mr. J.H. (Johri) Maat,
werkzaam bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Verwijtbaar lekken = vermijdbaar lekken

In het domein van nationale veiligheid en crisisbeheersing is de juistheid en toegankelijkheid van informatie van groot belang. Als kennisname van informatie door niet gerechtigden nadeel of schade kan opleveren, dan is ook de exclusiviteit essentieel. Dit kan gerealiseerd worden door deze informatie te rubriceren (vaststellen en aangeven zwaarte vertrouwelijkheid en beveiligingseisen) en als zodanig te behandelen. Soms gaat dit mis en versterkt het uitlekken van gevoelige informatie een crisissituatie of creëert deze er zelfs een.

Operatie 'Pathway'

Een treffend voorbeeld hiervan werd veroorzaakt door het toenmalige hoofd van de Britse antiterreurdienst van Scotland Yard, commissaris Quick. Toen hij op 8 april 2009 de minister van Binnenlandse Zaken ging inlichten over een op handen zijnde antiterreuractie, stapte hij in Downing Street uit zijn dienstauto met de papieren over deze operatie 'Pathway' duidelijk leesbaar onder zijn arm. De altijd aanwezige journalisten fotografeerden hem hiermee en de details – namen en locaties – over de operatie werden al snel wereldkundig gemaakt. Het uitvaardigen van een publicatieverbod mocht niet baten omdat buitenlandse media hier niet aan gebonden zijn. Als gevolg hiervan moest de operatie vervroegd worden van de vroege ochtend naar de drukke avondspits – onder andere tussen het publiek voor een bibliotheek en een doe-het-zelfzaak – omdat gevreesd werd dat de twaalf terreurverdachten óf op de vlucht zouden slaan óf hun plannen vervroegd zouden uitvoeren.[1] Quick zag zich gedwongen zijn functie neer te leggen. Want ook al was er natuurlijk geen sprake van opzet, het uitlekken van de informatie en de gevaarlijke situatie die daardoor ontstond vielen hem wel aan te rekenen.

Verwijtbare compromittering

Het lekken van informatie valt te onderscheiden in intentionele en verwijtbare compromittering. In het eerste geval is er sprake van opzet, het uitlekken van informatie wordt bewust gedaan. Dit kan om persoonlijke (geld, positie, aanzien), institutionele (voortbestaan organisatie) of publieke (melden van misstanden) redenen zijn. In dit artikel wordt de focus gelegd op het tweede geval: verwijtbare compromittering. Er is dan sprake van schuld. Ook al is het lekken van informatie niet beoogd, er is wel sprake van slordigheid, onderschatting van de risico's of belangen, gebrek aan motivatie of in het algemeen een gebrek aan kennis en ervaring om op de juiste wijze met gevoelige informatie om te gaan.

De casus van commissaris Quick is niet uniek. Verwijtbare compromittering komt veel vaker voor, bijvoorbeeld door het verlenen van ongeautoriseerde toegang tot locaties of systemen, het zich verspreken of anderen (onbewust) mee laten lezen (recepties, horeca, openbaar vervoer, vliegtuig), het verliezen van documenten en onbeveiligde digitale gegevensdragers (usb-sticks) en het verzenden van informatie via onbeveiligde kanalen (per post, e-mail, fax). De ontwikkelingen in de technische infrastructuur (goedkope digitale gegevensdragers met grote capaciteit, internet, e-mail) en het tijd- en plaatsonafhankelijk werken (Het Nieuwe Werken) vergroten de risico's als hier onvoldoende rekening mee wordt gehouden.

Verwijtbare compromittering is vermijdbare compromittering omdat het voorkomen of beperkt kan worden door het treffen van de juiste maatregelen aangaande het rubriceren, verwerken, opbergen, verzenden of vernietigen van gevoelige informatie. In de ideale situatie is er sprake van een gelaagdheid aan onafhankelijk van elkaar werkende technische en organisatorische maatregelen. Mocht één maatregel falen, dan wordt dit door een andere maatregel opgevangen.

Practical drift

Het zijn de organisaties die de juiste voorwaarden moeten creëren, zoals het beschikbaar stellen van gebruiksvriendelijke middelen en het vaststellen van hanteerbare procedures, maar uiteindelijk zijn het de gebruikers van de gevoelige informatie die hier op een juiste wijze mee om moeten gaan. Uit onderzoek is gebleken dat het verschijnsel van 'practical drift' op de loer ligt. Dit is 'the slow, steady uncoupling of local practice from written procedure'.[2] Bij dit verslappen van de aandacht of discipline gaat men er overigens wel vaak vanuit dat de ander zich wel aan de norm houdt.

[1] H. Jippes, 'Britse antiterreurchef Quick weg na blunder', in: *NRC Handelsblad*, 9 april 2009.

[2] S.A. Snook, *Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*, Princeton (NJ): Princeton University Press, 2000, 193.

Hierdoor ontstaan situaties waarbij het vroeg of laat mis gaat.
Bijvoorbeeld indien men gerubriceerde informatie bij het tijdelijk verlaten van de ruimte niet opbergt omdat er vanuit wordt gegaan dat de toegangsbeveiliging tot het gebouw of de sociale controle op de gang voorkomt dat kwaadwillenden beschikking krijgen over de gerubriceerde informatie. Van dit vertrouwen maken 'social engineers', zoals undercover-journalisten, dankbaar gebruik.
Een ander voorbeeld is het onversleuteld per e-mail verzenden van gerubriceerde informatie omdat dit 'binnen het netwerk van de organisatie' blijft, zonder hierbij rekening te houden met zaken als het automatisch doorsturen van e-mail – bijvoorbeeld naar een huisadres of andere collega's bij vakantie – of het per abuis doorsturen naar een andere partij door een typefout in de adressering. Op een dergelijke wijze kwam in 2009 een gevoelige notitie in de openbaarheid die de politieke spanningen tussen Aruba en Nederland verder deed toenemen.
Maar zelfs het beginsel 'need to know, nice to know' is hier een voorbeeld van: de houder van de gevoelige informatie deelt de informatie met een derde – uit sensatiezucht of om interessant te doen – onder voorwaarde dat dit 'entre nous' blijft, dat het niet met anderen gedeeld wordt. Deze derde deelt het opnieuw met een onbevoegde om dezelfde reden en onder dezelfde voorwaarde. Menig 'affaire' is zo in de Haagse 'kletsmachine' ontstaan.

Juist rubriceren

Wat ook meespeelt, is dat het enerzijds voorkomt dat gevoelige informatie niet of te laag gerubriceerd wordt en anderzijds dat er ten onrechte of te hoog gerubriceerd wordt. Voor het onjuist rubriceren geldt in het algemeen dat er vaak onvoldoende besef is van het belang van de informatie waarmee gewerkt wordt. Niet of te laag rubriceren gebeurt nogal eens om de als omslachtig ervaren beveiligingsmaatregelen – zoals beveiligd e-mailen of faxen, opslag in kluizen en het gebruik van veiligheidsenveloppen – te omzeilen.
Gevolg is dan wel dat onvoldoende beveiligingsmaatregelen worden getroffen en de kans bestaat dat gevoelige informatie in verkeerde handen komt.
Onterecht of te hoog rubriceren kan om allerlei redenen gebeuren: uit gewoonte of gemakzucht, om betwistbare informatie (intern) achter te houden en in het ernstigste geval om misstanden te verhullen. Gevolg hiervan is dat er onnodige kosten gemaakt worden voor het treffen van maatregelen, onnodige extra handelingen en een inflatie op het terrein van rubriceringen, waardoor de aandacht en discipline kunnen verslappen, ook bij gevoelige informatie die wel terecht gerubriceerd is.

Need to know

Uit veel onderzoeken naar lekken blijkt dat de kring van geïnformeerden van gerubriceerde informatie groter is dan noodzakelijk én hanteerbaar. De Rijksrecherche concludeerde bijvoorbeeld dat het in 2009 uitgelekte ministerraadstuk rond het ontpolderen van de Hedwigepolder toegankelijk was voor minstens 235 personen. Deze affaire heeft de spanningen binnen het toenmalige kabinet versterkt. De Rijksrecherche constateerde in 2009 tevens dat het aanstaande rechtbankverzoek aangaande de noodregeling voor de DSB-bank bij meer dan 500 personen bekend was. Het uitlekken hiervan heeft de ondergang van de DSB-bank in ieder geval versneld.
Het bekendste voorbeeld is waarschijnlijk het uitlekken van circa 250.000 Amerikaanse diplomatieke berichten via WikiLeaks ('Cablegate'-affaire). De verdachte lekker was één van de circa drie miljoen personen die ongelimiteerd toegang hadden tot de digitale informatie en die deze ook zonder restricties buiten het beveiligde netwerk kon kopiëren.

Afsluiting

Om het uitlekken van gevoelige informatie te voorkomen is het voor functionarissen werkzaam in de nationale veiligheid en crisisbeheersing van belang dat:

- men beschikt over gebruiksvriendelijke middelen en hanteerbare procedures;
- informatie op de juiste wijze gerubriceerd en behandeld wordt; en
- de kring van geïnformeerden beperkt wordt: 'need to know', in plaats van 'nice to know'.

Een crisis 'managen' is al uitdagend genoeg, daar heb je geen zelfgecreëerde crises door vermijdbaar lekken bij nodig.

Foto en analyse Quick:

http://news.bbc.co.uk/2/hi/uk_news/7992101.stm