

Veilig is geen eigenschap. **Het is een instelling.**

Wat Microsoft regelt, wat jij moet regelen,
en tien instellingen om vandaag te
controleren.

Whitepaper 02

OctaOne · Jean de Jongh

Parkweg 37, 4153 XL Beesd

0345 782 500 · help@octaone.nl · octaone.nl

01 — DINSDAGMIDDAG

Een vraag van een klant.

"Klopt het dat jullie rekeningnummer is gewijzigd?"

Je hebt geen nieuw rekeningnummer. Je hebt die mail nooit gestuurd. Maar hij kwam wel van jouw adres.

Zo begint het meestal. Niet met een zwart scherm. Met een mailbox die al weken door iemand anders wordt meegelezen.

Laat ik eerlijk zijn. Ik werk zelf op Google Workspace. Veel van de bedrijven die ik spreek, werken op Microsoft 365. Beide zijn prima platforms. Mits je ze goed inricht.

En daar zit het.

Microsoft 365 is niet veilig. Of onveilig. **Het is zo veilig als jij het instelt.**

02 — VERANTWOORDELIJKHEID

Microsoft of jij?

Microsoft zorgt dat het platform draait. De datacenters, de servers, de software. Dat doen ze goed.

Wat jij ermee doet, is jouw verantwoordelijkheid. Wie mag inloggen. Wat er gedeeld mag worden. Wie beheerrechten heeft. Microsoft noemt dat zelf het model van gedeelde verantwoordelijkheid.

En back-up? Microsoft zorgt dat je data niet verdwijnt door een storing bij hén. Niet dat je die verwijderde map van drie maanden terug weer krijgt. Of een versleutelde SharePoint. Daarvoor heb je een eigen back-up nodig.

Veel ondernemers denken: het staat in de cloud, dus het is geregeld. Begrijpelijk.

Niet waar.

03 — IN DE PRAKTIJK

Waar het misgaat.

Het overgenomen account

Eén phishingmail. Eén ingevuld wachtwoord. Geen MFA. De aanvaller logt in, maakt stilletjes een regel die mail doorstuurt, en wacht. Op een factuur. Op het juiste moment.

Te veel rechten

Drie mensen met beheerrechten "omdat het handig was". Het account van een oud-collega dat nog actief is. Een gastgebruiker van een project uit 2023. Elk account is een deur.

Delen zonder grens

"Iedereen met de link." Handig. Tot die link in de verkeerde mailbox belandt. En niemand weet meer welke links er allemaal rondgaan.

Oude deuren

Verouderde aanmeldmethodes en apps die ooit toegang kregen en die nooit is ingetrokken. Niemand kijkt ernaar. Een aanvaller wel.

En de wachtwoorden

Hier moet ik mezelf corrigeren. Ik heb jarenlang geroepen: wijzig je wachtwoord regelmatig. Dat werkt averechts. Mensen maken dan *Zomer2026!*, en volgend kwartaal *Herfst2026!*.

Beter: lang, uniek per dienst, en opgeslagen in een wachtwoordmanager. Wijzigen doe je als er reden voor is. Niet omdat de kalender het zegt.

04 — CHECKLIST

Tien instellingen om te controleren.

Geen hogere wiskunde. Wel werk dat iemand een keer goed moet doen. En daarna moet blijven controleren.

- 1 MFA voor iedereen.** Liefst via een app of passkey. Sms is beter dan niets, maar niet veel.
- 2 Regels voor aanmelden.** Laat je licentie het toe? Gebruik Conditional Access: inloggen alleen vanaf bekende apparaten of locaties.
- 3 Oude aanmeldmethodes uit.** Controleer of verouderde protocollen echt dicht staan. Niet aannemen. Kijken.

- 4 **Beheer apart en klein.** Een handvol beheerders, elk met een apart beheeraccount. Niet je dagelijkse account.
- 5 **Logboeken aan.** Zet audit logging aan. En spreek af wie er kijkt. Een logboek dat niemand leest, is een dagboek.
- 6 **Doorsturen naar buiten blokkeren.** Automatisch doorsturen naar externe adressen hoort standaard uit te staan. Controleer het.
- 7 **Je domein beschermen.** SPF, DKIM en DMARC goed ingesteld. Dan kan niemand zomaar mailen alsof hij jou is.
- 8 **Links en bijlagen laten controleren.** Met Defender for Office 365: Safe Links en Safe Attachments aan.
- 9 **Delen begrenzen.** Geen "iedereen met de link" in SharePoint en OneDrive. Gasttoegang in Teams periodiek nalopen.
- 10 **Eigen back-up.** Van mail, OneDrive, SharePoint en Teams. En test het terugzetten. Echt.

05 — TOT SLOT

Kijk, of laat kijken.

Je kunt deze lijst zelf aflopen. Of met je huidige IT-partner. Doe het vooral.

Wil je dat iemand onafhankelijk meekijkt? Iemand die het niet zelf heeft ingericht? Dan doe ik dat graag. Geen verkooppraatje. Gewoon: wat staat goed, wat niet, en wat eerst.

Veilig is geen eigenschap. Het is een instelling.

Jean de Jongh

OctaOne, Beesd

Rust in je IT geeft **ruimte aan je bedrijf.**

Ik geloof dat technologie pas waarde heeft als mensen haar begrijpen en kunnen gebruiken. Daarom begint bij OctaOne alles bij de medewerker. Niet bij het product. En daarom geef ik weg wat ik weet. Deze whitepaper is daar een stukje van.

• Slim werken

• Verbonden blijven

• Beveiligd zijn

• Betrokken blijven

OVER DE SCHRIJVER

Jean de Jongh

Ruim twintig jaar in IT. Mijn eerste bedrijf startte ik op 1 oktober 2001. De afgelopen jaren hielp ik grote organisaties in Nederland, België en Duitsland met security en strategie.

Nu doe ik dat voor het MKB. Vanuit Beesd. Met een voorkeur voor objectief boven subjectief, en voor oplossingen die over vijf jaar nog kloppen.

Strategie eerst. Tech volgt wel.

VOLGENDE STAP

Even sparren?

Plan een gesprek

Geen verkooppraatje. Gewoon kijken waar je staat en wat de volgende stap is. Remote, bij jou op locatie, of bij ons in Beesd.

Afspraak plannen →

octaone.nl/afspraak



Telefoon

0345 782 500



E-mail

help@octaone.nl



Web

octaone.nl

