

Informatiebeveiliging door bewustwording

Om problemen met informatiebeveiliging aan te pakken, kiezen bedrijven steeds vaker voor een focus op automatisering. Daarmee verschuift de aandacht van informatiebeheer naar systeembeveiliging. Op dit vakgebied hebben informatie-professionals veelal het nakijken. Met als gevolg: beheertaken van digitale informatie worden verwaarloosd en achteloos gebruik van informatie neemt toe. De informatieprofessional moet hier (weer) zijn verantwoordelijkheid nemen, betogen Marinka Voorhout en Jeroen Tegelaar.

Marinka Voorhout en Jeroen Tegelaar

De wildgroei aan digitale informatie is de afgelopen jaren zodanig in omvang toegenomen dat dit een reële bedreiging vormt voor het adequaat functioneren van organisaties en bedrijven. Medewerkers komen om in bergen mails en verschillende versies van documenten. Deze informatie-explosie komt ook omdat we steeds beter de mogelijkheden van virtueel samenwerken benutten en tegelijkertijd steeds sneller een reactie van elkaar (en van vreemden) verwachten. Dat beperkt zich niet alleen binnen een bedrijf, maar gaat steeds vaker ook via online services als cloud computing, social media en webbased applicaties. Tweets, blogs, wiki's maar ook sms en rss zijn niet meer weg te denken uit onze hui-

dige wereld. Anders gezegd: er zijn nieuwe manieren gekomen waarop informatie bedoeld of onbedoeld en op elk gewenst moment kan worden gedeeld – en het einde is nog niet in zicht. Deze verschuiving in informatiegebruik en -behoefte heeft grote gevolgen. We zijn onzorgvuldiger geworden bij het beheren en afgeven van onze informatie en onze wachtwoorden blinken vaak niet uit in originaliteit. De hedendaagse roep om betere beveiliging van digitale informatie is dan ook zeer terecht. Maar de huidige benadering vanuit de techniek is naar onze mening onvoldoende en zelfs gevaarlijk. Gevaarlijk omdat bedrijven en organisaties een gevoel van schijnzekerheid creëren. Beveiliging is niet alleen het borgen van – de toegang tot – de systemen, maar ook een beveiliging van de content van die systemen, de informatie zelf. Dit laatste is wezenlijk iets anders en het is hier waar de informatieprofessional zijn verantwoordelijkheid in dient te nemen.

Onzorgvuldig gebruik

Informatiebeveiliging komt als onderwerp voornamelijk in het nieuws wanneer er spectaculair iets misgaat. Wie her-

**Wie
zijn...**



Marinka Voorhout is senior adviseur informatiemanagement bij Content Strategy.
Jeroen Tegelaar is redacteur van InformatieProfessional.





innert zich niet de geslaagde hackpoging in de servers van het Amerikaanse Pentagon? Dit voorbeeld van ongewenste toegang tot vaak vertrouwelijke informatie en data door onbevoegden vormt een groot risico voor de maatschappij. Niet alleen worden personen geschaad in hun privacy en welzijn, ook organisaties lijden imagoschade en zien hun concurrentiepositie aangetast. Toch betreft het hier, in onze optiek, afzonderlijke incidenten, omdat in de regel bedrijven hun toegang afdoende op orde hebben.

Een veel vaker voorkomend en daarmee in potentie veel groter probleem is het onzorgvuldig gebruik en beheer van informatie. Herinnert u zich nog het verhaal van een verloren USB-stick met gevoelige info van het ministerie van Defensie, achtergelaten in een huurauto? De computer van de Amsterdamse Officier van Justitie Tonino? Het wachtwoord van een directeur op een geeltje op zijn computer? En, recent nog, de plaatsing van gevoelige en vertrouwelijke informatie op de website van het ministerie van Justitie? Dit zijn alleen nog maar voorbeelden van onzorgvuldig informatiegebruik *binnen* een organisatie.

Ook de opkomst van social media geeft

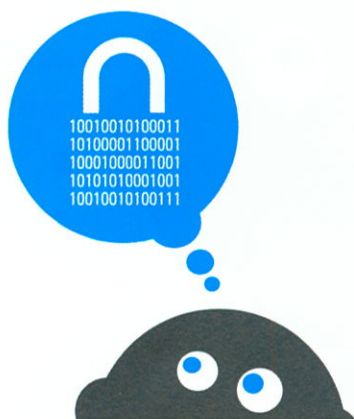
extra reden tot zorg over de juiste omgang met informatie. Denk bijvoorbeeld aan de tweets van kamerleden die achteraf moesten worden gerectificeerd – met ontslag tot gevolg. Een ander voorbeeld is de echtgenote van de nieuwe directeur van een Britse veiligheidsdienst die op Facebook naast vakantiefoto's ook het vakantieadres en andere privégegevens plaatste. Misschien herinnert u zich

'Aandacht verschuift van informatiebeheer naar systeembeveiliging'



Illustratie: Tom van Staveren

‘Vertrouwelijke informatie die op straat komt te liggen, is meestal al een jaar oud’



ook nog het verhaal van de Zwitserse werknemer die ziekte claimde vanwege gevoeligheid voor licht en beeldschermen, waarna collega's zagen hoe ze op datzelfde moment thuis haar Facebook-pagina bijwerkte.

Al deze voorbeelden van onzorgvuldig gebruik dienen zo snel mogelijk binnen organisaties en bedrijven geadresseerd te worden. De huidige aanpak van informatiebeveiliging biedt hiervoor op dit moment onvoldoende antwoorden. Voor de informatieprofessional is het moment aangebroken dit vacuüm op te vullen.

Verleiding van technologie

Informatieprofessionals in de analoge wereld waren oorspronkelijk verant-

woordelijk voor informatiebeveiliging. Zij beheerden en creëerden de dossiers met de status 'geheim', 'vertrouwelijk' of 'staatsgeheim'. Zij adviseerden over versiebeheer, kenden en bepaalden de locatie van informatie en beslisten wat weg mocht en wat mocht blijven. Nu informatie steeds meer digitaal gemaakt en benaderbaar is, kiezen bedrijven echter vaker voor een focus op automatisering om de problemen met beveiliging aan te pakken. Door deze focus verschuift de aandacht van informatiebeheer naar systeembeveiliging. De firewall wordt spreekwoordelijk nog dikker, er worden diodes geplaatst en USB-sticks krijgen een extra beveiligingscode ingebouwd. Op dit speciale vakgebied heeft de informatieprofessional momenteel veelal het nakijken, al is hij hier zelf ten dele ook de oorzaak van wanneer hij vast blijft houden aan de gestelde principes uit de oude analoge wereld. Het gevolg: genoemde behertaken van digitale informatie worden verwaarloosd en het achteloos gebruik van informatie neemt toe.

Waarde van informatie

Zoals gezegd, het is hoog tijd dat de professional zich gaat bezighouden met de beveiliging van informatie in een digitale wereld. Om te beginnen dient hij vanuit zijn vakgebied meer tegenwicht te bieden aan de groeiende onachtzaamheid van werknemers ten opzichte van informatie. Daarbij moet snel duidelijk worden gemaakt wat de gevolgen kunnen zijn van het verspreiden van presentaties met mogelijk gevoelige informatie via mail of applicaties als Slideshare. Werknemers realiseren zich vaak onvoldoende dat de informatie niet hun eigendom is, maar die van organisaties en bedrijven.

De professional dient vervolgens in overleg met ICT richtlijnen op te stellen voor beheer, locatie en gebruik van informatie. In deze richtlijnen moet duidelijk worden vastgelegd welke verantwoordelijkheden werknemers zelf hebben in beheer en gebruik van informatie en het belang van goed eigenaarschap. Handhaving is een belangrijke taak, waarbij de mogelijkheden van voldoende informatie delen niet mogen worden beperkt. Op deze manier wordt het voor werknemers ook duidelijk welke informatie uitgesloten is om te delen.

Onzorgvuldigheid aangepakt

Het creëren van bewustzijn en het afgeven van richtlijnen is slechts een begin. De professional dient zich nu te richten op de grootste uitwassen van onzorgvuldig informatiegebruik, te weten: 1. uitlekken¹ van vertrouwelijke digitale data; 2. toegang hebben tot – gevoelige – informatie; 3. onachtzame omgang met informatie.

Uitlekken van digitale informatie

Wist u dat de meeste vertrouwelijke informatie die op straat komt te liggen, meestal meer dan een jaar oud is? De meeste mensen zullen een document met vertrouwelijke data eerst in een map plaatsen die afgeschermd is, maar een jaar later zijn ze het document vaak vergeten. Als dan via een routine-back-up het document wordt overgeheveld naar een andere, minder beschermde (archief-)locatie, is het de vraag of hetzelfde beveiligingsregime in stand blijft. Zeker als de nieuwe digitale locatie zich bevindt op een dataserver in India of het Oostblok.

Mede om deze reden zouden vooral grote organisaties en bedrijven gebruik moeten maken van een informatiebeveiligingsplan dat samenhangt met een onderhoudsplan voor informatie. Voor het tegengaan van lekken is een dergelijk beveiligingsplan zelfs onontbeerlijk. Het plan omvat de huidige maatregelen en in te zetten technologie, niet alleen voor de korte termijn, maar ook voor de middellange en lange termijn. De informatieprofessional is in dit plan verantwoordelijk voor het benoemen van de beheersmaatregelen, het eigenaarschap en de vernietiging van verschillende soorten informatie. Op deze manier kan ook worden voorkomen dat werknemers onbeveiligde communicatiekanalen, zoals webbased applicaties, gebruiken voor organisatie-eigen informatie. Denk daarbij aan e-mailverkeer met bijlagen naar onbeveiligde mailproviders en bovengenoemde onbeveiligde back-up-procedures.

Toegang hebben tot – gevoelige – informatie

De informatie- en netwerksamenleving is door digitalisering meer en meer gemeengoed geworden.² De nieuwste generatie³

kan het delen van informatie – ook of zelfs juist met het eigen netwerk – niet meer uit haar leven wegdenken. Bovendien is zij gewend eigen oplossingen te zoeken en creëert zij graag haar eigen weg. Internet speelt hier uiteraard een cruciale rol. Op het web zijn binnen één muisklik tientallen online applicaties te vinden waar virtuele samenwerking tot de mogelijkheden behoort. Dit werkt het delen van informatie en kennis enorm in de hand, maar tegelijkertijd vervagen door virtuele samenwerking ook de grenzen van organisaties.

Wat ontbreekt bij de nieuwe generatie, is een breed besef wie wel of niet toegang mag hebben tot welke informatie. Een complicerende factor is dat wat nu nog geen gevoelige informatie is, dat op een later tijdstip wel kan worden.

Onachtzaam omgaan met informatie

In de regel is er bij onachtzaam gebruik van informatie geen sprake van kwade opzet. Sterker nog, vaak wordt toegang tot informatie verschaft omdat men graag wil helpen. Die hulp gaat verder dan eigen organisatie of bedrijf en wordt steeds meer doorgetrokken naar het eigen netwerk. Wie heeft er wel eens een mailtje ontvangen waarin gevraagd werd of je ooit een presentatie hebt gegeven over een specifiek onderwerp, met de achterliggende vraag om deze te mogen verkrijgen?

Zowel bij verzender als ontvanger zijn er vaker goede dan kwade bedoelingen in het spel. Gesteld kan worden dat men zich niet realiseert dat het gebruik van (bedrijfseigen) informatie risico's met zich meebrengt, simpelweg omdat men niet goed beseft wat zorgvuldige omgang met digitale informatie precies inhoudt. Opnieuw geldt dat informatieprofessionals medewerkers op de gevolgen van onachtzaam gebruik dienen te wijzen.

Informatieprofessional hergewaardeerd

Voor informatieprofessionals ligt er dus een uitdaging: het vormgeven van de taak om het onzorgvuldig gebruik van informatie terug te dringen. Toch denkt een organisatie of bedrijf in deze tijden niet meteen aan de informatiebeheerders van weleer. Om deze reden volgt hieronder

een korte uiteenzetting wat de professional moet doen om zijn nieuwe rol te kunnen en mogen vervullen in de nabije toekomst:

- > Claim (opnieuw) binnen de eigen organisatie de toegevoegde waarde. Dit kan door het in kaart brengen van de risico's van het huidige informatiegebruik.
- > Verwerf verdere inzichten in ICT. Belangrijk hierbij is begrip krijgen van de verschillende systemen, koppelingen en gebruik om zo de impact, context, prioritering en waarschijnlijkheid van informatierisico's te kunnen bepalen. Andersom geldt dat ook ICT begrip dient te krijgen van informatie zoals informatieprofessionals die hebben. Vaak verstaan beide groepen onder informatie iets anders.
- > Zorg voor aansluiting bij de traditionele beveiligingsafdeling, zoals een auditafdeling. Bestaande beveiligingsmodellen kunnen aangevuld worden met informatierisico's.
- > Behoud de juiste balans tussen informatiebeveiliging en het delen van informatie. Denk daarbij ook aan het feit dat informatiebeveiliging lang niet altijd nodig is. Wanneer men een weloverwogen keuze heeft gemaakt om bepaalde informatie niet te beveiligen, zijn in ieder geval de consequenties vooraf onderkend en daardoor beter beheersbaar.

Tot slot

De komende jaren zullen de risico's rondom het delen van informatie alleen maar toenemen. Als dan zoals nu de oplossing alleen wordt gezocht in zwaardere beveiligingsregimes en moeilijkere wachtwoorden en de informatie vrij wordt gelaten, is het wachten op de volgende 'databreach'. De nieuwe generatie medewerkers weet straks niet beter dan dat informatie overal en nergens verkrijgbaar is, maar beseft pas welke risico's men loopt als het te laat is. Eenmaal geplaatste (privé-)informatie blijkt soms lastig te verwijderen, waardoor personen en bedrijven met name op de langere termijn geschaad kunnen worden. Het besef van de waarde van informatie en de risico's van onzorgvuldig gebruik is een boodschap die om die reden alleen al veel vaker dient te worden verkondigd. <

'Als we niets doen, is het wachten op de volgende databreach'

Noten

- 1] Onder uitlekken wordt in dit geval verstaan zowel het zogenaamde inbreken of hacken van data alsook het niet voorzichtig omgaan met data, zoals het niet schonen van hardware. Denk hierbij ook aan het verliezen van USB-sticks.
- 2] 'Invloed generatieverschillen op informatiemanagement', Aart Bontekoning en Marinka Voorhout. *InformatieProfessional* 4/2009, p. 22-27.
- 3] Uiteraard zijn ook voorgaande generaties zeer goed bekend met internet en digitale mogelijkheden. Echter, de nieuwste generatie geldt als een katalysator voor digitalisering. Zij denkt en handelt steeds meer volkomen digitaal. Bovendien behoren jongeren van deze generatie tot de eersten op de arbeidsmarkt die geheel 'digitaal' zijn opgegroeid. Ze zijn zo gewend om met informatie en netwerken om te gaan, dat het ze meer moeite kost om de risico's van informatie delen in te schatten. Vandaar dat er hier de nadruk op wordt gelegd.