



Zo houd je Microsoft 365 veilig én gebruiksvriendelijk

De IT-infrastructuur is het fundament waar een moderne bedrijfsomgeving op rust. Bedrijfskritische applicaties worden steeds belangrijker voor het inrichten en stroomlijnen van bedrijfsprocessen, terwijl data de moderne bouwstenen zijn voor een succesvolle bedrijfsvoering. Communiceren en samenwerken gebeurt bovendien steeds vaker op verschillende locaties en tijdstippen. Wat betekent dit voor je ICT? Allereerst dat data centraal beschikbaar moet zijn. Dat je medewerkers 24/7 toegang hebben tot het bedrijfsnetwerk, applicaties en bestanden, vanaf elke gewenste locatie. En dat gebruikers onderling efficiënt kunnen communiceren en samenwerken aan projecten of documenten. Alleen dan is er sprake van optimale samenwerking. ICT is dan ook geen kostenpost meer, maar een strategisch middel, dat de primaire processen van je organisatie faciliteert en ondersteunt. En niet te vergeten; dit alles moet perfect beveiligd zijn.

Naast productiviteit en gebruiksgemak speelt veiligheid dan ook een belangrijke rol. Een hot topic, aangezien we steeds meer online-toepassingen gebruiken en cybercriminelen ook niet stilzitten. Malware en ransomware worden steeds ingenieuzer, terwijl ook de amateuristische en van mijlenver herkenbare phishingmail steeds vaker plaatsmaakt voor een levensecht uitziende variant (inclusief officiële logo's en kloppende adresgegevens van de 'verzender').

Microsoft 365 is een platform dat functionaliteit en veiligheid combineert. Voor dat laatste aspect moet je alleen wel iets doen. Microsoft 365 biedt veel mogelijkheden om de beveiliging te controleren, aan te scherpen en te bewaken. Tegelijkertijd betekent 'meer beveiliging' vaak 'minder gebruiksvriendelijkheid'. De keuze is dan ook volledig aan jou. Maar weet je welke mogelijkheden er zijn en hoe je deze optimaal kunt inzetten? Wat zijn de risico's als je niets doet?

INHOUD

- Veilig werken op afstand met mobiele devices
- Data beveiligen in Microsoft 365
- De menselijke factor
- Denk na over beleid en gebruik
- Een veilige 365-omgeving die past bij jouw organisatie

Veilig werken op afstand met mobiele devices

Op afstand werken wordt steeds meer de norm, zeker nu mobiele devices steeds krachtiger en multifunctioneler worden. Een situatie waarin medewerkers op verschillende locaties en tijdstippen kunnen werken – al dan niet op eigen devices (BYOD/CYOD) – vraagt om solide security-maatregelen. Dankzij oplossingen als Teams en SharePoint Online is Microsoft 365 een platform dat werken op afstand faciliteert. Maar hoe zorg je ervoor dat medewerkers de 365-omgeving ook op hun eigen pc, de computer van de zaak of hun mobiele devices veilig benutten?

De eerste factor is de techniek. Zeker als medewerkers op afstand werken is het belangrijk om de toegang tot belangrijke applicaties, data en documenten te beveiligen. Een van de beste middelen die tot je beschikking staan is multi-factor authenticatie (MFA). Gebruik je MFA? Microsoft 365 vraagt dan naast het wachtwoord nog naar een extra authenticatie-methode wanneer iemand toegang wil krijgen tot een applicatie of dienst. Denk bijvoorbeeld aan een sms'je, authenticatie-app op de smartphone of een telefoontje naar jouw nummer vanuit Microsoft.

Is een hoger beveiligingsniveau noodzakelijk, bijvoorbeeld omdat je als zorginstelling of financiële dienstverlener veel privacygevoelige informatie (persoonsgegevens, patiëntgegevens of financiële en transactionele data) beheert en verwerkt? Microsoft Advanced Threat Protection (ATP) biedt dan extra beveiligingsfunctionaliteiten. Denk bijvoorbeeld aan het beveiligen van e-mails en bijlagen en bescherming tegen phishing door het inzetten van realtime-detectie.

Data beveiligen in Microsoft 365

Data zijn het nieuwe goud en hebben een groot strategisch belang. Maar data zijn ook kostbaar. Komt privacygevoelige of bedrijfskritische informatie in verkeerde handen of op straat te liggen? Dan is de impact groot en kun je rekenen op omzetverlies, reputatieschade of torenhoge boetes. Zeker in sectoren als de zorg en het onderwijs zijn datalekken een prominent schrikbeeld. Gelukkig herbergt Microsoft 365 de tools om zorgvuldig om te gaan met datamanagement. Met Conditional Access kun je heel nauwgezet én op detailniveau bepalen welke apparaten toegang hebben tot het uitgebreide dienstenaanbod van Microsoft 365. Conditional Access biedt bijvoorbeeld de mogelijkheid om de toegang voor unmanaged devices niet volledig te ontfemen, maar dusdanig te beperken dat het onmogelijk wordt om documenten af te drukken, te downloaden of te bewerken in de desktop-applicaties. Handig als je bijvoorbeeld veel werkt met zzp'ers die gebruikmaken van hun eigen laptop.

“Komt privacygevoelige of bedrijfskritische informatie in verkeerde handen of op straat te liggen? Dan is de impact groot.”

Informatie die voor veel medewerkers toegankelijk moet zijn en een betrekkelijk laag risiconiveau heeft, kun je het predicaat baseline geven. Privacygevoelige of bedrijfskritische data en documenten kun je daarentegen voorzien van de strengst mogelijke beveiliging door er het label 'classified' aan te hangen. De classificaties kun je koppelen aan documentenmappen, waardoor je gelijk een helder overzicht hebt van de status van je data en documenten.

De menselijke factor

Je hebt de techniek en werkprocessen helemaal op orde. Dat is goed, maar dit wil niet zeggen dat je er al bent. In de praktijk is de menselijke factor vaak de zwakste schakel in de beveiligingsketen.

We kennen allemaal wel het voorbeeld van de medewerker die toch op dat linkje klikt of die geïnfecteerde bijlage opent. En het apparaat waar je thuis mee werkt kan nog zo veilig zijn, maar als je jouw laptop hartje zomer in de tuin hebt staan met een belangrijk document open en bloot op het scherm, waardoor de buurman kan meelezen als je even naar binnen gaat, zetten geavanceerde beveiligingsmaatregelen weinig zoden aan de dijk.

Adoptie en bewustwording zijn dus minstens zo belangrijk als de technische en procesmatige aspecten. Zorg dat je medewerkers zowel de belangrijkste ins en outs van 365 als de belangrijkste cyberdreigingen (her)kennen. Vooral het onjuiste gedrag of de onwetendheid van eindgebruikers is vaak de zwakke plek in de digitale verdedigingslinie.

Denk na over beleid en gebruik

Hoewel Microsoft 365 een erg toegankelijk en veelzijdig platform is, moet je zelf wel veel instellen om het af te stemmen op je specifieke organisatorische wensen en veiligheidsbehoeften. Het is geen kwestie van simpelweg wat dingen aan- en uitzetten. Dit betekent dat je ook goed na moet denken over het beleid en gebruik. Hoe ondersteunt het platform jouw core business? Welke securitymaatregelen heb je nodig om je kerntaken te ondersteunen en verbeteren? Dit zijn vragen die verder gaan dan alleen de techniek. Microsoft Teams zonder duidelijk plan voor iedereen openzetten leidt bijvoorbeeld vaak tot een wildgroei aan kanalen en teams. Een handige communicatie- en samenwerkingstool wordt zo een onwerkbaar gedrocht.

Ook de vaak delicate balans tussen productiviteit, gebruiksgemak én veiligheid is een belangrijk aandachtspunt. 'Hoe veiliger, hoe minder gebruiksvriendelijk' is een wijsheid die in de praktijk nogal eens geldt. Het is dus belangrijk dat je goed definieert hoe die verhouding tussen gebruiksgemak en veiligheid er voor jouw type organisatie uit ziet.



Een veilige 365-omgeving die past bij jouw organisatie

Wil jij weten hoe veilig jouw Microsoft 365 omgeving is én hoe je deze in de toekomst veilig kunt houden? Dat is precies waar de security scan van Hands on voor bedoeld is. Aan de hand van de Microsoft Secure Score Card en concrete vragen kijken we hoe het gesteld is met jouw beveiligingsniveau. We toetsen je actuele beveiligingsinstellingen aan de drie beveiligingsniveaus van Microsoft:

- Baseline (het minimale beveiligingsniveau voor Microsoft 365);
- Advanced;
- Classified (het niveau voor organisaties met ISO/IEC 27001-certificeringen met audits).

Na de inventarisatie volgt een advies waarin we aangeven wat er nodig is om het vereiste beveiligingsniveau te bereiken. Wij weten uit ervaring dat Baseline het absolute minimum is waaraan een veilige 365-omgeving moet voldoen.

De derde stap is een planning, die aangeeft wanneer welke verbeteringen worden doorgevoerd. In de realisatiefase gaan we de verbeteringen doorvoeren en geven we de medewerkers een praktische uitleg over de wijzigingen, als dat nodig is. Het waarom is voor ons namelijk net zo belangrijk als het hoe.

Na de realisatie blijven we jouw 365-omgeving volgen, monitoren en aanscherpen. Als je niet continu de vinger aan de pols houdt, sla je op het gebied van cybersecurity namelijk de plank mis.

Bij ons kun je er met een gerust hart van uitgaan dat je 365-omgeving in goede handen is, en wel om de volgende redenen:

- Onze kennis en expertise is toegespitst op Microsoft 365. We kennen het platform dan ook door en door.
- We hebben niet alleen oog voor de techniek, maar leggen ook sterk de nadruk op bewustwording en de businesskant van het 365-platform. Hoe ondersteunt het jouw core business? En welke securitymaatregelen heb je nodig om je kerntaken te ondersteunen en verbeteren? Dit zijn vragen die verder gaan dan alleen de techniek en die wij altijd stellen.
- We kijken niet alleen naar het heden, maar ook naar de toekomst. Managed security zorgt ervoor dat jouw 365 ook gewapend is tegen nieuwe bedreigingen en meegaat met nieuwe ontwikkelingen.
- Ontdek waar je staat en waar je naartoe moet zonder veel van je tijd te hoeven investeren. Onze scan neemt een dag of twee in beslag.

Meer weten?

Wil je ook het beste uit je 365-omgeving halen en je medewerkers een veilige en productieve werkplek bieden? Dan helpen we je graag! Met onze security scan weet je precies waar je staat met jouw beveiliging en waar nog ruimte is voor verbetering. Meer weten? Bel ons dan gerust op +31 (0)88 18 10 100 of stuur ons een bericht: info@handson.nl.

Over de Hands on Group

Hands on Information Management maakt deel uit van de Hands on Group. De Hands on Group bestaat daarmee uit Hands on, Compello en ITSN. In totaal werken hier ruim 125 professionals met allemaal hun eigen expertise op ICT-gebied. De Hands on Group bedient een breed scala aan opdrachtgevers in uiteenlopende branches zoals zorg, industrie, wonen, zakelijke dienstverlening en onderwijs.

De Hands on Group heeft een landelijke dekking met kantoren in Venlo, Weesp en Zwolle, waardoor wij als landelijke organisatie altijd op regionaal niveau kunnen schakelen. De samenwerking van de drie bedrijven verzekert opdrachtgevers van snelle ondersteuning op locatie en geeft hen toegang tot een breed kennisnetwerk van ICT-specialisten die organisaties én mensen helpen om productiever, efficiënter en slimmer te werken.

CONTACT