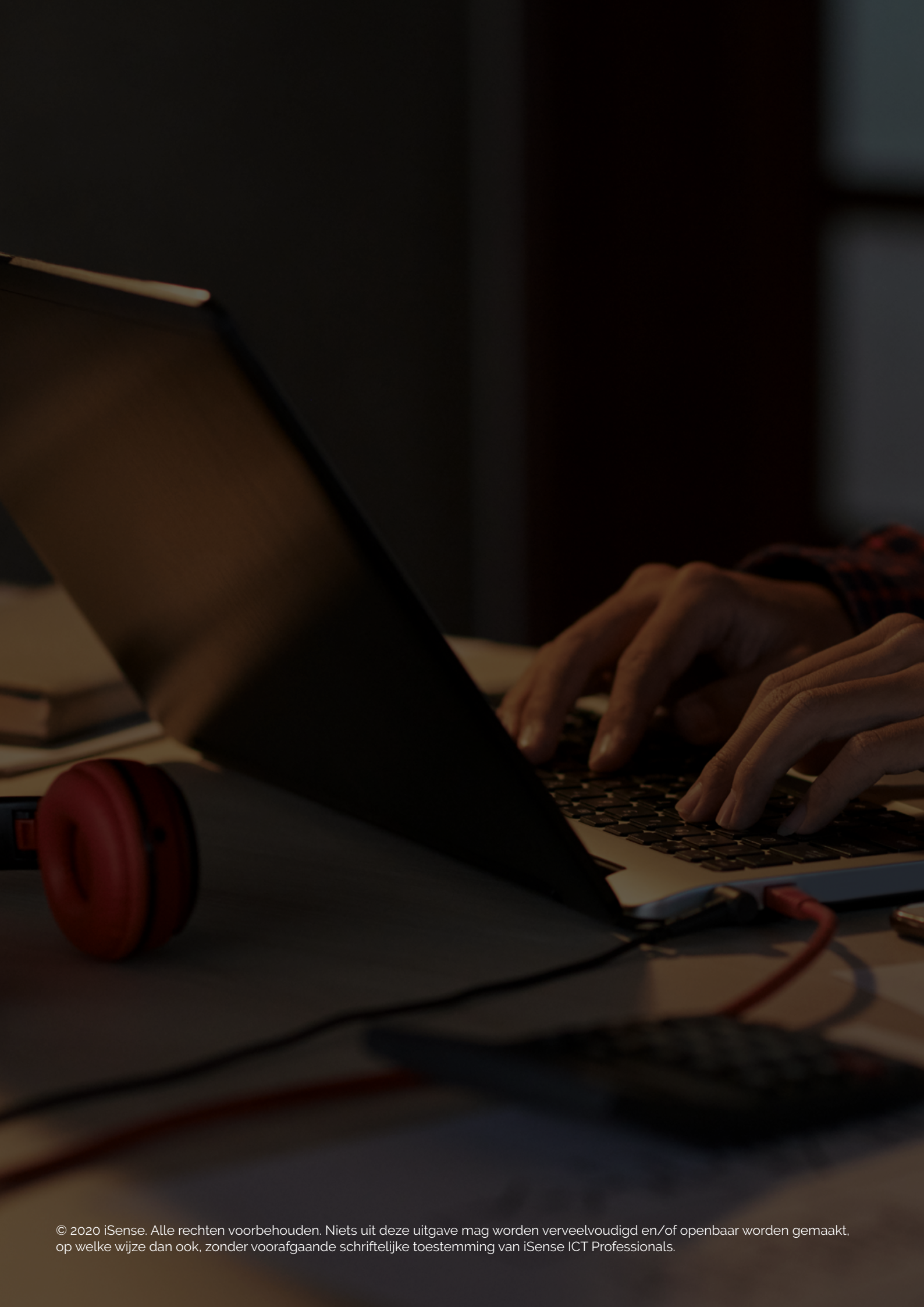
Experis
ManpowerGroup

< iSense >
ICT PROFESSIONALS

SECURITY SUMMIT

WHITEPAPER



INHOUD

4. ‘Cyber Security is nog te weinig gerelateerd aan bedrijfscontinuïteit’

Marco van Vliet over het belang van gedegen weerbaarheid in een organisatie.

10. ‘Een Veilige Cloud-Infrastructuur: zorg altijd voor controle over data, waar die ook staan’

Sebastiaan Kors over de securitytrends en best practices bij een migratie naar de cloud.

12. ‘We moeten een einde maken aan de Fear, Uncertaincy en Doubt’

Jan Martijn Broekhof en Michiel Mak over hun optimistische visie op security.

‘CYBER SECURITY IS NOG TE WEINIG GERELATEERD AAN BEDRIJFSCONTINUÏTEIT’

MARCO VAN VLIET OVER HET BELANG VAN GEDEGEN WEERBAARHEID IN EEN ORGANISATIE.

Als het gaat om cyber security is een gedegen weerbaarheidsplan nodig. Zo omvat digitale dreiging veel meer dan enkel aanvallen vanuit hackers of criminele organisaties. We zitten in een snel veranderende wereld, waarin we meer grip moeten krijgen. Bijvoorbeeld als het gaat om de beveiliging van informatie. Volgens Marco van Vliet, CEO bij SQNetworks Cyber Security, is dit essentieel ter bevordering van de bedrijfscontinuïteit.

WAT ZIE JIJ ALS EEN GROTE DIGITALE DREIGING?

"Onder meer het verzamelen van rest-informatie. Je kunt je afvragen hoe het mogelijk is dat zoveel data van iedereen beschikbaar is voor onbevoegden. Het is cruciaal om te weten wie dat in zijn bezit heeft en wat daarmee gebeurt. Al die informatie kan tegen ons worden gebruikt. Ik merk dat bij veel organisaties dit besef niet afdoende is. Ook weten we hier niet goed mee om te gaan. Die restdata worden als onbelangrijk beschouwd, terwijl je met dit soort data bepaalde zaken, zoals gedrag, kunt voorspellen. Het is complex om degenen die informatie verzamelen hierop aan te spreken. We geven dit immers zelf ook uit handen vanwege bijvoorbeeld gemak of gratis services. Tegelijkertijd kunnen we dit ook niet zomaar een halt toeroepen. Een goede voorbereiding en acties zijn nodig. "

OP WAT VOOR MANIER UIT DIT ZICH IN DE PRAKTIJK?

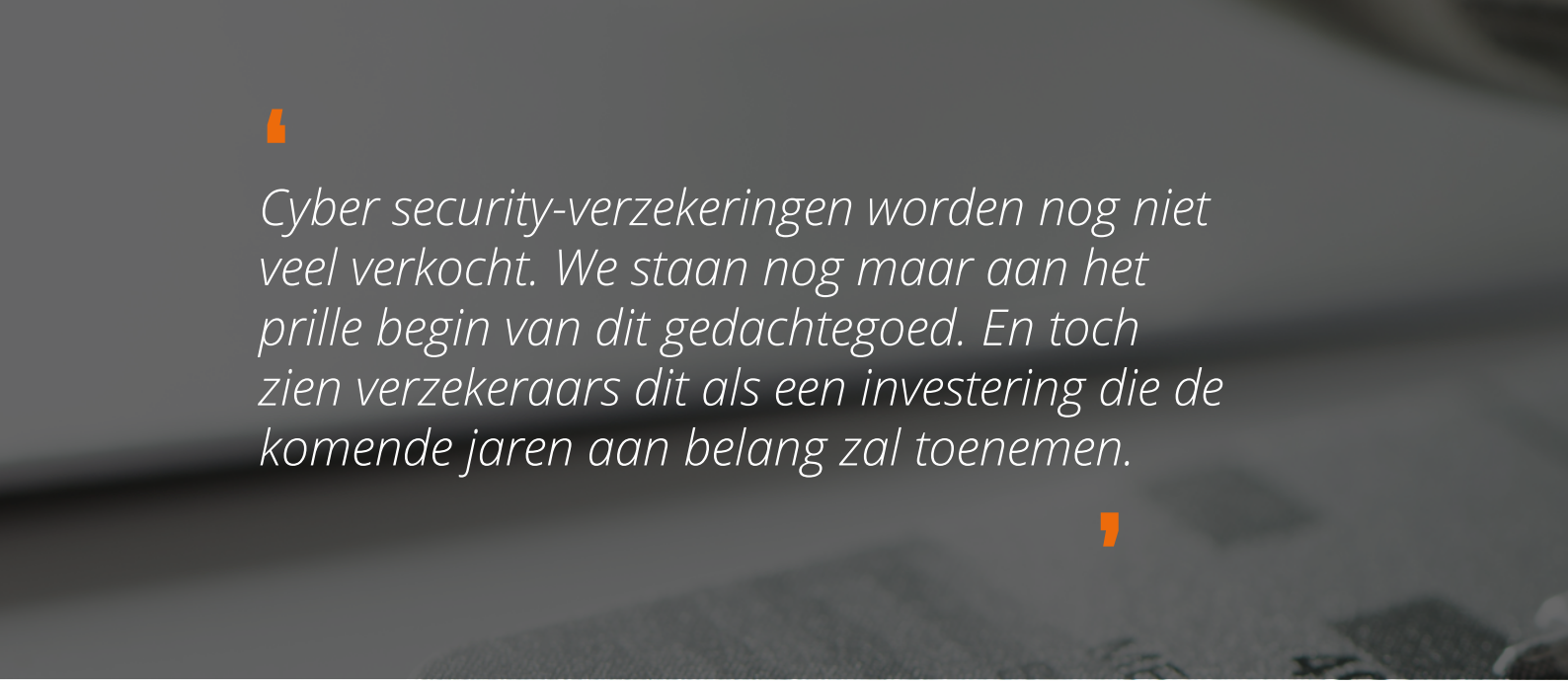
"Vele manieren. Zo koop je voor 1700 dollar software op het internet, waarmee je foto's manipuleert op een CT-scanner in het ziekenhuis. Dat betekent dat iemand kan denken dat die ziek is, terwijl het in werkelijkheid niet zo is.
Je kunt je voorstellen dat bepaalde medicijnen dan veel worden verkocht. Het gaat mij erom dat (criminele) organisaties dergelijke technologieën inzetten om zoveel mogelijk informatie te verzamelen en geld te verdienen, zodat ze concurrentievoordeel behalen. Veel informatie wordt verkregen zonder dat eenvoudig kan worden aangetoond dat dit strafbaar is. En als het strafbaar is, zijn maar weinig organisaties in staat om tot actie over te gaan. Als het onder meer gaat om onze smartphones, laders, thermostaten en ledlampen, moeten we opletten. Daarin zitten sensoren verwerkt die niet in de productomschrijving staan vermeld. Zo worden opnames gemaakt die onze communicatie, houding, stemming en ander gedrag verzamelen. Op basis van die gegevens worden correlaties gemaakt. In relatie tot bijvoorbeeld medische informatie kan bepaald gedrag worden voorspeld. Op basis van dit soort gegevens kan een profiel vastgesteld worden dat uniek is voor jou en je gedrag."

HOE MOETEN BEDRIJVEN HIERMEE OMGAAN?

"We moeten het heft meer in eigen handen nemen aangaande de risico's van zowel binnen als buiten de organisatie. Je ziet dat vele IT-transities leiden tot bepaalde risicovariabelen. Die zijn van een omvang en veranderingssnelheid die nooit eerder zijn geweest. Er verandert zoveel, onder meer doordat we meer data opslaan en er veel informatie over ons wordt verzameld.
Nu worden aanvallen op onze bedrijven al ondersteund door artificial intelligence. Het is hoog tijd om nu meer kennis te vergaren over dreigingen en weerbaarheid, en dit integraal beet te pakken."

EN LUKT DAT OOK?

"Nee, we beschikken nog lang niet over voldoende kennis. Zo kwam uit een verzekeringsonderzoek naar voren dat het voor een IT-afdeling lastig is om het juiste beveiligingsbudget en bewustzijn te krijgen vanuit het management. Anderzijds zien we de afgelopen tijd dat het management van organisaties minder vertrouwen heeft aangaande de beveiligingskennis van de IT-organisatie. Als deze afdoende zou zijn, dan zou bijvoorbeeld de impact van aanvallen als een ransomware niet zo hoog zijn.
De trend is geweest dat bepaalde specialisaties en verantwoordingen bij bedrijfsonderdelen werden ondergebracht in verschillende onderdelen. Zo hebben we bijvoorbeeld Security, Finance en HR binnen organisaties. Maar als het gaat om de bedrijfscontinuïteit en de IT-transities van je organisatie, kun je security niet overlaten aan enkel een IT-afdeling.
Er verandert momenteel zoveel en dat raakt de business, security, compliance en nog veel meer facetten. De kennis zit van oudsher bij de IT-organisatie. Maar Finance bepaalt bijvoorbeeld of er geïnvesteerd wordt. Het management moet dit integraal aanpakken, om zo de problematiek te begrijpen en een gezamenlijk plan te maken. Door een risicoplan multidisciplinair op te pakken, wordt al veel gewonnen. Neem je dit niet serieus genoeg, dan barst vroeg of laat ergens de bom."



‘Cyber security-verzekeringen worden nog niet veel verkocht. We staan nog maar aan het prille begin van dit gedachtegoed. En toch zien verzekeraars dit als een investering die de komende jaren aan belang zal toenemen.’

ZIJN ER ZAKEN DIE ONDERSCHAT WORDEN?

“Ja. Er zijn meer externe dreigingen dan iedereen denkt. Zo staan bijvoorbeeld zero day malwares gemiddeld 171 dagen in huis voordat ze worden waargenomen. Non malwares en manipulatieve softwares worden vaak niet eens beschouwd als risico. Interne dreigingen zijn er ook, vooral bij veranderende organisaties. We kijken niet naar de indirecte impact en beschouwen deze voor het gemak maar niet. We weten daarom niet wat we moeten weten, zodat we erop kunnen acteren. We richten ons uitsluitend op de directe impact. Het gaat dan niet alleen om een hack of ransomware, maar ook om informatie die gestolen wordt. Helaas zie ik dat als de grotere organisaties een CISO in dienst nemen, deze te snel wordt afgerekend en dat is niet terecht. Soms zijn ze nog geen half jaar in dienst. Dan denk ik, is dit nou de continuïteit die je als bedrijf wilt hebben? Een CISO moet wel over de middelen beschikken om een organisatie te beschermen tegen de dreigingen. Vaak is er te weinig budget en staan mensen onder te zware druk. De continuïteit wordt niet gediend door af te rekenen met de CISO.”

WAAR MOETEN BEDRIJVEN IN DE TOEKOMST REKENING MEE HOUDEN?

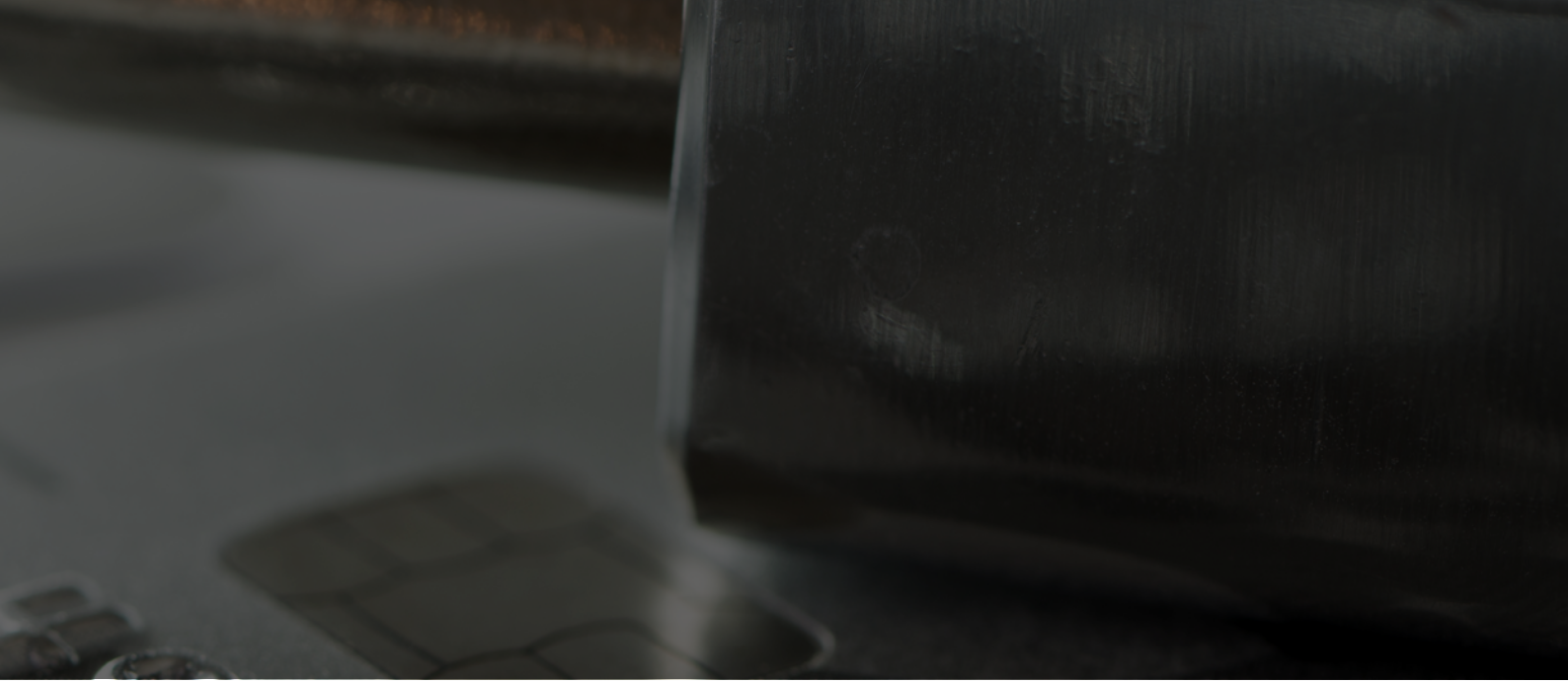
“Cyber security-verzekeringen worden nog weinig verkocht. We staan aan het prille begin van dit gedachtegoed. En toch zien verzekeraars dit als een investering die de komende jaren veel aan belang zal toenemen. Als je als bedrijf een toeleverancier bent van een grote organisatie, zal steeds meer gevraagd worden of de beveiliging op orde is. Want wat gebeurt er bij een cyberaanval? Kunnen de producten dan ook geleverd worden of valt alles om? Gemiddeld zijn bedrijven 60 dagen na een cyberimpact nog bezig dit op te lossen en weg te werken. Eén van de acties die je kunt nemen, is een verzekering afsluiten om je cyber-risico’s af te dekken. Dat wordt steeds belangrijker om je bedrijfscontinuïteit te managen. Een belangrijke factor hierbij is de onderliggende weerbaarheids- of risicoanalysesystemen die je continu over de stand van veiligheid kunnen informeren. Periodieke metingen, een keer per jaar, dragen hier maar marginaal aan bij. Een andere factor is dat je aan de hand van de momentane informatie op altijd kunt bepalen hoe je beveiliging ervoor staat. Ook kun je dan veel sneller reageren.”

MAAR VERWERKEN ZE DIT STRAKS OOK NIET ALS EIS IN DE ISO-CERTIFICERING?

“Ik denk dat een ISO-normering niet wordt gekoppeld aan een verzekeringspolis. De normeringen worden in de aankomende tijd wel vaker aangescherpt vermoed ik.”

MAAR HOE WORDT BEPAALD WAT VERZEKERAARS GAAN VERGOEDEN?

“Daar raak je een belangrijk punt, want verzekeraars hebben een protocol, een draaiboek en een impact-procedure klaarliggen. Zoals ik al zei, veel informatie in organisaties wordt onzichtbaar door buitenstaanders verkregen en deze impact wordt vaak niet beschouwd. Kijk bijvoorbeeld naar de impact van bijvoorbeeld restdataverzameling. Soshana Zuboff schrijft daarover in haar boek ‘the age of surveillance capitalism’. Informatieverzameling via het internet kan leiden tot een situatie waarbij je ‘one of those companies’ wordt ‘who wondered what the hell happened’. Amerikanen, Russen, Engelsen, Israëliërs en Aziaten zijn veel meer bezig dan wij in West-Europa met de economische impact vanuit internet. We wanen ons nog te veel veilig of denken dat het wel gaat meevallen met de impact. De verzekering dekt nu wel schade door een ransomware-aanval. De cyberverzekeringen zullen zich qua dekking in de aankomende jaren nog gaan ontwikkelen.”



WAT KUN JE NU ALS BEDRIJF DOEN OM IN DEZE SITUATIE MEER WEERBAAR TE WORDEN?

"Kies voor een business-, strategisch- of een keten-risicoanalyse. Bekijk welke factoren je beter wilt maken en hoe je dit gaat doen. Veel maatregelen overlappen elkaar in verschillende normen, zoals de AVG en de ISO 27001/2-normering. Bijvoorbeeld als het gaat om onderwerpen zoals waar staat je data, heb je die geclassificeerd en wie heeft via welke mogelijkheid daar toegang toe? Dat zijn inderdaad de processen die hierin terugkomen. Wat volgens ons handiger is, in relatie tot normeringen, is om de opbouw te starten met het bepalen van de risico's via een keuze die je het beste bij je organisatie vindt passen. Denk aan strategie, ketenaansprakelijkheid of een combinatie daarvan. Vervolgens kijk je naar de normeringen waarvan je besluit dat je die gaat volgen. Dan bepaal je de gemeenschappelijke deler. Bekijk welke werkelijke variabelen je gaat managen en hoe je dat doet. Daarna kijk je naar de specifieke acties bij een norm. Deze aanpak is efficiënter dan alle normeringen separaat te beschouwen zonder samenhang. Kies dan bijvoorbeeld voor continue risicomonitoring en voor gepaste weerbaarheids-diensten. Antivirus en een firewall zijn niet meer afdoende en een standaard back-up ook niet. Kijk naar de nieuwste en meer complete technieken zoals Endpoint Detectie en Response (EDR) en een Notary Cloud. Maar ook naar een websitebeschermingsservice met protectie tegen DNS spoofing, malware-injecties en DDoS-aanvallen."

'Een andere dreiging is informatie-scraping vanuit internet. Via websites wordt belangrijke informatie van je organisatie en processen verzameld. We ervaren hier al dan niet hinder van, maar dit vindt wel plaats.'

| iSENSE ICT PROFESSIONALS

Bij iSense kijken we niet alleen naar hoe groot je als ICT Professional nu al bent, maar ook naar hoe groot je nog kan worden! Want waarom zou je een baan nemen die straks niet meer past?! Door middel van onze kennisevenementen, het iSense Learning Center, field coaching en actieve begeleiding laten we mens en organisatie groeien.
iSense, op de groei!

Specialist in ICT arbeidsbemiddeling

Wij vinden ICT net zo fascinerend als jij, daarom bemiddelen wij alleen ICT'ers. Je hoeft ons niet uit te leggen dat Java niets met Javascript te maken heeft en .NET geen programmeertaal is. iSense'ers krijgen regelmatig trainingen om hun ICT- kennis up-to-date te houden. Zo zorgen wij ervoor dat je altijd met iemand in contact komt die dezelfde taal spreekt, wij snappen wat je doet!

Uitgebreid opleidingsaanbod

Helpt iSense jou aan een nieuwe baan of opdracht? Dan krijg jij toegang tot het iSense Learning Center; ons eigen opleidingsplatform met honderden ICT-opleidingen. Wij geven iedereen de mogelijkheid zich te ontwikkelen op technisch én persoonlijk vlak. Lees meer over het iSense Learning Center op www.isense.nl/learningcenter

6x 'ICT-Detacheerder van het jaar'

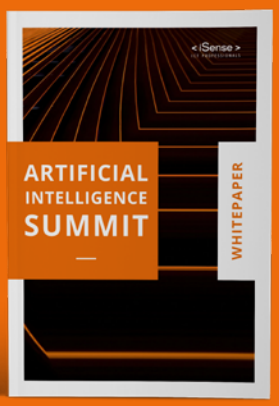
iSense heeft zes keer de Computable Award 'ICT-Detacheerder van het Jaar' gewonnen. iSense won deze award in 2012, 2013, 2014, 2015, 2016 en 2018. Hier zijn we enorm trots op!

Op de groei!

Samen met de ICT-community streven we naar ontwikkeling op technisch en persoonlijk vlak: daarom organiseren wij regelmatig een IT-event voor jou en jouw collega's.
Bekijk de volledige eventkalender op www.isense.nl/events

| WHITEPAPERS

Iedere maand organiseren wij een Summit, de Security Summit is daar natuurlijk één van! De inhoud van de andere Summits hebben we ook gebundeld in een whitepaper. Vrij te downloaden op: www.isense.nl/it-whitepapers



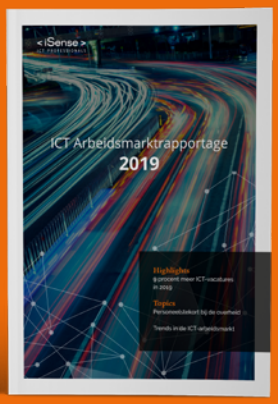
AI Summit

IoT Summit

BI Summit

| JAARRAPPORTAGE

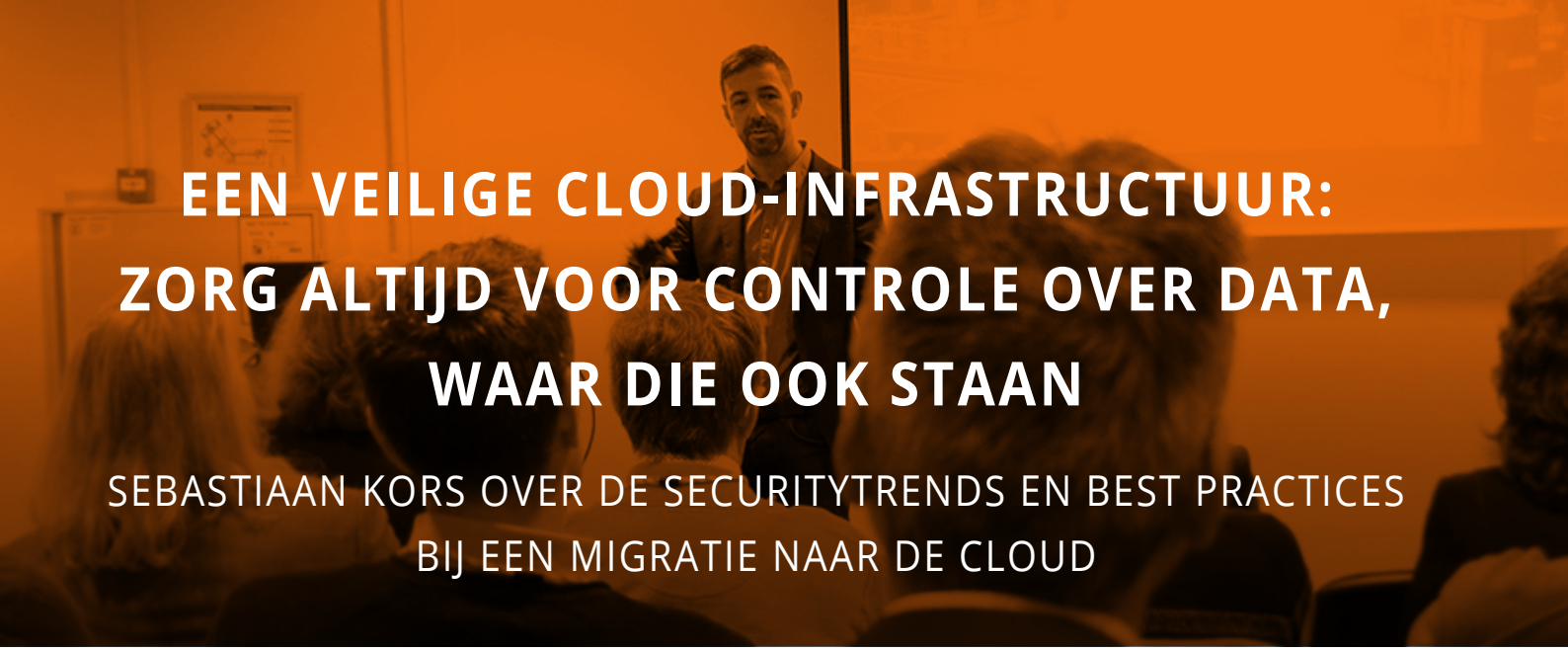
Uit de cijfers van de ICT Arbeidsmarktrapportage 2019 blijkt dat de vraag naar vacatures die vallen onder de functiegroep dataspecialisten sinds 2017 enorm toeneemt. In het afgelopen jaar steeg de vraag het snelst naar data scientists. Daarnaast deelt Marco Berkhout de trends in de ICT-Arbeidsmarkt. Ontdek alle trends in de uitgebreide jaarrapportage van 2019. Te downloaden op: www.isense.nl/ict-kwartaalrapportages



Jaarrapportage 2019

| MUST READS

Vond je dit interessant? Wij hebben nog veel meer toffe artikelen en video's over solliciteren, de ICT-arbeidsmarkt, evenementen, ICT-ontwikkelingen en natuurlijk nog veel meer! Check onze Must Reads pagina op www.isense.nl/must-reads of scan de QR code hiernaast.



EEN VEILIGE CLOUD-INFRASTRUCTUUR: ZORG ALTIJD VOOR CONTROLE OVER DATA, WAAR DIE OOK STAAN

SEBASTIAAN KORS OVER DE SECURITYTRENDS EN BEST PRACTICES BIJ EEN MIGRATIE NAAR DE CLOUD

DE OPKOMST EN HET VEELVULDIG GEBRUIK VAN PUBLIC EN PRIVATE CLOUD-STRUCTUREN LIJKT HAAST NIET MEER TE STOPPEN. SECURITY IS DAARBIJ EEN ONMISBAAR ONDERDEEL. OM ALS BEDRIJF HIER GOED OP IN TE KUNNEN SPELEN, IS VOLGENS SEBASTIAAN KORS, MANAGING DIRECTOR VAN NETWERK EN SECURITYBEDRIJF LANTECH, EEN AANPAK NODIG MET MINDER COMPLEXITEIT EN MEER VISIBILITEIT.

Het idee dat een hacker in bivakmuts achter zijn computer met een stapel pizzadozen zit verscholen, gaat natuurlijk allang niet meer op. In plaats daarvan zijn het de machines die aanvallen realtime uitvoeren. Bijvoorbeeld AI-malware dat continu van gedaante verandert en zich aanpast op basis van alles wat die tegenkomt. Maar het is de vraag of het bedrijfsleven tegen dit soort technologieën is opgewassen.

Veel bedrijven zijn sterk afhankelijk van third-party software. Criminelen doen daarmee hun voordeel door bijvoorbeeld een zwakke plek in de software te misbruiken en daarmee malware effectief in te kunnen zetten. Dit wordt in veel gevallen pas heel laat opgemerkt waardoor de malware zijn werk kan doen en van binnenuit andere computer-systemen worden geïnfecteerd. Dit soort aanvallen kunnen enorme financiële schade veroorzaken en wordt gezien als een gevaarlijke trend in cybercriminaliteit.

GEBREK AAN OVERZICHT

Een probleem waar veel IT-afdelingen mee te maken hebben, is een gebrek aan overzicht. “We gebruiken daarvoor allerlei middelen. Maar het gevolg daarvan is een samengesteld lappendeken van allerlei tools”, vertelt Kors. Door onder meer een gebrek aan mankracht is er te weinig tijd om alle binnenkomende alerts en incidenten te onderzoeken. “En dat terwijl het gemiddeld vier dagen kost om één incident te onderzoeken. Ondertussen komen per week tientallen tot zelfs wel duizenden alerts binnen. Dan zie je door de bomen het bos niet meer.”

DIVERSE ONTWIKKELINGEN IN DE MARKT

Ondertussen spelen diverse ontwikkelingen in de markt, die gevolgen hebben voor de manier waarop wij omgaan met onze infrastructuur en security. Zo werken we steeds meer toe naar een 24-uurseconomie. Dat betekent dat de manier waarop we werken verandert. “Netwerken en connectiviteit wordt steeds belangrijker. We willen immers op elk gewenst tijdstip en plaats kunnen werken en daarbij toegang krijgen tot het liefst zoveel mogelijk data”, vervolgt Kors. “De business-modellen worden dynamischer, waardoor meer behoefte is aan schaalbaarheid en flexibiliteit van de infrastructuren.” Waar voorheen security makkelijk te managen was, is dat nu een stuk onoverzichtelijker. “Op veel meer plekken dan alleen in je eigen infrastructuur staan nu kritische data, ook wel de kroonjuwelen, opgeslagen.”

Daarnaast blijft de hoeveelheid data enorm groeien. Zo vertelt Kors dat in 2025 naar verwachting wereldwijd 175 zetabyte is gegenereerd aan gegevens. “Wanneer je die hoeveelheid data op discs stapelt, kan je daarmee twintig keer naar de maan op en neer. De komende vijf jaar slaan we dan ook tien keer zoveel data op in vergelijking met alles wat is verzameld in de afgelopen

dertig jaar." Voor ons betekent dit dat security compliancy, de wet-en regelgeving steeds urgenter wordt.

De regelgeving omtrent de Algemene verordening gegevens-bescherming (AVG) is nog maar net geïmplementeerd. "We staan nog aan het begin van dit proces. Te merken is dat met name kleine tot middelgrote bedrijven hier nog moeite mee hebben", zegt Kors. Zo is duidelijke wetgeving inmiddels aanwezig, maar nog niet voldoende geborgd. "Nu maakt niemand zich daar nog druk om. Er is immers nauwelijks handhaving. De eerste grote boetes worden ondertussen wel al uitgedeeld aan overheidsinstellingen."

The Internet of Things (IoT) is van grote invloed op de infrastructuur, onder meer doordat het aantal kwetsbaarheden vele malen groter wordt. Het is makkelijk om bijvoorbeeld een auto of koelkast te hacken. Zo worden aanvals-vectoren, een hackmethode, alsmaar meer uitgevoerd. "Het grootste gevaar zit niet in hoe een bedrijf zijn security an sich regelt, maar hoe mensen in hun privé-omgeving hiermee omgaan", benadrukt Kors. Zo zitten mensen thuis vaak op devices die niet of nauwelijks beveiligd zijn. "Ze gebruiken dan bijvoorbeeld een VPN-tunnel, die dwars door de firewall heengaat. Alles wat daarin zit verstopt, is door geen firewall of IPS-systeem te detecteren." Voor hackers is dit een mooie manier om een aanval te maskeren. "Als je dan eenmaal binnen bent, is het ontzettend makkelijk om als criminele organisatie een virus achter te laten. Zo wist een hacker bijvoorbeeld in te breken bij een ziekenhuis via software van een systeem dat de liftmonteur gebruikte."

EEN GROTE UITDAGING

En dan is er natuurlijk nog de cloud, bij uitstek dé optie die de toenemende behoefte wat betreft schaalbaarheid en flexibiliteit tegemoetkomt. "Je hoeft nu niet meer grote ICT-voorzieningen te bouwen. Binnen drie klikken heb je immers al een infrastructuur staan in Azure, Amazon of private cloud", zegt Kors. Tegelijkertijd vormt dit een grote uitdaging voor security. "Zo is security on-premise makkelijker te controleren, bij de cloud hebben we een gezamenlijke verantwoordelijkheid. Auditing wordt dan ook lastiger. Je moet daarom goed nadenken in welke mate je de controle over de data uit handen geeft. Bekijk daarom welke soorten applicaties in de infrastructuur staan en waar die ondergebracht worden." Een migratie naar de cloud roept volgens Kors nieuwe vragen op. "Wat heb ik in de cloud staan? Wie kan bij de data? Hoe ga ik om met de toegang? Voldoe ik aan wet- en regelgeving? Zijn mijn containers veilig genoeg? En als je alles al in huis hebt staan, hoe zorg je ervoor dat alle data in een multi-cloud net zo goed controleerbaar en beheersbaar is als voorheen?"

Veelal werkt men in een hybride-omgeving, waarbij kritische data worden verzameld op meerdere plekken. Ga je over naar de cloud, dan moet je volgens Kors in gedachte houden welke prioriteit security heeft. "Is maximale controle gewenst, dan is on-premise het meest geschikt. Maar bekijk je dit vanuit een beschikbaarheids-perspectief, dan is een public of private cloud-oplossing beter." Het is een afweging die hierin gemaakt moet worden. "Denk daarom ook goed na over de data en de impact daarvan. Voldoet het aan de wensen en eisen die je stelt vanuit security en beschikbaarheids-perspectief?", vervolgt Kors. "De meest flexibele optie is de hybride-cloud. Wij zien dat klanten al één applicatie op drie verschillende platformen draaien. Zo kan frontend in Azure draaien, backend in Amazon en data-analyse in een beter beveiligde private cloud-omgeving. Bovendien kan je de business gemakkelijk op- en afschalen. Ook kan er makkelijk doorgeschaald worden naar de public cloud. En wanneer je tijdelijk veel capaciteit nodig hebt, kan dit later makkelijk weer afgeschaald worden."

AANDACHT VOOR VISIBILITEIT

Meer focus op visibiliteit kan helpen om de eerder gestelde vragen, die komen kijken bij een migratie naar de cloud, te kunnen beantwoorden, zodat daarmee ook meer controle is over het beheer van de security-infrastructuur. "We zijn hard op weg om al onze applicaties en data naar de cloud te migreren", zegt Kors. Maar over beveiliging wordt volgens hem te laat nagedacht. "Dan zou je kunnen zeggen, we brengen alles bij Azure onder. Die zullen dat wel voor elkaar hebben. Maar dat is gedeeltelijk het geval. Ze bieden wel oplossingen aan, mogelijkheden om toegang te geven om de zaken te regelen die je gewend was om te doen, maar dan blijf je toch bij die single cloud-providers." Iedere cloudprovider heeft namelijk zijn eigen native tools. "Die werken goed, zolang je binnen de silo van de cloudprovider blijft", zegt Kors. "Maar dan blijven processen en gegevens op afzonderlijke servers of in afzonderlijke datacenters bewaard en die kunnen dan niet met elkaar communiceren."

CYBERSECURITYMONITOR CBS

Uit de Cybersecuritymonitor 2019 van het CBS blijkt dat bedrijven steeds meer maatregelen nemen om zich te weren tegen digitale aanvallen. Met name middelgrote bedrijven maken nu een inhaalslag, zo'n 40 procent hiervan geeft aan meer dan zes cybersecurity maatregelen te nemen. Van de grotere organisaties zegt 90 procent dit te doen. Daarentegen is het voor bedrijven met twee werknemers slechter gesteld, daarvoor geldt dat slechts zeventien procent meer dan zes maatregelen neemt.

EEN HOLISTISCHE BENADERING

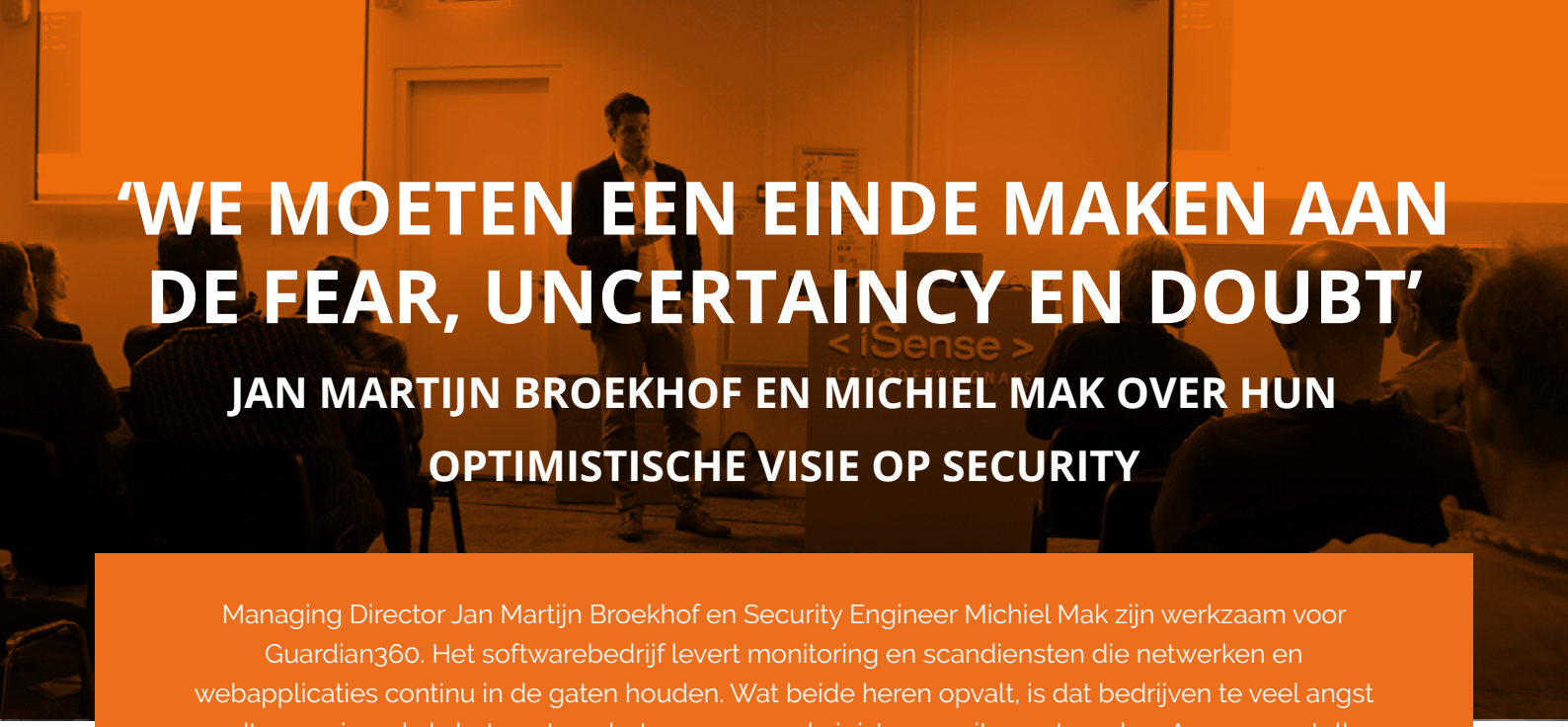
Het beste is om een integraal overzicht te hebben. “Kies daarom in een multi-cloudomgeving voor een holistische benadering.” Dat kan volgens Kors op basis van het NIST Cybersecurity Framework, een beleidskader van richtlijnen voor het securitylandschap. In het kort zijn daarbij vier verschillende elementen van belang.

- Protect. Zorg voor de juiste middelen om je omgeving, netwerk, data en toegang te beschermen. Dat betekent niet alleen het toepassen van een VPN, firewall of antivirus, maar ook het verzorgen van de benodigde updates.
- Detect. Enkel beschermen is niet genoeg. Kwetsbaarheden zijn onontkoombaar. In diverse infrastructuren moet tijdig gedetecteerd worden. Monitor in ieder geval het netwerk, toegang en gebruik van je kritische data en je end-points.
- Respond. Als een kwetsbaarheid of security breach is gedetecteerd, moet zo snel mogelijk ingegrepen worden. Maar hoe reageer je op het moment dat een hack in het weekend plaatsvindt? Dat soort zaken kan je ook uitbesteden.
- Recover. Is er gereageerd, dan moet alles zo snel mogelijk weer gerepareerd worden. Mitigeer alles weer tot een aanvaardbaar risico. Ook al is na het ontdekken van een kwetsbaarheid geen schade aangericht, toch is het goed om een specialist in te schakelen om te kijken of er toch niet iets over het hoofd is gezien. Vervolgens moet alles weer geüpdatet worden.

PRAKTISCHE AANBEVELINGEN

Om een hack te voorkomen, moeten we het net wat moeilijker maken dan bij de buren. Volgens Kors moet er altijd controle zijn. Data staat namelijk niet alleen in de serverkast, maar overal: in branches, SaaS, public of private cloud en mobiel. Om dit te bewerkstelligen, biedt Kors een aantal praktische aanbevelingen.

- Inventariseer het ICT-landschap. Het is nog vaak een uitdaging om te weten waar de data precies staan. Als dat bekend is, kan prioriteit gegeven worden aan hoe omgegaan dient te worden met visibiliteit, controle en security.
- Maak een cloud roadmap. Classificeer het applicatielandschap. Zo leent de ene applicatie zich goed voor de public cloud, waar de ander weer beter is voor private cloud.
- Creëer visibiliteit. Kies niet alleen voor een puntoplossing per infrastructuur, maar probeer dat zoveel mogelijk over het hele landschap te leggen.
- Bedenk welke rol je wilt als organisatie en individu. Het wordt steeds complexer om alles bij te houden als organisatie. Doe je dat zelf? Kies je voor outsourcing? In de markt is er een enorme vraag naar securityspecialisaties. Je hoeft niet alles zelf te regelen. Er zijn genoeg partners die je daarbij weten te helpen.



‘WE MOETEN EEN EINDE MAKEN AAN DE FEAR, UNCERTAINCY EN DOUBT’

JAN MARTIJN BROEKHOF EN MICHIEL MAK OVER HUN OPTIMISTISCHE VISIE OP SECURITY

Managing Director Jan Martijn Broekhof en Security Engineer Michiel Mak zijn werkzaam voor Guardian360. Het softwarebedrijf levert monitoring en scandiensten die netwerken en webapplicaties continu in de gaten houden. Wat beide heren opvalt, is dat bedrijven te veel angst wordt aangejaagd als het gaat om het nemen van de juiste securitymaatregelen. Aan ons vertellen ze daarom hoe we, zonder al te veel moeite, om kunnen gaan met vulnerability management, hackers en welke rol scrum bij hen speelt in het ontwikkelen van veilige software.

Veel bedrijven investeren in mooie en dure securitymiddelen om zodoende te automatiseren, het bedrijfsproces efficiënter te maken en concurrentievoordeel te behalen. Maar Broekhof noemt het onrechtvaardig dat bedrijven zich vervolgens zorgen moeten maken of ze überhaupt van die middelen gebruik kunnen maken. Daarnaast is het volgens Broekhof zonde dat veel organisaties angst wordt aangejaagd als het gaat om digitale veiligheid. Tenslotte werkt angst eerder verlammend bij mensen dan dat het aanzet tot actie.

Natuurlijk is de kans op een aanval een belangrijk punt van aandacht. Want als een organisatie de zaken niet op orde heeft, kan dit rampzalige consequenties hebben. Feitelijk gezien klopt het dat veel organisaties vatbaar zijn voor digitale aanvallen. Maar als we blijven roepen wat de mogelijke schade is en het niet hebben over oplossingen, komen we niet verder. Broekhof wil een einde maken aan Fear, Uncertainty en Doubt in security. Ook wel FUD genoemd, een strategie waarbij verwarring en angst onder consumenten wordt aangewakkerd ten behoeve van de verkoop van bepaalde producten en diensten.

De nieuwe helden in security

Toegegeven, het is niet makkelijk security intern te organiseren. De vraag naar opgeleide specialisten neemt toe, maar deze is op korte termijn niet op te vangen. Broekhof en Mak pleitten daarom voor meer automatisering. Zo kan veel repeterend werk worden opgevangen. Dat geeft professionals meer ruimte om zich bezig te houden met complexere vraagstukken.

System engineers en developers zijn volgens Broekhof de nieuwe helden op securitygebied. Eigenlijk houden deze professionals zich hier al mee bezig. Denk bijvoorbeeld aan patchen, updaten, het beheren van de firewall, aanzetten van multi-factor authentication of het verder beveiligen van een webapplicatie. Die trend is in een organisatie gemakkelijk verder door te voeren. Bovendien merken Broekhof en Mak dat bedrijven die zelf hun systeembeheer regelen, engineers in dienst hebben die de business goed kennen en zo weten wat er speelt binnen een organisatie. Dat is minder het geval wanneer een derde partij een dergelijk product of dienst regelt.

Meer aandacht vanuit het mkb

Niet alleen de grote corporates, maar ook het midden- en kleinbedrijf (mkb) besteedt meer aandacht aan security. Alhoewel mkb-bedrijven meestal geen tonnen te besteden hebben, zijn er nog genoeg haalbare maatregelen te nemen om de basisbeveiliging op orde te brengen. Dat is onder meer afhankelijk van het risico dat je wilt lopen en de grootte van het budget. Zo zijn er diverse gratis tools en methoden beschikbaar. Bovendien hangt dit ook af van het type bedrijf. Een groenteboer heeft immers weer een heel ander profiel dan een ziekenhuis.

Succes en technologie wordt vaak aangehaald als essentiële securitycomponenten. Broekhof en Mak koppelen dit aan risicobeheersing. Daarbij zijn diverse zaken van belang. Want hoe voorkom je zoveel mogelijk ellende? Wat gebeurt er op het moment dat je organisatie wordt getroffen door een digitale aanval? Hoe ga je snel handelen waardoor de schade zoveel mogelijk beperkt blijft? Zo focust het ene bedrijf op techniek, waar het andere zich richt op het bewustzijn binnen de organisatie. Dan is gedragsverandering weer ontzettend belangrijk.

Strengere securityeisen

Verder vermoedt Broekhof dat klanten in de toekomst meer securityeisen gaan stellen aan bedrijven. Dat betekent dat je moet kunnen aantonen dat je als bedrijf beschikt over een gedegen beveiliging. Er is nog niet veel vraag naar een cyberrisicoverzekering. Verder vindt Broekhof dat de businesscase van veel verzekeraars nog niet klopt. Zo is er nu een te lage premie berekend waar een relatief hoog uitkeringsbedrag tegenover staat. Daarentegen is bij Amerikaanse verzekeraars al te zien dat de premie gaat stijgen en andere partijen zich weer van de markt af bewegen.

Verzekeraars bieden bedrijven wel begeleiding, maar het mkb heeft het nog wel lastig. Sinds de invoering van de Algemene verordening gegevensbescherming (AVG) is de hackalert populairder geworden. Maar verzekeren en schadeherstel is onder mkb-bedrijven nog weinig te zien. En dat terwijl het volgens Broekhof een mooie sluitsteen is voor de totale risico-beheersing van een organisatie. Je verzekert je namelijk voor iets waarvan de kans relatief klein is dat het gebeurt. Maar als het gebeurt, heeft dit een enorme impact. Wat verder opvallend is, is dat ransomware nog wordt vergoed door verzekeraars. Broekhof snapt de afweging, maar vindt dit niet handig. Zo wordt het gehele fenomeen in stand gehouden. Bovendien beloon je hiermee min of meer kwaadwillenden met hun misdaad.

Scrum en het ontwikkelen van veilige software

Volgens Mak is vulnerabililty management een onderdeel dat ieder bedrijf eigenlijk als basisvereiste zou moeten integreren. Met de software die hij bouwt, is het mogelijk om on-premise te scannen, maar ook in de cloud of hybrid.

"Op het moment dat we een VM kunnen deployen ergens op een VMware of Hyper-V instance, dan kunnen we ook in de cloud scannen. Als je kijkt wat Azure al doet, is heel veel security al geregeld. Maar een vulnerability scan zit er nog niet in. We hebben op Azure een scanner draaien, maar nog niet vanuit de marketplace. Daar werken we nu naar toe. Het kan zijn dat Microsoft zegt dat ze ook aan vulnerability scanning gaan doen, maar vooralsnog laten ze dat aan derden over."

"We doen scrum, in sprints van twee weken. En natuurlijk hebben we retrospectives. Zo kijken we hoe we ervoor kunnen zorgen dat de code goed is, om zo constant te kunnen doorgaan met ont-wikkelen en integreren. Het gaat dus om de CI/CD pipelines. Eerst kijken we naar onze sprintplanning. Dan gaan we programmeren natuurlijk. Het bouwen en testen gebeurt automatisch in onze pipelines. Dat gaat allemaal via Gitlab, wat vergelijkbaar is met Github. Hetzelfde is bij de delivery. Ook moet het alle testen doorkomen, want anders kan je de code niet uploaden.

Het securitydeel zit in het testen. Zo moet ervoor gezorgd worden dat alles het goed doet en dat de formatting klopt. In de test doen we ook hardening. Onder meer wordt gekeken naar onze docker containers. En dat is een groot gedeelte van onze dev-omgeving. Want alles draait eigenlijk in docker, alles zit in losse containers, vanwege de microservices. In die pipelines kan je zelf definiëren waar alles aan moet voldoen. Bijvoorbeeld of je een bepaald woord in je code mag hebben of wachtwoorden die niet mogen. Je kan er alles in bouwen waarmee je wilt testen. Pas als die door de test heen komt, kan die door een ander gereviewd en gemerged worden. En dan gaat die de volgende pipeline in voor delivery."

Experis ManpowerGroup | < iSense > ICT PROFESSIONALS

Bezoekadres hoofdkantoor iSense:
Zuidelijk Halfrond 11
2801 DD, Gouda

Tel: 0182 69 20 20
E-mail: info@isense.nl

Bezoekadres iSense Eindhoven:
Flight Forum 840
5657 DV Eindhoven

Tel: 040 800 2240
E-mail: info@isense.nl

6x WINNAAR
ICT-DETACHEERDER VAN HET JAAR
COMPUTABLE AWARDS
2015 2016 2018 2013 2014 2012