Nationale Richtlijn Protective Intelligence 2012 - 2017

Versie 1.00

Inhoudsopgave

1 Inleiding

Voor u ligt de eerste versie van de Nationale Richtlijn Protective Intelligence 2012-2017. De Vakgroep Inlichtingen & Criminele Trends van de Vereniging Beveiligingsmanagers Nederland heeft, in samenwerking met vertegenwoordigers van de ASIS Benelux Chapter en de European Security Intelligence Foundation, deze Nationale Richtlijn opgesteld. De directe aanleiding om deze richtlijn op te stellen is het feit dat er in de praktijk nog steeds veel onbeantwoorde vragen zijn over nut en noodzaak van het (beveiligings)instrument Protective Intelligence.

Uitgangspunt voor deze richtlijn is dat een security professional die (tijdig) effectieve preventieve en mitigerende beveiligingsmaatregelen wil treffen om de eigen organisatie te beschermen, moet beschikken over inlichtingen op het vlak van:

a. criminele, terroristische (en competitive) intelligence dreigingen en;
b. de door deze (dader)groepen gebruikte modus operandi.

Het proces Protective Intelligence voorziet in het op transparante en juridisch verantwoorde wijze verkrijgen van deze dreiginginformatie.

Aan de totstandkoming van deze Nationale Richtlijn Protective Intelligence hebben de onderstaande personen, medewerking verleend:

- Mr. Drs. W. Aerdst, ESIF European Security Intelligence Foundation
- C. van der Giessen CPP, ASIS Benelux Chapter
- H. de Kruijs, VBN Vereniging Beveiligingsmanagers Nederland
- F. van der Linden, VBN Vereniging Beveiligingsmanagers Nederland
- R. Pronk CPP, VBN Vereniging Beveiligingsmanagers Nederland
- J. van Twillert CPP, ASIS Benelux Chapter
- Dr. G. de Valk, ESIF European Security Intelligence Foundation

De doelstelling die de Vereniging Beveiligingsmanagers Nederland (VBN), de ASIS Benelux Chapter en de European Security Intelligence Foundation (ESIF) met het uitbrengen van deze Nationale Richtlijn wil bereiken is dat u als security professional met dit document een leidraad in handen heeft waarmee het effectief en transparant inzetten van het instrument Protective Intelligence binnen uw organisatie mogelijk wordt.

Berndt Rif MSc MBA CPP
Voorzitter Vakgroep Inlichtingen & Criminele Trends

2 Definitie

Het is belangrijk om in de procesbeschrijving Protective Intelligence een duidelijke omschrijving van het begrip op te nemen. Het moet duidelijk zijn waarvoor het proces Protective Intelligence wordt ingezet (reikwijdte) en waarvoor het proces Protective Intelligence niet wordt ingezet (uitsluitingen). In de volgende drie paragrafen worden voorbeelduitwerkingen gegeven.

VOORBEELDUITWERKING

2.1 Omschrijving

Onder Protective Intelligence wordt verstaan (organisatieperspectief):
Het verzamelen, evalueren en analyseren van gegevens over realistische (be)dreigingen, trends en ontwikkelingen die de belangen van bedrijven en organisaties onbevoegd kunnen aantasten of beïnvloeden. Dit verzamelen, evalueren en analyseren van voornamelijk in 'open bronnen' aanwezige gegevens dient op een transparante en controleerbare wijze te gebeuren. Het verzamelen, evalueren en analyseren van gegevens omvat ook (be)dreigingen die voortkomen uit 'onbewust menselijk handelen' en zogenaamde 'acts of God'.

Onder Protective Intelligence wordt verstaan (daderperspectief):
Het verzamelen, evalueren en analyseren van gegevens over de identiteit, capaciteit en intentie van individuen of organisaties die zich bezighouden met spionage, sabotage, terrorisme of andere (criminele) subversieve activiteiten. Dit verzamelen, evalueren en analyseren van voornamelijk in 'open bronnen' aanwezige gegevens dient op een transparante en controleerbare wijze te gebeuren. Het verzamelen, evalueren en analyseren van gegevens omvat ook (be)dreigingen die voortkomen uit 'onbewust menselijk handelen'.

2.2 Scope

Het proces Protective Intelligence wordt, als input voor het proces Risicoanalyse, ingezet om:

- *Tijdig informatie te verzamelen over de identiteit, herkomst, capaciteit, werkwijze, intentie en motivatie van individuen of organisaties die zich bezighouden met spionage, sabotage, terrorisme of andere (criminele) subversieve activiteiten.*
- *Tijdig informatie te verzamelen over de kwetsbaarheid van <NAAM ORGANISATIE> door middel van het zelf aanvallen van <NAAM ORGANISATIE> om de effectiviteit en de werking van bestaande beveiligingsmaatregelen te toetsen.*

2.3 Uitsluitingen

Het proces Protective Intelligence voorziet niet in:

- *Het benoemen van 'de kans' dat individuen of organisaties, die zich bezighouden met spionage, sabotage, terrorisme of andere (criminele) subversieve activiteiten, zich op een bepaald moment tegen <NAAM ORGANISATIE> richten;*
- *Het benoemen van 'de kans' dat zich bedreigingen manifesteren naar aanleiding van 'onbewust menselijk handelen' en zogenaamde 'acts of God'.*

3 Doelstelling

Het is belangrijk om in de procesbeschrijving Protective Intelligence een duidelijke omschrijving van de doelstelling van het proces op te nemen. Hieronder volgt een voorbeeld van een mogelijke doelstelling.

VOORBEELD UITWERKING

De doelstelling van het proces Protective Intelligence is het vaststellen of er individuen of organisaties zijn die de capaciteit en de intentie hebben om, met gebruikmaking van kennis over de kwetsbaarheid van <NAAM ORGANISATIE>, de belangen van <NAAM ORGANISATIE> te kunnen aantasten. Dit omvat ook het identificeren van (be)dreigingen die voortkomen uit 'onbewust menselijk handelen' en zogenaamde 'acts of God'

4 Beleidsbasis

Het is belangrijk om in de procesbeschrijving Protective Intelligence een duidelijke relatie te leggen met het door de organisatie vastgestelde beleid. Hieronder volgt een voorbeeld van een mogelijk op te nemen verwijzing.

VOORBEELD UITWERKING

Het proces Protective Intelligence vindt haar oorsprong in de ‘’Business Code of Ethics” of “Business Principles” en het Beleidsplan Beveiliging <NAAM ORGANISATIE>, te weten in hoofdstuk XXX:

Overeenkomstig het gestelde in het Beleidsplan Beveiliging <NAAM ORGANISATIE> zijn de dreigingen die voortkomen uit de vastgestelde risicoanalyse, vertaald in beveiligingsdoelstellingen en het daarbij behorende weerstandsniveau (zie document XXX).

Op welke wijze het proces Protective Intelligence een bijdrage dient te leveren aan het creëren van voldoende weerstand tegen de onderkende (be)dreigingen blijkt uit het door de directie vastgestelde tactische kader (zie hoofdstuk 5).

5 Tactisch kader

Het is belangrijk om in de procesbeschrijving Protective Intelligence uitgangspunten op te nemen waaraan de organisatie zich gecommitteerd heeft. Dit voorkomt vragen met betrekking tot verantwoordelijkheden en bevoegdheden. Ook is het belangrijk om vast te leggen welke kaders noodzakelijk zijn om het proces goed te kunnen uitvoeren en deze kaders nader uit te werken in specifieke documenten. In de volgende twee paragrafen worden voorbeelden gegeven.

VOORBEELD UITWERKING

5.1 Tactische uitgangspunten

- *Voor het proces Protective Intelligence wordt een intern en extern relatienetwerk opgezet en onderhouden;*
- *Voor iedere in het proces in te zetten bron wordt vooraf gedefinieerd wat de relevantie en het noodzakelijke beschermingsniveau van de bron is;*
- *Er vindt toetsing plaats op de mate van relevantie van iedere bron;*
- *Er vindt toetsing plaats op de mate van betrouwbaarheid van iedere bron;*
- *Bronnen worden uitsluitend geraadpleegd en niet aangezet tot of gevraagd om (aanvullende) inlichtingen te verzamelen;*
- *Bij het verzamelen van informatie in het kader van Protective Intelligence wordt alleen gekeken naar realistische (be)dreigingen';*
- *Bij de uitvoering van het proces Protective Intelligence wordt altijd voldaan aan de vigerende wet- en regelgeving.*

5.2 Uitwerking in documenten

De uitwerking van de bovengenoemde tactische beleidsuitgangspunten komt terug in de volgende documenten (niet limitatief):

- *Leidraad uitvoering Protective Intelligence*
- *Leidraad Red Teaming*

6 Procesbeschrijving

Het is belangrijk om in de procesbeschrijving Protective Intelligence duidelijk aan te geven uit welke deelprocessen het bestaat. Tevens zal duidelijk moeten zijn:
- welke input nodig is voor het uitvoeren van elke specifieke processtap;
- welke output het resultaat is van een processtap en
- wat het (rest)risico is als de processtap wordt overgeslagen.

Ook zal duidelijk moeten zijn:
- wat de doelstelling van een processtap is;
- welke relaties er bestaan met andere beveiligingsprocessen en
- wie er voor de uitvoering van welke (deel)activiteit verantwoordelijk is.

In de volgende zeven paragrafen worden voorbeelden gegeven van een mogelijke uitwerking. In de bijlage is een schematisch overzicht van de totale procesbeschrijving gevoegd.

VOORBEELD UITWERKING

6.1 Opdeling in deelprocessen

Het proces Protective Intelligence is opgedeeld in de navolgende deelprocessen:
1. *Tactische kaders bepalen*
2. *Data verzamelen*
3. *Data verwerken*
4. *Data analyseren*
5. *Informatie exploiteren*

Hieronder volgt een beschrijving van de deelprocessen.

6.2 Deelproces 1: Tactische kaders bepalen

6.2.1 Doel

Op hoofdlijnen bepalen op welke wijze het proces Protective Intelligence wordt vormgegeven en welke kaders daarvoor noodzakelijk zijn.

6.2.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.2.3 Input

- *Mission statement, Business Principles, Business Code of Conduct.*
- *Beveiligingsbeleid < naam organisatie>.*
- *Beveiligingsplan <naam organisatie>.*
- *Vastgestelde risicoanalyse <naam organisatie>.*

6.2.4 Stappenplan

Activiteit	Toelichting	Functionaris
Verzamelen informatie		*Medewerker (operationeel niveau)*
Uitwerken en aanpassen tactische uitgangspunten		*Medewerker (operationeel niveau)*
Beoordelen tactische uitgangspunten		*Proceseigenaar (tactisch niveau)*
Vaststellen tactische uitgangspunten		*Portefeuillehouder (strategisch niveau)*

6.2.5 Output

- *Geactualiseerde en vastgestelde tactische uitgangspunten*

6.2.6 Relaties

- *Proces Risicoanalyse*
- *Operationele Beveiligingsprocessen*

6.2.7 Restrisico's

- *Indien in het beveiligingsbeleid en in het beveiligingsplan geen of onvoldoende door de portefeuillehouder geaccordeerde waarborgen zijn opgenomen voor de inzet van het instrument Protective Intelligence, kan dit instrument niet effectief worden ingezet.*

6.3 Deelproces 2: Data verzamelen

6.3.1 Doel

Het verzamelen van data uit open en uit gesloten bronnen die relevant is voor de verwerking tot exploiteerbare informatie.

6.3.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.3.3 Input

- *Jaarplanning Protective Intelligence*

6.3.4 Stappenplan

Activiteit	Toelichting	Functionaris
Raadplegen van open bronnen	*Waarnemen trends en ontwikkelingen*	*Medewerker (operationeel niveau)*
Raadplegen van gesloten bronnen	*Informatie-uitwisseling op basis van een convenant (formeel vastgesteld door een portefeuillehouder op strategisch niveau)*	*Medewerker (operationeel niveau)*
Uitvoeren van (contra)observatie	*Gericht observeren of voorspelbare en voorstelbare dreigingen in de omgeving kunnen worden waargenomen*	*Medewerker (operationeel niveau)*
Inzet van een ´red team´	*Ontdekken nieuwe MO´s en verdachte kenmerken*	*Medewerker (operationeel niveau)*

6.3.5 Output

- *Data over (nieuwe) MO's*
- *Data over (nieuwe) verdachte indicatoren*

6.3.6 Relaties

- *Proces Risicoanalyse*

6.3.7 Restrisico's

- *Het onvoldoende voorbereid en/of niet structureel inzetten van een red team heeft tot gevolg dat de kwetsbaarheid van de eigen organisatie en de effectiviteit van getroffen beveiligingsmaatregelen niet of onvoldoende inzichtelijk is.*

6.4 Deelproces 3: Data verwerken

6.4.1 Doel

Het verwerken en reduceren van de data tot een voor analyse bruikbare inhoud.

6.4.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.4.3 Input

- *Data (deel)stap verzamelen*

6.4.4 Stappenplan

Activiteit	*Toelichting*	*Functionaris*
Data rangschikken		*Medewerker (operationeel niveau)*
Data prioriteren		*Medewerker (operationeel niveau)*

6.4.5 Output

- *Voor analyse bruikbare data*
- *Koppeling van verdachte kenmerken aan MO*

6.4.6 Relaties

- *Proces Risicoanalyse*

6.4.7 Restrisico's

- *Het niet vrijmaken van capaciteit om data te rangschikken en te prioriteren gaat ten koste van de effectiviteit van het gehele proces Protective Intelligence*

6.5 Deelproces 4: Data analyseren

6.5.1 Doel

Het omzetten van data naar bruikbare en gevalideerde informatie.

6.5.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.5.3 Input

- *Data (deel)stap verwerken*

6.5.4 Stappenplan

Activiteit	Toelichting	Functionaris
Collatie data	Regelgeving bescherming persoonsgegevens is van toepassing	Medewerker (operationeel niveau)
Evaluatie data	Er dient een protocol beschikbaar te zijn.	Medewerker (operationeel niveau)
Analyse data	Uitvoeren binnen kaders van vigerende wet- en regelgeving c.f. tactische uitgangspunten (par 5.1)	Medewerker (operationeel niveau)
Integratie data	Er dient een protocol beschikbaar te zijn.	Medewerker (operationeel niveau)
Interpretatie data	Er dient een protocol beschikbaar te zijn.	Medewerker (operationeel niveau)
Opstellen rapportage over data		Medewerker (operationeel niveau)

6.5.5 Output

- Rapportage over onderkende
  - scenario's
  - MO's
  - verdachte indicatoren
  - dreigingen

6.5.6 Relaties

- Proces Risicoanalyse
- Tactische uitgangspunten

6.5.7 Restrisico's

- Het niet vrijmaken van capaciteit om data te analyseren gaat ten koste van de effectiviteit van het gehele proces Protective Intelligence

6.6 Deelproces 5: Informatie exploiteren

6.6.1 Doel

Het ter beschikking stellen van informatie aan de afnemers van het proces Protective Intelligence zodat tijdige juiste preventieve en mitigerende (beveiligings)maatregelen genomen kunnen worden.

6.6.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.6.3 Input

- *Data (deel)stap analyseren*

6.6.4 Stappenplan

Activiteit	***Toelichting***	***Functionaris***
Opstellen voorstel aanpassen en/of uitbreiden: *- scenario´s risicoanalyse* *- MO´s* *- verdachte kenmerken* *- interne en externe bronnen*	*Scenario's en MO's dienen realistisch te zijn*	*Medewerker (operationeel niveau)*

6.6.5 Output

- *Dreigingsanalyse*
- *Voorstel voor aanpassing*
    - *scenario's risicoanalyse*
    - *MO's*
    - *Verdachte indicatoren*

6.6.6 Relaties

- *Proces Risicoanalyse*
- *Proces Toezicht (Predictive Profiling)*

6.6.7 Restrisico's

- *Het niet vrijmaken van capaciteit om informatie structureel te exploiteren gaat ten koste van de effectiviteit van het gehele proces Protective Intelligence*

7 Operationele randvoorwaarden

Het is van belang in de procesbeschrijving Protective Intelligence vast te leggen over welke competenties de verschillende functionarissen moeten beschikken teneinde de proceswerkzaamheden effectief en efficiënt te kunnen uitvoeren. Daarbij dient tevens duidelijk te zijn welke systemen en instrumenten hen ter beschikking staan en welke procedures en werkinstructies dienen te worden gevolgd.

7.1 Competenties

Bij het bepalen van de benodigde competenties is het van belang rekening te houden met complexe besluitvormingsprocessen, waarbij zowel juridische consequenties als (potentiële) gevolgen op beveiligingsvlak moeten worden overzien. Daarnaast is een zeer flexibele instelling noodzakelijk, alsmede een realistische kijk op en gevoel voor organisatorische- en omgevingsfactoren en/of veranderingen.

7.2 Systemen

De uitgangspunten bij het identificeren van noodzakelijke ondersteunende systemen zijn:

- De Protective Intelligence professional moet op een systematische wijze historie, trends en ontwikkelingen kunnen vastleggen.
- De professional moet de beschikbare gegevens op een transparante en controleerbare wijze kunnen analyseren.

7.3 Documenten

Voor een efficiënte en deugdelijke operationele werking van het proces Protective Intelligence zijn vastgestelde protocollen en werkinstructies noodzakelijk. Alleen dan kan aan de eis van transparantie en herleidbaarheid worden voldaan. Iedere organisatie zal zelf moeten bepalen, uitgaande van het eigen kwaliteitmanagementsysteem, wat de minimaal benodigde protocollen en werkinstructies zijn

8 Kwaliteitsborging

Het is belangrijk om in de procesbeschrijving Protective Intelligence een paragraaf op te nemen waarin normen en indicatoren staan beschreven. Dit om achteraf te kunnen vaststellen of het proces goed is uitgevoerd. Teneinde misverstanden te voorkomen, zal tevens beschreven moeten worden op welke wijze meting zal plaatsvinden.

8.1 Norm

Er kan pas worden vastgesteld of voor het proces Protective Intelligence sprake is van een voldoende niveau indien normen smart geformuleerd zijn. Tevens dient er, bij de inrichting van het proces, sprake te zijn van een gesloten kwaliteitscirkel.

8.2 Indicator

In het benoemen van indicatoren is het belangrijk om te bepalen wat het verschil is tussen de geïdentificeerde BRUTO-dreiging (output proces Protective Intelligence en input proces Risicoanalyse) en de vastgestelde NETTO-dreiging (output proces Risicoanalyse en input tactische beveiligingsprocessen).

8.3 Meting

Meting is alleen mogelijk als voldaan is aan de eis van smart geformuleerde processen en daarvan afgeleide normen.

9 Begrippenlijst in het kader van deze Richtlijn

Acts of God	Een plotselinge, gewelddadige, zonder menselijke tussenkomst optredende, natuurlijke oorzaak, waarvan de gevolgen niet door in de gegeven omstandigheden redelijkerwijs te betrachten zorg kunnen worden voorkomen.
Belangen	De 'kroonjuwelen' van de organisatie die bescherming behoeven en beveiliging noodzakelijk maken.
Bruto dreiging	Output proces Protective Intelligence en input proces Risicoanalyse. Kenmerk van deze dreiging is dat hij '1' of '0' is. Er heeft geen weging plaatsgevonden
Dreiginganalyse	Een dreiginganalyse is een beschrijving van een voorspelbare of voorspelbare aanvallers methode van operatie (AMO) gericht tegen één of meerdere personen, objecten of organisaties. Een dreiging is altijd '0' of '1'.
Modus operandi	Modus operandi, ook wel aanvallers methode van operatie (AMO) genoemd, is de manier van werken van een individu, van een groep personen, criminele- of terroristische organisatie.
Netto dreiging	Output proces Risicoanalyse en input tactische beveiligingsprocessen. Aan de hand van een weging heeft risicoacceptatie plaatsgevonden.
Onbevoegd	Zonder recht of toestemming dan wel onwettige handeling verrichten
Protective Intelligence	Het op een transparante en controleerbare wijze verzamelen, evalueren en analyseren van voornamelijk in 'open bronnen' aanwezige informatie over (be)dreigingen, trends en ontwikkelingen die de belangen van bedrijven en organisaties onbevoegd kunnen aantasten of beïnvloeden. De (be)dreigingen die voortkomen uit 'onbewust menselijk handelen' en zogenaamde 'acts of God' behoren niet tot de scope van security intelligence.
Realistische (be)dreigingen	Dreigingen zijn voorstelbaar en/of voorspelbaar. Dit betekent dat een dreiging zich eerder heeft vertoond of dat, op basis van red teaming, is gebleken dat een nieuwe dreiging gezien de kennis en capaciteiten van tegenstanders uitvoerbaar is.
Red teaming	Het vanuit een onafhankelijke positie (laten) doen van aanvallen op de eigen organisatie om te bepalen of een aanvallers methode van operatie (AMO) uitvoerbaar en realistisch is, en om te bepalen of getroffen beveiligingsmaatregelen op basis van een eerder getest AMO effectief zijn.
Risicoanalyse	Op basis van de afweging belang-dreiging-weerstand bepalen wat de kans is dat zich een bepaalde dreiging zal gaan manifesteren.
Sabotage	Het opzettelijk verrichten van handelingen die zijn gericht op het verhinderen van normaal functioneren van een dienst, onderneming of proces dan wel het veroorzaken van schade aan de doelorganisatie of aanwakkeren van onveiligheidsgevoelens
Scenario's	Een scenario is een aannemelijke theoretische beschrijving van de manier waarop toekomstige gebeurtenissen kunnen plaatsvinden op basis van data uit het verleden en veronderstellingen in het heden

Smart	Specifiek, meetbaar, acceptabel, realistisch, tijdgebonden
Spionage	Het op heimelijke wijze verzamelen van (veelal) vertrouwelijke gegevens of informatie
Subversieve activiteit	Activiteit die erop is gericht gezag te ondermijnen en/of de bedrijfsvoering van een organisatie dan wel de samenleving te ontwrichten.
Terrorisme	Terrorisme is het uit ideologische motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappijontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden.
Verdachte kenmerken	Kenmerken in relatie tot de begrippen: bedenkelijk, dubieus, louche, obscuur, onbetrouwbaar, onwaar, twijfelachtig, ongeloofwaardig, duister.