

OFFICE 365

**ER IS GEEN
ONTKOMEN AAN**

CEO-MAILS

*een gewaarschuwde
organisatie telt
voor twee*

**HELP!
DE SERVER IS
(WEER) TRAAG!**

**NA DE AVG
KOMT NU DE ePV**

Wat betekent dat?

**BEVEILIGD
E-MAILS VAN
BESTANDEN: DÉ
OPLOSSING**

OEI, IK GROEI!

*9 ICT-tips voor als
uw organisatie uit
zijn jasje groeit*

IS UW SERVER AAN VERVANGING TOE?

GRATIS SECOND OPINION OP UW COMPUTERNETWERK?
KIJK OP **OBI.NL** OF BEL **088 - 900 8100**

SERVER- EN WERKPLEKBEHEER | ONLINE WERKPLEKKEN | WIFI
VOIP TELEFONIE | OFFICE 365 | GEGEVENSBEVEILIGING

OBI, Hét ICT team

Systeembeheerders die met u meedenken!



Beste lezer,

Zoals u op de cover van onze magazines kunt lezen wordt **BITS&BYTES** speciaal uitgegeven voor managers en ondernemers die op de hoogte willen blijven van relevant ICT-nieuws. Daarom vindt u ook in deze vijfde uitgave weer een schat aan waardevolle ICT-informatie.

Zoals bijvoorbeeld het artikel over Office 365 op pagina 4. Hierin leest u niet alleen wat Office 365 nu eigenlijk is, maar ook over de voor- en nadelen van deze software.

De trouwe **BITS&BYTES** lezer zal verwachten dat ook deze keer weer veel over de AVG geschreven wordt. Dat is niet helemaal het geval. Wel hebben we het over de ePV, het broertje van de AVG. Deze verordening richt zich speciaal op het juridisch gebied rondom digitale privacy.

In dit nummer waarschuwen we u voor CEO-mail. In het artikel 'CEO-mails; een gewaarschuwde organisatie telt voor twee' leest u hoe u en uw medewerkers CEO-fraude kunnen herkennen en voorkomen.

Getriggerd door een van de artikelen in deze **BITS&BYTES**, is uw server aan vervanging toe of bent u op zoek naar een systeembeheerder die met u meedenkt? Neem dan contact op met Hét ICT Team van OBI. Wij zijn u graag van dienst. Want OBI zorgt dat ICT werkt. Altijd. Overal.

Ik wens u veel leesplezier toe,

Roger Zweegers
Directeur OBI Automatisering



COLOFON

BITS&BYTES is een uitgave van:
OBI Automatisering
De Hooge Akker 10 b
5661 NG Geldrop
088 - 900 8100
info@obi.nl
obi.nl

Redactie:
Serge van Uden
Riumssen B.V.
hello@riumssen.nl
riumssen.nl

Vormgeving:
Brit grafisch werk
info@brit.nu
brit.nu



Ondanks de constante zorg en aandacht die OBI en Riumssen aan de samenstelling van deze uitgave van **BITS&BYTES** hebben besteed is het mogelijk dat de informatie die in dit magazine wordt gepubliceerd onvolledig c.q. onjuist is. OBI en Riumssen aanvaarden dan ook geen aansprakelijkheid voor enigerlei directe of indirecte schade, van welke aard ook, die voortvloeit uit of in enig opzicht verband houdt met het gebruik van **BITS&BYTES**.

inhoud

- p. **4** Office 365: er is geen ontkomen aan
- p. **8** Oei, ik groei! 9 ICT-tips voor als uw organisatie uit zijn jasje groeit
- p. **11** Beveiligd e-mailen van bestanden: dé oplossing
- p. **14** CEO-mails: een gewaarschuwde organisatie telt voor twee
- p. **17** Na de AVG komt nu de ePV: wat betekent dat?
- p. **20** Help! De server is (weer) traag!

Office 365: er is geen ontkomen aan

De kans is groot dat u al vaker heeft gehoord over Office 365 van Microsoft. Logisch, want door de sterke marketpush vanuit de ICT-branche is er bijna geen ontkomen aan. Maar is Office 365 eigenlijk wel de beste optie voor uw bedrijf? En zo ja, op welke manier dan? Wij leggen u graag uit wat de voor- en nadelen zijn van de software en waar u aan moet denken als u de keuze maakt om het pakket wel of niet te implementeren binnen uw bedrijf.

Meest gebruikte softwareplatform

Sinds de lancering in 2012 is Office 365 snel een begrip geworden in het bedrijfsleven. Daarom is het nu het meest gebruikte softwareplatform om samen mee aan documenten te werken. Uit onderzoek van Barracuda Networks bleek dat in oktober 2017 al 62% van alle Europese bedrijven gebruikmaakt van de Microsoft-dienst. Dat komt enerzijds doordat het pakket laagdrempelig en veelzijdig is. Anderzijds heeft het ook zeker te maken met de zeer interessante prijs

van de mailserver van Office 365. Dat maakt het wel heel makkelijk om over te stappen van uw huidige server naar Office 365. Het is immers voordelig en het overstappen is zo geregeld.

Zie Office 365 als een vervanger van uw fileserver en Exchange-server in de cloud. Het addertje onder het gras is dat Microsoft gebruikers van Office 365 eigenlijk dwingt om ook Word, Excel en PowerPoint af te nemen. Want bijna

alle applicaties op de markt hebben wel een koppeling met Office of Exchange, zodat u bijna verplicht bent om ook de traditionele Office-programma's te gebruiken. Een groeiend bedrijf heeft naast een mailserver vaak ook documentruimte nodig. Dat faciliteert Office 365 door naast de mailserver Outlook ook cloudopslag te bieden in de vorm van SharePoint. Zo wordt het uitwisselen van bestanden en het tegelijkertijd werken aan documenten heel eenvoudig. Net als het delen van agenda's.

De voordelen van Office 365

• Delen van agenda's en bestanden

Zodra een medewerker wijzigingen aanbrengt in een document, is altijd te herleiden wie wat heeft veranderd en wanneer dat is gebeurd. Ook het samenwerken met externe partijen of medewerkers op andere locaties wordt hiermee heel eenvoudig. Ieders aandeel in het geheel is direct zichtbaar. Dat scheelt veel tijd en (mis) communicatie.

• Opslag in de cloud

Dat ene bestand dat uw medewerker op het werk heeft opgeslagen en tijdens het thuiswerken niet meer kan bewerken? Dat probleem is opgelost. Office 365 zorgt namelijk voor altijd toegankelijke opslag in de cloud met OneDrive voor Bedrijven. Uw medewerkers kunnen, eventueel samen met hun collega's, op elk moment op elke plek aan hun documenten werken. Het steeds weer opnieuw opslaan van bestanden, waardoor er meerdere versies in omloop kunnen zijn, is daardoor verleden tijd. Bovendien is de opslagruimte van de cloud oneindig groot.

• Geen grote investeringen

Met Office 365 is uw bedrijf 365 dagen per jaar online, zonder dat u daarvoor grote investeringen hoeft te doen. Voorheen moest een bedrijf ongeveer elke 5 jaar nieuwe hardware en software aanschaffen om up-to-date te blijven. Dankzij het abonnementsmodel van Office 365 kunt u direct aan de slag, terwijl u een relatief klein bedrag betaalt per maand of jaar. →

Office 365: wat is dat nu eigenlijk?

Vergeet de vorige versies van Microsoft Office die u kent van vroeger. Ja, in Office 365 kunt u ook Word, Excel en PowerPoint gebruiken, maar de basis van het systeem is eigenlijk veel eenvoudiger. Office 365 is een online mailserver (Outlook) en biedt cloudopslag (zoals Dropbox) in de vorm van SharePoint. Zo wordt het uitwisselen van bestanden en het tegelijkertijd werken aan documenten heel eenvoudig. SharePoint is een veilige locatie voor het opslaan, organiseren, delen en gebruiken van informatie vanaf elk apparaat. Uw medewerkers hebben alleen een webbrowser nodig, zoals Microsoft Edge, Internet Explorer, Chrome of Firefox. Zie Office 365 als een vervanger van uw fileserver en Exchange-server in de cloud.

- **Communicatie op vele manieren**

Zonder dat uw medewerkers fysiek bij elkaar hoeven te zitten, kunnen zij op verschillende manieren met elkaar overleggen. Bijvoorbeeld via Instant messaging, videochat, Skype for Business of Microsoft Exchange Online. Daarnaast is er het sociale bedrijfsnetwerk Yammer, een onderdeel van Office 365. Hiermee kunnen teams hun eigen communicatiekanaal opzetten, ongeacht de locatie.

- **Bekende software die gewoon werkt**

Uw kantoormedewerkers zijn stuk voor stuk bekend met Microsoft Office. Daarom is de stap naar Office 365 maar heel klein. Zij kennen Excel, Word, PowerPoint, Exchange en andere Office-programma's al jaren. Daardoor verloopt de overgang naar Office 365 veel sneller dan wanneer uw hele bedrijf met nieuwe software gaat werken.

De nadelen van Office 365

- **Eenmaal gekozen, altijd gekozen**

Als u eenmaal de keuze heeft gemaakt voor Office 365, dan is overstappen naar een ander pakket wel écht een uitdaging. U krijgt van Microsoft veel terabytes aan opslagruimte voor bestanden en mail. Maar voordat u dat allemaal gemigreerd hebt... Dat zou je een bepaalde mate van lock-in kunnen noemen.

- **Ook in slechte tijden een abonnement**

Met eigen serverhardware kunt u in slechtere tijden makkelijk beslissen om nog een jaartje door te gaan zonder investeringen te doen. Met Office 365 zit u altijd vast aan het abonnementsgeld dat u betaalt per maand of jaar. Deze kosten lopen continu door.

- **Microsoft kan de prijs omhoog gooien**

U betaalt een abonnementsbedrag voor Office 365. Maar wie zegt dat dit bedrag altijd hetzelfde blijft? Microsoft kan zomaar de prijs flink verhogen, want de fabrikant weet dat overstappen naar een ander pakket niet zomaar gebeurt. Dat blijft dus altijd een risico.

- **Aan de cloud kleven altijd risico's**

Misschien heeft u nog nooit nagedacht over een 'cloud crash', maar zo'n ramp kan zomaar een keer voorvallen. Net zoals clouddiensten gehackt kunnen worden. In beide gevallen loopt u risico's als u een clouddienst gebruikt zoals Office 365. Terwijl u zeker wilt weten dat u alles goed geregeld heeft en dat de software altijd werkt.

Zijn er ook alternatieven?

Ja, die zijn er. Wanneer we een online concurrent willen noemen die ook een mailserver, online opslag, gedeelde agenda's en bewerkingsprogramma's aanbiedt, dan komen we uit op G Suite van Google. Dit pakket kan alles wat Office 365 ook kan. Maar doordat veel bedrijven toch al werken met software van Microsoft, is voor hen de overstap naar Office 365 beter te overzien.

"Office 365 is een online mailserver (Outlook) en biedt cloudopslag in de vorm van SharePoint"

Een ander alternatief is een lokale server of een private cloud. Dit zijn opties voor bedrijven die niet willen dat hun documenten in een 'externe' cloud opgeslagen worden. Bijvoorbeeld om privacyredenen, vanuit beveiligingsoogpunt of om het risico te voorkomen dat de cloud 'down' gaat.

Vraag uw IT-partner om maatwerkadvies

Het is belangrijk om de specifieke mogelijkheden van Office 365 voor uw bedrijf te onderzoeken. Zorg dus dat u een partner vindt die u kan ondersteunen met maatwerk en advies. Maak een bewuste keuze door goed uw opties op een rij te laten zetten. Vraag uw IT-partner gerust naar vorige implementaties die zij hebben uitgevoerd en naar hun ideeën voor uw specifieke situatie. Zo komt u er vanzelf achter of er een match is.

(advertentie)

OVERSTAPPEN NAAR OFFICE 365?

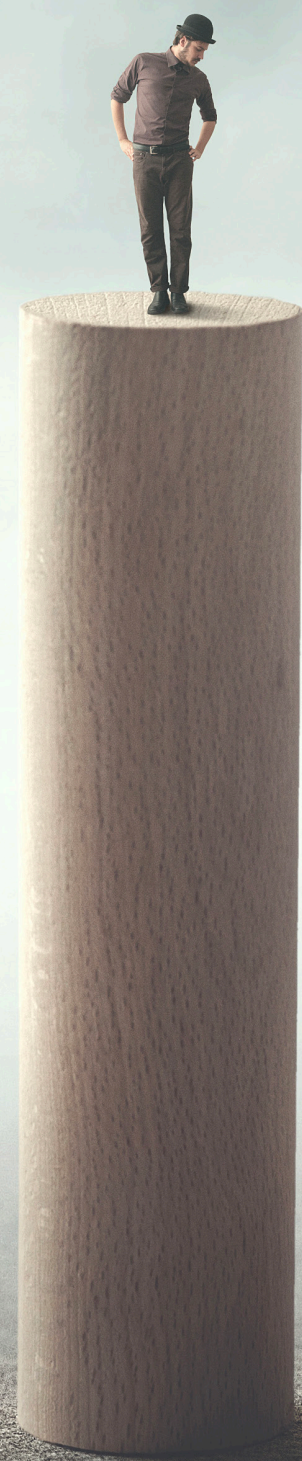
HÉT ICT TEAM VAN OBI ONDERSTEUNT U MET MAATWERK EN ADVIES.

Bel of mail ons voor een gratis Office 365 update gesprek.

obi.nl | 088-9008100 | info@obi.nl



SERVER- EN WERKPLEKBEHEER | ONLINE WERKPLEKKEN | WIFI
VOIP TELEFONIE | OFFICE 365 | GEGEVENSBEVEILIGING



Oei, ik groei!

9 ICT-tips voor als uw organisatie uit zijn jasje groeit

De vaart zit er lekker in: uw bedrijf heeft de wind in de zeilen en groeit als kool. Meer mensen, meer opdrachten en meer omzet, heerlijk! Maar kan uw ICT deze groei eigenlijk wel bijbenen? Juist bij groeiende organisaties is dit vaak een bottleneck. Wij vertellen u wat u eraan kunt doen om zo toekomstbestendig mogelijk te zijn op ICT-gebied.

Groeit mijn ICT dan niet automatisch mee?

Was het maar waar. De ICT-oplossingen die u aanschaft, zijn afgestemd op uw behoefte op dat moment. En dat geldt ook voor de ondersteuning die u inkoopt bij externe partijen. U zult merken dat deze ICT-ondersteuning minder betrouwbaar wordt op de piekmomenten als het druk is op kantoor. Uw ICT-leverancier kampt dan misschien met onderbemanning of heeft niet de kennis om uw gegroeide organisatie nog te kunnen helpen. Daarom is het belangrijk om altijd een ICT-leverancier te kiezen die uw groei kan bijbenen.

Ook de bestaande infrastructuur groeit niet zomaar mee met uw bedrijf. Een simpel voorbeeld: een bestaand WiFi accesspoint kan 20 aansluitingen misschien makkelijk aan. Maar het is niet geschikt om 100 verschillende aanmeldingen te verwerken. En als u 40 medewerkers heeft, dan wilt u

“Uw bestaande infrastructuur groeit niet zomaar mee met uw bedrijf”

die toch niet afhankelijk laten zijn van één switch of één server? De kans dat er iets mee gebeurt is klein, maar de impact is groot. Het is dan ook een verstandige overweging om toch een extra ‘redundant’ apparaat aan te schaffen.

Wat is ISO 27001?

ISO 27001 is de internationale norm voor het Information Security Management System (ISMS). Met een ISO 27001 certificering voldoet u aantoonbaar aan de informatiebeveiligingseisen van uw (potentiële) klanten. Daarnaast neemt u hierin ook de maatregelen voor de nieuwe privacywetgeving mee. Met een ISO 27001 certificering laat u zien dat uw organisatie een procesmatige aanpak hanteert bij het vaststellen, implementeren, bewaken, onderhouden, uitvoeren en verbeteren van informatiebeveiliging.

Het geeft u de vrijheid om te ondernemen en te innoveren in de wetenschap dat uw informatiebeveiliging altijd op orde is en blijft. Daarnaast specificiert ISO 27001 eisen voor het implementeren en beheersen van beveiligingsmaatregelen. U kunt dan denken aan bescherming van persoonsgegevens, bescherming tegen inbraak, hackers en datalekken. ISO 27001 heeft als doel de vertrouwelijkheid, beschikbaarheid en integriteit van informatie en informatiesystemen te garanderen.

Groei kan ook leiden tot onveiligheid

Als uw organisatie hard groeit, worden niet alleen de technische grenzen van uw ICT-infrastructuur opgezocht. Ook de veiligheidsgrenzen kunnen dan makkelijker overgegaan worden door kwaadwillenden. De beveiliging op gebied van ICT is vaak verbonden aan sociale controle op de werkvloer bij kleine bedrijven tot 20 medewerkers.

Als er dan iemand binnen komt lopen die u niet kent, worden er meteen vragen gesteld. Dit is niet meer het geval als er 100 medewerkers rondlopen. Het gaat helemaal naar een ander niveau wanneer er 500 mensen rondlopen. Dan wordt beveiliging een proces. En dit is ook de reden waarom het voor veel ICT-bedrijven moeilijk is om mee te groeien met uw organisatie. Zij kunnen dit proces niet faciliteren.

Om onveiligheid te voorkomen, is het bijvoorbeeld verstandig om de veiligheid van uw ICT-systemen op regelmatige basis te laten

testen. Een penetratietest (ook wel pentest genoemd) is in dat geval heel nuttig. Dit is een test van een of meer computersystemen op kwetsbaarheden, waarbij de gevonden kwetsbaarheden ook daadwerkelijk gebruikt worden om in deze systemen in te breken. Na afloop weet u precies wat u en uw ICT-partner te doen staat om de veiligheid te verhogen.

Hoe groeit mijn organisatie op een veilige manier?

De belangrijkste beslissing die u kunt nemen op dit gebied: maak voor de buitenwereld aantoonbaar dat u uw ICT op orde heeft met een ISO 27001 certificering. Dankzij het proces voorafgaand aan deze certificering wordt u gedwongen om goed na te denken over uw ICT en informatiebeveiliging op procesniveau. U brengt samen met uw ICT-partner de risico's in kaart, gaat nadenken over oplossingen die voor uw bedrijf relevant zijn en beschrijft dit zodat iemand het kan controleren.

Een voorbeeld van een risico is uitval van een persoon op een sleutelpositie binnen uw organisatie. In het kader van informatiebeveiliging brengt u dan in kaart welke informatie u nodig heeft om die persoon vervangbaar te maken. Zo brengt u uw organisatie op ICT-gebied van een 6 of 7 naar minimaal een 8.

MET DEZE 9 ICT-TIPS KOMT U VERDER:

1. Denk 5 jaar vooruit bij de aanschaf van nieuwe hardware.
2. Denk 10 jaar vooruit bij de aanschaf van nieuwe (ERP-)software.
3. Denk 15 jaar vooruit als u gaat verhuizen. Kies een locatie met glasvezel!
4. Kies voor een ICT-partner die kan meegroeien.
5. Vergeet niet de baas te blijven over uw eigen ICT. Vraag minstens eenmaal per jaar om de documentatie en admingegevens.

6. Vergeet de back-ups niet! De cloud is niet heilig.
7. Denk ook aan de beveiliging. Laat ieder jaar een QuickScan uitvoeren van uw complete ICT.
8. Vergeet niet te communiceren met medewerkers over ICT-veranderingen. Vertel ze waarom u kiest voor welke oplossing.
9. Overweeg ISO27001 en zorg dat u al uw processen op orde hebt.

Voer een ICT-updategesprek!

Wilt u weten of uw ICT nog wel geschikt is voor uw gegroeide bedrijf? Zorg dat u een partner vindt waarmee u een goed ICT-updategesprek kunt voeren. Vraag vooral door naar de toekomstbestendigheid van de oplossingen die de ICT-partner aandraagt. Zo weet u zeker dat u niet weer zomaar uit uw jasje groeit op technisch gebied.

(advertentie)



NIEUW!
ISO27001 ONLINE
(VAN DE MAKERS VAN AVG ONLINE)

**DOE-HET-ZELF MET
ISO27001 ONLINE!**

ISO27001ONLINE.NL

ISO 27001 ONLINE



Beveiligd e-mailen van bestanden: dé oplossing

Met het oog op de AVG/GDPR is het belangrijk dat u weet hoe u bepaalde bestanden en gegevens beveiligd kunt versturen per e-mail. Wij vertellen u graag welke mogelijkheden er zijn op dat gebied en hoe u voldoet aan de wettelijke voorwaarden. —>

Hoe gaat u om met het mailen van privacygevoelige gegevens?

Waarom moet het eigenlijk?

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) ingegaan. Dit is de vernieuwde privacywet op Europees niveau. Internationaal wordt hij GDPR genoemd. Als organisatie bent u verplicht om aantoonbaar te voldoen aan de nieuwe wet. Daarop houdt de Autoriteit Persoonsgegevens toezicht. Bij controle moet uit uw documentatie blijken dat u voldoende maatregelen heeft genomen om persoonsgegevens van uw klanten, medewerkers en leveranciers te beschermen. Wat nu precies passende maatregelen zijn, is afhankelijk van het soort gegevens dat u verwerkt en het type document dat u gebruikt. Staan er persoonsgegevens in en stuurt u deze op structurele basis? Dan moet er ook een structurele oplossing voor komen in het kader van de AVG.

Een prima argument voor u om te voldoen aan de nieuwe wet is het feit dat de Autoriteit Persoonsgegevens boetes kan uitdelen tot maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet. Reden genoeg dus om eens te onderzoeken hoe u gevoelige gegevens beveiligd via e-mail kunt versturen.

De mogelijkheden van beveiligd e-mailen

Maar hoe werkt dat nu precies, zo'n beveiligde e-mail versturen? U kunt het vergelijken met een fysiek document dat u stuurt. Als u dat via de gewone post doet, is het kwetsbaarder dan wanneer u het aangetekend per koerier

verstuurt. De techniek van beveiligd e-mailen zou u kunnen vergelijken met een aangetekend briefje: er wordt extra goed voor gezorgd en een onbevoegde kan niet zomaar de inhoud ervan zien.

Er zijn verschillende mogelijkheden als het gaat om beveiligd e-mailen. We lichten er een aantal uit:

1. SSL-versleuteling tussen de servers

Kent u het groene slotje bij de url in uw browser? Dat is het symbool van SSL-versleuteling. Die afkorting staat voor Secure Sockets Layer en betekent dat alle data die u stuurt versleuteld wordt verzonden. Tijdens het versturen kunnen hackers niets met de data. SSL-versleuteling vindt plaats op serverniveau. Als u zorgt dat beide mailservers hiermee werken, zijn uw documenten onderweg beveiligd.

2. Een bestand beveiligen met een wachtwoord

Door de bestanden met een wachtwoord te beveiligen, kan alleen de ontvanger met het juiste wachtwoord de documenten openen. Hiervoor is het wel essentieel dat u het wachtwoord ook op een veilige manier communiceert met de ontvanger.

3. Geautomatiseerd versleutelen én beveiligen met wachtwoord

Wilt u écht zeker weten dat uw e-mails met privacygevoelige documenten veilig aankomen? Dan kunt u ervoor kiezen

om software te gebruiken die automatisch alle documenten versleutelt via SSL en deze ook nog eens beveiligt met een wachtwoord.

En ja, er zijn nog veel meer opties, maar die gaan te diep de techniek in. Als u meer wilt weten over mailservertechnieken, PKI-systemen of mail versturen met two factor-authenticatie: uw ICT-partner weet er alles over.

Deze software helpt u verder

Uiteraard heeft u verschillende opties wanneer u wilt werken met software die uw e-mails beveiligt. Er zijn talloze programma's die u daarbij kunnen helpen. Wij zetten drie verschillende softwaremogelijkheden op een rij voor u.

Office 365 Message Encryption

Gebruikt u al Office 365 in uw organisatie? Dan kunt u hiermee ook uw e-mails automatisch laten versleutelen en beveiligen met een wachtwoord. Het enige dat u daarvoor hoeft te doen is uw ICT-partner de juiste vorm van encryptie te laten instellen. Daarna hoeft een medewerker alleen nog maar 'Encrypt' in het onderwerpveld te zetten en de e-mail wordt automatisch versleuteld. De ontvanger krijgt dan eerst een e-mail met het wachtwoord voor de versleutelde mail. Dit wachtwoord verloopt binnen bepaalde tijd voor extra veiligheid.

ZorgMail

Speciaal voor zorginstellingen en overheidsorganisaties, maar ook bedrijven biedt ZorgMail software voor veilig e-mailen én chatten. De software maakt gebruik van de bestaande e-mailomgeving.

FileCap

De software van FileCap biedt naast versleuteld e-mailen ook veilige filetransfertools aan voor grote privacygevoelige bestanden.

Meer weten? Vraag het uw ICT-partner!

Wilt u weten of uw ICT wel voldoet aan de AVG of wilt u meer info over beveiligd e-mailen? Zorg dat u een partner vindt waarmee u een goed ICT-updatesprek kunt voeren. Ook een AVG-check zou in dat geval uitkomst kunnen bieden. Vraag uw ICT-partner naar de mogelijkheden voor uw organisatie.

Tip: nog 6 ICT-maatregelen voor de AVG

Naast versleutelde overdracht bij communicatie van privacygevoelige gegevens zijn er nog zes ICT-maatregelen die u kunt nemen om helemaal klaar te zijn voor de AVG. Wij zetten ze voor u op een rij:

1. Goed wachtwoord(beleid)

Uiteraard moeten de wachtwoorden die uw medewerkers gebruiken veilig zijn. U kunt ze bijvoorbeeld verplichten om een wachtwoordapp te gebruiken die automatisch veilige wachtwoorden genereert en opslaat.

2. Two factor-authenticatie

Mocht er toch een wachtwoord zijn buitgemaakt, dan kan een kwaadwillende dankzij two factor-authenticatie nog niet zomaar in het systeem. Er wordt dan eerst nog een bericht naar de smartphone van de medewerker gestuurd wiens wachtwoord buitgemaakt is om te kunnen inloggen.

3. Firewall

Indringers houdt u het beste buiten met een goede firewall. Zo voorkomt u dat zij privacygevoelige gegevens kunnen stelen uit uw ICT-systemen.

4. Back-ups

Door regelmatig back-ups te maken en deze fysiek veilig te bewaren op een andere plaats dan waar de server zich bevindt, zorgt u voor risicospreiding.

5. Periodieke software-updates

In elke nieuwe update worden ontdekte veiligheidsproblemen opgelost. Door zeer regelmatig te updaten zorgt u dus voor een zo veilig mogelijke ICT-omgeving.

6. Antivirussoftware

Door de garantie van actuele virusdatabases verkleint u de kans op kwaadaardige software die voor een datalek kan zorgen.

Let op! U bent juridisch zelf verantwoordelijk voor de juiste invulling van de richtlijnen die van toepassing zijn op uw organisatie én voor het nemen van passende ICT-maatregelen. Die verantwoordelijkheid ligt dus niet bij uw ICT-partner.

CEO-mails: een gewaarschuwd organisatie telt voor twee

Al is uw ICT-infrastructuur en -security nog zo goed op orde, sommige dingen zijn daarmee eenvoudigweg niet op te lossen. CEO-fraude door middel van valse e-mails is daar een goed voorbeeld van. Het herkennen hiervan blijft altijd mensenwerk, dus bewustwording binnen uw bedrijf is hierbij van het grootste belang. U heeft immers vast wel gelezen over bioscoopketen Pathé, die door valse e-mails maar liefst 19 miljoen euro heeft verloren. Wij leggen u graag uit wat CEO-mails zijn, hoe u ze herkent en hoe u voorkomt dat u hier schade door ondervindt.



Wat is dat eigenlijk, CEO-fraude?

E-mails die gestuurd worden naar een medewerker met financiële bevoegdheid en die afkomstig lijken van de CEO of CFO van het bedrijf, noemen we CEO-mails. De strekking van de mail is vrijwel altijd 'maak met spoed een groot bedrag over naar een buitenlandse rekening en houd deze belangrijke overboeking geheim'. Deze techniek werkt het beste wanneer het bedrijf echt een buitenlandse vestiging heeft en de afstand tussen de directeur en de medewerker groot is door de grootte van het bedrijf.

Om de mail echter te laten lijken, staat er soms een telefoonnummer vermeld van een zogenaamd advocatenkantoor. De medewerker kan dit kantoor bellen om de geldigheid van de transactie te checken. Alleen is dit nummer van een criminele handlanger.

Soms wordt de CEO-mail niet uit naam van de directeur verstuurd, maar uit naam van de IT-leverancier of een andere leverancier. De boodschap is in dat geval dat er een 'nieuw bankrekeningnummer' is waar de overboekingen naartoe moeten of dat het systeem om geld over te boeken 'getest' moet worden. Al deze varianten samen noemen we 'spoofing': je via e-mail voordoen als iemand anders.

"Een hacker van enig niveau kan altijd een mail versturen met de CEO als afzender"

Social engineering

CEO-mails zijn een typisch voorbeeld van de hackersmethode 'social engineering'. Dit is een hackerstechniek die de zwakste schakel op beveiligingsgebied kraakt: de mens. In dit geval wordt een medewerker door middel van angst aangezet tot het overboeken van geld. Hij of zij zou immers niet zomaar durven ingaan tegen de wens van een directeur. Ook tijdsdruk wordt door de criminelen ingezet om slachtoffers eerder te laten betalen.

Hoezo kan iemand mail versturen vanuit mijn adres?

Door de afzendernaam en het afzenderadres aan te passen in de code van een e-mail, lijkt het net alsof de mail verstuurd is door iemand anders. Zo simpel kan dat dus. In 2017 bleek dat zelfs de e-mailsystemen van de Tweede Kamer zich lieten misleiden. Hierdoor konden buitenstaanders zich voordoen als Kamerleden. Normaal gesproken checkt het e-mailsysteem eerst of de afzender wel echt degene is die hij zegt te zijn. Dat gebeurde in dit geval niet.

Vanuit de overheid wordt er al sinds 2015 gestuurd op beveiliging tegen spoofing en phishing (ontvangers laten klikken op foute links in e-mails). Het factsheet 'Bescherm domeinnamen tegen phishing' van het Nationaal Cyber Security Centrum vindt u hier: <https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html>

Hoe herkent u CEO-fraude?

Vaak wordt er in een CEO-mail gezegd dat de betaalopdracht geheim moet blijven, dus dat zou al een belletje moeten doen rinkelen. Ook wordt de overboeking als een bevel gegeven door de 'valse CEO', die de druk opvoert door te eisen dat het geld heel snel moet worden overgemaakt.

Dit is waar het mis ging bij Pathé. De medewerker in kwestie herkende niet snel genoeg dat de mails niet echt afkomstig waren van de CEO. Daardoor werd er zo veel geld buitgemaakt door de criminelen.

Is CEO-fraude ook te voorkomen?

Een hacker van enig niveau kan altijd een mail versturen met de CEO als afzender, als hij weet wat de naam en het e-mailadres is. Dan is het aan de ontvanger om alert te zijn en niet zomaar in de val te trappen.

U kunt schade voorkomen door duidelijke afspraken te maken met medewerkers die financiële verantwoordelijkheid hebben. Bijvoorbeeld dat e-mails met vragen over overboekingen altijd telefonisch bevestigd moeten worden. —>

Dat soort afspraken legt u vast in een informatie-beveiligingsbeleid op basis van ISO 27001. Daarin staan alle processen benoemd die uw organisatie doorloopt als het op beveiliging van informatie doorloopt. Ook de processen die niet direct te maken hebben met ICT. Want met een firewall of antivirusprogramma houdt u deze mails niet tegen. Met bewustwording, training van medewerkers en goede processen wel.

Nog een belangrijk pluspunt: als u kiest voor een certificering op basis van ISO 27001, heeft u in aanbestedingen een streepje voor. Veel opdrachtgevers stellen namelijk als eis dat u voldoet aan deze norm. Ook de Baseline Informatiebeveiliging Rijksdienst is bijvoorbeeld gebaseerd op ISO 27001.

Wat moet u doen als u slachtoffer bent geworden?

Aangifte doen bij de politie is belangrijk wanneer uw organisatie slachtoffer is geworden van CEO-fraude. Wellicht kunnen de daders nog opgespoord worden.

Daarnaast kunnen banken misschien nog iets voor u betekenen na een dergelijke overboeking. Bijvoorbeeld omdat ze mogelijk een betaling kunnen bevriezen of omdat ze de identiteit van de daders kunnen achterhalen via de bankgegevens. Doe ook een melding bij de Fraudehelpdesk.

Tot slot: deel uw ervaringen binnen het bedrijf en met andere bedrijven, zodat er meer bewustwording komt. Het is misschien pijnlijk om toe te geven dat het fout is gegaan, maar uw voorbeeld kan anderen helpen om niet dezelfde fout te maken.

Meer weten? Vraag uw ICT-partner om maatwerkadvies. Onze tip voor uw bedrijf als het gaat om het voorkomen van CEO-mails: zorg dat u een partner vindt die u kan ondersteunen met maatwerk en advies. Door uw ICT-partner te vragen om u te ondersteunen bij het voldoen aan de ISO 27001 norm, slaat u een grote slag op het gebied van informatiebeveiliging.

(advertentie)

ZOEKT U EEN ICT'ER DIE MET U MEEDENKT?

OOK BIJ DE IMPLEMENTATIE VAN OFFICE 365!



Bel of mail voor advies op maat
obi.nl | 088-9008100 | info@obi.nl



SERVER- EN WERKPLEKBEHEER | ONLINE WERKPLEKKEN | WIFI
VOIP TELEFONIE | OFFICE 365 | GEGEVENSBEVEILIGING



Na de AVG komt nu de ePV: wat betekent dat?

De afkorting ePV staat voor e-privacyverordening. Nadat op 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) is ingegaan, komt vanuit het Europees Parlement deze nieuwe wet. Wij leggen u uit wat de ePV precies betekent voor uw organisatie. —>

Nieuwe realiteit, nieuwe wetten

De ePV vervangt de Europese privacyrichtlijn (EPR) uit 2002 en de Telecommunicatiewet. Dat was ook wel nodig, want de wetgeving loopt vaak een beetje achter op de maatschappelijke ontwikkelingen. En als érgens de ontwikkelingen snel gaan, dan is het uiteraard op het gebied van internet en elektronische communicatie.

Vandaar dus die nieuwe wet, de ePV. Samen met de AVG zorgt hij voor meer duidelijkheid op juridisch gebied rondom digitale privacy. Er is een nieuwe technologische realiteit en daar speelt de wetgever op in met deze twee nieuwe wetten. Eigenlijk was het de bedoeling om de AVG en de ePV op dezelfde dag te laten ingaan, maar de lidstaten waren het nog niet eens over de precieze invulling van de ePV. Vandaar dus deze uitgestelde lancering.

Het doel van de ePV is eindgebruikers betere privacybescherming bieden bij elektronische communicatie, zoals via chat, online formulieren, WhatsApp en cookies. Iets wat we zelf in onze rol als eindgebruiker zeker waarderen. Maar voor uw organisatie is het wel weer even opletten geblazen.

“Eerst treedt de ePV in werking en daarna is de AVG er nog als vangnet”

Maar wat verandert er dan?

Nou, de ePV zorgt voor een aantal veranderingen ten opzichte van de huidige wetgeving. We zetten ze op een rij voor u.

Metadata is nu ook vertrouwelijk

Niet alleen daadwerkelijke persoonsgegevens, maar ook de metadata van elektronische communicatie moeten voortaan vertrouwelijke behandeld worden. Metadata gaan bijvoorbeeld over het tijdstip waarop een bericht verstuurd is, hoe groot het bericht was, wie de afzender is en wie de ontvanger. Om deze data te verwerken, moeten betrokkenen vanaf nu ook echt toestemming hebben gegeven. Toestemming is sowieso een belangrijk onderdeel van de ePV.

Wat is het verschil tussen de AVG en de ePV?

De AVG is een algemene wet (dat blijkt al uit de naam) die van toepassing is op alle vormen van persoonsgegevensverwerking. De 'e' van de ePV geeft aan dat dit een heel specifieke wet is die gaat over de verwerking van persoonsgegevens voor elektronische communicatiediensten. Door zijn specifieke karakter heeft de ePV voorrang op de AVG.

Om die reden kunnen de AVG en de ePV dus ook prima naast elkaar bestaan. Voor een deel hebben ze betrekking op dezelfde onderdelen, maar het onderscheid is ook duidelijk. Gaat het om elektronische communicatie, dan treedt eerst de ePV in werking en daarna is de AVG er nog als vangnet.

Ook voor cookies is toestemming nodig

Na het in werking treden van de AVG zijn website-eigenaren heel bedreven geworden in het plaatsen van cookiewalls. Maar dan wel zo dat de cookies vaak standaard worden geaccepteerd, want anders kun je de site niet bezoeken. Dat mag niet meer van de ePV. De gebruiker moet per cookie-onderdeel toestemming geven, ook voor bijvoorbeeld 'device fingerprinting', het verzamelen van hard- en softwaregegevens over het gebruikte toestel.

Nieuwe media vallen ook onder de ePV

Voorheen was het lastig om de bestaande wetgeving toe te passen op elektronische communicatiemiddelen zoals Slack, Skype, WhatsApp, Facebook en Twitter. De bedoeling van de ePV is dat de bestaande nieuwe media hieronder vallen én dat de verordening meegroeit met toekomstige media.

Geen bel-me-niet, maar bel-me-wel

De ePV heeft ook duidelijk impact op direct marketing. Automatische communicatiesystemen zonder menselijke tussenkomst mogen niet meer gebruikt worden zonder toestemming. Dat geldt ook voor telemarketing gericht op consumenten: alleen met toestemming van de gebelde mag u een potentiële klant telefonisch benaderen en dan ook alleen met een zichtbaar nummer. Bestaande klanten mag u uiteraard gewoon blijven bellen zoals u gewend was.

Bestaande klanten mogen bezwaar maken

Het was altijd al toegestaan om bestaande klanten mailings te sturen, ook als zij daarvoor geen toestemming hebben gegeven. Dit blijft zo. Daar is alleen aan toegevoegd dat de klant duidelijk gewezen moet worden op zijn recht om bezwaar te maken tegen deze mailings. In principe is dit dus de 'Afmeld-link' die al verplicht was in digitale mailings.

Al bezig met de AVG? Mooi, dan zit het met de ePV ook goed! Het grote voordeel van de ePV is dat veel van de maatregelen die nu specifiek gelden voor elektronische communicatie ook al in de AVG stonden. Als het goed is, is uw organisatie dus al helemaal compliant op dit gebied. In dat geval hoeft er waarschijnlijk nog maar weinig te gebeuren om ook uw zaken goed op orde te hebben voor de ePV.

Om er écht zeker van te zijn dat u voldoet aan de laatste regelgeving kunt u de genomen AVG-maatregelen nog even

naast de nieuwe verordening leggen. Dan ziet u al snel of er nog dingen over het hoofd zijn gezien. Een deel van deze nieuwe Europese wetgeving wordt bepaald op landelijk niveau, namelijk het gedeelte 'business-to-business'. Daardoor kan het zijn dat de Nederlandse regering nog bepaalde extra onderdelen opneemt. Wees hier alert op en neem passende maatregelen waar nodig.

Uw ICT-partner checkt het graag samen met u

Bent u benieuwd of uw ICT wel voldoet aan de ePV/AVG of wilt u meer weten over de nieuwe wetgeving? Dan helpt uw ICT-partner u graag. Zo is een ICT-updatesprek en eventueel een ePV-check een prima idee. Vraag uw ICT-partner naar de aandachtspunten voor uw organisatie.

(advertentie)



Wilt u ook voldoen aan de ISO 27001 normering, maar geen idee waar te beginnen?

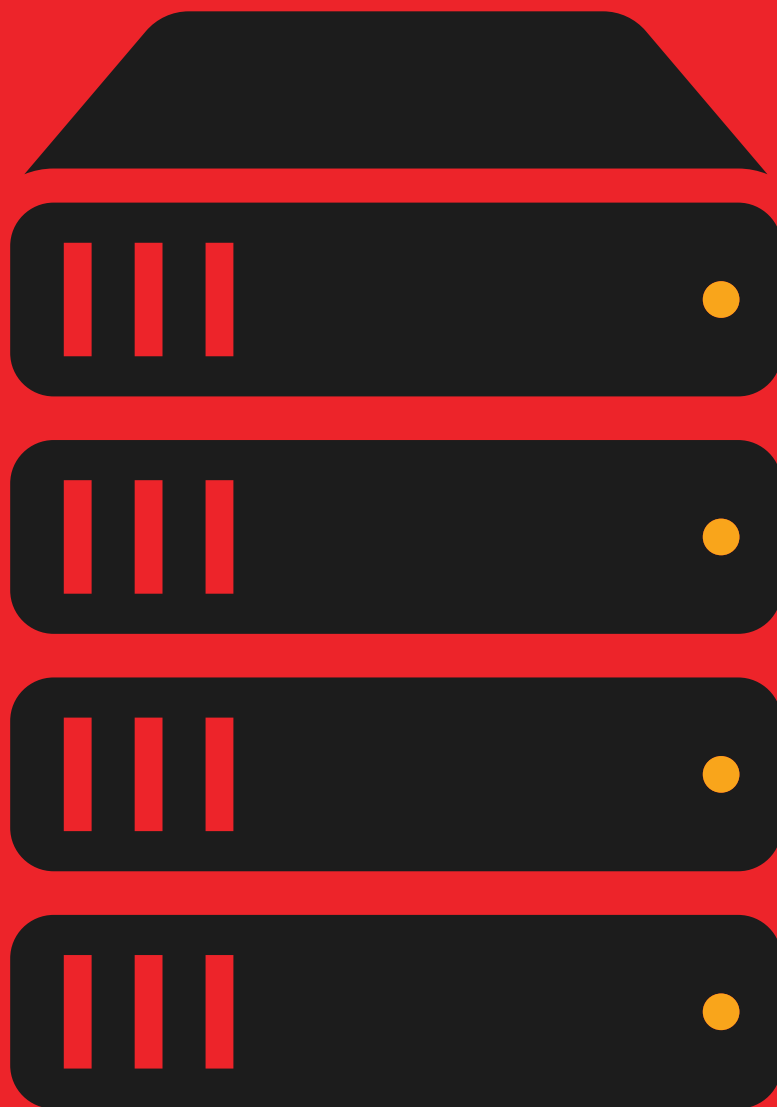
ISO Privacy Advies begeleidt en adviseert organisaties naar een ISO 27001 certificering.

ISO PRIVACY ADVIES

BEL OF MAIL VOOR EEN GRATIS ADVIESGESPREK VAN 1 UUR
ISOPRIVACY.NL | 040-7878750 | INFO@ISOPRIVACY.NL

Help!

De server is (weer) traag!



Een grote ergernis binnen allerlei bedrijven is dat het lang duurt om bestanden op de server te vinden, te openen of op te slaan. 'Trage server', zeggen we dan vaak met ingehouden woede. Maar ligt het wel echt aan de server? Of kunt u er op andere manieren voor zorgen dat u de productiviteit binnen uw bedrijf verhoogt en de frustratie verlaagt? Een nieuwe server kost veel geld. Die investering wilt u dus niet zomaar doen. Alleen als het echt nodig is. Wij leggen u graag uit welke opties u heeft.

Wanneer is het nu écht tijd om de server te vervangen?

Dat computernetwerkproblemen één van de grootste ergernissen op de werkvloer zijn, is ook daadwerkelijk onderzocht. Recentelijk bleek uit onderzoek van de Universiteit Twente dat ruim 8 procent van de werktijd verloren gaat aan computernetwerk gerelateerde problemen. Dat kost uw onderneming dus al snel bijna twee werkdagen per (fulltime) werknemer per maand!

In het Rapport Circulaire Dataservers van FFact uit 2018 staat dat servers gemiddeld tussen de 8 en 10 jaar aan vervanging toe zijn. Maar voordat ze vervangen worden, na een jaar of 5 à 6, worden de servers te oud om nog dienst te doen als netwerkserver. Enerzijds worden ze te traag en anderzijds vervalt de garantie.

Deze oudere servers kunnen echter nog prima dienst doen als back-upservers. Het is dus niet nodig om ze al direct af te danken zodra ze wat trager worden. Maar na 5 of 6 jaar



Waar moet u op letten bij de aanschaf van een nieuwe server?

Natuurlijk denkt u bij de aanschaf van een nieuwe server goed na over de opslagcapaciteit, de snelheid, de hoeveelheid geheugen en de prestaties. Maar er zijn meer dingen die belangrijk zijn. De belangrijkste tip die we u kunnen geven: denk 5 jaar vooruit. Zorg voor minimaal 5 jaar garantie op de nieuwe servers, zodat u zeker weet dat u pas over een handvol jaren opnieuw hoeft na te denken over dit deel van uw ICT-infrastructuur. Ga dus niet uit van uw huidige behoefte, maar die van de toekomst.

Nog een goede tip: vergelijk geen appels met peren bij het opvragen van meerdere offertes. Zorg dat u weet wat u wilt en vraag daarvan offertes op, zodat ze goed te vergelijken zijn. Denk ook goed na over het aantal servers dat u nodig heeft. Misschien past een SAN-oplossing wel beter bij uw bedrijf dan een losse server. SAN staat voor Storage Area Network. Hierbij wordt de opslagcapaciteit verdeeld over meerdere servers, zodat u niet in de problemen komt als één van de servers uitvalt. Bij ongeveer 30 medewerkers ligt hiervoor het omslagpunt. Denkt u ook aan de back-ups van uw server? Hardware kan ook omvallen, dus het zou verstandig kunnen zijn om de server redundant uit te voeren. Stel uzelf de vraag: hoe belangrijk is het om meteen door te kunnen bij hardwareproblemen?

"Ga niet uit van uw huidige behoefte, maar die van de toekomst"



zijn ze dus niet echt geschikt meer om als server te dienen waarop dagelijks gewerkt wordt. Doet u dit wel, dan is het logisch dat medewerkers op een bepaald moment gaan klagen over het gebrek aan snelheid.

U heeft verschillende opties

Is het tijd om iets te doen aan uw trage server, dan wilt u graag weten welke opties u op dat moment heeft. Dit zijn de drie belangrijkste:

- **Nieuwe fysieke server**

Als u overstapt op een nieuwe server, dan kunt u dat doen op verschillende manieren. Zo kan de server fysiek bij u in het pand staan of in een datacenter. Ook de uitvoering, bijvoorbeeld één server of juist meerdere servers, is afhankelijk van de wensen die u voor uw bedrijf heeft. Eén ding is zeker: de tijd van de trage server is zeker voorbij zodra uw nieuwe hardware draait.

- **Overstappen op de cloud**

Kiest u ervoor om geen fysieke server meer te gebruiken, dan gaat uw bedrijf werken in de cloud. Met deze optie betaalt u naar gebruik en hoeft u vooraf geen grote investeringen te doen. Een goed voorbeeld hiervan is overstappen op Office 365. Daarmee werken uw medewerkers met opslagruimte, een mailserver en Office-programma's, allemaal vanuit de cloud.

- **Een combinatie: hybrid cloud**

Heeft u veel bedrijfskritische programma's of gevoelige documenten die u niet zomaar in de cloud wilt zetten? Dan

is een hybrid cloud voor u een goede optie. Hierbij draait een deel van de cloud waarop uw bedrijf werkt op eigen hardware. Die kan in uw pand staan of ergens anders, maar deze server is altijd alleen voor uw bedrijf. Voor de overige zaken maakt u gebruik van de public cloud, waarbij u profiteert van hoge snelheid en lage kosten per gebruiker.

Maar de traagheid kan natuurlijk ook een andere oorzaak hebben...

Misschien lijkt het alsof de server traag is, maar er kan ook best iets anders aan de hand zijn. Bijvoorbeeld:

1. Uw organisatie is de afgelopen jaren verdubbeld in aantal medewerkers, maar uw server is niet meegegroeid.
2. De hardware en software van de server of het workstation zijn niet meer compatible met elkaar.
3. Sommige netwerkdonderdelen, zoals een switch, internetverbinding of router, zijn verouderd en zorgen daardoor voor vertraging.
4. Uw draadloze netwerk wordt gehinderd door straling van bijvoorbeeld mobiele telefoons, magnetrons of Bluetooth-apparaten.

Uw ICT-partner helpt u verder

Wilt u weten of uw bedrijf al toe is aan nieuwe servers? Zorg dat u een partner vindt die een check kan uitvoeren op dit gebied en voer een updategesprek. Uw bedrijf verdient advies op basis van maatwerk, dus laat uw ICT-partner goed onderbouwen waarom zij u bepaalde servers adviseren. En vraag ook meteen welke mogelijkheden zij nog zien voor uw huidige servers.

(advertentie)

OOK EEN RELATIEMAGAZINE ALS BITS&BYTES VOOR UW ORGANISATIE?



RIUMSSEN MAAKT UW RELATIEMAGAZINE VAN A TOT Z. BEL NU VOOR MEER INFORMATIE.

Riumssen B.V. • Torenallee 20 • 5617 BC Eindhoven • 040 - 211 09 53
hello@riumssen.nl • www.riumssen.nl



**ZORGT DAT ICT WERKT.
ALTIJD. OVERAL.**



**SERVER- EN
WERKPLEKBEHEER**

**ONLINE
WERKPLEKKEN**

WIFI

VOIP TELEFONIE

OFFICE 365

GEGEVENS BEVEILIGING

OBI.NL