Bedrijven zijn niet gewapend tegen datalek

PIETER HAECK

Driekwart van de Belgische bedrijven heeft nog geen stappen gezet om de nieuwe Europese regels rond databescherming, die over een jaar ingaan, na te leven. De nieuwe richtlijnen moeten burgers weer controle geven over hun data en schrijven ook voor hoe bedrijven moeten reageren op een cyberaanval en datalek.

Dat blijkt uit een studie van de verzekeringsmakelaar Vanbreda in een week waarin cybercriminelen met malware, het kwaadaardige zusje van software, honderdduizenden computers wereldwijd gijzelden in ruil voor een betaling met de virtuele munt bitcoin.

Uit een rondvraag bij de Belgische cybersecurity-experts blijkt dat ook in ons land aanvallen en datalekken meer regel dan uitzondering zijn. De vraag is niet of er een aanval komt, maar wel wanneer, klinkt het.

Het is opmerkelijk dat bedrijven amper bezig zijn met hun data. De helft van de bedrijven heeft geen verantwoordelijke voor databescherming. En het gros van de bedrijven maakt zijn personeel niet bewust van cyberrisico's. **P13-14**

Niemand gewapend tegen digitaal geweld

Bedrijven beleven hun ergste digitale nachtmerrie. Terwijl cybercriminelen continu op hun **data-infrastructuur** inbeuken, dreigen toezichthouders met monsterboetes als ze die niet adequaat beveiligen. Weinig ondernemers lijken echt voorbereid.

PIETER HAECK

Een beetje georganiseerde dievenbende berooft in één nacht een handvol bedrijven en houdt er een leuke buit aan over. Maar dat is niets in vergelijking met hun digitale collega's. De voorbije week gijzelden cybercriminelen met de hulp van malware, het boosaardige broertje van software, in geen tijd 200.000 computers in 150 landen. Het WannaCry-virus gooide cruciale bestanden, data en systemen van overheden en bedrijven op slot. Pas na betaling kwamen ze weer vrij.

De digitale dreiging komt van verschillende kanten. Amper enkele dagen na WannaCry bleken wereldwijd honderdduizenden pc's besmet door Adylkuzz, een virus dat de rekenkracht van je computer misbruikt om virtuele munten te creëren. Ook dit keer doken de criminelen in een lek in oudere versies van het besturingssysteem Windows, waarvoor Microsoft drie maanden geleden nochtans al een reparatiekit online gooide.

Het legt een lakse houding tegenover digitale beveiliging bloot. En dat is pijnlijk, zeker nu het aantal cyberaanvallen zo snel toeneemt. Volgens de beveiligingsreus Gemalto was er in 2016 wereldwijd 1.792 keer een datalek bij bedrijven. Daarbij waren 1,4 miljard stukjes data betrokken, 86 procent meer dan in 2015.

Daar is niets abstracts aan. 1,4 miljard stukjes data, dat is 1,4 miljard keer een bankkaartnummer van een werknemer, een e-mailadres van een sollicitant of een gsm-nummer van een klant. Het zijn allemaal gegevens die ook de Vlaamse bedrijven, van multinationals tot kmo's, massaal opslaan in databases. 'Voor veel bedrijven is het niet meer de vraag óf, maar

Lees verder pagina 14

Niemand gewapend tegen digitaal geweld

Vervolg van pagina 13

wannéér het kwaad toeslaat', zegt Peter Van Dyck, partner bij het advocatenkantoor Allen & Overy.

Taboesfeer

Cyberaanvallen en datalekken zijn drama's, zowel voor bedrijven als voor burgers. Het vergroot de bereidwilligheid om de criminelen te betalen.

'Een groot Belgisch bedrijf zag vorig jaar zijn computersystemen gegijzeld door een virus. Ze kwamen pas vrij na betaling van 5.000 euro via de virtuele munt bitcoin', zegt Matthias Vierstraete, advocaat IT-recht bij Laga. Begin deze week vertelde Danielle Van Wesenbeeck, de zaakvoerder van Mastermail, dat ook zij het gevraagde bedrag heeft betaald nadat ze een gijzelvirus had binnengekregen.

De getuigenissen zijn slechts het topje van de ijsberg. Op cybercriminaliteit rust een taboe. Bedrijven zijn als de dood voor reputatieschade. Het draagt ertoe bij dat veel ondernemers nog geen wakeupcall kregen. Ze blijven ook onverschillig bij de druk die Europa opvoert.

De Europese instellingen gaven midden vorig jaar groen licht voor nieuwe regels die de gegevens van de burgers beter moeten beschermen. De General Data Protection Regulation (GDPR) moet burgers weer controle geven over hun e-mailadressen, gsm-nummers en bankkaartnummers, die in de databases van bedrijven rondklotsen. Minstens even belangrijk zijn de regels voor wat bedrijven moeten doen als cybercriminelen data stelen. Tegen 25 mei 2018 moeten ze in staat zijn adequaat te reageren.

Een jaar voor die deadline is het gros van de Belgische bedrijven totaal niet klaar om op te treden bij een datalek, leert een studie van de verzekeringsmaatschappij Vanbreda. De enquête bij 110 Belgische bedrijven levert ontluisterende resultaten op. 36 procent hoorde nog nooit van het vierletterwoord GDPR, 40 procent enkel vaag. Slechts 24 procent deed al stappen om zich te beveiligen en gepast te reageren. In de helft van de bedrijven is niemand verantwoordelijk voor veiligheid of databescherming.

Perfecte storm

Als de veelvuldige datalekken de ondernemers de ogen niet openen, dan misschien de torenhoge boetes die Europa in petto heeft. Wie vanaf mei volgend jaar door slordig databeheer in het vizier van de privacycommissie komt, riskeert boetes tot 4 procent van de wereldwijde jaaromzet. Voor multinationals kan dat in de tientallen miljoenen lopen. 'Bedrijven zitten eigenlijk in de perfecte storm, met langs de ene kant steeds meer cyberaanvallen en langs de andere kant fors strengere regels om zich ertegen te beschermen', stelt Peter Van Dyck van het advocatenkantoor Allen & Overy.

Bedrijven zullen heel anders moeten reageren als ze na de Europese deadline het slachtoffer worden van een aanval zoals WannaCry. 'Als systemen met persoonsgegevens worden gegijzeld door zo'n specifiek virus zijn ze in feite onbeschikbaar. Op dat moment is sprake van een inbreuk op die persoonsgegevens',

Voor veel bedrijven is het niet meer de vraag óf, maar wannéér het kwaad toeslaat.

Peter Van Dyck, partner Allen & Overy

76%

76 procent van de Belgische bedrijven heeft nog niets ondernomen om in orde te zijn met de Europese databeschermingsregels. Dat leert een studie van de verzekeringsmaatschappij Vanbreda.

Kmo's met een bedrijfsjurist zijn al in gang geschoten. Voor andere dringt de tijd.

Frederik Debusseré, advocaat IT-recht

zegt Frederic Debusseré, advocaat IT-recht van het advocatenkantoor time.lex.

Getroffen bedrijven moeten zo'n aanval binnen 72 uur melden aan de privacycommissie en aan het brede publiek. Die 'meldingsplicht' is een van de beeinbreekers in de GDPR-wetgeving. Van Dyck: 'Stel, een werknemer verliest een USB-stick of een niet-beveiligde pc met daarop persoonsgegevens. De werknemer in kwestie moet dat signaleren aan de juiste persoon, die dat vervolgens op de juiste manier meldt. Nagenoeg elke medewerker in je bedrijf moet dus de procedures kennen.'

Het staat mijlenver van een andere vaststelling in de Vanbreda-enquête: 58 procent van de ondervraagde bedrijven zegt zijn werknemers niet bewust te maken van cyberrisico's.

De nieuwe databeschermingsregels overstijgen de muren van het IT-departement. Bedrijven die het hele proces nog moeten doorlopen, verzamelen maar beter mensen uit al hun departementen om de tafel. 'Persoonsgegevens stromen nu eenmaal door het hele bedrijf', zegt Vierstraete. 'Een hr-manager heeft vast een lijst met gegevens van mogelijke kandidaten. De logistiek manager regelt dan weer toegangsbadges en ander persoonlijk materiaal. Hij ziet ook persoonsgegevens door zijn handen glijden.'

Het telecom- en mediabedrijf Telenet gaf het voorbeeld met een 'basic privacy training' voor al zijn medewerkers. Bij de retailer Colruyt Group zitten juridische en technische profielen zij aan zij om het GDPR-proces in goede banen te leiden.

Klantenkaarten

Het Europese regime dat in mei 2018 in werking treedt, is een immens monster met veel nuances en uitzonderingsclausules. Zo geldt de meldingsplicht van 72 uur niet altijd. En de aanstelling van een data protection officer die aanwankelijk algemeen verplicht was, is intussen enkel nog verplicht voor overheden en data-intensieve bedrijven.

Ondernemers doen maar beter eerst aan 'soulsearching' voor ze zich in het doolhof begeven. 'De eerste fase is er sowieso één van datamapping', zegt Van Dyck. 'Je moet oplijsten welke systemen welke data bevatten, wie er toegang tot heeft en waar ze heen gaan.' Bij die oefening komen enkele klassieke gevoeligheden naar boven, zoals hoelang data mogen worden opgeslagen en of ze zomaar naar het buitenland mogen worden verstuisd.

Het maakt dat de spurt naar mei volgend jaar ook voor bedrijfsgiganten een hordeloop blijft. Colruyt Group, dat al lang een pak data vergaarde via de registraties voor klantenkaarten, maakte het eerder al mogelijk dat klanten hun gegevens online konden opvragen en aanpassen. 'De macht daarover in handen van de klant leggen is iets wat we al veel langer deden', zegt Karel De Wilde van Colruyt. 'Maar de GDPR-regels leggen andere formaten op, wat een aanpassing vergt.'

Een ander pijnpunt voor Colruyt is dat klanten telkens hun toestemming moeten geven als in de privacyregels iets verandert. 'Mensen zijn het niet gewoon om aan de kassa documenten te moeten ondertekenen. Daar zullen we iets op moeten vinden. Dat zal ook een stevige administratieve impact hebben.'

Drukke tijden

Bij kmo's zijn de vraagtekens nog groter. 'Bedrijven met een huisjurist zijn dit voorjaar al in gang geschoten. Voor andere dringt de tijd', zegt Debusseré. De experts zijn duidelijk: bedrijven moeten er vandaag mee bezig zijn, niet morgen. 'Het vereist meerdere maanden om alles in kaart brengen en de maatregelen te implementeren', zegt Vierstraete.

Advocatenkantoren en consultants staan voor drukke tijden. Een recente rondvraag van Beltug, de vereniging van zakelijke ICT-gebruikers, bij 330 bedrijven leert dat databeveiliging veruit de ICT-prioriteit nummer één is. 'Het aantal dossiers over cyberveiligheid en databescherming gaat in exponentieel stijgende lijn. In ons team zijn vier à vijf advocaten er continu mee bezig', bevestigt Van Dyck.

Geen enkel bedrijf ontsnapt aan de dwingende toezichthouders. Ook Facebook, de absolute koning in dataverzameling, niet. Het sociaal netwerk liep deze week tegen liefst twee Europese boetes aan. De Franse privacywaakhond CNIL eiste 150.000 euro voor enkele inbreuken op de Franse databeschermingsregels.

De Europese commissaris voor Mededinging Margrethe Vestager zwaaide met een boete van 110 miljoen euro, omdat Facebook 'misleidende informatie' zou hebben gegeven bij de overname van de berichtendienst Whatsapp. Het belang van Vestagers demarche werd kracht bijgezet door de actualiteit. Diezelfde ochtend bleek dat nog eens 243 miljoen unieke e-mailadressen op het web te grabbel lagen na hacks bij het zakelijk netwerk LinkedIn, de clouddienst Dropbox en de microblogger Tumblr.

WAT IS?

GDPR
General Data Protection Regulation is een set nieuwe Europese databeschermingsregels die op 25 mei 2018 van kracht wordt. De regels moeten burgers meer controle geven over de gegevens die bedrijven over hen opslaan. Nalatige ondernemers riskeren boetes van 4 procent van de wereldwijde jaaromzet.

Datagijzeling
Ransomware is een vorm van malware, kwaadaardige software die erop uit is binnen te dringen in computers. Het virus dringt veelal binnen via phishing mails, mails die echt lijken maar besmette links of bestanden bevatten. Zodra de ontvanger erop klikt, dringt het virus zijn computer binnen en zet het bestanden 'op slot'. Om de gegijzelde bestanden weer vrij te krijgen, moet hij losgeld betalen via de virtuele munt bitcoin.

DATA BESCHERMEN IN TWEE FASEN

De bedrijven die nog geen stappen hebben gezet om in orde te zijn met de Europese databeschermingsregels, moeten ruuweg twee fases doorlopen.

Fase 1: Identificeren waar zich de persoonsgegevens bevinden. In welke systemen zitten ze? Wie heeft er toegang toe? En waar gaan ze naartoe? Die oefening moet niet alleen het IT-departement maken. Ook de afdelingen human resources en marketing zien heel wat persoonsgegevens passeren. Het is 'soulsearching' voor het hele bedrijf.

Fase 2: Een risicoanalyse opstellen. Welke zaken zijn het precairst? Vrijwel alle bedrijven moeten hun procedures aanpassen om een datalek binnen 72 uur te kunnen melden. De aanstelling van een data protection officer kan handig zijn. Er moeten nogal wat gevoeligheden worden nagegaan. Hoelang mogen data opgeslagen blijven? Hoe mogen ze binnen het wettelijk kader naar andere landen, onderaannemers of andere vestigingen worden verstuisd? Veel bedrijven moeten daar nog aan sleutelen.