oktober 2009 nummer 6

INFORMATIEBEVEILIGING

Cybercriminaliteit kost bedrijfsleven en overheid handenvol geld

De Leidraad voor de uitwisseling van gevoelige informatie van NAVI

Cybercrime trendrapport: geen verbetering van de veiligheid van internet

Voorkom schijnveiligheid door een veilig ontwerp

DEMO architectuur met security

ib

creative commons

PvIB
Platform voor InformatieBeveiliging

Uitwisseling van gevoelige informatie

Auteurs: Hans Muller en Erwin van der Zwan > Hans Muller en Erwin van der Zwan zijn senior adviseurs (security) bij het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en ze zijn bereikbaar via Hans.Muller@minbzk.nl en Erwin.Zwan@minbzk.nl.

Informatie is essentieel voor, zo niet het meest belangrijke bezit van, veel organisaties. Veel bedrijven en instanties hebben een eigen informatie-beveiligingsbeleid. Dit beleid beperkt zich meestal tot interne procedures en maatregelen over hoe de medewerkers om moeten gaan met informatie. Regelmatig is het echter wenselijk of noodzakelijk dat gevoelige informatie wordt uitgewisseld met externe partijen. Samen met een klankbordgroep (waar ook het PvIB deel van uitmaakte) heeft het NAVI de Leidraad voor de uitwisseling van gevoelige informatie ontwikkeld.

Aan het verstrekken, het ter beschikking stellen of op andere wijze uitwisselen van gevoelige informatie zijn beperkingen en risico's verbonden. Zo is het slechts zeer beperkt en onder strikte voorwaarden mogelijk om gevoelige informatie van de rijksoverheid met bedrijven te delen. Ook bedrijven kunnen terughoudend zijn met het delen van gevoelige informatie aan de overheid. De op die manier in bezit van de overheid gekomen informatie zou met een beroep op de Wet openbaarheid van bestuur (Wob) mogelijk openbaar gemaakt moeten worden.

Bedrijven, overheid en instanties wisselen ook onderling gevoelige informatie uit, bijvoorbeeld tijdens bijeenkomsten over de kwaliteitsverbetering van de beveiliging van bedrijven binnen de vitale sectoren. Door bedrijven en instanties worden hierbij verschillende termen gebruikt om de gevoeligheid en de vertrouwelijkheid aan te duiden. Deze termen of de te nemen maatregelen zijn onderling niet altijd gelijkwaardig. Er is daarom behoefte aan helderheid over hoe en welke informatie op een veilige wijze gedeeld kan worden en welke maatregelen tussen betrokken partijen afgesproken kunnen worden.

Op verzoek van diverse bedrijven uit vitale sectoren organiseerde het NAVI in 2008 en 2009 enkele bijeenkomsten over de uitwisseling van informatie. De bedrijven stelden drie vragen centraal:

1 Hoe om te gaan met rubricering en informatiebeveiliging bij de vitale infrastructuur?
2 Hoe informatie te delen in multidisciplinaire en organisatieoverstijgende projectteams?
3 Hoe om te gaan met vertrouwelijke informatie in relatie tot bijvoorbeeld een vergunningaanvraag en/of in relatie met de Wet openbaarheid van bestuur?

De deelnemers aan de bijeenkomsten gaven aan dat er bij vitale bedrijven grote behoefte bestaat aan meer duidelijkheid en afspraken over hoe om te gaan met intersectorale en publiekprivate informatie-uitwisseling en tevens de noodzakelijke vertrouwelijkheid van de informatie te borgen. Ofwel, hoe kunnen we veilig communiceren zonder het risico te lopen dat informatie in verkeerde handen valt? Uitvoerig is gesproken over referentiekaders en een set van afspraken die daarbij behulpzaam zou kunnen zijn. In het bijzonder gaat het hierbij om de aspecten van rubricering van informatie en de bijbehorende afspraken en maatregelen voor wat betreft de uitwisseling van informatie met andere partijen.

Om bij het uitwisselen van gevoelige informatie dezelfde taal te spreken, heeft het NAVI in samenspraak met diverse vitale bedrijven, brancheorganisaties en overheden een leidraad opgesteld. Deze kan bijvoorbeeld uitgereikt worden bij platformbijeenkomsten of werkoverleggen. Het gebruik van de leidraad is vrijwillig, maar niet vrijblijvend. Van partijen die betrokken zijn bij een informatie-uitwisseling en die afspreken de leidraad te hanteren, wordt verwacht dat zij zich aan de voorgestelde afspraken en afgestemde beveiligingsmaatregelen houden. De leidraad gaat niet over het intern informatiebeveiligingsbeleid. Het NAVI heeft daar wel voorbeelden van beschikbaar.

Het indelen naar gevoeligheidsniveaus helpt het duiden van de informatie. De leidraad werkt met een kleuraanduiding voor de mate van gevoeligheid van de informatie:

Rood (geheim)
Geel (vertrouwelijk)
Groen (besloten)
Wit (openbaar)

Kleuren hebben als voordeel dat ze worden geassocieerd met een mate van exclusiviteit daar waar termen als 'geheim', 'vertrouwelijk' of 'intern' in verschillende bedrijfsculturen een geheel andere betekenis kunnen hebben. De leidraad sluit met deze kleuren aan op bestaande schema's zoals het *Traffic Light Protocol*. Om de mate van gevoeligheid extra te benadrukken, wordt naast de kleuraanduiding een generieke aanduiding van het gevoeligheidsniveau toegevoegd.

Het is van belang dat informatie alleen in bezit is van en toegankelijk is voor bevoegde personen. Een principieel uitgangspunt bij de verstrekking van informatie is dat de informatie-eigenaar of -verstrekker beslist binnen welke kaders de informatie gedeeld mag worden. Hierbij geeft de verstrekker aan welke gevoeligheidswaarde de informatie heeft en welke voorwaarden hij aan de verstrekking stelt. De ontvanger beoordeelt vooraf of hij/zij de aangeboden informatie wil en kan ontvangen.
De ontvanger verplicht zich tegenover de

verstrekker om de informatie vervolgens op de overeengekomen wijze te behandelen. Bij de verschillende gevoeligheidsniveaus zal ten minste moeten worden aangegeven wie mag kennisnemen van de informatie (het verspreidingsgebied), de wijze van verstrekken en de te treffen beveiligingsmaatregelen.

De beperkingen voor de gevoeligheidsniveaus zijn als volgt:

- **Rood:** De informatie is uitsluitend toegankelijk voor geselecteerde personen (op basis van noodzakelijkheid) die zijn aangewezen door, of bekend zijn bij de informatie-eigenaar. De informatie wordt in principe mondeling gedeeld. Indien de informatie-uitwisseling schriftelijk of elektronisch plaatsvindt, worden er expliciet afspraken gemaakt over de beveiliging van de informatie. Hierbij worden afspraken gemaakt over de borging dat de geadresseerde ook de juiste en enige ontvanger is.

- **Geel:** De informatie is alleen toegankelijk voor een selecte groep van direct betrokken personen, bijvoorbeeld voor deelnemers aan de specifieke besprekingen. Zij mogen de informatie ook delen met mensen binnen hun organisatie die deze informatie nodig hebben, hetzij om maatregelen te treffen of om een bijdrage te kunnen leveren aan de discussie en meningsvorming van de deelnemer.

- **Groen:** De informatie is alleen toegankelijk voor een bepaalde (besloten) groep van personen. De informatie mag worden gedeeld met andere organisaties, informatiefora of personen werkzaam in beveiligingsfuncties. De informatie mag niet openbaar gemaakt worden door publicatie of plaatsing op openbare internetsites.

- **Wit:** De informatie is specifiek gemaakt om openbaar te maken. Informatie is (op aanvraag) vrij toegankelijk of is vrijgegeven voor publicatie via openbare bronnen zoals internet en de pers.

Maatregelen waar de verstrekker en ontvanger afspraken over kunnen maken, zijn onder andere de wijze van (de-)

classificeren, het verwerken en opslaan op computersystemen (versleuteling), fysieke maatregelen, toegangscontrole (fysieke en ICT), verzenden per post of e-mail (onweerlegbaarheid), transport en duiden van gevoeligheidsniveau op documenten en gegevensdragers of personele maatregelen (zoals een geheimhoudingsverklaring en screenen).

De leidraad geeft per gevoeligheidsniveau aan wat het verspreidingsgebied is, maar laat het maken van specifieke afspraken over verstrekking en te nemen maatregelen over aan de verstrekker om te bepalen. Het voert te ver om in de leidraad dergelijke specifieke maatregelen op te nemen. Diverse deelnemers aan de gehouden bijeenkomsten gaven bovendien aan dat dit bedrijven zou kunnen weerhouden de leidraad te volgen omdat het dan ingrijpt in het eigen interne beveiligingsbeleid. Om dezelfde reden legt de leidraad bovendien geen directe koppeling tussen verschillende bestaande classificatieschema's en bevat de leidraad geen transformatietabel. Wel is een toelichting beschikbaar, waarin suggesties voor maatregelen zijn opgenomen.

In de leidraad zijn verder enkele aanbevelingen voor regels tijdens besprekingen en bijeenkomsten opgenomen. Daarnaast besteedt de toelichting onder andere (kort) aandacht aan de verstrekking van gevoelige informatie aan de overheid met het oog op de Wet openbaarheid van bestuur.

Deelnemende partijen aan een uitwisseling van (gevoelige) informatie wordt geadviseerd om vooraf altijd duidelijke afspraken te maken en verwachtingen af te stemmen. Organisaties worden aangemoedigd om de leidraad te hanteren en deze af te stemmen met een eigen informatiebeveiligingsbeleid.

De leidraad en de toelichting zijn te downloaden van www.navi-online.nl/producten.

Wat is het NAVI?
In het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) werken overheid en bedrijfsleven samen aan de verbetering van de bescherming van de vitale infrastructuur in Nederland tegen moedwillig menselijk handelen (security). In haar activiteiten richt het NAVI zich op fysieke, personele, organisatorische en digitale dreigingen.

Het NAVI ondersteunt beheerders en eigenaren van de vitale infrastructuur door het bieden van een veilig platform voor informatie-uitwisseling, kennis & expertise en een (inter)nationaal contactpunt.

Met een serie handreikingen ondersteunt het NAVI thematisch de beveiligingspraktijk bij vitale bedrijven. Een deel van deze handreikingen zijn door het NAVI zelf ontwikkeld, zoals een Risicoanalyse, een Beveiligingsafstemming Vitaal en Overheid, een Operator Security Plan, Security Awareness en Informatie-uitwisseling. Het NAVI levert daarnaast een bijdrage aan andere publicaties en heeft ook internationale uitgaven geschikt gemaakt voor de Nederlandse markt.

Alle handreikingen zijn beschikbaar via www.navi-online.nl