Thema Veiligheid
Tekst Brenno de Winter
Beeld 123RF®

Komt de digitale **Titanic**-ramp eraan?

In mei 2018 horen organisaties klaar te zijn met de implementatie van de privacyrichtlijn GDPR (General Data Protection Regulation). Het pad erheen is een helse toer. De regelgeving legt pijnlijk bloot hoe onvolwassen we eigenlijk met data omgaan.

Het kan behoorlijk rommelen in de bestuurskamer. Althans, als men ook maar een beetje door heeft wat de GDPR of de Algemene Verordening Gegevensbescherming betekent. Veel regels rond het beschermen van persoonsgegevens stonden al in de bestaande wetgeving. Eén groot verschil: het woord 'boete' is nu gevallen. De GDPR is een compliancefeestje, omdat niet de autoriteiten moeten aantonen dat een organisatie de zaken op orde heeft. Nee, in de nieuwe situatie moet het bedrijf zelf bewijzen dat het aan de spelregels voldoet.

Nemen we digitale rampen wel serieus genoeg?
Juist aan dat serieus nemen lijkt het te ontbreken. Als een hack in 2011 het einde van DigiNotar inluidt, blijkt vooral het toezicht te hebben gefaald. Ook de ingehuurde auditor blijkt onvoldoende te hebben geacteerd. De Onderzoeksraad voor Veiligheid trekt na een onderzoek vernietigende conclusies. Velen trekken zich die conclusies aan en ze maken ook de Nederlandse auditors alerter. Maar DigiNotar is niet uniek. Andere hacks – waar ook ter wereld – krijgen niet de aandacht die ze verdienen. In tegendeel, de meeste onderzoeken naar beveiligingsincidenten gaan met schimmigheid gepaard. Zelfs al willen we ervan leren, dan nog gaat het op deze manier niet lukken.

Zwijgen helpt niet
Zes jaar na de hack op DigiNotar blijkt Deloitte gehackt. Het bedrijf staat bekend als prominente speler op het gebied van accountancy, audits en cybersecurity. Uit de mediaberichten wordt duidelijk dat het beheerdersaccount is gekraakt. Dat bleek nog relatief eenvoudig, aangezien 'two-factor authentication' ontbrak. Mogelijk zijn e-mails van klanten met zeer gevoelige informatie door de daders ingezien. Ook lijkt het er sterk op dat met deze hack meer gegevens te benaderen zijn geweest. De organisatie ontdekte het lek – dat ergens in 2016 ontstond – in maart 2017, maar heeft geen idee wie erachter zit: een land, een concurrent, een kind op een zolderkamer of een groep criminelen. Als het lek eind september 2017 naar buiten komt omdat *The Guardian* er lucht van krijgt, is het onderzoek nog bezig. Door het zwijgen is er geen mogelijkheid om lering te trekken en opnieuw worden we er professioneler niet beter van.
De hack op Deloitte is meer een gegeven dan een schok. Wat de zaak opmerkelijk maakt zijn indicaties van basale fouten die naar buiten sijpelen. De zaak roept de vraag op hoe een organisatie kan voldoen aan de toekomstige GDPR. Ook roept het de vraag op wanneer organisaties aansluiting bij de ISO-27001-normering gaan zoeken.[1] We moeten ons afvragen wat er toch aan de hand is in de ICT-industrie wanneer het gaat over informatiebeveiliging. De norm om 10% van alle IT-uitgaven aan beveiliging te besteden wordt in bitter weinig organisaties gehaald. De daden stroken bij veel organisaties niet bij de risicovolle realiteit en een kritische boodschap is iets waarop de boardroom niet zit te wachten.

Digitale rampen gebeuren vaker dan je denkt
Bij ieder incident komt de ernst van het nieuws in eerste instantie hard aan. Een greep uit recente voorbeelden, en het zijn er veel. Neem de honderdduizenden Internet of Things-apparaten die opeens een massale DDoS-aanval uitvoerden op één website; het platleggen van DigiD

waardoor zakendoen met de overheid lastiger werd; cyber attacks op banken waardoor het doen van betalingen met bijvoorbeeld iDeal lastiger werden, KLM dat door de aanvallen het betalen voor bagage moest uitstellen; de meer dan een miljard records die bij Yahoo werden gestolen (en wat lang werd stilgehouden); de zeer gevoelige persoonsgegevens die bij Equifax – over onder andere creditwaardigheid – werden buitgemaakt en wat uiteindelijk leidde tot het aftreden van de CEO; het uitbreken van het Wannacry-virus met gijzelsoftware dat veel organisaties, waaronder ziekenhuizen, industrie en transport, trof; de op Wannacry lijkende uitbraak van gijzelsoftware van Petya of Non-Petya, dat ervoor zorgde dat grote bedrijven maanden digitaal van slag waren. En ga zo maar door. Iedere keer zijn er de 'oeh's en ah's', de media-aandacht en de obligate kamervragen. Veel minder is er het doel om echt door te graven naar de oorzaken en het delen van leereffecten.

Waarom we niet leren van digitale rampen

Een datalek leidt zelden of nooit tot een voor de hand liggend spervuur aan vragen van onderzoekende aard: hoe heeft het daar zover kunnen komen? Had een (internal) auditor de gevaren wel gesignaleerd en, zo ja, waarom is er niet op geacteerd? Loopt mijn organisatie niet precies datzelfde risico? Hoe komt het dat keer op keer dezelfde problematiek zorgt voor dezelfde problemen en niemand iets leert van eerdere fouten? Vragen die kunnen helpen met het op een verantwoorde wijze omgaan met data om zodoende herhaling te voorkomen.
De ernst van de materie lijkt nog niet door te dringen, omdat – zo hoor ik vaak – je data niet kunt 'voelen'. En precies dat argument komt vaak voor bij mensen die te weinig onderzoeken. Neem een zelfrijdende Tesla die concludeert dat een lange vrachtwagen met oplegger uit twee auto's bestaat waar het voertuig nét nog tussen past. De bestuurder overlijdt. Data is niet iets onschuldigs. Bij incidenten is onderzoek geboden, hier kan een internal auditor meerwaarde creëren.

De historische context, de Titanic en de maatregelen

De problematiek is zichtbaar en wordt erkend, maar de risico's dringen nog niet echt door. Dit verschijnsel is niet nieuw. In mijn laatste boek, *Digitale stormvloed*, wijs ik op de stappen die de mensheid moest zetten om volwassen met veiligheid om te gaan. De basis is lang geleden in de zeevaart gelegd. Daar vielen door de loop der eeuwen veel doden, met als dieptepunt de 13e eeuw waar in Mongolië gedurende twee 'goddelijke' stormen meer dan honderdduizend mensen om het leven kwamen bij aanvallen op Japan. Maar ook later, als de stoomboot wordt ingevoerd, neemt het aantal incidenten fors toe. Dit komt onder andere door de hogere snelheid van deze schepen.
Nederland ziet vroeg in dat regelgeving onvermijdelijk is en sluit in 1815 een handelsverdrag met daarin ook afspraken over veiligheid (het Rijnverdrag). Het drukke verkeer en de rivier-engtes maken dat voor de veiligheid noodzakelijk.
In de 19e eeuw loopt een poging om tot wereldwijde regels te komen voor de veiligheid tijdens een zes maanden durende

Stappen in de goede richting als de GDPR – die dwingen over data na te denken – worden gezien als een moetje, gezeur of een hoofdpijndossier

conferentie mis. Vooral de Britten zijn tegen het verdrag. Zij stellen dat de Britse regels volstaan. Die stemming slaat om als in 1912 de SS Titanic na een aanvaring met een ijsberg uiteindelijk in tweeën breekt en zinkt. Vele levens gaan verloren ondanks dat de SS California vlak bij de plaats des onheils vaart. Het gebrek aan uniforme afspraken heeft als gevolg dat de noodsignalen niet goed worden opgepikt. Tijdige hulpverlening blijft uit. Omdat de Titanic zijn eerste tocht maakt en veel hoogwaardigheidsbeklederes aan boord zijn, slaat de ramp in als een bom. Er volgt een luide roep om maatregelen.
In 1914 treedt het SOLAS-verdrag (Safety of Life at Sea) dat een aantal basale zaken rond veiligheid regelt in werking, zoals opleiding, reddingsboten, reddingsvesten, communicatieapparatuur, marifoon, brandblusmiddelen en radarsystemen. Het zijn allemaal zaken die óf de kans op een incident kleiner maken óf juist de gevolgen beperken, mocht er toch een ongeluk optreden. Ook is het verdrag zo vormgegeven dat als inzichten veranderen, nieuwe dreigingen ontstaan of er redenen zijn het verdrag aan te scherpen, dit kan gebeuren zonder een ingewikkeld ratificatieproces. Zo is recentelijk beveiliging onderdeel van SOLAS geworden. De regels zijn toetsbaar en daarom kan een overheid van een verdragsland ingrijpen op alle schepen die niet voldoen. Een Nederlands schip kan zo bijvoorbeeld bij non-compliance in de VS aan de ketting worden gelegd.

Komen tot regelgeving
De manier van denken over risicomanagement bij SOLAS zou eigenlijk hetzelfde moeten zijn als bij informatiebeveiliging. Onderzoek na onderzoek laat zien dat veel digitale rampen dezelfde oorzaken hebben, zoals slecht patchmanagement, zwak wachtwoord- en autorisatiebeheer, slechte compartimentering, gebrekkige detectie van incidenten, niet veilig ontwikkelde software, gebrekkig bewustzijn bij medewerkers met ongelukkig gedrag tot gevolg, en ga zo maar door.
Al deze punten zijn eigenlijk – net als in de zeevaart – hygiëneregels. Voor de meeste zaken hebben we standaarden, waardoor toetsing door bijvoorbeeld een internal auditor prima mogelijk is. Grote incidenten als DigiNotar, KPN, Sony (een aantal malen), Hacking Team, Deloitte, Equifax, lijken allemaal zeer basale oorzaken te kennen. Net als bij het Rijnverdrag loopt ook nu Nederland ten opzichte van veel andere landen voor met eigen ontwikkelde standaarden of het verwerken van de standaarden in concrete toepassingen. Erg nuttig in een 'digitale' zee waar we verbonden zijn met systemen over de hele wereld en er mogelijk slecht beveiligde Internet of Things-apparaten met honderdduizenden tegelijkertijd op de markt komen. Internationaal zijn de geesten echter nog niet rijp voor uniforme regelgeving. Hoewel de ongelukken vaak omvangrijk zijn leiden ze niet tot een brede, fundamentele verandering. Sterker nog, stappen in de goede richting als de GDPR – die dwingen over data na te denken – worden gezien als een moetje, gezeur of slechts als een hoofdpijndossier. Geen klimaat om als internal auditor je lekker bij te voelen. Het ontbreekt daarvoor nog aan die ene Titanic, althans zo lijkt het. Als dat moment aanbreekt hebben wij in Nederland in ieder geval wel een mooie aanzet gegeven met een eigen set aan standaarden, denk aan Grip op Secure Software Development of Grip op Privacy – laat ik het SODADS (Safety of Data at the Digital Sea) noemen. Misschien is dat dan ook het moment dat de sprong wordt gemaakt naar een internationaal framework. Het is mijn overtuiging dat het tijdperk van de internal auditor als onderkenner van dit soort risico's en als adviseur over te treffen maatregelen, echt gaat aanbreken. Het duurt misschien nog even voordat dit ook erkend zal worden in bestuurskamers, hoewel een (digitale) Titanic dit proces zeker zal bespoedigen. <<

Noot
1. ISO 27001 is een ISO-standaard voor informatiebeveiliging.

Brenno de Winter, onder meer bekend van het kraken van de OV-chipkaart, heeft meerdere boeken op zijn naam staan. In zijn meest recente boek *Digitale stormvloed* breekt hij een lans voor een stringentere vorm van beveiliging door een parallel te trekken met de zeevaart.