

OVER CLOUD, SECURITY, DATALEKKEN EN
DE NIEUWE ROL VAN DE ICT-DIENSTVERLENER

Is mijn ICT wel in goede handen?

DEELNEMERS



PETER VAN DER GUN

Commercieel directeur Insign.it

www.insign.it



JEAN HUVENEERS

Technisch directeur Xillion ICT
Solutions

www.xillion.nl



JEROEN MOM

Directeur Square

www.square.nl



COR ZELISSEN

ceo Mainport

www.mainport.nl

De wereld om ons heen verandert snel en de ICT, waar we als ondernemers niet meer zonder kunnen, verandert zo mogelijk nog sneller. Moeten je data in de cloud of niet? Is het beheer van confidentiële informatie en data van je klanten wel in veilige handen? Wat gebeurt er in geval van datalekken? Hoe blijf ik als goed ondernemer, maar feitelijke digibeet, bij in die snel veranderende ICT-wereld?



Vragen, antwoorden, meningen en ervaringen vlogen tijdens een kennis-intensieve sessie over de rondetafel rond dit thema bij gastheer Insign.it in Venlo. Slotconclusie: ICT blijft een complexe wereld, waarin degene overleeft die zich als een echte partner onmisbaar maakt voor zijn opdrachtgever en bereid is kennis te delen om zijn klanten sterker en beter te maken.

CLOUD

De cloud, je ontkomt er niet aan. Iedereen doet wel iets in de cloud, al kun je ook zonder in de cloud te acteren prima ondernemen en je ICT op orde houden. “Niks moet”, zegt Peter van der Gun van Insign.it, gespecialiseerd in het bedenken en bouwen van IT-infrastructuren. “De klant heeft een behoefte en afhankelijk daarvan kijk je welke technieken je moet inzetten. Cloud- of traditionele on-premise-oplossingen. Cloud is geen doel op zich en kent bovendien vele gezichten. Public, private of de combi van beide.”

Hoe dan ook, er is altijd een infrastructuur op locatie nodig om je data in die cloud te bereiken. En die moet goed beveiligd zijn, want IT-systemen zijn ervan afhankelijk, evenals de daaraan gekoppelde machines, zegt Jean Huveneers van Xillion ICT Solutions. “Je moet goed kijken naar de behoeftes van je klant en waar jouw toegevoegde waarde zit. De vraag is: hoeveel cloud wil je?”

Kent het cloudverhaal nog nieuwe ontwikkelingen? Er wordt in elk geval steeds meer naar gevraagd, ook in relatie tot productiemachines en toegangssystemen. Maar uitbreiding van de mogelijkheden, maakt ook dat sommige applicaties moeilijker efficiënt te maken zijn. “Als een ERP-systeem op locatie je machines aanstuurt, wil je daar geen internetverbinding tussen hebben die voor meer complexiteit en risico’s zorgt”, zegt Huveneers.

SECURITY

Om die risico’s te minimaliseren, is er security. Daar wordt steeds vaker om gevraagd. Van der Gun: “Veiligheid is een thema. Waar staan mijn data, hoe zijn die beveiligd, wie kan er aankomen?” Ervaart ook Luud Willemsen van de ICT-coach voor het mkb, die bedrijven onafhankelijk adviseert in het omgaan met ICT. “Beveiliging heeft echter vooral met geld te maken. Bedrijven moeten aan de wet- en regelgeving voldoen maar zijn niet zo bezig met security. Pas als ze geconfronteerd worden met malware worden ze kritischer. Organisaties tot dertig medewerkers zijn te goedgelovig, in tegenstelling tot grotere organisaties, die daar echt beleid op loslaten. Mkb-ondernemers zitten vaak in de spagaat tussen veilig en safe moeten werken en al die andere zaken die ook hun aandacht vragen. De fiscus, de webshop, en tegelijkertijd moeten zij meters maken.” Dat is wel mede afhankelijk van de branche”, vindt Ton Luyk van Valid. “Maar regel je het niet goed, kan de impact gigantisch zijn.”

Sommigen interesseert het zelfs helemaal niks, is de ervaring van Cédric Müller van intermarketingbureau MediaZo! “Het is voor mkb’ers een ver-van-mijn-bedshow”, stelt Van der Gun. “Pas als er boetes worden uitgedeeld, wordt het concreet.”

DATALEKKEN

Boetes voor bijvoorbeeld datalekken. Bedrijven worden geacht zorgvuldig met hun eigen data en die van anderen om te gaan. Volgens Huveneers wordt dit pas echt spannend als op 26 mei 2018 de AVG, de Algemene Verordening Gegevensbescherming van toepassing wordt en ook de verantwoordelijkheid van subcontractors in de keten wordt geborgd, hoe ingewikkeld dat ook is. De impact van die Europese regel wordt volgens hem veel groter dan de Nederlandse meldplicht datalekken die per 1 januari 2016 van kracht werd. Handhaving is er straks ook in de vorm van flinke boetes. Het mkb wil daar niet

mee lastiggevallen worden, maar zal er toch in mee moeten. “Het komt snel dichtbij”, weet Willemsen. “Maar veel ondernemers denken: wat moet ik ermee?”

Bert Nottelman van Benefit Security Experts, totaalleverancier op het gebied van beveiliging, laat weten dat de Nederlandse economie jaarlijks 10 miljard euro schade lijdt door datalekken. Wereldwijd zal dat dit jaar neerkomen op 290 miljard euro. “Pak je security dus integraal aan. Als we bedrijven laten zien wat de gevolgen kunnen zijn van slechte beveiliging, schrikken ze. Je moet de maatregelen die je neemt ook borgen, want de risico’s worden steeds groter. Hackers zijn zo binnen. Wij kunnen criminele activiteiten traceren in samenwerking met experts, vaak oud-politiemensen. Dus ken je mensen, ken de wet en pak het op in je organisatie. Kijk wie waarvoor verantwoordelijk is en spreek mensen daar op aan.”

Ook om bedrijfsspionage tegen te gaan. Daar zitten we in Nederland niet genoeg bovenop, omdat we de regels maar lastig vinden. Maar met een USB-stick zijn data snel gejat. Het is geen onwil zegt Willemsen, maar security heeft geen hoge prioriteit, terwijl ICT zelf dat wel heeft. Heeft te maken met onwetendheid en keuzes maken. Cor Zelissen van Mainport, een bedrijf dat zich naast video conferencing bezighoudt met mobile device management, ziet in datalekken zelfs de grootste security-uitdaging op dit moment, zeker in zijn circuit van de mobile devices. Bijvoorbeeld in de medische wereld, waar het lekken van medische dossiers voor giga-problemen kan zorgen. Uitgedaagd een oplossing te creëren, is het idee ontstaan van het pushen van apps op basis van de locatie van een patiënt. Of anders, om apps zodanig te bewerken dat ze alleen nog tijdens werktijden beschikbaar zijn. “Dat heeft nogal wat impact op de relatie met onze klanten”, zegt hij. “Je hebt een sterk samenspel nodig met andere domeinen.



LUUD WILLEMSSEN

Directeur-eigenaar en adviseur De ICT-coach voor het MKB
www.de-ictcoach.nl



BERT NOTTELMAN

Directeur-eigenaar Benefit Security Experts
benefitsecurity.nl



TON LUYK

Accountmanager zakelijke dienstverlening Valid
www.valid.nl



CÉDRIC MÜLLER

directeur-eigenaar MediaZo!
www.mediazo.nl

Zo werken wij samen met een advocatenkantoor, want je moet je diensten juridisch beter embedden. Het werken in de cloud van klanten heeft ook gevolgen voor je aansprakelijkheid. Grote bedrijven verschuiven hun backoffice naar het mobile front office, en dat heeft gevolgen voor de datastromen. Het wordt heel complex allemaal. Om dit goed te managen, wordt de grootste uitdaging de komende jaren. Een spectaculaire ontwikkeling.”

ZWAKKE PLEKKEN

Veiligheid triggert. Niet alleen een antivirusprogramma, ook opleiding en het kweken van awareness op het gebied van veiligheid bij je medewerkers, waarbij sociale controle hoort, zijn belangrijk in het beveiligen van je data. Je kunt wel alles door middel van techniek dichttimmeren, maar mensen vormen de zwakke plekken. Dat vraagt om extra beveiliging van bijvoorbeeld apps waar medewerkers mee werken. Als je het gebruik van die apps niet goed beveiligt, kun je er beter niet aan beginnen, vindt Huveneers. Luyk noemt een app op de mobiele telefoon om in je boekhouding te kunnen zelfs een potentieel gevaar voor je bedrijf, zeker als thuis de kinderen aan de bedrijfs-telefoon van pa of ma kunnen. Laptop of tablet? Zelfde verhaal. Bij het monitoren van de beveiliging van bedrijven blijkt vaak dat zij daar totaal geen beleid op voeren.

SHARED PROFIT

Müller stelt dat veel mkb'ers niet over veiligheid nadenken, omdat zij vinden dat er bij hen toch niets te halen valt. “Zij zijn zich niet bewust van de risico's die ze lopen”, stelt hij. Willemsen vindt het legitiem als ondernemers andere keuzes maken voor hun core business dan voor de rest. Hoe dan ook, kosten vormen een bepalende rol. Wordt beveiliging meegenomen bij het ontwikkelen van nieuwe applicaties? “Je moet wel”, antwoordt Jeroen Mom van Square, dat klantspecifieke webapplicaties ontwikkelt. “Als je een product ont-

wikkelt voor een bedrijf dat met medische gegevens werkt, krijg je meteen met een hoog niveau van beveiliging te maken.” Hoe scope je dat, wil Van der Gun weten. “Je wil een leuke applicatie, maar ook weten wat je kwijt bent.” Vertrouwen speelt een rol, maar vooral de inzet van Agile-ontwikkelmethoden helpt om het risico voor beide partijen overzichtelijk te houden, luidt het antwoord. “Een open end applicatieontwikkeling starten, wil niemand meer.” De klant heeft graag voortschrijdend inzicht in de kosten, zeker bij langere ontwikkeltrajecten, stelt Huveneers, die vraagt of er met shared profitmodellen wordt gewerkt. Het blijkt dat als je in de productontwikkeling veel creativiteit toevoegt, zoals Square doet, een vorm van co-ontwikkeling ontstaat, waarbij de aan beide kanten gedane investering wordt terugverdiend. “Dat is de leukste manier om te werken”, is de ervaring van Mom. Er is steeds vaker sprake van een shared profitaanpak in het mkb.

DOCUMENT MANAGEMENT

Beveiliging is belangrijk, maar toegang tot je data is minstens zo belangrijk. Bedrijven hebben een groeiende behoefte aan goede document managementsystemen. Willemsen en Luyk zien een aantal trends. Nieuwe, mooie oplossingen, zoals Microsoft SharePoint, Exact Synergy en Filelinx, waarin CRM, 360 graden-views, cockpit- en dashboardsystemen al je managementinformatie in één keer toegankelijk en inzichtelijk gemaakt worden dankzij voortschrijdende technieken en een betere infrastructuur. Want je managementdata, die vaak versnipperd is opgeslagen, op één plek inzichtelijk krijgen, blijft een issue. Minder in het grootbedrijf, maar vooral in het mkb. Dat komt mede doordat het grootbedrijf meer beleid en structuur kan aanbrengen in zijn document management. Maar, coacht Willemsen, ook de mkb'er zal koppelingen moeten kunnen leggen om bij grotere opdrachtgevers binnen te komen. En dan komt ie weer in een kosten-batenafweging: wat wil je, wat kun je. “Ik

ben al blij als een mkb'er überhaupt een risicoafweging maakt, als hij erover nadenkt, maar veel bedrijven denken er niet over na.” Omdat het mkb volop bezig is met de business en minder met dit soort zaken. Pas als een bedrijf groter groeit, wordt het belang van beleid en structuur van ICT en security belangrijk”, zegt van der Gun. En de certificering, vullen Mom en Luyk aan. “Security hangt erbij, tot je wordt geconfronteerd met de noodzaak tot certificering. Dan krijg je vaak een draai om je oren”, zegt Luyk. “Vooral bij zakendoen in Duitsland worden de kleine lettertjes in de leveringsvoorwaarden niet gelezen, tot het misgaat. Weg klant.” Nottelman heeft vanuit zijn security-praktijk mooie voorbeelden van hoe laks bedrijven met de eigen regels omgaan. Zijn bedrijf toetst en screent dat en de social media spelen daarbij een steeds grotere rol. Van der Gun bevestigt dat organisaties steeds vaker de combi van private en public willen en daar het beste gevoel bij hebben. “Hackers worden echter steeds slimmer en nestelen zich al in applicaties. Dus moet je een firewall hebben die ook daarnaar kijkt.” Met een social mediaprotocol zou je het gebruik van social media in een bedrijf tot een minimum moeten beperken.

VERANDERENDE ROL

Waarna het rondetafelgesprek wordt afgesloten met een gedachtewisseling over de veranderende rol van de ICT-dienstverlening, afgezet tegen de steeds dominantere strategie van de Googles en Microsofts van deze wereld om rechtstreeks zaken te willen gaan doen met consument en bedrijfsleven en zo de 'tussenhandel' uitschakelen. Dus: minder op producten focussen en meer op adviesfunctie, klanten een goed alternatief voor hun licenties aanbieden en je richten op kennis en toegevoegde waarde. Goed nadenken ook hoe de markt van de toekomst in elkaar zit, waarin zich andere verdienmodellen gaan aftekenen. En minder uit zijn op eigen gewin en je als een echte partner van je klant opstellen. <<

