<HET DIGITALE KOMPAS>

</DE ZIN EN ONZIN VAN CYBERSECURITY>



#2

<BRANDARIS>

</CYBERSECURITY>

<BRANDARIS CYBERSECURITY B.V.>
Keesomstraat 10-G
1821 BS Alkmaar

+31 (0)72 202 97 95
info@brandaris.it
www.brandaris.it

<KVK> 94696675
<BTW> NL866862833B01
<IBAN> NL58REVO7619561102
<BIC> REVONL22



<WAT STAAT ERIN?>

INTRODUCTIE 1

AUTHENTICATIE & WACHTWOORDBEHEER 3

HET FUNDAMENT VAN EEN VEILIGE DIGITALE ORGANISATIE 3

- WAT MOET JE DOEN? 3
  - 1. STERKE WACHTWOORDEN EN WACHTZINNEN 3
  - 2. CENTRAAL BEHEER VAN WACHTWOORDEN 4
  - 3. MULTIFACTOR AUTHENTICATIE (MFA) 4
  - 4. PASSKEYS EN ANDERE VORMEN VAN PASSWORDLESS WERKEN 4
  - 5. CONDITIONAL ACCESS 5
  - 6. INZICHT IN ACCOUNTS 5
  - 7. SINGLE SIGN-ON (SSO) 6
- FUNCTIES OM OP TE LETTEN ALS JE EEN WACHTWOORDENMANAGER KIEST 6

AUTORISATIE OP MAAT 7

- NOOIT MEER STANDAARD WERKEN MET BEHEERDERSRECHTEN 8
- ROLE-BASED ACCESS 8
- PERIODIEKE CONTROLE 9

PRODUCTEN, LICENTIES EN KEUZES 10

- WAT HEB JE ÉCHT NODIG? 10
  - WAAROM EEN STERKE BASIS GELD BESPAART 11
- INZOOMEN OP MICROSOFT: HOE MAAK JE SLIMME KEUZES? 11
  - MINIMALE MICROSOFT- BEVEILIGINGSFUNCTIES DIE JE ECHT WILT GEBRUIKEN 12
  - DEFENDER FOR ENDPOINT (LICHTE VARIANT) 12

ADEQUATE E-MAILBEVEILIGING 13

- HOE SPF, DKIM EN DMARC JE ORGANISATIE BESCHERMEN 13
  - SPF: WIE MAG ER NAMENS JOU MAILEN? 13
  - DKIM: IS DE MAIL ONGEWIJZIGD AANGEKOMEN BIJ DE ONTVANGER 14
  - DMARC: WAT TE DOEN ALS ER IETS NIET KLOPT 14
- WAAROM IS DIT ZO BELANGRIJK? 14
- HOE STEL IK DIT IN? 15
  - SPF INSTELLEN 15
  - DKIM INSTELLEN 15
  - DMARC INSTELLEN 15

BACKUPS: JE LAATSTE REDDING, ALS JE ZE GOED REGELT. 17

- WAAROM BACK-UPS ZO BELANGRIJK ZIJN 18
- WAT EEN GOEDE BACKUP ECHT BETEKENT 18
- WAT KUN JE NU AL DOEN? 19

AFSLUITING 21

</INTRODUCTIE>



Na de goede ontvangst van het eerste Digitaal Kompas kon een tweede editie natuurlijk niet uitblijven. In deze editie staan we stil bij de zaken die op het gebied van digitale veiligheid geregeld moeten worden voor (beginnende) ondernemers. Digitale veiligheid is geen luxe en ook geen project met een kop en een staart: het is een doorlopend proces. Het is een fundament dat je legt en regelmatig controleert, evalueert en corrigeert. Wanneer je net als beginnend ondernemer start met je organisatie is dit het uitgelezen moment om een stevige digitale fundering te leggen waar jarenlang op gebouwd kan worden.

Je kan het zogenoemde security-by-design- principe integreren in alle processen die nog opgesteld gaan worden en alle productkeuzes die nog gemaakt gaan worden. Voor wie al langer onderneemt is het van belang om regelmatig, bijvoorbeeld ieder half jaar, te toetsen of het fundament nog actueel, passend en volledig is. Dit gebeurt in de praktijk vaak pas na een incident, het beste moment is vanzelfsprekend daarvoor.

Cyberdreigingen veranderen voortdurend. Wat gisteren voldoende leek, kan vandaag een zwakke plek zijn. Daarom is het belangrijk om keuzes te maken die niet alleen nu werken, maar ook meegroeien met jouw organisatie. Het gaat om overzicht, controle en het voorkomen van vervelende verrassingen die je bedrijfsvoering raken.

In deze editie van het Digitale Kompas helpen we je om die basis scherp en toekomstbestendig te krijgen. We geven praktische inzichten waarmee je direct kunt handelen en tegelijk een strategie opbouwt. Zo creëer je rust en zekerheid om te focussen op wat echt telt: jouw onderneming laten groeien en je klanten met volle aandacht en zekerheid verder helpen.



</AUTHENTICATIE & WACHTWOORDBEHEER>

<AUTHENTICATIE & WACHTWOORDBEHEER>

HET FUNDAMENT VAN EEN VEILIGE DIGITALE ORGANISATIE

Toegang tot jouw systemen en data vormt het eerste verdedigingsfront van je organisatie. Als dit niet goed geregeld is, maakt het weinig uit hoeveel andere maatregelen je neemt. Eén zwak account kan de deur wagenwijd openzetten voor cybercriminelen. Vergelijk het met een huis: je laat de voordeur niet openstaan en je geeft ook niet zomaar iedereen een sleutel. In de digitale wereld werkt dat precies hetzelfde. Authenticatie is daarom geen technisch detail dat ergens in een menu staat, maar een strategische keuze die bepaalt hoe veilig en beheersbaar jouw organisatie werkelijk is.

Cybercriminelen richten zich bijna altijd op het eenvoudigste pad naar binnen. Dat is zelden een ingewikkelde kwetsbaarheid, maar meestal een zwak account met een slecht wachtwoord, een vergeten inlog of een onhandige klik op een phishinglink. In de praktijk zien we dat veel incidenten voortkomen uit menselijke fouten of nalatigheid, niet uit vernuftige hacks. Dat vraagt om een sterk, consistent en toekomstbestendig authenticatiebeleid dat menselijke fouten opvangt en kwetsbaarheden minimaliseert. Die basis is essentieel, want hierop rusten alle andere beveiligingslagen binnen jouw organisatie.

<WAT MOET JE DOEN?>

1. STERKE WACHTWOORDEN EN WACHTZINNEN

Een goed wachtwoord begint met helder beleid en sterke eisen. In plaats van korte, ingewikkelde codes die niemand kan onthouden, kies je voor wachtzinnen: langere, begrijpelijke combinaties van woorden die juist door hun lengte veel moeilijker te kraken zijn. Dit maakt het voor aanvallers aanzienlijk lastiger om toegang te krijgen, terwijl het voor medewerkers juist makkelijker wordt om veilig te werken. Veel mensen denken dat een wachtwoord veilig is als het vol rare tekens staat en moeilijk te onthouden is. Maar: **W8w0ord-I$-St3rk** is veel moeilijker te onthouden dan **DIT-is-1-sterke-OPTIE**, terwijl die laatste minstens zo veilig is door de lengte en combinatie van cijfers, letters en leestekens.

Het oude advies “bedenk een moeilijk wachtwoord en verander het regelmatig” werkt niet meer. Sterker nog, het zorgt juist voor onveilig gedrag. Mensen die elke paar maanden iets nieuws moeten bedenken, kiezen varianten zoals Welkom2023! → Welkom2024! of plakken er gewoon een uitroepteken bij.

Cybercriminelen weten dat. Ze beschikken over miljoenen gestolen wachtwoorden en gebruiken geautomatiseerde tools om dezelfde combinaties op andere diensten te testen. Eén hergebruikt wachtwoord kan daardoor toegang geven tot bedrijfsgegevens.

<WAT MOET JE DOEN?>

2. CENTRAAL BEHEER VAN WACHTWOORDEN

Het tijdperk waarin medewerkers zelf al hun wachtwoorden moesten bedenken en beheren, ligt achter ons. Losse wachtwoorden leiden vrijwel altijd tot onveilig gedrag: hergebruik, variaties, notities in Excel, screenshots op telefoons of opgeslagen wachtwoorden in browsers. Precies wat cybercriminelen graag zien.

Een wachtwoordmanager biedt een centraal, veilig systeem waarin medewerkers al hun wachtwoorden kunnen beheren zonder dat ze die zelf hoeven te onthouden. De kracht hiervan zit in de combinatie van gemak, veiligheid en beheer. Deze wachtwoordmanager moet wel goed aansluiten bij de organisatie. De gekozen variant moet op alle apparaten kunnen functioneren binnen je organisatie zodat adoptie en gebruik gemakkelijk is.

Veel professionele wachtwoordmanagers bieden functies zoals automatische generatie van sterke wachtzinnen, controles op gelekte wachtwoorden en veilige teamkluizen. Dit geeft grip op wie welke toegang heeft en maakt het intrekken van rechten eenvoudig, bijvoorbeeld wanneer iemand de organisatie verlaat. Dashboards geven beheerders overzicht en inzicht in het gebruik, zodat risico's vroegtijdig zichtbaar worden.

<WAT MOET JE DOEN?>

3. MULTIFACTOR AUTHENTICATIE (MFA)

MFA is een van de meest effectieve maatregelen die je kunt inzetten. Waar een wachtwoord kan uitlekken of worden geraden, biedt MFA een extra verificatiestap die voorkomt dat cybercriminelen met alleen die informatie binnenkomen. Kies altijd voor moderne vormen van MFA, zoals app gebaseerde verificatie of fysieke hardware tokens. Deze zijn betrouwbaarder en veiliger dan SMS, dat kwetsbaar is voor onderschepping en SIM swaps. MFA is geen garantie op volledige veiligheid, maar het verkleint de kans op misbruik enorm en maakt het werk van aanvallers vele malen moeilijker.

<WAT MOET JE DOEN?>

4. PASSKEYS EN ANDERE VORMEN VAN PASSWORDLESS WERKEN

Passkeys zijn de toekomst van veilig inloggen. Het mooie is: je hoeft geen wachtwoord meer te bedenken of te onthouden. Toegang wordt gekoppeld aan biometrie zoals een vingerafdruk of gezichtsherkenning, of een fysiek apparaat dat jij in bezit hebt. Dat vermindert het risico op wachtwoorddiefstal praktisch tot nul.

Het belangrijkste voordeel van passkeys is dat ze phishing resistent zijn. Zelfs als iemand probeert jou naar een nagemaakte website te lokken, werkt de passkey daar simpelweg niet. De techniek controleert automatisch of je op de echte omgeving zit voordat je überhaupt kunt inloggen. Dit maakt dit type authenticatie niet alleen veiliger, maar ook veel gebruiksvriendelijker.

Voor organisaties biedt dit een enorme stap vooruit in zowel veiligheid als dagelijkse efficiëntie.

Nog niet elke organisatie is klaar voor passkeys, en dat hoeft ook niet. Een tussenstap die vandaag al veel veiligheid en gemak oplevert, is het gebruik van authenticatorapps zoals Microsoft Authenticator om in te loggen op Microsoft accounts. Daarmee kun je inloggen zonder wachtwoord, puur door een pushmelding te bevestigen op je telefoon.

Het werkt simpel: je probeert in te loggen, je ontvangt een melding, en met één tik geef je toegang. Geen gedoe met codes, geen wachtwoord dat je moet onthouden en het is veel lastiger te misbruiken bij phishing. Criminelen kunnen jouw wachtwoord niet stelen als je er helemaal geen gebruikt.

Voor veel organisaties is dit een laagdrempelige manier om meteen stappen te zetten richting passwordless werken. Minder radicaal dan passkeys, maar wel een enorme verbetering ten opzichte van traditionele wachtwoorden of sms codes.

<WAT MOET JE DOEN?>

5. CONDITIONAL ACCESS

Niet elke inlogpoging is hetzelfde. Iemand die vanaf kantoor op een beheerd apparaat inlogt, vormt een ander risico dan iemand die vanaf een hotelkamer in het buitenland probeert binnen te komen.

Met Conditional Access stel je beleid op dat rekening houdt met de context van een inlog: locatie, apparaatstatus, risico-indicatoren en gebruikspatronen. Hierdoor kun je aanvullende controles afdwingen op risicovolle locaties en tegelijkertijd de dagelijkse ervaring voor medewerkers verbeteren doordat zij op vertrouwde plekken minder vaak opnieuw hoeven te authenticeren.

Het resultaat is een balans tussen veiligheid en gebruiksgemak, afgestemd op de realiteit waarin medewerkers werken.

<WAT MOET JE DOEN?>

6. INZICHT IN ACCOUNTS

Overzicht is cruciaal. Veel organisaties blijken vergeten accounts te hebben die al maanden of zelfs jaren niet meer gebruikt worden. Deze accounts vormen stille toegangspoorten die door criminelen kunnen worden misbruikt.

Door regelmatig inzicht te creëren in welke accounts actief zijn en welke kunnen worden verwijderd of gedeactiveerd, verklein je het aanvalsoppervlak aanzienlijk. Stel beleid in voor maximale levensduur van accounts en zorg dat toegang onmiddellijk wordt ingetrokken wanneer iemand de organisatie verlaat. Dit voorkomt dat verouderde of ongebruikte accounts onbewust een risico vormen.

<WAT MOET JE DOEN?>

7. SINGLE SIGN-ON (SSO)

Single Sign-On zorgt ervoor dat medewerkers met één centrale identiteit toegang krijgen tot verschillende systemen binnen de organisatie. Dit vermindert het aantal afzonderlijke wachtwoorden, waardoor het risico op zwakke plekken drastisch afneemt. Wanneer medewerkers minder inlogmethoden hoeven te onthouden, neemt de kans op fouten af en groeit de veiligheid vanzelf mee.

SSO biedt daarnaast meer consistentie, eenvoud en overzicht in het beheer van identiteiten: Wanneer een medewerker de organisatie verlaat is het een kwestie van een enkel account uitschakelen om direct alle toegang in te trekken.

</FUNCTIES OM OP TE LETTEN ALS JE EEN WACHTWOORDENMANAGER KIEST>

Een goede wachtwoordmanager biedt meer dan de opslag van wachtwoorden alleen. De volgende functionaliteiten zorgen in de praktijk voor de grootste impact:

Veilige gedeelde kluizen voor teams
Voor gedeelde accounts binnen afdelingen, zoals social media of leveranciersportalen. Dit voorkomt dat wachtwoorden via e-mail of chatberichten worden rondgestuurd.

Automatisch invullen zonder opslag in de browser
Browsers zijn niet ontworpen als veilige opslagplaats. Een professionele wachtwoordmanager neemt het gebruiksgemak over zonder concessies aan beveiliging.

Auditlogs voor beheerders
Overzicht is essentieel. Een dashboard dat inzicht geeft in gebruik, naleving en risico's, helpt organisaties om snel te handelen wanneer dat nodig is.

Herstel van toegang
Als iemand uitvalt of vertrekt, moet er altijd een gecontroleerde manier zijn om toegang over te nemen zonder dat wachtwoorden op straat belanden. Deze functies maken het beheer betrouwbaar en toekomstbestendig.

Authenticatie en wachtwoordbeheer vormen samen het fundament van moderne digitale veiligheid. Het is niet nodig alles tegelijk in te voeren of te compliceren. Begin met de basis, bouw stapsgewijs verder en maak veilige keuzes zo gemakkelijk mogelijk voor medewerkers. Daarmee zet je een grote stap naar een digitale omgeving die veilig, beheersbaar en toekomstbestendig is.

</AUTORISATIE OP MAAT>

Toegang verlenen is één ding. Bepalen wat iemand mag doen is een heel ander verhaal. Want als iedereen overal bij kan, en alles mag doen, heb je geen controle maar een risico. Autorisatie draait om het scheiden van verantwoordelijkheden en het beperken van schade bij misbruik van de rechten. Niet omdat je medewerkers niet te vertrouwen zijn, maar omdat misbruik of vergissingen anders te grote gevolgen krijgen.

Als iedereen alles kan, is één fout voldoende om de organisatie stil te leggen. Een verkeerd geklikte cruciale instelling, een kwaadwillende met te brede rechten of een stagiair die in systemen kan waar diegene niets te zoeken heeft. Een foutje kan gebeuren, alleen maar doordat niemand heeft bepaald waar de grenzen van een individu liggen. Goede autorisatie voorkomt deze situaties zonder in te leveren op productiviteit.

<AUTORISATIE>

NOOIT MEER STANDAARD WERKEN MET BEHEERDERSRECHTEN

Voor vrijwel elke organisatie, ook voor de kleinere mkb'er, is het cruciaal dat de accounts waaronder gewerkt wordt nooit standaard beheerdersrechten hebben, ook niet voor beheerders. Dit is nog regelmatig wel het geval en wordt gezien als "handig voor de IT er" of "even praktisch voor updates", maar het is in werkelijkheid één van de grootste risico's binnen bedrijven. Waarom? Omdat één fout genoeg is.

Stel je voor: Een medewerker krijgt een geloofwaardige phishingmail die lijkt te komen van Microsoft 365. De medewerker klikt, logt in op een nagemaakte pagina en zonder dat deze het merkt, heeft een aanvaller zijn sessie of token te pakken. Bij een normaal account levert dat vooral toegang tot mail op. Vervelend, maar te overzien. Maar wat als dit account ook beheerdersrechten heeft?

DAN ONTSTAAT ER EEN COMPLEET ANDER SCENARIO:

- Er is direct toegang tot alle systemen waar die beheerdersrechten toe reiken.
- De aanvaller kan nieuwe accounts aanmaken.
- Er kan heimelijk software geinstalleerd worden die niet opgemerkt wordt.
- Instellingen kunnen aangepast worden.
- Beveiligingsmechanismen kunnen uitgeschakeld worden.
- Back ups kunnen gewist worden.

Eén klik op een phishinglink kan dan uitmonden in volledige controle over het netwerk. Je hebt geen geavanceerde hack nodig; je geeft de 'keys to the kingdom' direct weg. Dit is precies waar veel aanvallen beginnen: een mens maakt



een fout, en beheerdersrechten maken de schade explosief groter. Maak daarom gebruik van normale account zonder bijzondere rechten voor de dagelijkse werkzaamheden, en gebruik een apart account voor de beheerderswerkzaamheden.

<AUTORISATIE>

ROLE-BASED ACCESS

Een autorisatiemodel moet duidelijk, schaalbaar en logisch zijn. Het moet nu werken, maar ook wanneer je een (groot) aantal nieuwe collega's erbij hebt. Het is om deze reden aan te bevelen om te gaan werken met Role-based Access

(RBAC). Dit betekent dat je een medewerker een gedefinieerd profiel met de minimaal noodzakelijke rechten toekend krijgt die passen bij de functie die deze persoon invult. Medewerkers met dezelfde functie krijgen hierdoor dezelfde toegang, omdat deze dezelfde 'functierol' toegewezen hebben gekregen. Dit voorkomt dat medewerkers individueel unieke en ongecontroleerde rechten opbouwen.

Je krijgt als nieuwe HR-medewerker het profiel "HR Employee" toegekend, en daarmee een "pakketje" met rechten dat geconfigureerd is om je toegang te geven tot data en functies die nodig zijn voor het uitvoeren van jouw functie. Zijn er voor de HR- medewerkers meer rechten nodig? Dan kunnen die rechten toegevoegd worden aan het profiel en zijn daarmee direct effectief voor alle HR-medewerkers. Mogen alle HR-medewerkers een specifieke actie niet meer uitvoeren? Kwestie van dit eenmalig aanpassen in het profiel: goed beheersbaar en voor iedereen gelijk.

Het gebruik van rollen maakt het ook mogelijk om verantwoordelijkheden helder te kunnen scheiden: De persoon die een factuur aanmaakt, kan deze niet goedkeuren en de persoon die technische wijzigingen voorstelt, kan deze niet direct doorvoeren.

Een goed RBAC-model hanteert het least-privilege principe: precies genoeg toegang, nooit meer.

<AUTORISATIE>

PERIODIEKE CONTROLE

Ook autorisatie is geen eenmalige instelling. Rechten die iemand ooit heeft gekregen maar al lang niet meer nodig heeft, vormen een risico. Opruimen dus. Zorg ervoor dat procesmatig elk half jaar toegekende rechten nagelopen worden en bij een functiewijziging rechten direct aangepast worden, waarbij oude rechten vervallen. Consistent controleren houdt de risico's klein en beheersbaar.

Autorisatie is geen bureaucratische last.
Het is één van de meest effectieve manieren om risico's te beperken. Met duidelijke rollen, gescheiden verantwoordelijkheden en regelmatige controles bouw je aan een organisatie die veilig én beheersbaar blijft.

</PRODUCTEN, LICENTIES EN KEUZES>

Na oriëntatie heb je een shortlist met producten die je organisatie gaan helpen: je maakt waarschijnlijk een afweging tussen Microsoft 365 en Google Workspace, wachtwoordmanagers, back-uptools, en ga zo maar door. Ongeacht welke keuzes je maakt: voor het gebruik van deze software is vervolgens een licentie nodig. Je hebt ze nodig om te kunnen werken, maar het aanbod is overweldigend en elk pakket belooft nét iets anders, maar zegt wel het gouden ei te hebben. Veel organisaties kopen daarom óf te veel, óf te weinig: beide met onnodige risico's en kosten. Met onderstaande tips kun je praktisch bepalen wat je wel en niet nodig hebt.

<PRODUCTEN, LICENTIES EN KEUZES>

WAT HEB JE ÉCHT NODIG?

De keuze voor de passende producten en bijbehorende licenties begint niet bij het advies van de leverancier, maar bij jouw eigen organisatie. Stel jezelf vier vragen:

- **Welke processen zijn cruciaal voor je organisatie?**
  Niet alles hoeft in de hoogste versnelling te draaien. Welke processen zijn echt onmisbaar voor jouw organisatie: de activiteiten die stilstand veroorzaken als ze niet werken? Denk aan zaken zoals facturatie, klantcommunicatie, planning, productie, of het verwerken van bestellingen. Welke systemen, accounts en gegevens zijn hiervoor noodzakelijk, en wat heb je nodig om deze processen zonder onderbreking veilig te kunnen blijven uitvoeren?

- **Waar zit je risico?**
  Risico's die een dreiging vormen zijn voor iedere organisatie anders. Voor de ene is een datalek van het klantenbestand een kritieke klap, voor de ander is dit wellicht het niet continu kunnen aanbieden van diensten. Maak een risicomatrix (risico = kans * impact) en bepaal welke risico's extra goed afgedekt moeten zijn.

- **Hoe volwassen is je organisatie?**
  Net zoals bij beveiliging geldt ook hier: je hoeft niet alles meteen perfect te regelen. Begin met wat echt nodig is en bouw stap voor stap door, steeds een beetje beter.

- **Welke wettelijke verplichtingen gelden voor jouw organisatie?**
  Controleer of jouw organisatie onder de NIS2 wetgeving valt en welke verplichtingen daaruit volgen. Denk aan strengere eisen op het gebied van risicobeheer, incidentmelding en continuïteitsmaatregelen. Weten wat er van je wordt verwacht voorkomt gedoe achteraf en helpt bij het maken van de keuzes wat je nodig hebt. Een goed startpunt is het NIS2 overzicht van het Digital Trust Center: https://www.digitaltrustcenter.nl/nis2/nis2-in-een-oogopslag

<PRODUCTEN, LICENTIES EN KEUZES>

WAAROM EEN STERKE BASIS GELD BESPAART

Veel bedrijven ontdekken pas te laat dat ze jarenlang licenties betaalden die ze nooit gebruikten, of juist essentiële functies misten toen het erop aankwam. Een goede basis voorkomt:

- Over dubbele tools beschikken die hetzelfde doen
- Gaten in je beveiliging of processen die je dacht afgekadert te hebben
- Dure herinrichtingen omdat de verkeerde licenties zijn gekozen

Daarnaast is het belangrijk waar je begint. Starten bij een willekeurige hostingpartij “die ook e mail kan doen” klinkt aantrekkelijk, maar zorgt in de praktijk al snel voor beperkingen. Dit varieert van het ontbreken van een solide agenda functionaliteit tot het missen van moderne beveiligingsopties. Een solide fundament voorkomt dat je later weer moet overstappen, extra kosten maakt of alsnog gaten moet dichten die je eenvoudig had kunnen voorkomen.

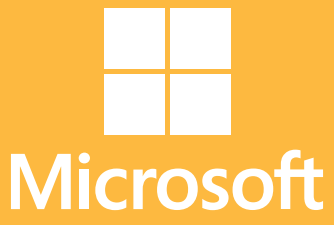
<PRODUCTEN, LICENTIES EN KEUZES>

INZOOMEN OP MICROSOFT: HOE MAAK JE SLIMME KEUZES?

Microsoft biedt een enorm portfolio: van basisproductiviteit tot geavanceerde beveiliging en compliance, maar het uitpluizen van de licenties is verre van eenvoudig. Veel organisaties gebruiken maar een fractie van waar ze voor betalen, simpelweg omdat ze niet helder hebben wat elke bundel doet. Voor de meeste organisaties vormt één van de Microsoft 365 bundels het technisch fundament. Het belangrijkste verschil zit meestal in:

- **Beveiliging** (MFA, identity beheer, e mailbeveiliging)
- **Apparaatbeheer** (policies, updates, compliance)
- **Gegevensbescherming** (Data Loss Prevention, versleuteling, back ups)

Veel bedrijven kopen losse tools voor dingen die al in hun pakket zitten, denk aan e mailfiltering, endpoint beveiliging en apparaatbeheer. Vaak blijkt dat Microsoft al prima (of zelfs betere) opties biedt binnen de licenties die je tóch al hebt.



<PRODUCTEN, LICENTIES EN KEUZES>

MINIMALE MICROSOFT- BEVEILIGINGSFUNCTIES DIE JE ECHT WILT GEBRUIKEN

Wanneer je binnen het Microsoft ecosysteem werkt, zijn er een paar beveiligingsfuncties die eigenlijk geen luxe zijn maar pure noodzaak. Dit zijn de voorzieningen die de basis vormen van een moderne digitale verdediging zonder complexe inrichting, maar met grote impact. Zie het als de rookmelders, brandblussers en sloten van je digitale kantoor: klein, maar onmisbaar door hun sterke impact.

<BEVEILIGINGSFUNCTIES>

SAFE LINKS

Phishing is nog altijd het grootste risico voor organisaties. Safe Links controleert links in e mails en documenten realtime, ook wanneer criminelen een link achteraf aanpassen. Zo voorkom je dat één klik op een “factuur” verandert in een ransomware incident of diefstal van inloggegevens.

Belangrijk om te weten: Safe Links is niet alleen beschikbaar in Microsoft 365 Business Premium, maar kan ook worden afgenomen als losse add on voor andere abonnementen, zoals Microsoft 365 Business Basic, Standard of zelfs standalone Exchange Online. Daardoor kan vrijwel elke organisatie dit extra beveiligingsniveau inzetten, zonder direct van pakket te hoeven wisselen.

<BEVEILIGINGSFUNCTIES>

SAFE ATTACHMENTS

Aanvallers verstoppen vaak malware in ogenschijnlijk onschuldige bijlagen. Safe Attachments opent bestanden eerst in een geïsoleerde omgeving. Pas als ze veilig blijken, komen ze bij de gebruiker aan.

<BEVEILIGINGSFUNCTIES>

IDENTITY PROTECTION

Denk aan verplichte MFA, bescherming tegen brute force aanvallen en risicogebaseerde toegang. Deze functies zorgen ervoor dat één gestolen wachtwoord niet meteen betekent dat iemand je hele organisatie binnenloopt. Identiteit is, zoals in dit Digitaal Kompas beschreven, je eerste verdedigingslinie.

<PRODUCTEN, LICENTIES EN KEUZES>

DEFENDER FOR ENDPOINT (LICHTE VARIANT)

Apparaatbeveiliging die malware blokkeert en verdachte processen stopt voordat ze schade kunnen veroorzaken, is een absolute must. Met de toename van remote en hybride werken is dit allang geen luxe meer.

ADEQUATE E-MAILBEVEILIGING

<E-MAILBEVEILIGING>

HOE SPF, DKIM EN DMARC JE ORGANISATIE BESCHERMEN

E-mail is nog altijd hét communicatiemiddel binnen organisaties. Offertes, facturen, klantvragen, interne communicatie: het gaat allemaal vaak nog via hetzelfde kanaal. Maar juist omdat e-mail zo belangrijk is, is het ook een van de favoriete doelwitten van cybercriminelen. Wat veel ondernemers niet weten: Zonder goede beveiliging kan iedereen e-mails versturen namens jouw domein. En dat gebeurt ook daadwerkelijk. Dagelijks.

Criminelen sturen dan bijvoorbeeld phishingmails vanuit wat lijkt op jouw adres, vragen klanten om betalingen aan te passen, of verspreiden malware alsof het van jou komt. Jij merkt er niets van, totdat de schade al is aangericht en relaties verhaal komen halen.

Gelukkig zijn er drie relatief eenvoudige maatregelen die dit voorkomen: SPF, DKIM en DMARC. Veel bedrijven hebben ze “ergens wel aangezet”, maar vaak niet goed ingericht. Het resultaat: schijnveiligheid. En daar heb je niets aan. Hier leggen we je in begrijpelijke taal uit wat ze doen en waarom het belangrijk is dat ze goed staan.

<SPF>

WIE MAG ER NAMENS JOU MAILEN?

Wat SPF doet: SPF kun je zien als een gastenlijst voor je e-mail. Je vertelt hiermee: “Deze servers mogen e-mail versturen namens mijn domein, en alle anderen niet.”

Waarom dit belangrijk is: Zonder SPF kan iedereen doen alsof hij vanaf jouw domein mailt. Criminelen kunnen dan phishing sturen die bijna niet van echt te onderscheiden is. Met een goed ingestelde SPF-record wordt ongeautoriseerd gebruik geblokkeerd of gemarkeerd als verdacht bij de ontvangende partij.

In gewone taal: SPF checkt **waar** de e-mail vandaan komt.

<DKIM>

IS DE MAIL ONGEWIJZIGD AANGEKOMEN BIJ DE ONTVANGER

Wat DKIM doet: DKIM plakt als het ware een digitale handtekening onder elke mail die jouw organisatie verstuurt. De ontvangende server kan daardoor controleren of het bericht onderweg niet is aangepast.

Waarom dit belangrijk is: Zonder DKIM kunnen aanvallers e-mails manipuleren of nepberichten versturen die technisch bijna niet van echt te onderscheiden zijn. DKIM voorkomt dat criminelen meegestuurde informatie kunnen aanpassen.

In gewone taal: DKIM checkt of de inhoud klopt en onderweg niet is gewijzigd.

<DMARC>

WAT TE DOEN ALS ER IETS NIET KLOPT

Wat DMARC doet: DMARC is de regelkaart die vertelt wat er moet gebeuren als SPF of DKIM falen.

Dit kan op de volgende manieren ingesteld worden:

- **none**: doe niets (alleen rapporteren)
- **quarantine**: zet verdachte mail in de spambox
- **reject**: blokkeer de mail volledig

Waarom dit belangrijk is: DMARC is de enige maatregel die ervoor zorgt dat misbruik van jouw domein daadwerkelijk wordt gestopt. Veel bedrijven zetten DMARC wel aan, maar laten de policy op ‘none’. Dat is alsof je een alarmsysteem hebt dat niet aanstaat. Met een goed ingestelde DMARC configuratie (liefst quarantine of reject) verklein je de kans op domeinmisbruik enorm en zorg je ervoor dat jouw legitieme e-mails juist beter aankomen.

In gewone taal: DMARC bepaalt wat er moet gebeuren als er iets verdachts wordt gevonden.

<E-MAILBEVEILIGING>

WAAROM IS DIT ZO BELANGRIJK?

Zodra criminelen namens jouw domein gaan mailen, is de schade groot:

- Klanten maken geld over naar fraudeurs.
- Je domein wordt op zwarte lijsten gezet.
- Je reputatie krijgt een klap waar je de gevolgen nog lang van zal merken.
- Jouw eigen legitieme mail komt niet meer aan.

En dat alles zonder dat je het direct doorhebt. In de vorige editie van het Digitaal Kompas benoemden we al dat e-mail een van de meest misbruikte aanvalskanalen is. Dat is onveranderd. Door SPF, DKIM en DMARC goed in te stellen, voorkom je dat jouw organisatie in zo’n scenario terechtkomt.

</HOE STEL IK DIT IN>

Oké, eerlijk is eerlijk: dit gedeelte is een beetje technisch. Maar het is wel belangrijk. Zie het als het instellen van een goed slot op je voordeur: je hoeft niet precies te weten hoe het mechanisme werkt, maar je moet wel zorgen dat het goed dicht zit. En als je twijfelt: vraag dan ondersteuning bij iemand die hier ervaring mee heeft. Hier volgt een beknopte uitleg per maatregel:

<SPF>
INSTELLEN

- Je voegt in de DNS instellingen van je domein een **SPF record** toe.
- Daarin geef je aan welke mailservers namens jouw domein mogen versturen.
  Voorbeeld: v=spf1 include:mailprovider.nl -all

<DKIM>
INSTELLEN

- Je e mailprovider genereert een **DKIM sleutel**.
- Deze sleutel plaats je als DNS record in jouw domein.
- Daarna worden e mails automatisch digitaal “ondertekend”.

<DMARC>
INSTELLEN

- Je maakt een **DMARC record** aan in je DNS.
- Je kiest een policy: none, quarantine of reject.
- Start desnoods op none, maar het uiteindelijke doel is **reject** voor maximale bescherming
- Een handige stap voor stap uitleg vind je hier:
  https://www.brandaris.it/nl/nieuws/van-none-naar-reject-stap-voor-stap-grip-op-je-e-maildomein~x3nCdXvC/

Houd er rekening mee dat, mocht je van hostingpartij en/of mailprovider wisselen, deze instellingen gelijktijdig opnieuw doorlopen moeten worden om te zorgen dat je mail goed blijft werken.



</BACKUPS:

JE LAATSTE REDDING, ALS JE ZE GOED REGELT>

Je denkt er liever niet over na: dat moment waarop je een map opent en alle bestanden versleuteld zijn. Of wanneer je mailbox op maandag opent, en deze blijkt leeg te zijn. Of wanneer een medewerker per ongeluk belangrijke klantdata verwijdert en het pas drie weken later ontdekt. Foutje, kan gebeuren.

Dataverlies hoeft niet eens het gevolg te zijn van een hacker in een donker kamertje aan de andere kant van de wereld. Eén fout, één klik, één corrupte bestandssynchronisatie in de cloud kan genoeg zijn om waardevolle bedrijfsinformatie kwijt te raken. En zonder een goede back up is er geen weg terug.

Toch zien veel organisaties back ups nog steeds als een bijzaak dat ooit nog een keer geregeld moet worden. Of als iets dat de IT partij “wel regelt”. Maar zoals je in de vorige editie van het Digitaal Kompas al kon lezen: cybercriminelen proberen doelbewust ook je back ups te versleutelen of onbruikbaar te maken. Laat het daarom duidelijk zijn: Een back up die niet te herstellen is, is gewoon géén back up.

<BACKUPS>

WAAROM BACK-UPS ZO BELANGRIJK ZIJN

Er zijn ontzettend veel situaties denkbaar waarin een back-up nodig kan zijn. Deze kunnen je bijvoorbeeld beschermen bij:

Menselijke fouten: De meest voorkomende oorzaak van dataverlies is geen hacker, maar een medewerker die per ongeluk iets verwijdert of overschrijft.

Technische storingen: Een corrupte mailbox of een crashende laptop met cruciale informatie kan meer schade aanrichten dan je in eerste instantie misschien denkt.

Ransomware: Cybercriminelen scannen je netwerk en versleutelen je bestanden. Als je dan geen functionele backup hebt sta je machteloos.

Synchronisatieproblemen in cloudplatformen: Cloudopslag is handig, maar is géén garantie tegen dataverlies. Als een bestand in OneDrive of SharePoint wordt verwijderd of overschreven, wordt dat netjes gesynchroniseerd, inclusief de fout.

Voor clouddiensten geldt doorgaans: De dienstleverancier is verantwoordelijk voor de beschikbaarheid van de dienst, je bent zelf verantwoordelijk voor je eigen data. Er worden functionaliteiten aangeboden voor bijvoorbeeld ‘prullenbakken’ en versioning, maar dit is geen gelijkwaardig alternatief voor een volledige backup.

<BACKUPS>

WAT EEN GOEDE BACKUP ECHT BETEKENT

Een back up is pas waardevol als je hem kunt terugzetten. Dat klinkt vanzelfsprekend, maar in de praktijk gaat het hier vaak mis. Dit is wat veel bedrijven denken dat een back up is: “We hebben toch iets in de cloud? OneDrive bewaart toch versies?” Maar dit is wat het werkelijk moet zijn:

Automatische back ups van alle belangrijke systemen
Niet af en toe. Niet “als iemand eraan denkt”. Dagelijks, automatisch, gecontroleerd en betrouwbaar.

Minimaal één back up die níet verbonden is met je netwerk
Ransomware houdt geen rekening met jouw planning. Ransomware groepen weten heel goed dat bedrijven afhankelijk zijn van back ups. Ze scannen bewust naar:

- gekoppelde NAS apparaten,
- back upservers,
- cloudvolumes die als schijf gekoppeld zijn,
- synchronisatie mappen.

Als ze die vinden, versleutelen ze deze of wissen ze de back-ups compleet. Een offline, 'air gapped' back up voorkomt dat criminelen je met lege handen laten staan. Maak bij voorkeur gebruik van de 3-2-1- regel om echt veilig te zijn:

- 3 kopieën
- 2 verschillende media
- 1 offline

Back ups moeten versleuteld zijn

Back-ups bevatten al je cruciale informatie. Wanneer je back-ups niet versleuteld zijn en een aanvaller krijgt hier toegang toe, heeft deze ook toegang tot je belangrijkste bedrijfsinformatie.

Terugzetten moet regelmatig getest worden

De belangrijkste stap die bijna niemand doet. Veel organisaties ontdekken pas dat er bij het maken van hun back-up iets misging op het moment dat ze deze nodig hebben.

<BACKUPS>

WAT KUN JE NU AL DOEN?

- Zorg dat er dagelijks automatische back ups worden gemaakt van alle kritieke data.
- Maak minstens één offline back up.
- Test maandelijks of het terugzetten van de back-ups werkt.
- Documenteer wie toegang heeft tot de back ups en beperk dat tot het minimum. Gebruik geen generieke accounts.
- Back ups horen binnen het reguliere netwerk te staan "zodat het makkelijk is". Je maakt het dan niet alleen jezelf makkelijk.
- Maak escalatieplannen voor het geval het toch misgaat en de back-ups ingezet moeten worden: wie bel je, welke stappen zijn het belangrijkst en welke systemen moeten als eerste hersteld worden?



</AFSLUITING>

Cybersecurity voelt soms als een enorme berg: veel keuzes, veel technieken, veel risico's. Maar zoals je in dit Digitaal Kompas hebt gelezen, draait het uiteindelijk om slechts enkele keuzes en werkwijzen die je organisatie vanaf het begin direct voorzien van een sterk fundament dat mee kan groeien. Geen ingewikkelde theorieën, geen dure projecten die na een jaar weer in de la verdwijnen, maar praktische stappen die elke ondernemer kan zetten.

Het belangrijkste inzicht? Je hoeft niet alles tegelijk te regelen. Het gaat er om dat je begint en dat je blijft bewegen. Met een solide basis voor authenticatie, autorisatie, wachtwoordbeheer, slimme licentiekeuzes en betrouwbare backups maak je jezelf al direct minder aantrekkelijk voor cybercriminelen. En dat is precies waar moderne beveiliging om draait: risico's verkleinen, controle vergroten, rust creëren.

Cyberdreigingen veranderen, maar jij kunt meebewegen zonder je organisatie te verlammen. Door bewust te kiezen, regelmatig te toetsen en het simpel te houden, bouw je een digitale omgeving die klaar is voor groei en tegen een stootje kan. Blijf nieuwsgierig. Blijf verbeteren. En vooral: blijf bouwen aan dat fundament dat jouw organisatie sterk houdt, vandaag én morgen.

Wil je sparren over hoe jouw fundament ervoor staat of waar de grootste winst te behalen valt? Je weet ons te vinden. Gewoon eerlijk advies, precies zoals je van ons gewend bent



<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION<SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD> VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION><SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE> AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY <BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIR S><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION><SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVAC ><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION<SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION><SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION<RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>



<BRANDARIS CYBERSECURITY B.V.>
Keesomstraat 10-G
1821 BS Alkmaar

+31 (0)72 202 97 95
info@brandaris.it
www.brandaris.it

<KVK> 94696675
<BTW> NL866862833B01
<IBAN> NL58REVO7619561102
<BIC> REVONL22

