Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat generaal Veiligheid
Programma Dreigingen & Capaciteiten

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.minbzk.nl

Kenmerk
2011-2000040980

Datum 22 februari 2011
Betreft Kabinetsreactie Kwetsbaarheidsanalyse Spionage Nederland

In april van dit jaar heeft u het rapport *Kwetsbaarheidsanalyse Spionage Nederland(KWAS)*[1] ontvangen. Heimelijke inlichtingenactiviteiten vormen een bedreiging voor de vitale belangen van Nederland, zoals vastgesteld in de Strategie Nationale Veiligheid[2].

Het Kabinet vindt deze bevindingen verontrustend en voert de komende jaren haar activiteiten op om de weerbaarheid tegen spionage te vergroten. Het Kabinet draagt deze verantwoordelijkheid niet alleen. Bedrijfsleven en organisaties zijn zelf verantwoordelijk voor hun weerbaarheid tegen spionage en de bescherming van hun kernbelangen. Hoewel Nederland bedrijven en organisaties kent die goed weerbaar zijn tegen spionage, laat de analyse zien dat er, met name waar het gaat om het bewustzijn ten aanzien van dit risico, nog veel werk te verrichten is. Het Kabinet wil een sterke bondgenoot zijn voor alle organisaties en onderschrijft de hoofdaanbevelingen van het rapport.

Het Kabinet zet daarom in op het verhogen van het waardebewustzijn ten aanzien van de informatie waarover organisaties beschikken, het versterken van het bewustzijn ten aanzien van veiligheidsmaatregelen om de kwetsbaarheid van die informatie te verminderen en het meenemen van dit waardebewustzijn bij lange termijn afwegingen. Met deze brief wil ik u namens het Kabinet op de hoogte brengen van onze voorgenomen aanpak naar aanleiding van het rapport.

De dreiging van spionage

Spionage is een dreiging waar wij ons meer bewust van moeten zijn. De AIVD constateert dat de dreiging van (digitale) spionage toeneemt, terwijl in Nederland spionagerisico's vaak worden onderschat.[3] Spionageactiviteiten behelzen niet alleen het heimelijk verwerven van kennis en informatie die kan worden gebruikt om Nederlandse belangen te schaden, maar ook het heimelijk beïnvloeden (manipuleren) van processen. Heimelijke beïnvloeding van bijvoorbeeld (democratische) besluitvormingsprocessen tast de sociale en politieke stabiliteit ons land aan. De fysieke veiligheid en de territoriale integriteit van Nederland kan door

[1] *TK 2009-2010, 30821, nr. 11*
[2] *TK 2006-2007, 30821, nr. 3*
[3] *TK 2009-2010, 30977, nr.32*

spionage in gevaar komen. (bijvoorbeeld door een cyberaanval of sabotage van Nederlandse vitale infrastructuur)

Uit het rapport KWAS blijkt dat de Nederlandse economische veiligheid door spionage bedreigd kan worden, doordat bedrijven slachtoffer worden van spionage door buitenlandse inlichtingendiensten die tot doel hebben de eigen nationale economische belangen ten koste van Nederland te versterken. Dit kan leiden tot aantasting van de (internationale) concurrentiepositie van Nederland, met als mogelijk gevolg verlies van inkomsten, banen en vooral ook economische voorsprong die Nederland op een aantal terreinen heeft.

Aanpak om de weerbaarheid tegen spionage te verhogen

Het Kabinet neemt de aanbevelingen van het rapport over. Kern van de aanpak tegen spionage is het vergroten van het waarde- en veiligheidsbewustzijn van niet alleen de (Rijks)overheid maar van alle organisaties in Nederland. Het begin van een goede weerbaarheid tegen spionage begint niet bij het plaatsen van een hoog hek rond een gebouw maar bij het verwerven van inzicht in kernbelangen en kwetsbaarheden.

Strategische kennis en bedrijvigheid, van groot belang voor de nationale veiligheid kan (op de langere termijn) weglekken naar het buitenland via aan- of uitbestedingen. Dit kan leiden tot aantasting van kernbelangen doordat vitale onderdelen van een proces worden gecompromitteerd

Daarnaast moet beveiliging van informatie en communicatietechnologie gezien het risico van spionage meer aandacht krijgen. Toenemende digitalisering van informatie en de koppeling van datasystemen maken een goede beveiliging noodzakelijk. De exclusiviteit, integriteit en beschikbaarheid van informatie staan hierbij centraal, niet alleen aangaande technische beveiliging maar ook het veiligheidsbewustzijn van medewerkers bij het gebruik van ICT-middelen. De Nationale Cyber Security Strategie (NCSS), die momenteel wordt ontwikkeld, sluit hier nauw bij aan.

Acties

Het Kabinet gaat de weerbaarheid bij de (Rijks)overheid versterken en het Nederlandse bedrijfsleven hiertoe stimuleren. Het Kabinet stelt hiervoor een instrument (*Handleiding KWAS*) ter beschikking. Organisaties kunnen hiermee voor zichzelf inzichtelijk maken wat hun kernbelangen zijn en wat bij die kernbelangen de mogelijke kwetsbaarheden zijn. Dit inzicht zal organisaties (nog) beter in staat stellen zelf af te wegen welke maatregelen zij in willen zetten om hun weerbaarheid te vergroten. De uitkomsten van deze individuele analyses worden in beginsel niet gedeeld met anderen om de kwetsbaarheid niet te vergroten. Het Kabinet roept organisaties op deze Handleiding KWAS te gebruiken.

Overheid

De Rijksoverheid geeft invulling aan de eigen verantwoordelijkheid door te investeren in het vergroten van het veiligheidsbewustzijn bij de medewerkers in elk ministerie en bij de Nederlandse Ambassades en Vertegenwoordigingen. De primaire verantwoordelijkheid hiervoor ligt volgens het Kabinet bij de hoogste managementraden.

- Binnen de gehele Rijksoverheid wordt de *Handleiding KWAS* toegepast om kwetsbaarheidsanalyses op te stellen en tegenmaatregelen te treffen. Waar

mogelijk gebeurt dit in samenhang met de invoering van het VIR-GI, het vernieuwde VIR-BI.
- Voor datasystemen (servers) die vertrouwelijke of geheime informatie bevatten maken alle departementen strikte afspraken met ICT-dienstverleners over de gewenste beveiligingsvoorzieningen.
- Periodiek worden, onder verantwoordelijkheid van de hoogste managementraden en hun Beveiligingsambtenaren, security audits en systeempenetratietesten gehouden, waarin nadrukkelijk aandacht wordt besteed aan spionagerisico's.
- De kennis over de kwetsbaarheden van ICT-technieken en – toepassingen wordt (verder) vergroot, met focus op waar specifieke kwetsbaarheden zich voordoen, hoe deze te herkennen en te voorkomen.
- *Awareness*-presentaties (op management- én medewerkerniveau), onder andere door de AIVD, worden voortgezet met specifieke focus op de voor het betreffende departement geldende kernbelangen en kwetsbaarheden.

Waar mogelijk wordt aangesloten bij bestaande activiteiten, zoals het integriteitbeleid van de Rijksoverheid en de veiligheidsmaatregelen die worden genomen tegen verstoring of uitval van ICT en elektriciteit.

Bedrijfsleven, onderwijs, medeoverheden en overige sectoren

Ter ondersteuning van het bedrijfsleven en andere organisaties onderneemt het Kabinet onderstaande acties:

- VNO-NCW en de Rijksoverheid zullen in 2011 een intentieverklaring tekenen. De Rijksoverheid stelt (waar mogelijk) kennis en expertise over het identificeren (en beschermen) van kernbelangen en kwetsbaarheden beschikbaar. VNO-NCW zet zich in voor het implementeren van de handleiding KWAS en het verhogen van het veiligheidsbewustzijn bij kwetsbare bedrijfstakken. Het bedrijfsleven wordt zo gestimuleerd om de weerbaarheid tegen spionage op het hoogste managementniveau te borgen.
- De *Handleiding KWAS* wordt ter beschikking gesteld aan organisaties buiten de Rijksoverheid.
- Sectorspecifieke *awareness*-presentaties (op management- én medewerkerniveau), onder andere door de AIVD, worden voortgezet. Deze presentaties beogen het inzicht te geven in het risico van spionage.
- Met betrokken koepelorganisaties wordt de samenwerking gezocht om voorlichtingsbijeenkomsten te organiseren en *best practices* te verzamelen en te delen.
- Alle organisaties worden opgeroepen om meldingen over spionage door te geven aan de AIVD. Op de website van de AIVD wordt extra informatie gegeven aan bedrijven en over de gevaren van spionage en instrumenten om deze gevaren te herkennen.
- Organisaties krijgen de beschikking over een checklist waarmee zij kunnen nagaan of producten en/of technologieën die zij ontwikkelen, potentieel inzetbaar zijn voor strategisch-militair gebruik, waardoor zij kernbelangen beter kunnen onderkennen.

Het Kabinet realiseert zich dat per sector de mate van weerbaarheid én de mate van kwetsbaarheid zeer kan verschillen. Departementen zullen bovenstaande activiteiten oppakken.

Datum
22 februari 2011

Kenmerk
2011-2000040980

Versterkte weerbaarheid

Het is de ambitie van dit Kabinet om de Nederlandse weerbaarheid tegen spionage zo snel mogelijk structureel te verhogen. Dit begint met het bewustzijn dat ook Nederland kwetsbaar is voor spionage door buitenlandse mogendheden. Het Kabinet wil dan ook in 2012 zichtbare stappen hebben gezet ter verbetering van de Nederlandse weerbaarheid tegen spionage. Het kabinet zal hiervoor de gezamenlijke inspecties verzoeken een onderzoek in te stellen naar de voortgang binnen het Rijksdomein.

De Minister van Veiligheid en Justitie,