Johri Maat
Mr. J.H. Maat MSSM, ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Lekken binnen de **overheid**

Ook in 2011 lekten Prinsjesdagstukken uit. Ditmaal was het de Miljoenennota 2012 die per abuis voortijdig online stond. Het voorval leidde tot een discussie over informatiebeveiliging bij de overheid. Lekken komt namelijk vaker voor, maar het ene lek is het andere niet. Er zijn meerdere oorzaken waardoor gevoelige informatie in onbevoegde handen kan geraken.

Dat er aandacht is voor informatiebeveiliging bij de overheid is begrijpelijk. Zij verzamelt en beheert een grote hoeveelheid – deels gevoelige – informatie, ook van burgers en bedrijven die hier zelf niet voor hebben gekozen. Het is overigens lastig te spreken over informatiebeveiliging bij de overheid. De overheid is immers een verzamelterm voor een groot aantal overheden die voor een belangrijk deel in hun bedrijfsvoering autonoom zijn. Bovendien hebben inbreuken op informatiebeveiliging soms geheel verschillende achtergronden. Het is niet voor niets dat de Wetenschappelijke Raad voor het Regeringsbeleid zijn zorg uitsprak over het verzamelen van informatie door de overheid: 'Ook de onvermijdelijkheid van lekken naar internet, of dat nu intentioneel is of het gevolg van fouten, slordigheden of grove nalatigheid, maar zeker ook de verdere consequenties die dergelijke lekken met zich meebrengen, zijn redenen om stil te staan bij de grenzen van de groei van de iOverheid'.[1]

Als gevoelige informatie in onbevoegde handen raakt, kan dat leiden tot nadeel of schade aan belangen van burgers en bedrijven, ook (inter)nationale economische, politieke of veiligheidsbelangen. Gevoelige informatie dient daarom te worden gerubriceerd (als 'geheim' gelabeld) en in opslag, bewerking, transport en vernietiging ook als zodanig te worden behandeld. Wanneer onbevoegden kennis (kunnen) nemen van gerubriceerde informatie, is sprake van compromittering.[2]

Intentioneel en verwijtbaar

Het uitlekken van Prinsjesdagstukken gebeurde in 2002, 2004, 2005, 2007, 2009 en 2011. In het geval van de Miljoenennota 2012 ging het om een vergissing. Een medewerker van een extern bedrijf, dat voor het ministerie van Financiën werkzaamheden verricht, had het bestand in een verkeerde directory geplaatst, waardoor het op internet direct geraadpleegd kon worden.[3] Door het aanpassen van het jaartal in het webadres wist een internetter de tekst van de Miljoenennota te vinden, waarna hij dit via Twitter bekend maakte. In 2009 lekte ook een Prinsjesdagstuk uit, namelijk de Macro Economische Verkenningen. Dat was geen vergissing, maar een opzettelijke handeling van een Tweede Kamerlid dat de stukken ter voorbereiding onder embargo had ontvangen en deze naar een journalist doorspeelde.[4] In beide gevallen ging het om personen die bevoegd waren over gevoelige informatie te beschikken, maar de achtergronden van de compromittering zijn verschillend.

In 2009 was sprake van intentioneel lekken, het lekken van informatie wordt dan bewust gedaan. Dit kan om persoonlijke motieven (geld, positie, aanzien, vriendendienst), institutionele (voortbestaan organisatie) of publieke redenen (melden van misstanden).[5] In 2011 ging het om verwijtbaar lekken. Ook al was het lekken niet beoogd, het was slordig, risico's of belangen werden onderschat, gebrek aan motivatie of in het algemeen gebrek aan kennis en ervaring om op de juiste wijze met gevoelige informatie om te gaan. Voorbeelden zijn het verlenen van ongeautoriseerde toegang tot locaties of systemen, zich verspreken, anderen (onbewust) mee laten lezen

1 Wetenschappelijke Raad voor het Regeringsbeleid 2011, *iOverheid*, Den Haag: WRR, p. 223.
2 Artikel 1 onder g Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004.
3 Minister-president aan de voorzitter van de Tweede Kamer, 15 september 2011.
4 J.L. de Wijkerslooth de Weerdesteijn e.a., *Publiek geheim. Commissie Prinsjesdagstukken*, Den Haag: Tweede Kamer, 2010, p. 20-21.
5 M.A.P. Bovens, H.G. Geveke, & J. de Vries, Strikt vertrouwelijk: lekken in het openbaar bestuur, *Beleid & Maatschappij*, 1993-2, p. 61-80.

Bewustwordingsposter Rijksoverheid uit Koude Oorlog over omgang met geheimen

of luisteren (recepties, horeca, openbaar vervoer), verliezen van documenten en onbeveiligde digitale gegevensdragers (usb-sticks) en verzenden van informatie via onbeveiligde kanalen (post, e-mail, fax).

Het imago van de totale organisatie wordt door het lekken beschadigd

Schadelijk effect

Lekken levert nadeel of schade op, zelfs als de gevoelige informatie 'maar een dag te vroeg' openbaar is. Voorbeelden zijn koersgevoelige informatie, de aanhouding van een terreurverdachte, een militaire operatie of zoals in 2009 de noodregeling van het ministerie van Financiën en De Nederlandsche Bank voor DSB Bank. Lekken heeft ook indirect een schadelijk effect. De Commissie-Lemstra – die onderzoek deed naar lekken binnen het ministerie van Defensie – beschreef dit in 2005: 'Het imago van de totale organisatie wordt door het lekken beschadigd; het vertrouwen van de buitenwereld in de gehele organisatie wordt beschaamd. Daarnaast bederft het de sfeer binnen de organisatie. De verhouding tussen het ambtelijk apparaat en de politieke leiding komt onder druk te staan. Het lekken van vertrouwelijke of geheime informatie zet ook de onderlinge verhoudingen op scherp. Medewerkers kijken elkaar vragend aan wie er gelekt heeft. Onschuldige medewerkers worden in een (strafrechtelijk) onderzoek ondervraagd, hetgeen als zeer belastend wordt ervaren. Lekken bedreigt de eenheid binnen de organisatie en zet medewerkers tegen elkaar op.'[6]
Lekken kan ook internationaal de verhoudingen onder druk zetten. Het State Department van de Verenigde Staten raakte ernstig in verlegenheid toen in november 2010 een grote hoeveelheid diplomatieke berichten uitlekte (*Cablegate*), mede vanwege de kwalificaties die Amerikaanse diplomaten soms in hun rapportages over situaties in hun standplaatsen bezigden.

Consternatie

Wanneer het lekken van informatie bekend raakt, leidt dat vaak tot consternatie. Veelvuldig is er verbazing over de ogenschijnlijk eenvoudige wijze waarop inbreuken op de informatiebeveiliging plaatsvinden, zeker met de kennis achteraf. Vaak wordt er onvoldoende rekening gehouden met de oorzaken die dergelijke inbreuken mogelijk maken. Idealiter worden onafhankelijk van elkaar informatiebeveiligingsmaatregelen genomen, zowel technische als organisatorische, zodat bij het falen van de ene maatregel de andere wel stand houdt. Technisch kunnen maatregelen worden genomen, zoals fysieke en digitale voor bewerking, opslag, vervoer en vernietiging. Bij organisatorische maatregelen kan gedacht worden aan bewustwording bij medewerkers, regelgeving, procedures, toezicht en handhaving. In de praktijk blijkt dat beide soorten maatregelen voortdurende aandacht vereisen.

Practical drift

Er dient rekening te worden gehouden met het verschijnsel *practical drift*, 'the slow, steady uncoupling of local practice from written procedure'.[7] Bij het verslappen van aandacht of discipline gaat men er

6 W. Lemstra, E. e.a., *Cultuur ondersteund door structuur: hét wapen tegen het lekken van vertrouwelijke informatie*, Den Haag: ministerie van Defensie, 2005, p. 8.
7 S.A. Snook, *Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*, Princeton (NJ): Princeton University Press, 2000, p. 193.

vaak vanuit dat de andere partij zich wel aan de norm houdt. Hierdoor kunnen situaties ontstaan waarbij het vroeg of laat misgaat, bijvoorbeeld het niet afsluiten van een kluis omdat men er vanuit gaat dat de toegangscontrole tot het gebouw kwaadwillenden wel tegenhoudt, of het onversleuteld verzenden van bestanden omdat het gebruik van speciale encryptieprogramma's zo omslachtig zou zijn. Incidenten kunnen aanleiding zijn om procedures heel strikt te volgen en maatregelen in te voeren die nog strenger of uitgebreider zijn. De eerste periode na een incident zullen leidinggevenden en medewerkers nog wel alert zijn, maar op den duur verslapt de aandacht en wordt het ongemak die de beveiligingsmaatregelen veroorzaken, als ernstiger gepercipieerd dan het risico op een nieuw incident. Als zo'n incident zich vervolgens voordoet, constateert men dat de regels niet gevolgd zijn en worden er nieuwe – weer strengere – ingevoerd. Hiermee creëert men een perpetuum mobile van lekken, aanscherping en verslapping van maatregelen.

Een voorbeeld van het verslappen van de aandacht is het uitlekken van een op handen zijnde anti-terreuroperatie onder de codenaam 'Pathway'. Op 8 april 2009 besprak commissaris Quick van Scotland Yard deze operatie met de Britse minister van Binnenlandse Zaken. Toen de commissaris in Downing Street uit de auto stapte, had hij de geheime documenten met daarop alle details zichtbaar onder zijn arm. De altijd aanwezige persfotografen legden dit vast en dankzij de hoge resolutie van de foto's waren details goed leesbaar. De foto's werden via internet verspreid, waardoor de operatie vervroegd moest worden uitgevoerd – midden tussen het publiek, met alle risico's van dien – omdat men vreesde dat de twaalf terreurverdachten op de vlucht zouden slaan of hun plannen vervroegd zouden uitvoeren. Commissaris Quick moest aftreden.[8] Men zou verwachten dat elke functionaris vanaf dat moment vertrouwelijke documenten op straat beter afgeschermd zou houden. Maar op 30 augustus 2011 beging de Britse minister Mitchell dezelfde fout door Downing Street 10 te verlaten met een geheim memo in zijn handen. Het memo ging over de situatie in Afghanistan en het vertrouwelijke Britse standpunt hierover, onder meer dat men het vertrek van de Afghaanse president Karzai zou verwelkomen. Dit kwam op een extra gevoelig moment, omdat men was begonnen met het terugtrekken van de Britse troepen uit Afghanistan.[9]

Need to know

Een andere oorzaak van het lekken van gevoelige of gerubriceerde informatie is de vaak grote groep van geïnformeerden, zonder dat daar een directe noodzaak voor is (*nice to know* versus *need to know*). In 2009 deed de Rijksrecherche onderzoek naar het lekken van de geheime notulen van de ministerraad van 28 augustus 2009 over de uitdieping van de Westerschelde en het ontpolderen van de Hedwigepolder in Zeeuws-Vlaanderen. Het onderzoek richtte zich vooral op het ministerie van Algemene Zaken, maar ook andere departementen werden er bij betrokken. De Rijksrecherche concludeerde dat tenminste 235 personen de mogelijkheid tot inzage of kopiëren hebben gehad. De dader van het lekken is dan ook nooit gevonden.[10]

Informatiebeveiliging begint met het bepalen van de gevoeligheid van informatie

Het meest bekende en aansprekende voorbeeld van een te grote groep van geïnformeerden is waarschijnlijk de *Cablegate*-affaire, waarin de Amerikaanse soldaat Manning ervan wordt verdacht (het strafrechtelijk onderzoek loopt nog) ruim 250.000 geheime documenten naar de website WikiLeaks te hebben gelekt. Manning was één van de meer dan drie miljoen functionarissen die ongelimiteerd toegang tot deze documenten had via het Secret Internet Protocol Router Network, een Amerikaanse overheidsdatabase met onder meer diplomatieke berichten. Saillant detail is dat de Amerikaanse overheid de informatie juist breder toegankelijk had gemaakt vanwege de strijd tegen terrorisme.

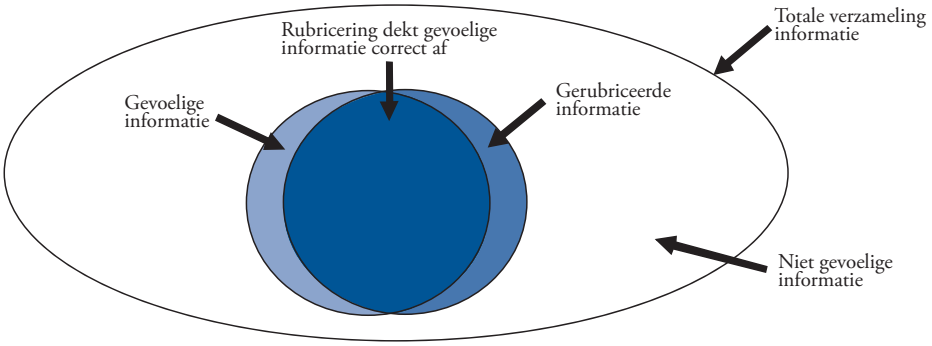
Technische infrastructuur

Cablegate illustreert dat het lekken steeds gemakkelijker wordt gemaakt door de veranderde technische infrastructuur zoals digitalisering van opslag en verzending. Databases worden steeds groter en zijn door

8 J.H. Maat, Verwijtbaar lekken = vermijdbaar lekken, *Magazine Nationale Veiligheid en Crisisbeheersing*, augustus 2011, p. 48-49.

9 I. Drury, Minister's blunder with memo outside No.10 reveals UK Government 'welcomes' Afghan president stepping down', *Daily Mail*, 31 augustus 2011.

10 Proces-verbaal van Bevindingen Feitenonderzoek Dieze (23 augustus 2010). Inzake notulen Ministerraad Dossier Westerschelde (proces-verbaalnummer 20090080), 7 maart 2011, kenmerk PaG/BJZ/35037 (openbaar via WOB).



Eclips Model. De twee 'maansikkels' geven ten onrechte gerubriceerde en niet-gerubriceerde informatie weer. Idealiter is er een volledige overlap van gerubriceerde en gevoelige informatie.

zoekmachines gemakkelijker te raadplegen. Bovendien kan digitale informatie tegenwoordig gemakkelijk buiten de beveiligde omgeving worden gebracht dankzij verzending via e-mail en het gebruik van goedkope gegevensdragers als harde schijven, usb-sticks en – zoals bij *Cablegate* – zelfgebrande cd-roms. Ook in Nederland zijn voorbeelden bekend van verloren usb-sticks en verkeerd doorgestuurde e-mailberichten, terwijl dit soort incidenten eenvoudig te voorkomen is door beveiligde usb-sticks en versleutelprogramma's te gebruiken. Mochten data toch in onbevoegde handen geraken, dan zijn deze zonder specialistische kennis niet uit te lezen. Maar ook papier heeft nadelen, zowel in opslag en transport, als in vernietiging. Het meenemen van dossiers buiten de werkplek levert risico's op. Zo verloor een politierechter vijf vertrouwelijke dossiers, toen ze onverwacht naar huis moest. Ze had de dossiers in een plastic tas onder haar snelbinder gebonden. Eenmaal thuis ontdekte ze dat de tas met inhoud weg was. Het buiten het vertrouwde domein brengen van gevoelige informatie – het nieuwe werken – kan dan ook tot een stijging van het aantal lekincidenten leiden als er onvoldoende beveiligingsmaatregelen getroffen worden.[11]

Besluit: Eclips Model

Informatiebeveiliging begint met het bepalen van de gevoeligheid van informatie. De Commissie-Davids – die in 2009 onderzoek deed naar de besluitvorming rond de inval in Irak – concludeerde dat bij het ene departement bepaalde informatie wel en bij het andere dezelfde of vergelijkbare informatie niet gerubriceerd was of op een ander niveau. De commissie zag ook ongerubriceerde stukken, waarbij men zich afvroeg of die niet gerubriceerd hadden moeten zijn, omdat openbaarmaking tot schade zou kunnen leiden.[12]

Informatie die ten onrechte niet of te laag gerubriceerd wordt, zal veelal niet of onvoldoende zijn beschermd. Soms gebeurt dit om de als omslachtig ervaren beveiligingsmaatregelen te omzeilen. Wanneer informatie ten onrechte wel of te hoog is gerubriceerd, levert dat niet alleen onnodig genomen maatregelen op (met de bijbehorende kosten en beperkingen), er ontstaat ook een inflatie van de rubricering, waardoor men slordig met correct gerubriceerde informatie omgaat. Het (te hoog) rubriceren kan voortkomen uit gewoonte of gemakzucht, om betwistbare informatie achter te houden of om concurrentie van eigen collega's uit te schakelen. In het ernstigste geval kan er sprake zijn van het onterecht rubriceren van informatie om zo misstanden te verhullen.

Hoeveel informatie ten onrechte gerubriceerd wordt, is moeilijk te onderzoeken, de informatie is immers gerubriceerd. De Commissie-Lemstra heeft aangegeven dat van verschillende zijden erop is gewezen dat 95 procent van het aantal gerubriceerde stukken ten onrechte zou zijn gerubriceerd.[13]

In het Eclips Model is dit probleem van onjuist rubriceren gevisualiseerd. Idealiter past binnen de totale verzameling informatie de schijf met gerubriceerde informatie naadloos over de schijf met gevoelige informatie: waar ze elkaar overlappen dekt de rubricering de gevoelige informatie correct af. In de praktijk is dat niet altijd het geval. De linker maansikkel is onbedekt, de gevoelige informatie is ten onrechte niet gerubriceerd. De rechter maansikkel bedekt informatie die niet gevoelig is, deze informatie is daardoor overgerubriceerd. ■

11 J.H. Maat, Het Nieuwe Werken of De Nieuwe Kwetsbaarheid, *Security Management* januari/februari 2011, p. 39.
12 W.J.M. Davids, *Gerubriceerd staatsgeheim: zeer geheim, geheim, confidentieel, vertrouwelijk*, Ketelaar-lezing 7 oktober 2010, p. 9.
13 W. Lemstra, E. e.a., op. cit., p. 26.

Erratum

In de gedrukte versie van Openbaar Bestuur ontbreekt de onderstaande passage.

Informatiebeveiligingsmaatregelen kosten geld en leveren (deels) beperkingen binnen werkprocessen op. Maar als ten gevolge van het niet naleven of gebruiken van deze maatregelen inbreuken ontstaan, kan dat nadeel of schade opleveren aan belangen van burgers, bedrijven en overheden. Lekken valt nooit helemaal te voorkomen, zeker niet als het intentioneel gebeurt. Maar als meer rekening wordt gehouden met factoren als *practical drift*, *need to know*, ontwikkelingen in de technische infrastructuur en het rubriceren van informatie kan het risico van het lekken van gevoelige of gerubriceerde informatie wel beter beheersbaar worden gemaakt. Zeker het verwijtbaar lekken kan hiermee worden teruggedrongen. ■