel in dit document buiten beschouwing.

IDENTITEITEN (EN DE TOEGANG DIE ZE HEBBEN)

Ten eerste is het belangrijk te kijken naar de identiteiten oftewel de gebruikers in je omgeving. Dit zijn de accounts die je aanmaakt voor medewerkers, maar bijvoorbeeld ook externen waarmee je samenwerkt. Je gebruikers zijn namelijk het voornaamste doelwit van hackers. Dit komt omdat deze rechten hebben en toegang krijgen tot jouw systemen.

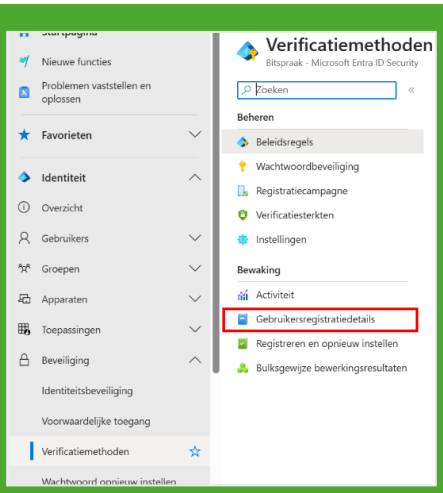
Het is dan ook belangrijk om de kans zo klein mogelijk maken dat hackers toegang krijgen tot een account. En om ervoor te zorgen dat áls er iemand een account heeft gehackt, dat de toegang van dat account zo veel mogelijk beperkt blijft.

Wachtwoorden - Identiteiten bescherm je op verschillende manieren. Zo is het verstandig om van gebruikers te eisen dat ze een complex wachtwoord gebruiken. Maar dat is niet altijd inzichtelijk en daarom is het verstandig hier technisch is voor te regelen. Denk aan het introduceren van een Password Manager, een digitale kluis waarin je wachtwoorden veilig kan opslaan en die complexe wachtwoorden voor je verzint.

MFA - Daarnaast is het noodzakelijk dat je gebruik maakt van meervoudige authenticatie, oftewel MFA (multifactor authentication). Met MFA zorg je ervoor dat je naast een gebruikersnaam en wachtwoord, nog een tweede stap moet doen doordat je toegang krijgt. Dat kan doormiddel van een SMS-code of de veiligere Microsoft Authenticator app. Deze laatste wordt bij nieuwe omgevingen standaard aangeboden. Heb je een oudere omgeving, dan is het noodzaak te controleren of MFA voor iedereen aanstaat én of de MFA-methode veilig is.

STATUS VAN MFA CONTROLEREN

Voor het beheren in inzichtelijk krijgen van de status van MFA, kan je het beste inloggen in Entra ID (https://entra.microsoft.com). Klik bij ‘Beveiliging’ op de optie ‘Verificatiemethoden’ en dan op ‘Gebruikersregistratiedetails’ voor een handig overzicht.



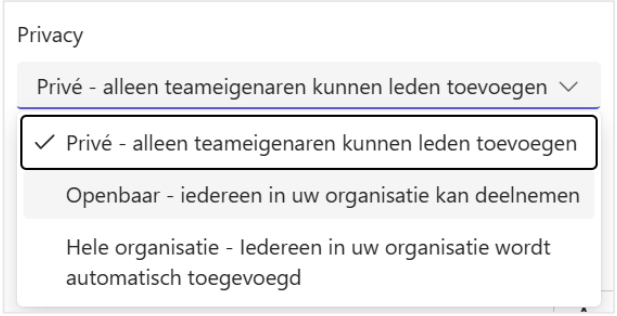
Zijn er gebruikers die geen MFA gebruiken? Je loopt dan een groot risico! Zorg er in dat geval voor dat een gebruiker MFA moet gaan gebruiken. Klik in dat geval op de desbetreffende gebruiker, kies in het menu voor ‘verificatiemethoden’ en selecteer in de knoppenbalk ‘Herregistratie van meervoudige verificatie vereisen’.

Voorwaardelijke toegang - Nog beter is om zogenaamde ‘voorwaardelijke toegang’ in te stellen, waarbij gebruikers op basis van het risico automatisch geconfronteerd worden met MFA. Hiervoor is wel een geschikte licentie vereist. Je kan in dat geval eenvoudig MFA instellen via de instellingen van de Microsoft 365 beheeromgeving.

INSTELLEN MFA
Ga hiervoor naar het Microsoft 365 beheer (https://admin.microsoft.com), klik op ‘Installatie’ en selecteer ‘Meervoudige verificatie instellen (MFA)’. Is de status nog niet voltooid, dan is het aan te bevelen dit alsnog te doen.

Rechten - Naast het beveiligen van gebruikers is het ook zaak om alleen toegang te geven aan gebruikers, voor hetgeen ze rechten nodig hebben. Dat kan zijn toegang tot Teams omgevingen of SharePoint, maar het gaat hierbij ook over beheerrechten. Denk in dit geval goed na óf en zo ja, wanneer, iemand rechten nodig heeft. Het is daarbij belangrijk dat het ‘zero-trust’ principe wordt gevolgd: geef daarbij enkel rechten op hetgeen iemand rechten nodig heeft, voor de tijd dat die persoon deze rechten nodig heeft.

Privé versus Openbaar - Veel voorkomende fouten die hierbij gemaakt worden is dat gebruikers rechten krijgen op alle SharePoint en Teams omgevingen, ook al hoeft dat niet. Het is belangrijk de het volgende te controleren: is een SharePoint site of Teams-omgeving als ‘Openbaar’ geconfigureerd of als ‘Privé’.



In het eerste geval kan iedereen met een account toegang krijgen. In het tweede geval alleen de gebruikers die als ‘Lid’ zijn toegevoegd. Je kan deze instellingen kiezen bij het aanmaken of configureren van een Team of SharePoint site.

DEVICES

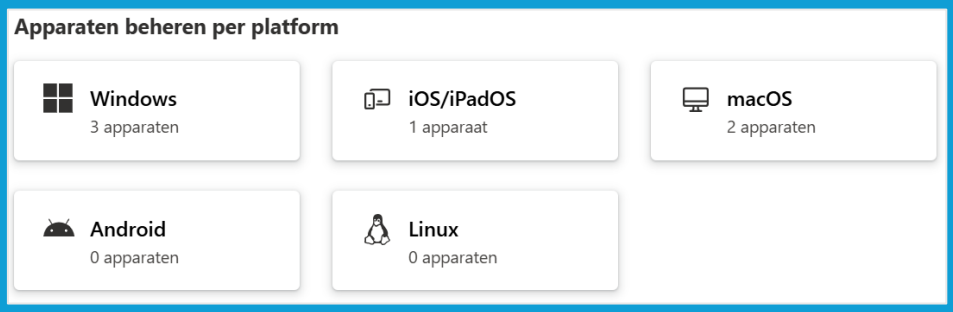
Devices, ofwel de apparaten die verbinding maken met jouw omgeving, vormen ook een risico als het gaat om beveiligen. Iedereen kent inmiddels wel de ellende als het gaat om laptops die besmet zijn met een virus of malware, of denk maar eens aan al jouw gegevens die je potentieel kwijt bent als iemand je telefoon steelt (en de code voor inloggen weet).

Het is dus van belang dat je bepaalt welke apparaten toegang mogen krijgen tot jouw omgeving én hoe je ervoor zorgt dat bedrijfsdata niet op een apparaat wordt opgeslagen. En als dat wel het geval is, hoe je dit data dan alsnog kan wissen.

Device management - Hier komt ‘device management’ om te hoek kijken. Dit is het mechanisme in Microsoft 365 waarmee je apparaten kan beheren en beveiligen op afstand. Dat kan op verschillende manieren.

Ten eerste is het verstandig zogenaamd beleid te maken waarmee je toegang kan weigeren als een apparaat daar niet aan voldoet. Denk dat aan bijvoorbeeld de aanwezigheid van een antivirussoftware, een firewall en de encryptie van je harde schijf. Maar ook het gebruik van een pincode op een telefoon.

Deels zijn deze zaken in te stellen onder ‘apparaten’ in Entra ID (https://entra.microsoft.com), onder het item ‘apparaten’. Maar als je de juiste licentie hebt, kan je dit professionaliseren in Microsoft Intune (https://intune.microsoft.com/).



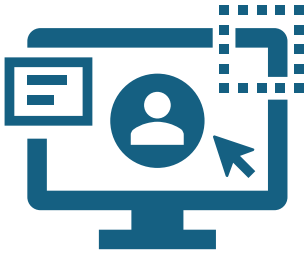
Het bepalen en uitrollen van apparaatbeleid is best complex, maar het geeft je wel inzicht in de risico's van apparaat.

Microsoft Defender - Naast het beheren van apparaten is het ook goed om inzichtelijk te krijgen wat er allemaal gebeurt en welke risico's een apparaat loopt. Microsoft Defender is hiervoor een belangrijk product. Het beschermt niet alleen het apparaat tegen virussen en ongewenste acties, heeft kan ook rapportages en beveiliging centraal inzichtelijk maken. Bijvoorbeeld door een overzicht te geven van software wat beveiligingsupdates nodig heeft of welke processen op een apparaat verdacht zijn.

Op Windows wordt Defender vaak standaard geïnstalleerd, maar op andere type systemen moet je hiervoor apart actie ondernemen.

APPS

Naast gebruikers en apparaten, is het ook verstandig te kijken naar de apps die gebruikt worden door gebruikers. Natuurlijk bevat Microsoft 365 een scala van handige toepassingen en ik zou ook zeker stimuleren deze te gebruiken. Je betaalt er immers voor.

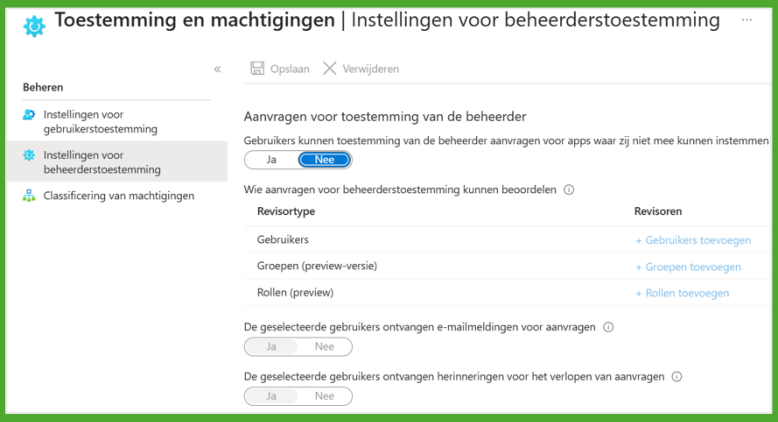


Apps van andere leveranciers - Maar naast deze standaard Microsoft apps, kunnen gebruikers ook tal van andere apps gebruiken die verbinding maken met jouw omgeving. Vaak gebeurt dit doordat een gebruiker inlogt met zijn/haar Microsoft-account. Als dat lukt, dan zal de app aan de gebruiker vragen of deze toegang mag krijgen tot jouw omgeving (namens de gebruiker). Als de gebruiker dit toestaat, dan kan de app acties uitvoeren die een gebruiker ook kan voeren. Een mogelijk risico dus.

Een nog groter risico is het als een beheerder deze vraag krijgt van een app. Een beheerder kan namelijk 'namens de organisatie' toestemming verlenen aan de app. Met als gevolg dat de app direct namens iedere gebruiker toegang heeft.

Het is daarom zaak om het toestaan van rechten van apps te monitoren en te beperken. Je kan hierbij onderscheid maken tussen de verschillende niveaus van rechten. Zo kan je bijvoorbeeld toestaan dat een profiel wel uitgelezen mag worden (de app bijvoorbeeld de naam van de gebruiker mag uitlezen), maar niet mails mag verzenden namens de gebruiker.

TOESTEMMING EN MACHTINGEN
Deze instellingen wat apps wel en niet mogelijk, zijn te beheren vanuit Entra ID (https://entra.microsoft.com). Ga hiervoor aan ‘Toepassingen’, ‘Bedrijfstoepassingen’ en dan ‘Toestemming en machtigingen’. Hier is het mogelijk om naar eigen wens in te stellen hoe je om wil gaan met apps en de permissies die deze apps nodig hebben.



DATA

Naast gebruikers, apparaten en apps, is het ook verstandig te kijken naar de beveiliging van jouw data. En eigenlijk bedoelen we hiermee dat we willen voorkomen dat er datalekken ontstaan, waarbij jouw waardevolle data in verkeerde handen valt. Want naast dat jouw data mogelijk vertrouwelijk is, kunnen de gevolgen groot zijn als dat gebeurt.

Zo zul je in sommige gevallen een melding moeten doen bij de Autoriteit Persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/), je veel moeten regelen om de schade beperkt te houden én kost dit je mogelijk onherstelbare imagoschade. Want zou jij zaken willen doen met een bedrijf wat te maken heeft met datalekken?

Classificeren - Daarom is het verstandig om je data te classificeren: in kaart brengen welke data hoeveel schade veroorzaakt. Op basis van deze inventarisatie kan je een indeling maken van hoe gevoelig data is. Denk bijvoorbeeld aan ‘Openbare data’ (reclamefolders, je website), ‘Interne data’ (werkdocumenten, klantpresentaties), ‘Vertrouwelijke data’ (financiële gegevens, persoonsgegevens) en ‘Geheime data’ (plannen voor bedrijfsovername, medische gegevens van personeel). Deze classificatie is een voorbeeld, het is natuurlijk zaak deze aan te laten sluiten op jouw specifieke situatie.

Microsoft 365 biedt de mogelijkheid om data te classificeren. Dit kan met het toekennen van labels aan groepen, Teams en SharePoint, maar ook aan documenten of rapportages. Niet alleen werkt dat mee aan het bewustzijn bij gebruikers dat ze mogelijk met

vertrouwelijke gegevens werken, het is ook nog eens mogelijk om technische maatregelen te nemen om deze data te beschermen.

Denk hierbij aan het wel of niet kunnen delen van gegevens met externen, het naar buiten kunnen e-mailen van documenten, of zelf het versleutelen van documenten. Dit allemaal ter voorkoming van datalekken.

Helaas is het instellen van classificatie labels iets waarvoor je veel technische kennis nodig hebt. En je hebt hiervoor ook de juiste licenties nodig. Maar als dit eenmaal is ingericht, dan werk je wel een stuk veiliger. Daarnaast zal de bewustwording onder gebruikers verbeteren, omdat deze classificaties in de verschillende Microsoftproducten tot uiting komt, zo ook het gebruik van Microsoft Copilot, de A.I. oplossing van Microsoft.

EN VERDER...?

Naast bovenstaande onderdelen zijn er tal van instellingen, controles en andere maatregelen die je kan nemen om veiliger te werken. Het kan daarbij helpen rond te kijken in de verschillende beheeromgevingen.

Kijk bijvoorbeeld eens bij de instellingen in het Microsoft 365 beheer centrum, en met name beveiliging en privacy: https://admin.microsoft.com/#/Settings/SecurityPrivacy . Hier zijn tal van basisinstellingen voor het beveiligen van je omgeving te configureren.

Maar heb je eenmaal instellingen geconfigureerd, dan wil je natuurlijk ook dat dit regelmatig wordt getoetst. Veel problemen kunnen voorkomen worden als je de volgende zaken regelmatig controleert:

- Inactieve externe gebruikers
- Teams en SharePoint sites die ‘te open’ staan
- Met wie en waar documenten gedeeld worden met externen
- Welke apparaten niet voldoen aan jouw beleid
- Of er gebruikers zijn die risico lopen

Kortom, veel rapportages en veel werk. Maar dit kan je veel ellende besparen.

De essentie is dat beveiliging niet alleen maar een technische aangelegenheid is. Sterker nog, het raakt ook jouw gebruikers, processen en zelf de branche waarin je werkzaam hebt.

WAT ALS HET MIS GAAT?

100% veilig werken kan niet gegarandeerd worden. Het blijft namelijk ook mensenwerk, en daar worden nu eenmaal fouten gemaakt. Maar als het dan toch mis gaat is het goed een plan klaar te hebben.

In dit plan is het goed om een lijst te hebben van je diensten en applicaties, zodat je het overzicht hebt wie je kan bellen en in welke systemen je actie kan ondernemen. Denk daarbij aan het blokkeren van accounts, het loskoppelen van apparatuur of de hulp inroepen van iemand die je kan helpen het probleem op te lossen.

Zorg daarbij dat je stapsgewijs werkt en het liefst in een kleine vast groep mensen. Bewaar de rust en maak een plan. Zorg ervoor dat je met dit team regelmatig overleg hebt over de status en de voortgang van het incident. Zorg er tevens voor dat je een logboek bijhoudt van de stappen die je hebt ondernomen.

Kijk voor meer handige tips eens op de website van Cyber Chain Resilliance Consortium (CCRC, https://ccrc.nl/).

Is het probleem onder controle? Bepaal dan welke stappen je moet nemen voor de afhandeling. In sommige gevallen zul je melding moeten doen bij de autoriteit persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/datalek-melden). Heb je een verzekering die cybercriminaliteit dekt, zorg dan dat je in een vroeg stadium contact opneemt.

Als je te maken hebt met een veiligheidsincident, kan dat potentieel veel schade veroorzaken. Wees daarom voorbereid en maak de kans op een incident zo klein mogelijk.

OVER BITSPRAAK

Bitspraak biedt de mogelijkheid om laagdrempelig expertise op het gebied van Microsoft 365 in huis te halen. Samen met jou zorgen we ervoor dat jouw omgeving veilig wordt ingericht, rapportages worden uitgevoerd, lekken en veiligheidsproblemen worden opgelost en je proactief advies krijgt om veilig en effectief online te werken.

We bieden deze dienst aan in abonnementsvorm: SpotOn365.

Met SpotOn365 leiden we je stapsgewijs door de onderwerpen en instellingen van Microsoft 365. Gebruikers, SharePoint, Teams, maar ook apparaten, apps en data. Daarbij hou jij de controle en kunnen wij jou ontlasten door de technische configuratie uit te voeren. Als er problemen zijn, zullen we die voor je oplossen of samen met je bespreken.

Daarnaast nemen we je mee in tal van rapportages, tips en zorgen we dat je nooit te veel betaalt voor je licenties.

We bieden deze dienst in abonnementsvorm aan, waarbij je laagdrempelig en regelmatig persoonlijk contact hebt met ons. Daarnaast heb je de mogelijkheid om onbeperkt vragen te stellen en voeren we ook nog het technisch beheer uit voor jouw omgeving.

Om vrijblijvend inzicht te krijgen in de beveiliging van jouw omgeving, bieden we een gratis beveiligingsscan aan. We doorlopen dan verschillende aspecten van jouw Microsoft 365 omgeving en bespreken dat na afloop.

Meer weten over dit abonnement? Kijk op https://bitspraak.nl/ of neem contact op met Mart Muller (mart@bitspraak.nl). We leggen je graag meer uit hoe we te werk gaan.