KWAS

Handleiding
Kwetsbaarheidsonderzoek
spionage

Inhoud

Voorwoord

Ten onrechte heerst soms het beeld dat spionage iets uit de Koude Oorlog is, of dat spionage zich uitsluitend richt op militaire gegevens. Niets is minder waar. Buitenlandse overheden verwerven ook vandaag de dag geheime economische en politieke informatie via hun inlichtingendiensten. Zo kan nieuw verworven, hoogwaardige technische kennis bijdragen aan de economische ontwikkeling, concurrentiepositie en welvaart van een land.

Mogelijk beschikt ook uw organisatie over waardevolle informatie die u niet wilt prijsgeven aan onbevoegden, zoals bijvoorbeeld buitenlandse inlichtingendiensten. Kennis over voorgenomen standpunten in zakelijke of politieke onderhandelingen kan bijvoorbeeld de uitkomst van die onderhandelingen sterk beïnvloeden. Voor u als gedupeerde partij kan spionage schadelijk zijn voor uw concurrentiepositie en bedrijfscontinuïteit.

Niet iedereen beseft echter wat de informatie waarmee hij werkt waard is. Het gaat namelijk niet alleen om 'officiële' bedrijfsgeheimen. Denk aan de mogelijkheid dat vertrouwelijke informatie af te leiden is uit meerdere, losse stukjes en relatief toegankelijke informatie, zoals klanten- en personeelsbestanden. Betalingsgegevens uit uw administratie vertellen, in combinatie met informatie over uw leveranciers en afnemers, misschien wel iets over uw (geheime) bedrijfsstrategie.

De beveiliging van informatie verdient dan ook de nodige aandacht. Als de medewerkers zich bewust zijn van spionagerisico's, kan een organisatie haar belangen immers beter beschermen.

Op 6 april 2010 publiceerde de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), in samenwerking met het Directoraat-Generaal Veiligheid van het huidige ministerie van Veiligheid en Justitie, het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid*. Dit rapport geeft voor enkele sectoren in Nederland een beeld van de belangrijkste te beschermen belangen en de bijbehorende kwetsbaarheden voor spionage.

Handleiding

Deze Handleiding Kwetsbaarheidsanalyse Spionage helpt u om voor uw eigen organisatie een inventarisatie te maken van de cruciale belangen en de daarbij behorende kwetsbaarheden. Onder *cruciaal belang* wordt hier verstaan een verzameling van gegevens waarvan onbevoegde kennisname uw bedrijfsbelangen aantast en waarvan redelijkerwijs aangenomen kan worden dat andere partijen er interesse in hebben. *Kwetsbaarheden* zijn al die factoren die de beveiliging van uw cruciale belangen tegen spionage aantasten.

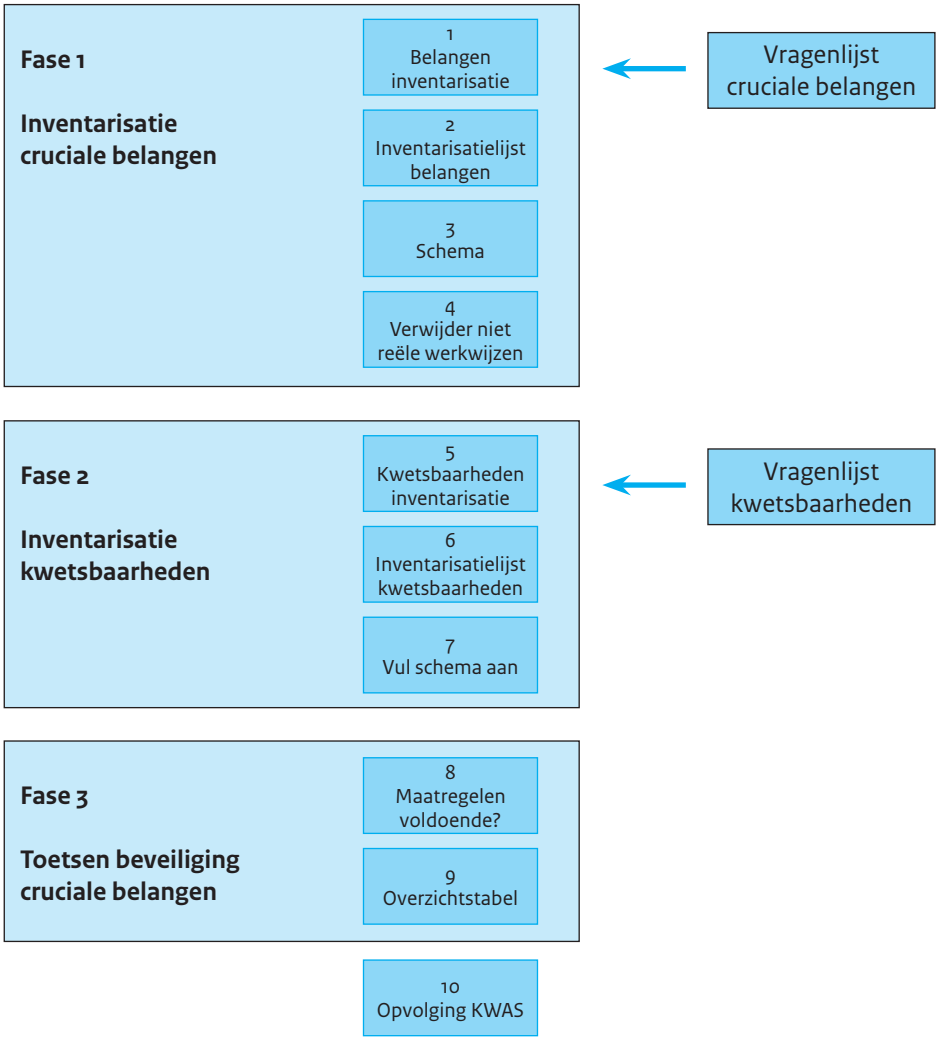
In welke specifieke informatie zijn inlichtingendiensten mogelijk geïnteresseerd? Welke cruciale informatie wilt u beschermen tegen onbevoegde kennisname? Welke factoren maken deze cruciale belangen binnen uw organisatie extra gevoelig voor spionage? Zou specifieke aandacht voor spionage misschien een plaats moeten krijgen in het risicoprofiel van uw organisatie? Deze Handleiding helpt u een antwoord te formuleren op dit soort vragen.

De Kwetsbaarheidsanalyse spionage bestaat uit drie fases:

- Inventarisatie cruciale belangen
- Inventarisatie kwetsbaarheden
- Toetsen beveiliging cruciale belangen

Stappenplan voor een kwetsbaarheidsanalyse spionage

Met dit stappenplan maakt u een analyse van de kwetsbaarheid voor spionage van uw eigen organisatie. De te volgen stappen staan hier schematisch weergegeven. U kunt voor uw kwetsbaarheidsanalyse, naast het stappenplan, onder meer gebruik maken van het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid* en de AIVD-brochures over spionage. Deze informatie kunt u vinden op ww.aivd.nl



Randvoorwaarden

Voor het uitvoeren van een kwetsbaarheidsanalyse zult u enkele randvoorwaarden moeten creëren. De directie is verantwoordelijk voor het beveiligingsbeleid van de organisatie. Het is dan ook een voorwaarde dat zij vooraf op de hoogte is van het onderzoek en het belang hiervan onderschrijft.

Overweeg een projectmatige benadering voor uitvoering van de analyse, afhankelijk van de specifieke situatie in uw organisatie. Benoem dan ook een projectleider. Dit kan de security manager of beveiligingsambtenaar (BVA) zijn, maar ook een projectleider uit een ander organisatieonderdeel. Betrek in dat laatste geval de security manager in een zo vroeg mogelijk stadium bij het project.

Om de analyse goed uit te kunnen voeren, is het belangrijk dat geïnterviewden vrijuit kunnen spreken. Garandeer daarom de anonimiteit van de geïnterviewden.

Fase 1

Inventarisatie cruciale belangen

Stap 1 Inventariseer uw cruciale belangen

U inventariseert de cruciale belangen van uw organisatie door aan de hand van de vragenlijst 'Cruciale belangen' gesprekken te voeren met medewerkers uit uw organisatie (zie bijlage 1). Bij voorkeur spreekt u een aantal mensen op strategisch niveau omdat zij waarschijnlijk het beste kunnen inschatten welke belangen het meest cruciaal zijn voor de organisatie. Interview daarnaast inhoudelijke experts die betrokken zijn bij de cruciale belangen. Maak een gespreksverslag van elk interview. Bereid u voor op de interviews door de eventueel al aanwezige informatie over de belangen van uw organisatie door te nemen. Raadpleeg bijvoorbeeld reeds bestaande (interne) documentatie waarin sleutelbelangen, bedrijfsgeheimen en dergelijke zijn vastgesteld. Deze potentiële 'cruciale belangen' kunt u opnemen in een lijst die u later ter toetsing aan respondenten voorlegt. Lees voor u het onderzoek begint het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid* en de AIVD-brochures over spionage om een gevoel te krijgen wat cruciale belangen zouden kunnen zijn.

Stap 2 Stel de Inventarisatielijst cruciale belangen op

Aan de hand van de gespreksverslagen maakt u een inventarisatielijst cruciale belangen. U vult in een tabel in welke cruciale belangen u heeft geïdentificeerd (zie tabel 1). Sommige van deze cruciale belangen trekken alleen de aandacht van concurrenten of criminelen, andere ook van inlichtingendiensten. Noteer in de tabel achter elk cruciaal belang of dit belang interessant is voor concurrenten of criminelen of ook voor inlichtingendiensten. Het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid*, biedt u voorbeelden van belangen die interessant kunnen zijn voor inlichtingendiensten.

Uiteindelijk ziet uw inventarisatielijst cruciale belangen er ongeveer zo uit:

Tabel 1 Voorbeeld Inventarisatielijst cruciale belangen

Cruciaal belang	Dreiging
Het volledige klantenbestand	Gegevens van klanten zijn mogelijk interessant voor concurrenten
Geheim recept	Interessant voor bijvoorbeeld concurrenten
Details van de offerte voor de bouw van een haven in Dubai	Mogelijk ook interessant voor inlichtingendiensten

Stap 3 Maak per cruciaal belang een schema

In deze stap vult u voor elk cruciaal belang één schema in. Dit doet u door op ieder schema één cruciaal belang en de bijbehorende dreiger in te vullen. In de bijlagen treft u een sjabloon van een schema aan (zie bijlage 3); dit schema is ook in digitale vorm beschikbaar op de AIVD-website. Elk schema is verder voorzien van een uitgebreide lijst werkwijzen van inlichtingendiensten en de werkwijzen van concurrenten en criminelen.

Stap 4 Schrap per schema de niet reële werkwijzen

In deze stap geeft u per cruciaal belang aan welke werkwijzen niet van toepassing zijn. Zo blijven in elk schema de werkwijzen over die u wilt toetsen. Sommige van de werkwijzen zijn namelijk exclusief voor inlichtingendiensten, andere kunnen ook gebruikt worden door concurrenten of criminelen. In hoofdstuk 8 van het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid* en de AIVD-brochures over spionage vindt u meer informatie over de diverse werkwijzen.

U houdt bij het schrappen van de niet reële werkwijzen nog geen rekening met reeds aanwezige beveiligingsmaatregelen in uw organisatie. Dit doet u pas in stap 8. In deze stap sluit u alleen werkwijzen uit die onmogelijk van toepassing kunnen zijn.

Wanneer de dreiger geen inlichtingendienst is, maar bijvoorbeeld een concurrent, kunnen alle werkwijzen die exclusief zijn voor inlichtingendiensten in principe buiten beschouwing worden gelaten. Het heeft immers geen zin rekening te houden met werkwijzen die concurrenten en criminelen niet zullen toepassen. Noteer daarom achter de werkwijzen die exclusief voor inlichtingendiensten gelden 'niet van toepassing' (in de kolom Beoordeling). Als de dreiger een inlichtingendienst is, moet u in eerste instantie rekening houden met alle werkwijzen.

Daarnaast moet de werkwijze natuurlijk wel toepasbaar zijn op spionage tegen het betreffende cruciale belang. Noteer dan ook 'niet van toepassing' achter alle onmogelijke werkwijzen (in de kolom Beoordeling). Denk hierbij bijvoorbeeld aan een cruciaal belang dat uitsluitend is vastgelegd op een handgeschreven document: dit kan in principe niet door hacking bedreigd worden.

Een schema kan er dan zo uitzien:

Tabel 2 Voorbeeld schema

Schema werkwijzen			
	Belang	**Geheim recept**	
	Dreiger	**Concurrenten**	
	Exclusief voor inlichtingendiensten		**Beoordeling**
1	Telecominterceptie		*Niet van toepassing.*
2	Doorbreken encryptie		*Niet van toepassing.*
	enzovoort		
	Ook mogelijk voor concurrenten	**Kwetsbaarheden uit interviews, te koppelen aan werkwijzen**	**Beoordeling**
10	Hacking		*Niet van toepassing.*
	enzovoort		...

Fase 2

Inventarisatie kwetsbaarheden

Stap 5 Voer de kwetsbaarheidsinventarisatie uit

Voor de inventarisatie van de kwetsbaarheden voert u wederom vraaggesprekken. Gebruik hiervoor de vragenlijst 'Kwetsbaarheden' (zie bijlage 2). Ter voorbereiding op het gesprek is het wenselijk dat de te interviewen personen hoofdstuk 8 van het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid* en de AIVD-brochures over spionage lezen. Maak een gespreksverslag van elk interview.

Bereidt u voor op de interviews door de eventueel al aanwezige informatie over de kwetsbaarheden van uw organisatie door te nemen. U kunt ook alvast enkele potentiële kwetsbaarheden bedenken die u tijdens de interviews ter illustratie kunt gebruiken. Het rapport *Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid* en de AIVD-brochures over spionage bevatten voorbeelden van kwetsbaarheden en werkwijzen.

Het is van belang dat u in deze gespreksronde juist ook medewerkers op de werkvloer spreekt. Zij kennen misschien 'gaten' die niet in het beveiligingsplan naar voren komen, maar in de praktijk wel bestaan. Juist zij weten bijvoorbeeld dat de achterdeur van uw verder hermetisch afgesloten gebouw vaak openstaat vanwege het gebruik van de rookruimte achter de parkeerplaats of dat voormalige personeelsleden nog kunnen inloggen op

het bedrijfsnetwerk. Ook kunnen inhoudelijke experts vanuit hun interesse en expertisegebied iets toevoegen, zoals een computerexpert die weet dat de (vertrouwelijke) personeelsadministratie met enige handigheid te vinden is op het computernetwerk. Ten slotte kunnen de mensen die direct betrokken zijn bij de beveiliging van uw organisatie natuurlijk die waardevolle ideeën hebben over kwetsbaarheden.

Een aanvullende mogelijkheid om kwetsbaarheden te ontdekken is het zogenaamde red teaming. Daarbij wordt een (in- of externe) partij expliciet gevraagd te proberen de beveiliging te omzeilen om een (bij voorkeur gesimuleerd) cruciaal belang te stelen. De analyse van een dergelijke exercitie levert vaak verrassende inzichten op over kwetsbaarheden.

Stap 6 Stel de Inventarisatielijst kwetsbaarheden op

Aan de hand van de gespreksverslagen maakt u een inventarisatielijst kwetsbaarheden. U geeft hiertoe in een tabel weer (zie als voorbeeld tabel 3) welke kwetsbaarheden voor spionage verzameld zijn.

Kijk bij het invullen van de tabel ook naar 'verborgen' kwetsbaarheden, door informatie uit verschillende gespreksverslagen te combineren. Bijvoorbeeld: als bijna niemand van de geïnterviewden zich bewust lijkt te zijn van het feit dat bepaalde informatie een cruciaal belang is (terwijl deze informatie wel als zodanig is vastgesteld na de eerste serie interviews), dan is dit een kwetsbaarheid op zich en verdient het een plaats in de tabel.

Ook verschillen in interpretatie en kennisniveau over de beveiliging kunnen een kwetsbaarheid zijn. Bijvoorbeeld: een medewerker van de ICT-afdeling stelt in haar interview dat het netwerk afdoende beveiligd is voor intern e-mailverkeer. Gevoelige informatie mag echter niet via het netwerk worden verstuurd. In een ander interview geeft een gebruiker van het netwerk aan 'altijd veilig te werken, omdat hij gevoelige informatie alleen via de interne e-mail verstuurt en niet via het internet'. Een dergelijke onbekendheid met protocollen en beveiligingseisen bij gebruikers kan een kwetsbaarheid vormen, terwijl op het eerste gezicht beide partijen die niet als zodanig in hun interview zullen benoemen.

Tabel 3 Voorbeeld Inventarisatielijst kwetsbaarheden

Kwetsbaarheid
Een medewerker merkt op dat de beveiliging van uw organisatie is uitbesteed. Zij vraagt zich af of dit niet een risico vormt voor spionage.
Een analist merkt op dat bezoekers vrij regelmatig zonder begeleiding over de gang rondzwerven, omdat ze niet naar de uitgang begeleid worden.
Een medewerker geeft aan vertrouwelijke informatie te verzenden over interne e-mail. De ICT-afdeling vertelt dat het netwerk niet bedoeld is voor het verzenden van vertrouwelijke informatie.
Uit verscheidene interviews komt een algemeen gebrek aan bewustzijn over spionagerisico's naar voren.
Een onderzoeker merkt op dat tijdens de rondleiding op het researchlab een van de (buitenlandse) delegatieleden foto's stond te maken met z'n gsm. Ze gaf aan daar verder niets van gezegd te hebben, omdat ze niet wist of en hoe ze een delegatielid hierop kon aanspreken of wat ze verder kon doen.

Stap 7 Vul de schema's aan met de bijbehorende kwetsbaarheden

Vul uw schema's nu aan met de informatie uit de inventarisatielijst kwetsbaarheden. Als een kwetsbaarheid hoort bij een cruciaal belang of bij meerdere belangen, vult u deze kwetsbaarheid in op de betreffende schema's. Is een kwetsbaarheid specifiek te relateren aan een of meer werkwijzen, dan noteert u die kwetsbaarheid in het schema in dezelfde rij als de betreffende werkwijze. Een voorbeeld ziet u in tabel 5, waar de kwetsbaarheid 'achterdeur open in verband met rookruimte' aan de werkwijze 'insluiting' is gekoppeld.

Als een kwetsbaarheid niet specifiek aan een werkwijze te relateren is, dan noteert u deze kwetsbaarheid op de schema onderaan de kolom Kwetsbaarheden, daar waar geen werkwijzen meer genoemd zijn. Een voorbeeld ziet u in tabel 5, bij de kwetsbaarheid 'gebrek aan bewustzijn over spionagerisico's'.

Tabel 5 Voorbeeld schema met kwetsbaarheden

Schema			
	Belang	**Geheim recept**	
	Dreiger	**Concurrenten**	
	Exclusief voor inlichtingendiensten		**Beoordeling**
1	Telecominterceptie		*Niet van toepassing.*
2	Doorbreken encryptie		*Niet van toepassing.*
	enzovoort		
	Ook mogelijk voor concurrenten	**Kwetsbaarheden uit interviews, te koppelen aan werkwijzen**	**Beoordeling**
10	Hacking		*Niet van toepassing.*
	…		
17	Gelegenheidsdiefstal	**Medewerkers begeleiden bezoekers niet altijd naar de uitgang**	
…	…	…	
19	Insluiting	**Achterdeur open vanwege rookruimte**	
	enzovoort		
		Kwetsbaarheden volgend uit interviews, niet te koppelen aan specifieke werkwijze	
23		**Gebrek aan bewustzijn over spionagerisico's**	

Fase 3

Toetsen beveiliging cruciale belangen

Stap 8 Toets de reeds genomen maatregelen

Ga na of de weerstand van uw organisatie voldoende is om spionage te voorkomen. Bij elk schema toetst u per werkwijze of de beveiligingsmaatregelen in uw organisatie voldoende zijn om spionage op deze wijze onmogelijk te maken. Denk hierbij aan organisatorische, elektronische en bouwkundige maatregelen. Houd bij de beoordeling rekening met eventueel bij de werkwijze behorende kwetsbaarheden die van invloed zijn op de beveiliging. Vervolgens toetst u of de kwetsbaarheden die niet specifiek aan een werkwijze gerelateerd zijn, voldoende ondervangen worden door bestaande maatregelen.

Als de beveiliging tegen een bepaalde werkwijze en/of kwetsbaarheid afdoende is, kleurt u de cel van de betreffende werkwijze en/of kwetsbaarheid in de kolom Beoordeling groen. Wanneer dit niet het geval is, kleurt u de cel van de betreffende werkwijze en/of kwetsbaarheid rood. Markeer op deze wijze alle werkwijzen en/of kwetsbaarheden die van toepassing zijn op dit belang. Als alle beoordelingen van de werkwijze en kwetsbaarheden die bij een belang horen groen gekleurd zijn, kleurt u uiteindelijk het cruciale belang groen. Als een of meer werkwijzen en/of kwetsbaarheden rood gemarkeerd zijn, kleurt u ook het betreffende belang rood. Op de volgende pagina ziet u een voorbeeld van een ingekleurd tabel (zie tabel 6).

Tabel 6 Voorbeeld schema

Schema			
	Belang	**Geheim recept**	
	Dreiger	**Concurrenten**	
	Exclusief voor inlichtingendiensten		**Beoordeling**
1	Telecominterceptie		*Niet van toepassing.*
...	enzovoort		*Niet van toepassing.*
	Ook mogelijk voor concurrenten	**Kwetsbaarheden uit interviews, te koppelen aan werkwijzen**	**Beoordeling**
10	Hacking		*Niet van toepassing.*
14	Chantage personen		De kleine groep werknemers met toegang is gescreend.
17	Gelegenheidsdiefstal	**Medewerkers begeleiden bezoekers niet altijd naar de uitgang**	Het recept ligt in een kluis, waartoe slechts een beperkte groep mensen toegang heeft.
19	Insluiting	**Achterdeur open vanwege rookruimte**	De goede fysieke beveiliging van het gebouw kan door deze open deur teniet gedaan worden. Een inbreker zou bijvoorbeeld kunnen proberen zich in te laten sluiten om vervolgens de kluis te kraken en leeg te halen.
20	Infiltratie	**Beveiliging is uitbesteed en deze beveiligers hebben toegang tot alle sleutels**	Slechts een zeer selecte groep mensen heeft toegang tot dit cruciale belang en het is onwaarschijnlijk dat een infiltrant tot deze groep kan doordringen. De sleutels voor de kluis worden echter bewaard in de loge. De externe beveiligers hebben toegang tot deze loge, daarmee tot de sleutels en daarmee tot de kluis.
		Kwetsbaarheden volgend uit interviews, niet te koppelen aan specifieke werkwijze	**Beoordeling**
21		**Bezoekers kunnen met een mobiele telefoon foto's maken in de productiefaciliteit**	Het recept ligt in een kluis, waartoe slechts een beperkte groep mensen toegang heeft. Het recept kan dus niet zomaar door een bezoeker gefotografeerd worden.
22		**Gebrek aan bewustzijn over spionagerisico's'**	Algemene kwetsbaarheid waardoor diverse spionage werkwijzen eenvoudiger worden (chantage, manipulatie)

Stap 9 Overzichtstabel

U heeft nu voor ieder cruciaal belang een schema. De door u gemaakte schema's tonen de huidige spionagerisico's voor uw cruciale belangen. Kwetsbaarheden en werkwijzen die niet of onvoldoende zijn ondervangen zijn rood gekleurd. Deze uitkomsten kunt u samengevat voorleggen aan het management. Het management kan dan bepalen welke (rode) kwetsbaarheden of werkwijzen onacceptabel zijn. Maak daarvoor een overzichtstabel zoals in onderstaand voorbeeld.

Geef in de eerste kolom alle vastgestelde cruciale belangen weer (in volgorde van meest naar relatief minst belangrijk). Neem de kleur die het cruciale belang in het schema gekregen heeft over.

In de tweede kolom vult u bij ieder cruciaal belang alle werkwijzen in die op uw schema rood gekleurd waren. In de derde kolom vult u bij ieder cruciaal belang alle kwetsbaarheden in die op uw schema rood gekleurd waren. De tabel bevat nu de cruciale belangen van uw organisatie en waar van toepassing de werkwijzen en/of kwetsbaarheden die de cruciale belangen bedreigen. U kunt nu in een oogopslag zien welke cruciale belangen beter beschermd zouden kunnen worden.

Voorbeeld overzichtstabel

Cruciale belangen	Werkwijzen	Kwetsbaarheden
Noem hier in steekwoorden per cel één cruciaal belang, kleur uiteindelijk de cel in.	*Benoem hier in steekwoorden alle werkwijzen die in het schema van dit belang rood gekleurd zijn.*	*Benoem hier in steekwoorden alle kwetsbaarheden die in het schema van dit belang rood gekleurd zijn.*
Geheim recept	Infiltratie	Beveiliging is uitbesteed aan externe partij.
	Gerichte diefstal met inbraak	Achterdeur open i.v.m. rookruimte
		Gebrek aan bewustzijn over spionagerisico's
Details van de offerte voor de bouw van een haven in Dubai	Niet aanwezig	Niet aanwezig
Het volledige klantenbestand	enzovoort	enzovoort

Stap 10 Opvolging kwetsbaarheidsanalyse spionage

Leg de uitkomsten van uw kwetsbaarheidsanalyse spionage voor aan het management. Doe voorstellen voor maatregelen ter (verbetering van de) beveiliging van de roodgekleurde belangen. Herhaal de kwetsbaarheidsanalyse periodiek. Borg de aandacht voor de kwetsbaarheden van uw organisatie voor spionage in de beveiligingsrapportages en het corporate awareness programma.

Informatie

Als u naar aanleiding van de uitkomsten van uw kwetsbaarheidsanalyse spionage behoefte heeft aan meer informatie over spionage, kunt u aanvullende informatie vinden op de volgende websites:

- www.aivd.nl
- www.govcert.nl

Op www.aivd.nl vindt u:

- het rapport *Kwetsbaarheidsanalyse spionage, Spionagerisico's en de nationale veiligheid*
- de brochure *Spionage in Nederland. Wat is het risico?*
- de brochure *Spionage bij reizen naar het buitenland. Wat is het risico?*
- de brochure *Digitale Spionage. Wat is het risico?*
- de jaarverslagen van de AIVD.

Daarnaast organiseert de AIVD voorlichtingsbijeenkomsten over spionage voor vertegenwoordigers van diverse sectoren die binnen hun organisatie verantwoordelijk zijn voor beveiliging.

Wees u bewust van het risico van spionage en creëer ook bewustzijn binnen uw organisatie. Als u zaken tegenkomt, waarvan u vermoedt dat ze het werk van een inlichtingendienst zijn, dan hoort de AIVD graag van u, ook als u twijfelt.

Algemene Inlichtingen- en Veiligheidsdienst
Adres: Postbus 20010
2500 EA Den Haag
Telefoon: 079 - 320 50 50
Fax: 070 - 320 07 33
Website: www.aivd.nl

Bijlage 1 Vragenlijst Cruciale belangen

Tips bij het gesprek

- Verdiep u vooraf in de dreigingen van spionage. Spionagedreigingen worden vaak óf onderschat óf overschat. Raadpleeg de website van de AIVD voor meer informatie en schets een reëel beeld van de dreiging.

- Verstrek voorafgaand aan het gesprek schriftelijk materiaal aan uw gesprekspartner, en vertel er eventueel bij wat voor type vragen u wilt gaan stellen. U biedt uw gesprekspartner zo de kans zich gedegen voor te bereiden. Schets in de inleiding de achtergronden bij het gesprek, de functie van dit gesprek in de gehele analyse, en het belang van het gesprek met betrokkene:
  - benoem doel, werkwijze en resultaten van deze Kwetsbaarheidsanalyse spionage. Leg uit dat cruciale belangen en kwetsbaarheden los van elkaar geïnventariseerd worden.

- Creëer een vertrouwelijke sfeer:
  - benoem dat het gesprek vertrouwelijk is, dat het gesprek wordt gevoerd op grond van de functionaliteit van betrokkene en dat gespreksverslagen niet worden teruggekoppeld naar de geïnterviewde of naar de directie.

- Houd in het gesprek de betekenis van begrippen als dreiging, weerstand/ beveiliging en kwetsbaarheid goed gescheiden.

- Onderstreep dat een cruciaal belang of de beveiliging daarvan in beginsel onafhankelijk van de dreiging moet worden bepaald. De mate waarin iets als 'belangrijk' beschouwd wordt, is in dit stadium van het onderzoek niet afhankelijk van een eventuele dreiging ertegen.

- Noem in de inleiding dat u in dit gesprek op zoek bent naar cruciale belangen. Een cruciaal belang kenmerkt zich door het feit dat de informatie (bijna) nergens anders te verkrijgen is, niet openbaar zou moeten zijn en aantrekkelijk is voor andere partijen omdat zij er hun voordeel (commercieel of strategisch) mee kunnen doen.

  Voorbeelden van cruciale belangen zijn:
  - financiële gegevens van de afdeling Facturatie of van de afdeling Trade;
  - klantenbestanden;
  - personeelsdossiers of persoonsgevoelige informatie over eigen medewerkers;
  - informatie over aanbestedingen op de afdeling Inkoop;
  - e-mailverkeer;
  - stukken op hoger directieniveau met strategische en/of tactische informatie;
  - intellectueel eigendom en handelsstrategie.

- Behandel steeds weer alle vragen.

- Als een gesprekspartner geen antwoord wil of kan geven, is het mogelijk zelf een antwoord aan te dragen. Doe dit pas nadat de mogelijkheden bij respondent zijn uitgeput. Maak in het verslag duidelijk welke antwoorden actief door de respondent gegenereerd zijn, en welke passief door hem bevestigd zijn.

- Voor alle vragen geldt dat steeds de motivatie achter een antwoord van belang is. Waarom is iets van belang? Waarom is de weerstand laag? Waarom treedt er schade op na aantasting van de cruciale belangen? Stevig doorvragen geeft u inzicht in achtergrond van de antwoorden.

- Geef bewust vorm aan archivering en verslaglegging, zodanig dat u uw afspraken (onder andere over vertrouwelijkheid/anonimiteit) met de gesprekpartners kunt nakomen.

Vragen

1. Stel u bent een buitenlandse inlichtingenofficier (een spion) en u wordt naar uw organisatie gestuurd om daar te spioneren. Welke drie cruciale belangen zou u dan bovenaan uw verlanglijstje hebben staan van meest belangrijke 'geheime' informatie die u zou willen verzamelen? *Benadruk dat we hier op zoek zijn naar cruciale belangen en daarmee dus naar zaken die, wanneer ze inderdaad zouden weglekken naar andere overheden of bedrijven, uw organisatie, of de Nederlandse samenleving, nadelig kunnen beïnvloeden. Benadruk ook dat het gaat om informatie die niet zomaar toegankelijk zou moeten zijn voor iedereen, dat het dus gaat om (bedrijfs)geheime informatie.*

2. Waarom zou u juist die informatie willen binnenhalen? *Deze vraag beantwoorden voor ieder van de drie cruciale belangen.*

3. Denkt u er weleens over na dat gegevens waar uw organisatie over beschikt zouden kunnen weglekken naar buitenlandse overheden of bedrijven? *Feitelijk dus: dat de organisatie bespioneerd kan worden.*

4. Hoe zou het weglekken van de drie cruciale belangen die u net noemde uw bedrijf of de Nederlandse samenleving negatief kunnen beïnvloeden? *Vraag beantwoorden voor ieder van de drie cruciale belangen.*

5. Wie heeft volgens u (mogelijk) toegang tot die drie cruciale belangen/informatie? *Vraag beantwoorden voor ieder van de drie cruciale belangen.*

6. Zijn de cruciale belangen die u noemt goed beschermd/afgeschermd? *Vraag beantwoorden voor ieder van de drie cruciale belangen.*

7. Welke kwetsbaarheden tegen spionage signaleert u, als het gaat om de bescherming van deze gegevens? *Vraag beantwoorden voor ieder van de drie cruciale belangen.*

8. Wie weet eventueel meer over deze kwetsbaarheden? *Vraag beantwoorden voor ieder van de drie cruciale belangen.*

Reeds verzamelde cruciale belangen

- U legt de door u reeds geïnventariseerde cruciale belangen voor aan uw gesprekspartner. Dit zijn dus zowel de belangen die u zelf heeft afgeleid uit bestaande bedrijfsinformatie, als de belangen die door andere geïnterviewden reeds benoemd zijn in eerdere interviews.

9. In hoeverre herkent u zich in de keuze van deze cruciale belangen?
Met andere woorden, met welke cruciale belangen is gesprekspartner het eens is, en met welke niet.

10. Geef per item aan waarom gesprekspartner het betrokken item juist wél of waarom juist níet een cruciaal belang vindt. *Hier goed doorvragen.*

11. Wat zijn volgens u de vijf meest cruciale belangen die net besproken zijn?

12. Op welke locatie (een gebouw, land, plek) zijn deze vijf meest cruciale belangen te vinden?
Behandel dit voor ieder van deze vijf belangen.

13. Welke partijen beheren deze vijf meest cruciale belangen?
Behandel dit voor ieder van deze vijf belangen.

14. Welke partijen hebben toegang tot deze vijf meest cruciale belangen?
Behandel dit voor ieder van deze vijf belangen.

15. Missen er nog cruciale belangen?

16. Heeft u verder nog opmerkingen en zaken te benoemen die in dit verband belangrijk zijn?

Bijlage 2 Vragenlijst Kwetsbaarheden

Tips bij het gesprek

- In beginsel gelden bij dit gesprek dezelfde opmerkingen als bij het gesprek over cruciale belangen.
- Maak het verschil met de eerste gesprekken over cruciale belangen duidelijk. Dit gesprek gaat over de weerstand/beveiliging van de geïdentificeerde cruciale belangen met als resultaat inzicht in de kwetsbaarheid (tegen spionage) van de organisatie.
- Houd ook hier de begrippen cruciaal belang, weerstand/beveiliging en kwetsbaarheid goed gescheiden. Schets zonodig voor de gesprekspartner de verschillen.
- Benoem als opening van dit gesprek de eerder geïdentificeerde cruciale belangen.
- Verstrek vooraf de eerder geïdentificeerde cruciale belangen schriftelijk aan gesprekspartner en draag er zorg voor dat deze lijst vertrouwelijk behandeld wordt.
- Niet iedere geïnterviewde zal in detail alle vragen kunnen beantwoorden. Wel kan zo gekeken worden in hoeverre beveiligingsmaatregelen globaal bekend zijn binnen de organisatie.
- Geef bewust vorm aan archivering en verslaglegging, zodat u de gemaakte afspraken (onder andere over vertrouwelijkheid) met de gesprekpartners kunt nakomen.

Vragen

Algemeen

1. Vindt u dat dit inderdaad de belangrijkste cruciale belangen in uw organisatie zijn? Zo nee, welke zijn dat volgens u?
2. Hoe kwetsbaar zijn die cruciale belangen, dus hoe makkelijk zouden ze in handen kunnen vallen van onbevoegde derden? Waarom? *Dit is nadrukkelijk een open vraag, vraag hier gericht door.*
3. Waar ziet u zelf de grootste kwetsbaarheid: zijn dat bijvoorbeeld de mensen, is dat fysieke beveiliging, digitale informatie en communicatie, of inhuur van externe partijen? Waarom?
4. Wat doet uw afdeling/organisatie zelf om te voorkomen dat de cruciale belangen in handen vallen van onbevoegde derden?
5. Is er, voor zover u weet, binnen uw organisatie beleid, specifiek gericht op het tegengaan en/of beheersbaar maken van spionagerisico's?
6. Huurt u externen in die (delen van) uw bedrijfsvoering of het beheer van bepaalde zaken (onder andere panden, logistiek, digitale infrastructuur) van u hebben overgenomen? Komen die uit het buitenland? Ziet u dat als een veiligheidsrisico?

7. Zijn er (van overheidswege) regels/ vereisten gesteld ten aanzien van de beveiliging van uw personeel, gebouw, digitale systemen, enzovoort?

8. Worden veiligheidsincidenten geregistreerd? Zo ja, wat gebeurt daarmee?

Menselijke factor

9. In hoeverre zijn mensen binnen uw organisatie zich ervan bewust dat uw organisatie over bijzondere kennis beschikt die interessant zou kunnen zijn voor andere overheden? Het gaat hier dus om de mate van awareness.

10. Wat doet uw eigen organisatie om dit besef bij uw medewerkers op een optimaal niveau te krijgen?

11. Worden mensen die toegang hebben/krijgen tot cruciale belangen ook vooraf gescreend? Indien ja: uit welke elementen bestaat die screening? *Screening is een containerbegrip en kent vele varianten. Van belang is hier om precies te achterhalen wat onder deze screening verstaan wordt.*

12. Is het beheer van de kennis/informatie (met betrekking tot de cruciale belangen) uitbesteed aan een andere organisatie? *Bijvoorbeeld een IT-beheerder die toegang heeft tot servers en mail- en dataverkeer.*

13. Moeten extern ingehuurde partijen aan dezelfde veiligheidseisen voldoen als het eigen personeel? Worden deze eisen in de praktijk ook altijd gehandhaafd?

14. Heeft de organisatie zicht op wie toegang heeft (gehad) tot gevoelige informatie en wanneer? Worden gegevens zoals computergebruik en toegang gelogd, zo ja worden deze logging-gegevens onderzocht?

Fysieke beveiliging

15. Hoe is de fysieke toegang tot de kennis/ informatie geregeld?
    Zijn er verschillen in het beveiligingsregime als het gaat om:
    - medewerkers;
    - bezoekers;
    - ingehuurde externen (zoals monteurs, catering).

16. Is er een beveiligingsplan als het gaat om fysieke beveiliging? Van wie komt de expertise?

Digitale informatie

U stelt vragen over de opslag van en toegang tot digitale informatie en dataverkeer. Deze zijn met name relevant als het cruciale belangen betreft die op computers zijn vastgelegd.
Bij de toegang tot digitale informatie wordt nogal eens over het hoofd gezien dat ook fysieke toegang tot computerruimtes behoort tot het begrip toegang. Neem beide mogelijkheden in het gesprek mee.

17. Waar is de digitale informatie die betrekking heeft op de cruciale belangen fysiek (serverlokaties) opgeslagen (eventueel buitenland)? Dus, waar staan de servers? Als dit niet in Nederland is, waarom is er voor deze lokatie gekozen?

18. Stelt de organisatie speciale beveiligingseisen aan de data-opslagmiddelen (zoals servers)? Zo ja, welke?

19. Worden de digitale data(-opslagmiddelen/ servers) beheerd door een externe partij? Zo ja, wie en waar?

20. Welke afspraken zijn er met deze externe partij gemaakt over de beveiliging van en toegang tot de informatie?

21. Als er sprake is van dataverkeer, wordt dit dataverkeer dan versleuteld/geëncrypteerd?

22. Wie heeft (fysieke en logische) toegang tot het dataverkeer en de data-opslagmiddelen? Is bij de organisatie bekend wie toegang heeft?

Bijlage 3 Sjabloon schema

Schema			
	Belang		
	Dreiger		
	Exclusief voor inlichtingendiensten		**Beoordeling**
1	Telecominterceptie		
2	Doorbreken encryptie		
3	Manipuleren van soft- en hardware		
4	Onbedoelde straling van (ICT-) apparatuur opvangen/meelezen		
5	Bedrijven binnen de invloedsfeer dwingen tot meewerken aan spionage		
6	Tijdelijk (fake)bedrijf opzetten		
	Ook mogelijk voor concurrenten	**Kwetsbaarheden uit interviews, te koppelen aan werkwijze**	**Beoordeling**
7	Afluisteren van binnenuit		
8	Afluisteren van buitenaf		
9	Onderscheppen van niet of slecht versleuteld draadloos data- en spraakverkeer		
10	Hacking		
11	Social engineering		
12	Trojans/virussen		
13	Chantage personen		
14	Cultivering		
15	Omkoping personen		
16	Gelegenheidsdiefstal		
17	Gerichte diefstal		

Schema			
18	Gerichte diefstal met inbraak		
19	Insluiting		
20	Infiltratie		
		Kwetsbaarheden volgend uit interviews, niet te koppelen aan specifieke werkwijze	**Beoordeling**
21			
22			
23			
24			

Colofon
Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010 | 2500 EA Den Haag

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Veiligheid

Postbus 20701 | 2500 ES Den Haag

Grafische verzorging
Zijlstra Drukwerk B.V., Rijswijk

Fotografie
Hollandse Hoogte

1e druk, november 2010
2e druk, december 2010
3e druk, januari 2011