EEN FYSIEKE UPS STANDAARD

Een onderzoek om tot een security standaard voor UPS centra in Nederland te komen.

Tristan Venderink
Security management student

Naam: Tristan Alexander Venderink
Studentnummer: 335554
Telefoonnummer: 06 – 54 30 73 44
Mail: T.A.Venderink@gmail.com
Titel: Een Fysieke UPS standaard.
Opdrachtgever: United Parcel Service
Opleiding: Security Management
Onderwijsinstelling: Saxion Hogescholen
1e Lezer: Drs. M.M.J. Paschedag
2e Lezer: Mr. B.J. den Tuinder
Praktijkbegeleider: Dhr. H. Houter
Datum: 23-04-2018

Voorwoord

Voor u ligt de scriptie ‘een fysieke UPS security standaard’, geschreven voor UPS Nederland, in opdracht van de security afdeling. Tijdens een periode die liep van 2018 tot 2019 ben ik bezig geweest met het vraagstuk om tot een minimale security standaard te komen voor UPS package centra in Nederland.

Omdat ik voor mijn afstudeeropdracht al werkzaam was binnen UPS, is mij inmiddels opgevallen dat sommige procedures volgens mij anders en/of beter kunnen. Daarom was de keuze snel gemaakt en had ik zin om het bedrijf verder proberen te helpen. Het is een mooie ervaring geweest UPS beter te leren kennen door met verschillende mensen te spreken, locaties te bezoeken en meegenomen te worden door dhr. Houter naar projecten.

De vordering van het onderzoek heeft op bepaalde momenten gehaperd, dit lag vooral aan een gezondheidsprobleem waardoor ik uiteindelijk geopereerd moest worden. Ook waren er momenten dat de communicatie met dhr. Houter minder goed verliep, dit kwam vooral door zijn hoge werkdruk. Ik heb hem dit dan ook geen moment kwalijk genomen.

Ik wil graag iedereen die heeft bijgedragen aan dit onderzoek hartelijk bedanken voor de medewerking en fijne manier waarop ik altijd werd ontvangen. Geen enkel moment had ik het gevoel dat ik weerstand ondervond.

In het bijzonder wil ik Hans en Marcel bedanken die ik voor één keer in dit verslag bij hun voornamen zal noemen. Zij hebben mij allebei ongelofelijk gesteund, begrip gehad, tijd vrijgemaakt, geholpen met vragen en goede tips gegeven.

Ik wens u veel leesplezier.

Tristan Venderink

Management samenvatting

UPS Nederland is de laatste jaren bezig geweest met een aantal bouw- en verbouw projecten. De belangrijkste hiervan zijn de nieuwbouw locaties Utrecht en Eindhoven. Tijdens deze projecten bestond er nog geen fysieke security standaard voor UPS package centra.

Het doel van dit onderzoek is om tot een minimale fysieke security standaard te komen voor UPS centra in Nederland. Hiermee zal UPS tijdens de ontwerp en bouwfase al een beeld krijgen van welke maatregelen er getroffen moeten worden, waar vervolgens rekening mee gehouden kan worden. Dit onderzoek is gedaan aan de hand van de volgende probleemstelling:

"Welke fysieke security maatregelen kunnen worden gestandaardiseerd om tot een nieuwe minimale securitystandaardisatie voor UPS package centra in Nederland te komen om zo de beveiliging te kunnen waarborgen?"

Om tot een antwoord op deze probleemstelling te komen zijn er meerdere onderzoeksvragen opgesteld:

- Zijn er op dit moment standaard maatregelen op het gebied van fysieke beveiliging binnen UPS Nederland en wat houden deze maatregelen in?
- Wat zijn de belangrijkste security incidenten bij huidige UPS centra in Nederland?
- Wat zijn de beveiligingsrisico's voor huidige en toekomstige UPS package centra?
- Welke maatregelen moeten uit deze risico's en incidenten voortkomen om deze te mitigeren?

Bij de eerste deelvraag is gekeken naar welke huidige maatregelen er zijn en welke beleid er op dit moment aanwezig is binnen UPS. De huidige maatregelen bij de centra is in kaart gebracht en er is geconcludeerd dat er op dit moment geen Nederlands beleid is op het gebied van fysieke beveiliging. Er is wel het corporate beleid dat als richtlijn word gezien.

Vervolgens is bij de tweede deelvraag gekeken welke security incidenten zich voordoen binnen UPS. Deze incidenten zijn risico's voor de organisatie en zijn dus meegenomen in het onderzoek. Voor additionele informatie is er gesproken met personen binnen UPS die over het oppakken en afhandelen van deze incidenten gaan. Te zien was dat er vooral sprake is van diefstal. Grote incidenten komen zelden voor.

Vervolgens is bij deelvraag 3 gekeken naar de verschillende risico analyses die UPS intern heeft uitgevoerd. Ook is er een algemene risicoanalyse uitgevoerd die betrekking heeft op alle centra in Nederland. Hieruit kwamen meer dreigingen voor UPS naar voren die gemitigeerd moeten worden. Ook is er met professionals binnen UPS gesproken over de verschillende processen en beveiligingsdoelen binnen UPS. Een opvallende uitkomst is het feit dat er weinig kritieke assets binnen een UPS center zijn.

Tot slot is er tijdens deelvraag 4 gekeken welke maatregelen hieruit naar voren zouden moeten komen. Hierbij is ook gekeken naar een verdeling van een package center in zones. Dit is gedaan om een beter overzicht te krijgen van welke maatregelen waar toegepast moeten worden.

Na het beantwoorden van de losse deelvragen zijn de conclusie en aanbevelingen geschreven. Aan de hand van de conclusies zijn maatregelen opgesteld en is er een matrix gecreëerd die de verschillende zones binnen een center weergeeft. Vervolgens zijn er per zone een minimaal, aanbevolen en een uitmuntend security niveau weergegeven.

Inhoudsopgave

Lijst met definities en afkortingen

Maatregelen
Een maatregel is de manier waarop iets opgelost of veranderd wordt. Hierbij kan onderscheid worden gemaakt tussen organisatorische, bouwkundige en elektronische maatregelen.

Fysiek beveiliging
Fysieke beveiliging is het onderdeel van security dat bestaat uit fysieke maatregelen die ervoor moeten zorgen dat assets veilig blijven.

Standaardisatie
Standaardisatie is een bewuste poging door een organisatie om een bepaalde standaard te ontwikkelen, ratificeren en te implementeren onder haar stakeholders.

Risico
Risico is de kans op schade die kan optreden als gevolg van externe dan wel interne omstandigheden.

Impact
Impact kan worden gezien als het effect wat een bepaald risico heeft op een proces. Dit kan worden uitgedrukt in financiële, materiële en immateriële schade.

CCTV
Closed-circuit television (CCTV) is een benaming voor een beeldverbinding over een gesloten circuit of netwerk of anders gezegd, televisie over een gesloten verbinding. Daarmee wordt bedoeld dat de televisiebeelden (of camerabeelden) niet vrijelijk of publiekelijk uitgezonden worden of te ontvangen zijn; er is in principe sprake van een absolute controle of afgrenzing van de ontvangstpunten of toeschouwers.

IDS
Een inbraak detectie systeem geeft bij een situatie van inbraak of poging tot inbraak direct een alarm en een melding door aan de alarmcentrale. Hierdoor kunnen mogelijke inbraken worden gedetecteerd.

Holdcage
In holdcage worden pakketten verwerkt en waar nodig bewerkt. Dit kan inhouden dat er nieuwe labels worden gemaakt, pakketten vast worden gehouden voor latere bezorging. Tot slot worden hier risico goederen of goederen van hoge waarde vast gehouden.

Smalls-sortering
Hier worden kleine pakketten gesorteerd en in zakken verpakt die vervolgens doorgestuurd kunnen worden.

Access control
Met toegangscontrole wordt het proces van wel of niet toegang verlenen tot een terrein of faciliteit bedoeld.

DWS
De dimensional weight scanner meet het volume van pakketten waardoor er wordt gezorgd dat klanten het juiste bedrag betalen voor het versturen van hun pakket.

1. Aanleiding, doelstelling, probleemstelling en betrokkenen

In dit hoofdstuk wordt ingegaan op de aanleiding, doelstelling, probleemstelling en betrokkenen voor het onderzoek naar de minimale fysieke security vereisten voor nieuwe UPS centra in Nederland. Het operationaliseren van de probleemstelling naar onderzoeksvragen komt in het derde hoofdstuk aan bod.

1.1. United Parcel Service

United Parcel Service oftewel UPS is een wereldwijd begrip op het gebied van logistiek. De logistieke multinational UPS is een van origine Amerikaans bedrijf dat zich bezighoudt met logistieke processen op mondiale schaal. Het kernproces van het bedrijf is het wereldwijd bezorgen van verstuurde pakketten van en aan haar klanten. Dit doet het bedrijf met grote efficiëntie waardoor UPS de werelds grootste pakketbezorger is geworden met een marktaandeel van 57%. In 2017 leverde UPS 5 miljard pakketten af, wat ongeveer 17 miljoen per dag is. Dit zorgde voor een totale omzet van 65,9 miljard dollar en een winst van 4,9 miljard dollar.

Om deze logistieke klus succesvol te kunnen uitvoeren heeft UPS 454.000 mensen in dienst, waarvan er op 01-01-2018 1365 in Nederland werkzaam zijn. Voor het grondtransport heeft UPS 120.000 voertuigen, en voor het luchttransport heeft UPS zijn eigen luchtvaartmaatschappij die over ruim 500 vliegtuigen beschikt.

Het doel van het bedrijf is helder: “het mogelijk maken van wereldwijde handel”, dit doet UPS door haar assets aan klanten aan te bieden. Een paar kernwaarden die hierbij zijn vastgesteld zijn: service, teamwork, duurzaamheid en innovatie. Vooral duurzaamheid en innovatie zijn momenteel een hot item door de verschillende klimaatakkoorden en met name het akkoord van Parijs. Omdat hierdoor de mondiale uitstoot van CO2 terug moet worden gebracht. Maar misschien de meest relevante kernwaarde voor dit onderzoek is veiligheid, het welzijn van onze mensen, zakenpartners en het publiek is van het grootste belang (UPS).

1.2. Aanleiding

UPS groeit ieder jaar en dat vraagt logischerwijs ook om uitbreiding van de logistieke infrastructuur. In Nederland zijn een aantal distributiecentra de laatste jaren verbouwd en uitgebreid, zoals de locatie Eindhoven. Ook is er onlangs een nieuw package center in Utrecht operationeel gegaan, en staan er nog meer bouwprojecten op de agenda. Uitbreiden is goed voor het bedrijf, echter is het gevaar hierbij dat security hierin niet meegaat en dus achterblijft. Op dit moment is er nog geen standaardisatie van fysieke security maatregelen waaraan centra in Nederland moeten voldoen. Dit is dan ook de aanleiding voor dit onderzoek.

De security afdeling UPS Nederland wil om deze reden een onderzoek laten uitvoeren naar een mogelijke standaardisatie van fysieke security maatregelen voor haar locaties in Nederland. Dit zijn er op dit moment zeven, namelijk: Rotterdam, Apeldoorn, Amsterdam, Tilburg, Heereveen, Utrecht en Eindhoven. Om hiertoe te komen moet UPS een beter beeld krijgen van mogelijke risico’s voor (nieuwe) centra en naar aanleiding van deze risico’s tot een standaard pakket van maatregelen komen.

1.3. Praktijkprobleem

Het praktijkprobleem is het probleem dat de aanleiding is vanuit de opdrachtgever om het onderzoek te starten. Het praktijkprobleem is: *'de security afdeling van UPS Nederland heeft op dit moment geen vastomlijnde standaard voor de fysieke beveiliging van haar package centra'.*

1.4. Doelstelling

De doelstelling van dit onderzoek is om te komen tot een advies voor een standaardisatie van fysieke security maatregelen voor UPS package centers in Nederland. Hierbij moet er wel ruimte blijven voor lokale behoefte van individuele centra. Met deze minimum standaard kan UPS haar security verbeteren op haar nieuwe en oude locaties, of tot de conclusie komen dat de huidige maatregelen toereikend zijn en verder geen verbetering vereisen.

Dit onderzoek zal dus leiden tot een aantal bruikbare minimale fysieke security maatregelen voor UPS centra om zo de veiligheid van deze centra te waarborgen.

Het onderzoek zal tenminste het volgende leveren:

- Een risicoanalyse voor de risico's die UPS package centra lopen.
- Een conclusie naar aanleiding van het literatuur onderzoek en de interviews met personen binnen UPS over hun ervaring met betrekking tot security en hun mening hierover.
- Aanbevelingen voor een standaardisatie van fysieke maatregelen voor UPS centra in Nederland.

1.5. Probleemstelling

Om de in de vorige paragraaf gestelde doelstelling te behalen zijn een aantal stappen vereist, om deze stappen inzichtelijk te maken is er een probleemstelling opgesteld. Dit is gedaan aan de hand van de doelstelling en de aanleiding van dit onderzoek. Hierdoor is tot de volgende probleemstelling gekomen:

"Welke fysieke security maatregelen kunnen worden gestandaardiseerd om tot een nieuwe minimale securitystandaardisatie voor UPS package centra in Nederland te komen om zo de beveiliging te kunnen waarborgen?"

Toelichting op de probleemstelling en een operationalisering in onderzoeksvragen volgt nog.

1.6. Onderzoeksvragen

Om de probleemstelling te kunnen beantwoorden zijn er een aantal onderzoeken nodig. Deze onderzoeken worden vanuit de volgende onderzoeksvragen uitgevoerd:

- Zijn er op dit moment standaard maatregelen op het gebied van fysieke beveiliging binnen UPS Nederland en wat houden deze maatregelen in?
    - Het in kaart brengen van de aanwezige maatregelen die UPS heeft op tactisch niveau
    - Het in kaart brengen van het huidige security beleid

- Wat zijn de belangrijkste security incidenten bij huidige UPS centra in Nederland?
    - Het in kaart brengen van relevante security incidenten die bij UPS in de afgelopen jaren bij package centra zijn voorgevallen

- Wat zijn de beveiligingsrisico's voor huidige en toekomstige UPS package centra?
    - Concretiseren van beveiligingsdoelen

- Literatuur bestuderen om de risico's en de gevolgen hiervan vast te stellen

- Welke maatregelen moeten uit deze risico's en incidenten voortkomen om deze te mitigeren?
  - Ontwikkelen vlinderdasmodel voor UPS
  - Opstellen te nemen maatregelen
  - Opstellen van de minimale fysieke security standaard

1.7. Scope

In dit onderzoek wordt er gekeken naar de fysieke aspecten van beveiliging van de UPS package centra, dit houdt in dat ICT security en de beveiliging van andere assets die buiten het centra vallen niet in dit onderzoek zijn meegenomen.

Tijdens dit onderzoek zal primair worden gekeken naar de risico's voor UPS centra in Nederland, de security incidenten die zich voordoen en welke huidige maatregelen er al zijn.

1.8. Hypothese

De verwachting van het onderzoek is dat er binnen UPS veel is nagedacht over de security van de processen, locaties en fysieke beveiliging hiervan. Ook is de kans aannemelijk dat de huidige security voorschriften en het huidige beleid vooral op locaties buiten Nederland zijn gericht zoals bijvoorbeeld de Verenigde Staten. Hierdoor is er op dit moment nog geen standaard die zich focust op de Nederlandse locaties, er zal door middel van dit onderzoek een standaardisatie gericht op de Nederlandse UPS tak ontstaan waarmee toekomstige en huidige UPS Nederland locaties een hoger niveau van fysieke beveiliging zullen bereiken. De verwachting voor deze minimale standaard is dat deze vrij basic zal zijn. Ook ligt het in de lijn van de verwachting dat er dat er een gat zal zijn tussen een minimaal en gewenst security niveau. Deze verwachtingen zijn gebaseerd op mijn persoonlijke ervaringen binnen UPS en het gegeven dat object beveiliging vrij basic kan zijn door bijvoorbeeld een hekwerk en toegangscontrole.

1.9. Betrokkenen

Logischerwijs zijn er bij een afstudeerscriptie meerdere partijen betrokken die belang hebben bij het eindresultaat van het onderzoek. De relevantie en de waarde van het onderzoek kan inzichtelijk gemaakt worden wanneer de belanghebbenden in kaart zijn gebracht. (Krabbe, 2014) In deze paraaf zullen de betrokkenen en belanghebbenden bij het vraagstuk worden geïdentificeerd en hun belangen beschreven (ABR&R Saxion, 2017).

1.9.1. De onderzoeker

De scriptie wordt geschreven door de student, in dit geval een student van Saxion Security Management in Apeldoorn met als doel om af te studeren. Om af te studeren zal er een onderzoek uitgevoerd worden dat met een positieve eindbeoordeling wordt afgerond. Het belang van de student is dan ook afstuderen en het afronden van de opleiding.

1.9.2. Opdrachtgever

In dit geval is de opdrachtgever de security afdeling van UPS Nederland. Het belang van UPS in dit onderzoek is het inzichtelijker maken van risico's en het komen tot een standaardisatie van maatregelen. Hierna kan UPS, als dat nodig is, haar security op het gebied van package centra in Nederland verbeteren.

1.9.3. Afdeling Loss Prevention

De afdeling Loss Prevention onderzoekt en handelt de verschillende security incidenten af en registreert deze. De afdeling zal dan ook benaderd worden in het kader van het onderzoek.

1.9.4. Afdeling Plant Engineering

Deze afdeling houdt zich bezig met inrichting en onderhoud van UPS panden. Security maatregelen kunnen worden geschaard onder inrichting, ook moeten deze maatregelen worden onderhouden.

1.9.5. Afdeling Building and Facilities

Deze afdeling gaat over de aanschaf/keuze van vastgoed. Het zou kunnen dat aan de hand van dit rapport er anders gekeken zal gaan worden naar de locaties van panden omdat er rekening gehouden moet worden met bepaalde fysieke maatregelen op het gebied van beveiliging.

1.9.6. Praktijkcoach

De praktijkcoach tijdens dit onderzoek is dhr. H. Houter van de security afdeling van UPS Nederland. Hij zal de kwaliteit en bruikbaarheid van de gemaakte stukken beoordelen. Het belang voor dhr. Houter is het verwerven van een mimimale standaardisatie omtrent de fysieke beveiliging van UPS centra in Nederland.

1.9.7. Schoolcoach

De schoolcoach is Drs M.J. Paschedag, verder is hij eerste lezer en beoordelaar. De schoolcoach helpt de student waar het gaat om procesmatige problematiek en indien mogelijk ook bij inhoudelijke problemen. Voor de begeleiding worden contact momenten gepland en zijn uren beschikbaar. Het belang van de schoolcoach ligt bij het begeleiden van student naar een voldoende eindresultaat in de beoordeling.

1.9.8. Tweede lezer

Dhr. B. den Tuinder vervult de rol van tweede lezer. De belangrijkste functie van de tweede lezer is dat hij/zij een onafhankelijker positie inneemt ten opzichte van de beoordeling. Omdat hij/zij geen contact heeft met de onderzoeker, is de kans dat de beoordeling van de scriptie en eventuele beroepsproducten zuiver kan plaatsvinden en niet kan worden vertroebeld door een oordeel over het werkproces (ABR&R Saxion, 2017).

1.10. Managementrelevantie

Het hoofddoel van dit onderzoek is het bereiken van een minimale standaard van fysieke beveiliging van UPS package centra in Nederland. Hiervoor zullen risico's, beveiligingsdoelen, schadeposten van incidenten en kwetsbaarheden worden bestudeerd. Het belang van deze doelstelling is het waarborgen van de veiligheid van mensen en goederen en het voorkomen van verstoring van bedrijfsprocessen. Wanneer er geen minimale security vereisten zijn voor UPS package centra in Nederland kunnen er in theorie kwetsbaarheden ontstaan in de beveiliging van UPS centra.

1.11. Maatschappelijke relevantie

"Vrachtwagen met duizend postpakketten gestolen" (AD, 2018). Een Nederlandse man zag kans om een trailer met duizenden pakketten van een logistiek bezorgingsbedrijf te ontvreemden. Gelukkig kon de trailer met inhoud door de politie worden terug gevonden. Deze gebeurtenis moet als een waarschuwing dienen voor andere logistieke bedrijven waaronder ook UPS. Dit onderzoek kan bijdragen aan het voorkomen van een dergelijk incident binnen UPS.

UPS heeft miljoenen klanten wereldwijd en duizenden in Nederland. Deze klanten versturen vele goederen via UPS waaronder ook veel goederen van grote waarde. De veiligheid van deze goederen is

dan ook van groot belang voor deze klanten en deze mogen dan ook verwachten dat hun goederen veilig zijn binnen UPS. Kwetsbaarheden binnen UPS kunnen effect hebben op de veiligheid van de goederen en dus ook op het service level dat UPS haar klanten wenst te bieden. Deze opdracht heeft als doel om de kwetsbaarheden zoveel mogelijk uit te sluiten, dankzij een optimale afstemming in fysieke maatregelen, zodat de klant met een gerust hart via UPS kan versturen en ontvangen.

1.12. Leeswijzer

Hoofdstuk twee geeft het theoretisch kader weer, hier wordt dieper ingegaan op de onderzoeksvragen door gebruik te maken van (wetenschappelijke) theorie en waarnemingen in de praktijk. In hoofdstuk drie worden de gemaakte keuzes en de methodiek van onderzoek onderbouwd. De verschillende onderzoeksvragen zijn behandeld door middel van het bespreken van de methodiek, operationalisatie, betrouwbaarheid en validiteit.

Hoofdstuk vier behandelt de resultaten van het onderzoek. Per onderzoeksvraag zijn de methodes uit hoofdstuk drie uitgewerkt. Vervolgens geeft hoofdstuk vijf antwoord op de onderzoeksvragen en de probleemstelling door conclusies te trekken uit de resultaten van hoofdstuk vier. Vervolgens vormt hoofdstuk zes aanbevelingen uit de getrokken conclusies. Hier zijn concrete aanbevelingen te vinden die voortkomen uit de resultaten van het onderzoek.

Tot slot vormen de laatste drie hoofdstukken de afsluiting van het onderzoek. Hoofdstuk zeven gaat over de methodologische verantwoording en bevat een evaluatie. De laatste twee hoofdstukken bevatten de bronnen en een biografielijst.

2. Theoretisch kader

Om meer duidelijkheid te verschaffen worden in dit hoofdstuk het kennisgebied, de thema's en andere relevante zaken toegelicht. Deze theorieën zijn allemaal onderbouwd met bronnen uit literatuurstukken die relevant zijn voor dit onderzoek.

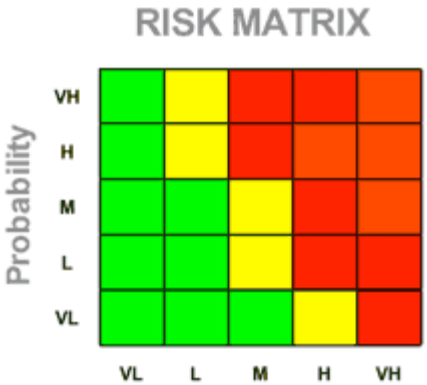
Binnen UPS is er op het gebied van risico's en dreigingen al data aanwezig die ondersteunend kan zijn bij het uitvoeren van het onderzoek. Daarom is het van belang om onderwerpen die hier op aansluiten te bestuderen en verder toe te lichten, dit zal in de onderstaande paragrafen gebeuren.

Twee belangrijke termen binnen dit onderzoek zijn security en risico's. Security is simpel gezegd het verdedigen van een asset tegen gevaar of verlies. Meerdere dingen worden getypeerd als assets, in essentie is een asset iets waar een bedrijf of een persoon over beschikt en dat bijdraagt tot het genereren van omzet. Dit kunnen mensen, machines, informatie etc. zijn, een asset hoeft niet perse tastbaar te zijn (Talbot & Jakeman, 2009). Assets kunnen worden onderverdeeld in vier groepen, namelijk: Mensen, bezit, informatie en imago (IFPO, 2010). Security wordt doorgaans behaald door het vermijden en voorkomen van moedwillige acties en aanvallen van anderen tegen een asset of meerdere assets door het nemen van preventieve maatregelen. Het doel hiervan is schade voorkomen en de operationele continuïteit van bedrijfsprocessen te garanderen. Cazemier (2010) onderscheidt twee soorten continuïteit, namelijk operationele continuïteit en crisiscontinuïteit. Operationele continuïteit is de normale gang van zaken, het is dan ook van groot belang dat dit niet wordt verstoord en dit dus te waarborgen.

De term risico is een veelgebruikte term, een goede en doeltreffende definitie luidt als volgt: "Risico is de kans op schade die kan optreden als gevolg van externe dan wel interne omstandigheden" (Verbart, 2013). Dit komt overeen met wat in het boek SRMBOK als risico wordt getypeerd, namelijk: een security risico is enig voorval dat kan leiden tot schade of verstoring van de assets van een organisatie. Tot slot stelt Appelman (2010) dat in het vakgebied een risico als volgt gedefinieerd kan worden: "de waarschijnlijkheid van de gebeurtenis van een ongewenst incident". Een risico komt van buiten de organisatie of intern vanuit de organisatie zelf. In het geval van UPS zullen de risico's en dreiging zowel intern als extern zijn.

Risico's kunnen dus ingedeeld worden in twee categorieën, namelijk intern of extern. Verbart en Goedhart (2013) stellen: Externe risico's zijn niet of nauwelijks rechtstreeks te beïnvloeden. Het komt er dus op aan ze tijdig te herkennen en adequaat te reageren, of ze uit de weg te gaan.

Risico's zijn te meten, de methode die hiervoor wordt gebruikt staat bekend onder meerdere benamingen, zo is de methode in Nederland onder andere bekend via de term Jaarsma-schaal. In de NAVI handreiking wordt de methode de Waarschijnlijkheid-impact-matrix (NAVI, 2008) genoemd en nog een andere bron noemt de matrix de methode van Kinney & Wiruth (van Alphen & Verhage, 2015). Tot slot spreekt SRMBOK over de 5x5 risk rating matrix.



Figuur 1: Risk Matrix (van Alphen & Verhage, 2015)

Alle boven genoemde methoden gaan uit van hetzelfde principe, namelijk: risico kan worden bepaald door de kans dat een bepaald incident zich voordoet te verbinden met een bepaalde hoeveelheid schade die voortkomt uit het desbetreffende incident. Zo kan het zijn dat incident A vaak voorkomt maar weinig schade oplevert en

incident B zelden voorkomt maar wel veel schade zou kunnen opleveren. Hierop zou besloten kunnen worden dat het niet de moeite waard is om maatregelen tegen incident A te treffen maar wel tegen incident B.

De twee variabelen zijn effect/impact en kans/waarschijnlijkheid. Impact kan worden uitgedrukt in geld (economische schade, maar ook milieuschade die in geld kan worden omgerekend), in slachtoffers (doden en gewonden) en in immateriële schade (zoals reputatieschade) (NAVI,2008). En bij het inschatten van waarschijnlijkheid wordt er gekeken naar de kans dat een bepaald scenario zich voordoet.

De formule die aan de matrix kan worden gekoppeld gebruikt de variabelen kans/waarschijnlijkheid (K) en effect/impact (E), hierbij is het risico het product van kans maal effect. In formulevorm ziet dit er als volgt uit: Risico = Kans x Effect (R = K x E). Met de formule kun je een risico inzichtelijk maken en in de matrix invullen, hieruit kun je vervolgens het risico voor het bedrijf vaststellen. SRMBOK noemt nog meerdere manieren om een risico vast te stellen, maar die zijn op dit moment niet van belang voor het onderzoek. In *figuur 1* is de risico matrix te zien. De rode vlakken staan voor een hoog risico en de groene voor een laag risico.

Er zijn meerdere soorten risico's waaraan gedacht kan worden als het gaat over risico's. Zo noemt Finch (2014) natural disasters, illegals acts, low confidential data security, unsuccessful management en other accidents als een paar risico's voor wereldwijde logistieke processen. In het kader van dit onderzoek zal er vooral worden gelet op de risico groep "illegale handelingen" zoals bijvoorbeeld:

- sabotage;
- diefstal;
- terrorisme;
- vandalisme;
- smokkelen.

Dit omdat deze soorten risico's vooral worden afgeschermd en voorkomen met fysieke maatregelen.

Standaardisatie
Standaardisatie is een bewuste poging door een organisatie om een bepaalde standaard te ontwikkelen, ratificeren en te implementeren onder haar stakeholders (Gao et al., 2014). Standaardisatie kan worden uitgevoerd door organisaties die hier gespecialiseerd in zijn zoals bijvoorbeeld de ISO die een groot aantal standaarden beheren. Maar standaarden kunnen ook door bedrijven zelf worden ontwikkeld om bijvoorbeeld een standaard voor een product of in het geval van dit onderzoek een beveiligingsmaatstaaf te creëren. In dit geval wordt er gesproken van een standaardisatie poging of inspanning. Argumenten voor standaardisatie zijn divers maar in dit geval is het belangrijkste argument het zorgen voor een minimaal niveau van security maatregelen om de bedrijfsprocessen te kunnen waarborgen. En schade aan assets en verstoring van de verschillende processen te voorkomen. Door deze standaard te ontwikkelen zal security tot een minimaal niveau worden getild, en zal het ook makkelijker zijn om goedkeuring voor maatregelen in nieuwe package centra goedgekeurd te krijgen. Een andere redenen voor standaardisatie zou een verhoging van efficiëntie kunnen zijn (Biggelaar, 2004).

Fysieke beveiliging
Fysieke beveiliging wordt gezien als het onderdeel van security dat bestaat uit fysieke maatregelen die ervoor moeten zorgen dat assets veilig blijven. Het tegengaan van ongeoorloofde toegang valt hier ook

onder. (Talbot & Jakeman, 2009). Simpel gezegd, fysieke beveiliging beschermt mensen, data, materiaal, systemen, panden en andere bedrijfsmiddelen (Harris, 2013).

Twee theorieën die zich focussen op fysieke beveiligingsmaatregelen zijn OBE en CPTED. De eerste theorie bestaat uit een aantal preventieve maatregelen, de zogenaamde organisatorische, bouwkundige en elektronische maatregelen. Deze zijn relevant voor UPS omdat ze zich voor een groot deel richten op fysieke maatregelen, namelijk elektronische en bouwkundige.
-*organisatorische maatregelen* hebben betrekking op het aanleren of juist afleren van bepaalde gewoonten. Meestal zijn ze niet kosten verhogend maar doen ze wel een beroep op een stukje discipline van personen;
-*bouwkundige maatregelen* hebben primair tot doel ongewenste incidenten te voorkomen of vertragen (Appelman, 2010). Bouwkundige maatregelen hebben een preventief doel en schrikken mogelijke vijandige actoren af. Een theorie die goed bij de bouwkundige maatregelen aansluit is de schillentheorie, wil je in het midden van een ui komen moet je door meerdere lagen/schillen heen (Appelman, 2010). Deze theorie is vergelijkbaar met het concept diepteverdediging of "defense in depth", dit is een beveiliging strategie waarbij meerdere verdedigingslagen in en rond een te beveiligen object zijn aangebracht. Het falen van één verdedigingslaag wordt daardoor opgevangen door de volgende laag;
-*elektronische maatregelen* hebben als primair doel ongewenste acties te signaleren te detecteren en te registreren. Denk hierbij aan toegangsbeheersystemen, inbraakdetectie systemen en andere vormen van elektronische hulpmiddelen.
Appelman heeft in zijn boek twee maatregelgroepen toegevoegd aan de drie bovenstaande klassieke maatregelgroepen, namelijk:

-*meldingen en stuurinformatie* wanneer zijn maatregelen nodig en wanneer is iets veilig, dit zijn vragen waren security professionals zich constant meer bezig houden. Dit kan worden getoetst met het registeren van meldingen en op basis hiervan kan worden onderbouwd welke maatregelen nodig zijn om herhalingen te voorkomen (Appelman, 2010).
-*communicatie en bewustwording* een kritische factor van succesvolle beveiliging is het verruimen van het beveiligingsbewust zijn van de medewerkers. Wanneer werknemers beseffen wat risico's en potentiele dreigingen zijn voor de organisatie kunnen zij hier ook naar handelen.

De tweede theorie is CPTED, wat staat voor Crime Prevention Through Environmental Design. De methodiek geeft in duidelijke principes weer hoe een gebouwde omgeving moet worden ingericht, om zowel de objectieve als de subjectieve criminaliteit te verlagen. Daarbij gaat het in principe niet om zware beveiligingsmaatregelen (Ivanović, 2007).

Bedrijfsprocessen en afhankelijkheden
Voordat je passende beveiligingsmaatregelen kan treffen is het belangrijk een goed beeld te krijgen van hoe het bedrijf functioneert en het goed in kaart brengen van de bedrijfsprocessen. Elk bedrijf heeft bedrijfsprocessen, een bedrijfsproces is een verzameling samenhangende activiteiten die gericht zijn op een klant en afgestemd zijn op organisatiedoelen. Kenmerkend is dat een bedrijfsproces een aantal activiteiten omvat die in samenhang met elkaar worden uitgevoerd. De deelactiviteiten zijn daarmee geen losse activiteiten, maar er is nagedacht over een samenhang (Mittelmeijer & Stratum, 2014). Bedrijfsprocessen kunnen worden onderverdeeld in drie groepen namelijk, primaire processen, secundaire processen en bestuurlijke processen. In het kader van dit onderzoek zijn het primaire en secundaire proces van belang.
Primaire processen: alle activiteiten die rechtstreeks een bijdrage leveren aan het tot stand komen van het product of de dienst (Marcus & van Dam, 2012).

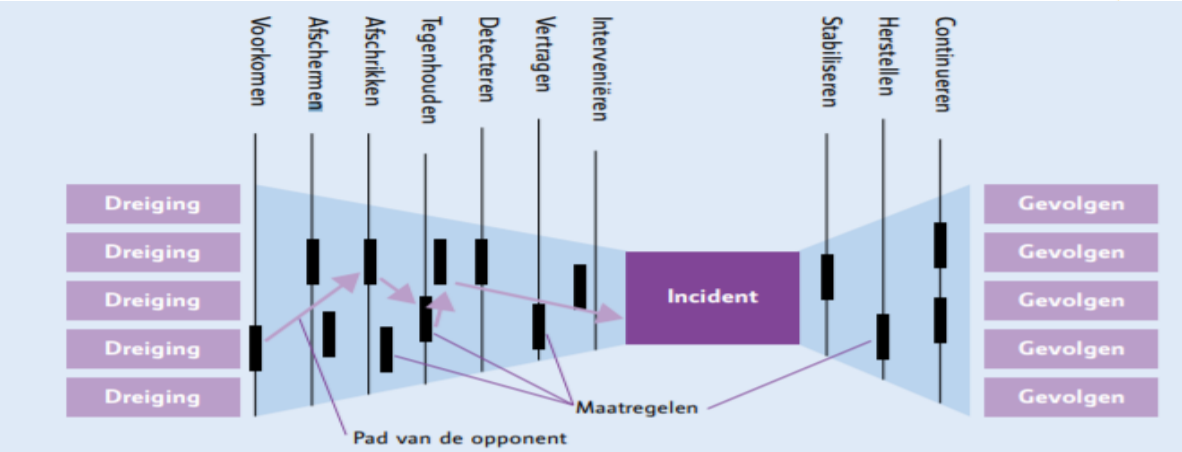
Secundaire processen: alle activiteiten die worden uitgevoerd om bepaalde productiefactoren in stand te houden (Marcus & van Dam, 2012).
Niet alle bedrijfsprocessen zijn cruciaal om te kunnen blijven functioneren, de vraag die hierbij gesteld kan worden is: "Wat zijn de cruciale (en gevaarlijke) bedrijfsonderdelen en -processen die in geen enkel geval mogen worden verstoord? Welke toevoer mag absoluut niet stagneren?" (NAVI, 2008). Een methode om dit vast te stellen is bijvoorbeeld een systeemanalyse die hieronder in *figuur 2* is afgebeeld.

Figuur 2: systeemanalyse (NAVI, 2008)

Een systeemanalyse is een model dat de gebruiker helpt om in kaart te brengen wat de belangrijke onderdelen en aspecten van de organisatie zijn en aan te geven wat er de organisatie 'in' gaat en wat er 'uit' komt. Kortom: alle stromen en externe toevoeren die een organisatie binnenkomen en die noodzakelijk zijn om te kunnen blijven functioneren (de afhankelijkheden) en de producten die er uiteindelijk 'aan de achterkant' uitkomen (NAVI, 2008). Dit model is zeer geschikt om de afhankelijkheden vast te stellen omdat je kijkt naar de input, throughput en output waardoor er een overzichtelijk beeld ontstaat.

Business continuity
De bedrijfsprocessen en afhankelijkheden houden nauw verband met de term business continuity. Business continuity gaat over het hebben van een plan en het omgaan met gevaarlijke situaties zodat de organisatie kan blijven functioneren met zo min mogelijk verstoring tijdens incidenten. Een goed business continuity plan maak je door een goed beeld te hebben van de risico's voor de organisatie en welke impact deze risico's kunnen hebben op de bedrijfsvoering. Business continuity is een doorlopend proces dat up to date gehouden moet worden (Business Continuity institute, 2018).

Bow-Tie/Padanalyse
De Bow-Tie methode is een kwalitatieve risicoanalyse methode waarmee op een systematische wijze een beeld kan worden geschetst van de risico's die in een organisatie aanwezig zijn en van de preventieve en beschermingsmaatregelen die hierop (kunnen) worden ingezet. In het model staan de risico's, bedreigingen en maatregelen. In het midden staat het incident, links hiervan de oorzaken en rechts mogelijke gevolgen. De Maatregelen die tegen het incident kunnen worden getroffen staan als barrières. Hieronder in *figuur 3* staat een voorbeeld van een Bow-Tie model.



Figuur 3: Bow-Tie model (NAVI,2008)

Security beleid UPS
UPS beschikt over een corporate security beleid. Dit beleid stelt: “We plan our buildings and facilities for safe and efficient operations. We develop detailed plans for the design of our buildings and the installation of equipment in our facilities. We provide safe, clean, and pleasant places to work” (UPS Policy). In het beleid staan verdere richtlijnen over te ontwikkelen maatregelen. Bij het ontwerpen van nieuwe locaties word security bijvoorbeeld meegenomen vanaf het eerste moment en worden er district security vertegenwoordigers aangesteld om te ondersteunen bij de planning van nieuwe locaties. Verder worden er een aantal zaken opgesomd waar naar moet worden gekeken als het gaat over security binnen een UPS pand.

Tot slot zijn er een aantal boeken, rapporten en handreikingen die veelvuldig gebruikt zullen worden tijdens dit onderzoek. Hieronder zal een overzicht worden gegeven.

OSP
Het Adviescentrum Bescherming Vitale Infrastructuur adviseert over risicomanagement, beveiliging, continuïteitsmanagement en cyber security. Zij werken volgens erkende werkwijzen en bieden opdrachtgevers bestendige en kostenefficiënte oplossingen. Eén van de documenten die het NAVI heeft uitgegeven is het Operator Security Plan (OSP) dat de beveiligingsmaatregelen die een organisatie heeft getroffen beschrijft. De benaming ‘Operator’ verwijst naar de beheerder van de infrastructuur. Samen met het Security Management Systeem (SMS) en een risicoanalyse sluit het OSP aan op de Europese richtlijn van de European Programme for Critical Infrastructure Protection (EPCIP). De Handreiking Operator Security Plan is geschreven voor bedrijven binnen de vitale infrastructuur. De handreiking is echter ook te gebruiken om beveiligingsmaatregelen te selecteren voor objecten van belang die niet aangewezen zijn als ‘vitale infrastructuur’.

SRMBOK
SRMBOK is een boek dat zich focust op security vraagstukken. Dit doet de auteur door een aantal geaccepteerde methodes toe te lichten. Hierdoor is het boek uitermate geschikt om een onderzoek naar fysieke beveiliging te ondersteunen.

Handreiking risicoanalyse
Het Nationaal Adviescentrum Vitale Infrastructuur is een initiatief waarin de overheid en bedrijfsleven samen aan de verbetering van bescherming van de vitale infrastructuur werken. Het document heeft als doel om op basis van de vele methodieken die er zijn een generieke methodiek te beschrijven waarin (1) alle relevante stappen van een risicoanalyse aan de orde komen, (2) specifiek gericht op risico’s

aangaande moedwillige verstoring (security) en (3) die toe te passen is in alle vitale sectoren (dus niet sectorspecifiek is).

Omgevingsanalyse
Een omgevingsanalyse brengt factoren in kaart, die niet beïnvloedbaar zijn, maar waar rekening mee moet worden gehouden. Voorbeelden hiervan zijn het economisch klimaat, sociaal-culturele ontwikkelingen en veranderende wetten en regels. Dit kan van belang zijn voor het kiezen van een nieuwe locatie of het nemen van bepaalde security maatregelen.

Wet en regelgeving
In het kader van het vrachtverkeer voor de Keulen hub zijn er op verscheidene locaties zogenaamde kooien geplaatst om pakketten te kunnen controleren voordat ze verscheept worden. Tot nu toe relevante wet- en regelgeving hiervoor zijn: EU 300/2008, EU 272/2009 en EU 2015/1998 Deze verordeningen zijn opgesteld door het EUROPEES PARLEMENT EN DE RAAD. De verordeningen focussen zich op regels op het gebied van de beveiliging van de burgerluchtvaart. Nederland zelf heeft de luchtvaartwet waarbij vooral artikel 37 van toepassing is. Tot slot is er nog de regeling uitvoering beveiliging burgerluchtvaart 2010 die bestaat uit voorschriften voor de uitvoering van controle van personen, bagage en van vracht op luchtvaartterreinen (Regeling uitvoering beveiliging burgerluchtvaart, 2010).

3. Onderzoeksmethoden

In dit hoofdstuk zijn de onderzoeksmethoden behandeld. Per onderzoeksvraag zal worden beschreven hoe de onderzoeksvraag zal worden beantwoord. Om te beginnen zal de aard van het onderzoek worden beschreven om zo duidelijkheid te schetsen over de manier waarop de onderzoeksvraag zal worden beantwoord. Daarop volgend zal worden beschreven welk proces er wordt doorlopen om de verschillende onderzoeksvragen te beantwoorden. Dit is per onderzoeksvraag uitgewerkt en er zal worden beargumenteerd waarom de betreffende keuze is gemaakt. Dit proces is voor elke vraag hetzelfde en ziet er als volgt uit:

- Beschrijving van de methode, op welke manier zal het onderzoek gedaan worden?
- Beschrijving van de variabelen, wat zijn de kenmerken van het te onderzoeken object? Welke zaken zullen onderzocht worden?
- Beschrijving van de operationalisatie, hoe kunnen de kenmerken van het te onderzoeken object worden gekarakteriseerd?
- Beschrijving van de betrouwbaarheid en validiteit.

3.1. Aard van het onderzoek

Het doel van het onderzoek is om een bijdrage te leveren aan een fysieke security standaard die voor UPS package centra in Nederland zou kunnen gaan gelden, om zo de security van deze centra te vergroten en op een minimaal niveau te brengen.

3.2. Onderzoeksvraag 1

- **Zijn er op dit moment standaard maatregelen op het gebied van fysieke beveiliging binnen UPS Nederland en wat houden deze maatregelen in?**

Variabelen
Huidige maatregelen
Huidig Nederlands UPS security beleid

Om deze onderzoeksvraag te beantwoorden zal er gebruik worden gemaakt van deskresearch en interviews. Aanvullend zullen de volgende UPS package centra worden bezocht om een indruk te krijgen van de fysieke security maatregelen: Amsterdam, Rotterdam, Utrecht, Eindhoven en Apeldoorn. Deskresearch zal worden gedaan aan de hand van security data die door de UPS security afdeling is vergaard. Tot slot zullen er interviews en gesprekken worden gehouden met mensen van de security afdeling. Deze interviews zullen een open karakter hebben. Door middel van de bovenstaande literatuurstukken, interviews en de observaties zal er een goed overzicht van de huidige standaard maatregelen, het huidige beleid en de manier waarop security maatregelen op dit moment tot stand komen ontstaan en kan hier tijdens de vervolg vragen op worden teruggevallen.

Operationalisatie

Om een goed beeld te krijgen van de huidige UPS eisen op het gebied van fysieke beveiliging zal gekeken moeten worden naar het huidige security beleid dat voor Nederland geldt. Ook zal er gekeken worden welke fysieke maatregelen er op dit moment bij UPS centra in Nederland zijn toegepast. Vragen die hierbij gesteld worden zijn:

-Welke huidige eisen en regels met betrekking op de fysieke beveiliging van UPS centra in Nederland zijn er?

-Welke fysieke maatregelen worden er op dit moment toegepast bij de verschillenden UPS package

centra in Nederland?
-Welke stappen worden er doorlopen bij het security gereed maken van UPS centra in Nederland?

Om deze vragen te beantwoorden wordt er gebruik gemaakt van literatuuronderzoek (kwalitatief onderzoek). UPS heeft verscheidene documenten die hierbij ondersteunend kunnen zijn. Zo is er het corporate security beleid wat een aantal richtlijnen voor de security van UPS package centra voorschrijft. Dit document zal hierom dan ook een goed beeld schetsen van de reeds aanwezige en voorgeschreven maatregelen. Aanvullend hierop zal er worden gekeken naar uitgevoerde security audits en zullen deze worden doorgenomen. Deze audits geven een goed beeld van security eisen die op dit moment binnen UPS gesteld worden aan locaties. Ook geven deze audits een goed inzicht of er aan de bestaande eisen wordt voldaan op dit moment. Ook zal er een interview worden gehouden met dhr. Houter, dit interview zal zich focussen op de huidige maatregelen en totstandkoming van deze maatregelen (de topics van dit interview zijn terug te vinden in *bijlage 1*). Tot slot zullen er bezoeken worden gedaan aan verschillende centra in Nederland, zo zal er worden gekeken op de locaties Eindhoven en Utrecht naar welke maatregelen daar zijn geïmplementeerd.

Door middel van de bovenstaande literatuurstukken en de observaties zal er een goed overzicht van de huidige standaard maatregelen ontstaan en kan hier tijdens de vervolg vragen op worden teruggevallen.

Betrouwbaarheid en validiteit
De betrouwbaarheid is geborgd door verschillende bronnen te raadplegen, zo zal er met een aantal personen binnen UPS worden gesproken die affiniteit hebben met security, met name dhr. Houter en zijn collega's. Verder zal er aanvullend deskresearch worden gedaan. Ook zullen er meerdere UPS locaties worden bezocht en geobserveerd om een goed beeld te krijgen van de verschillende fysieke security maatregelen die UPS heeft geïmplementeerd.

De validiteit is geborgd door alleen te focussen op wat nodig is, zo zijn bij maatregelen hun doel belangrijk en waar deze maatregelen op dit moment zijn toegepast. De technische werking heeft verder geen relevantie.

3.3. Onderzoeksvraag 2

- **Wat zijn de belangrijkste security incidenten bij huidige UPS centra in Nederland?**

Variabelen
Incidenten
Risico's

Bij deze onderzoeksvraag zal er worden gekeken naar welke security incidenten zich voordoen binnen UPS package centra. En zo het in kaart brengen van relevante security incidenten die bij UPS in de afgelopen jaren bij package centra voorgevallen. Door hier naar te kijken zal er een beter beeld ontstaan van welke incidenten voorkomen en welke risico's UPS hierdoor loopt. Deze doelstellingen zullen worden voltooid door middel van deskresearch en interviews.

Operationalisatie
Voor de tweede deelvraag zullen de incidenten registers, intern bekend als facility statistics, worden ingekeken. UPS houdt bij welke incidenten voorvallen binnen het bedrijf, zo ook security gerelateerde incidenten. Hierbij hoeft alleen gekeken worden naar de relevante incidenten die zich binnen de verschillende package centra in Nederland voordoen aangezien deze relevant zijn voor het onderzoek. De incidenten zullen in kaart gebracht moeten worden om zo een beeld te krijgen welke incidenten het meest voorkomen en waar dus risico's zitten voor UPS. Aanvullend hierop zullen er een aantal

interviews worden gehouden, in de interviews zal gevraagd worden naar welke incidenten de betreffende persoon heeft meegemaakt, en wat in zijn/haar ogen de meest voorkomende incidenten zijn. Voor alsnog is een interview met dhr. Beusekom ingepland, dhr. van Beusekom is werkzaam bij de afdeling loss prevention (LP), deze afdeling onderzoekt en handelt de verschillende security incidenten af en registreert deze in de verschillende facility statistics sheets. De interview topics voor dit gesprek zijn terug te vinden in *bijlage 2*.
Bij deze onderzoeksvraag zal er dus gebruikt worden gemaakt van de al bestaande informatie die UPS heeft over de incidenten binnen het bedrijf. Door deze in kaart te brengen zal een goed en gegrond beeld ontstaan van het type security incidenten die veelvuldig voorkomen. Door dit vervolgens terug te laten komen binnen de interviews zal een goed en gegrond beeld ontstaan van de incidenten en wat als de belangrijkste incidenten gezien worden. Hiermee wordt een kwalitatieve onderzoeksmethode aangewend om tot data te komen.
Vragen die bij deze deelvraag gesteld worden zijn:
-Welke security incidenten komen voor binnen UPS package centra?
-Welke incidenten hebben de meeste impact?
-Hebben deze incidenten een intern of extern karakter?

Betrouwbaarheid en validiteit
De betrouwbaarheid is geborgd door relevante en recente up to date data te gebruiken, in dit geval de facillity statistics documenten die worden aangeleverd door de afdeling LP. Deze documenten richten zich puur op incidenten binnen UPS package centra. Ook zal er een interview worden gehouden met de persoon die deze incidenten registers bijhoudt, dhr. van Beusekom.

De validiteit is gewaarborgd door alleen de security incidenten binnen UPS package centra in Nederland mee te nemen in het onderzoek en niet alle security incidenten. Hierdoor wordt data die niet in verband staat met de UPS package centra eruit gehaald en wordt de validiteit gewaarborgd. Ook is voor het interview iemand benaderd die zich volledig focust op incidenten en incident afhandeling.

3.4. Onderzoeksvraag 3

- **Wat zijn de beveiligingsrisico's voor huidige en toekomstige UPS centra?**

Deze onderzoeksvraag zal worden beantwoord door middel van deskresearch en interviews. Door middel van het analyseren van UPS risicoanalyses en het houden van interviews met personen die over de day to day operatie gaan binnen UPS. Het belang van deze onderzoeksvraag is het vaststellen van beveiligingsdoelen en de risico's die deze assets/beveiligingsdoelen lopen.

Variabelen
Beveiligingsdoelen
Risico's

Operationalisatie
Bij deze onderzoeksvraag moeten de verschillende beveiligingsdoelen in kaart worden gebracht. Hiervoor moeten ook de risico's bekend zijn, om deze in kaart te brengen is de vorige deelvraag dan ook ondersteunend. Dit omdat de incidenten die al zijn voorgevallen binnen UPS voort kunnen komen uit een risico. Ook worden de al bestaande risicoanalyses waar UPS over beschikt doorgenomen en bestudeerd. Bij deze deelvraag zullen ook interviews worden gehouden met security supervisors en centrum managers, dit zijn de heren A. Bliek (centrum manager Rotterdam) en P. Peters (operations supervisor Apeldoorn), deze zullen een goed beeld hebben van de primaire beveiligingsdoelen en welke risico's prioriteit hebben. De interviewtopics zijn terug te vinden in *bijlage 3*. Aanvullend zijn er meerdere korte gespreken geweest met verschillende mensen binnen UPS om tot aanvullende

informatie te komen. Tot slot zal een interview worden gehouden met dhr. R. Kinds, door zijn werk als aviation security officer binnen UPS Benelux heeft hij een goed beeld van de beveiligingsdoelen omtrent de UPS luchtvracht (topics voor dit interview staan in *bijlage 4)*. Ook kan tijdens deze onderzoeksvraag worden teruggevallen op bronnen zoals het Centraal Bureau Statistiek en de politie monitor.

Naar aanleiding van de interviews, literatuurstukken en optionele aanvullende bronnen kan er een Jaarsma-matrix worden opgesteld hetgeen een helder beeld geeft van een risico's. Hierna kan vervolgens een concrete lijst van beveiligingsdoelen worden opgesteld. Wederom zal er een combinatie van interviews en literatuurstukken worden gebruikt om data te verzamelen.

Vragen die bij deze onderzoeksvraag naar voren komen zijn:
-Welke primaire beveiligingsdoelen zijn er binnen een UPS package center?
-Welke risico's komen naar voren in de risk-assessments?

Betrouwbaarheid en validiteit
De betrouwbaarheid is geborgd door relevante en recente up to date data te gebruiken, in dit geval de UPS security riskassessments. Ook zal er tijdens verschillende interviews worden gesproken over primaire assets en andere mogelijke beveiligingsdoelen. Deze interviews zullen worden gehouden met personen die verantwoordelijkheid dragen bij de dagelijkse operatie van UPS en hier kennis van en ervaring mee hebben. Dit maakt hen zeer geschikt om te interviewen bij deze deelvraag.

De validiteit is gewaarborgd door alleen de security risksassessments binnen UPS package centra in Nederland mee te nemen in het onderzoek. Ook wordt er gesproken met mensen die inhoudelijke en praktische kennis hebben van de processen binnen UPS, namelijk supervisors en center managers.

3.5. Onderzoeksvraag 4

- **Welke maatregelen moeten uit deze risico's en incidenten voortkomen om deze te mitigeren?**
  - Ontwikkelen vlinderdasmodel voor UPS
  - Opstellen te nemen maatregelen
  - Opstellen van de minimale fysieke security standaard

Deze onderzoeksvraag focust zich op te nemen maatregelen. Naar aanleiding van de vastgestelde beveiligingsdoelen en risico's kunnen de te nemen aanbevolen maatregelen worden opgesteld. Hierbij zal het Bow-Tie model worden gebruikt om duidelijk te kunnen aangeven welke maatregelen welke risico's wegnemen en hoe deze maatregelen een beveiligingsdoel veiligstellen. Vervolgens kan aan de hand hiervan een geadviseerde fysieke security standaard worden opgesteld. Vragen die bij deze deelvragen horen zijn:

Variabelen
Te nemen fysieke maatregelen
Zones van een package center

-Welke mogelijke security incidenten moeten in acht genomen worden?
-Welke maatregelen kunnen hier tegen genomen worden?
-Welke minimale fysieke security maatregelen kunnen er worden geadviseerd?
-Welke security maatregelen zouden aanvullend kunnen zijn?

Operationalisatie
Voor het beantwoorden van deze deelvraag zal er worden teruggevallen op de vorige deelvragen. Uit

die vragen zijn een aantal risico's en beveiligingsdoelen gekomen. Vervolgens zullen deze omgezet worden naar maatregelen. Dit zal gebeuren door middel van het vlinderdasmodel hierbij zullen vijandige actoren en risico's worden geanalyseerd en zullen er passende maatregelen kunnen worden opgesteld om zo het desbetreffende incident te voorkomen.
Ook zal er gekeken worden naar de verschillende zones van een UPS package center en hoe deze kunnen worden onderscheiden.

Betrouwbaarheid en validiteit
De data die gebruikt zal worden is bij de vorige deelvragen al op een valide en betrouwbare verzameld. Ook is het opdelen van een UPS package center met verschillende personen overlegd. Hierdoor zal een goed overzicht van zones ontstaan.

4. Resultaten

In dit hoofdstuk zullen de onderzoeksvragen beantwoord worden. Dit zal gebeuren aan de hand van de vastgestelde onderzoeksmethoden.

4.1. Resultaten onderzoeksvraag 1

"Zijn er op dit moment standaard maatregelen op het gebied van fysieke beveiliging binnen UPS Nederland en wat houden deze maatregelen in?"

4.1.1. Inleiding

In dit hoofdstuk zal worden gekeken naar de huidige fysieke maatregelen die op dit moment veelvuldig bij UPS package centra in Nederland aanwezig zijn. Hiermee zal de eerst deelvraag worden beantwoord. De informatie die hiervoor wordt gebruikt is afkomstig uit meerdere bronnen, namelijk; interviews, observaties en deskresearch.

De deskresearch documenten zijn de verschillende phsysical security assessments die intern zijn uitgevoerd door de security afdeling van UPS Nederland. Ook zal er worden gekeken naar het Corporate security beleid en met name naar section 47 waarin richtlijnen staan voor fysieke beveiliging omtrent UPS faciliteiten. Tot slot wordt er gekeken naar de UPS Corporate security matrix. Met deze documenten kan er een goed overzicht van de mogelijke maatregelen worden gecreëerd. Het Corporate document geeft een handvat aan de verschillende UPS divisies en is bedoeld om te assisteren op een groot aantal gebieden bijvoorbeeld; de locatie van een nieuw UPS center, de planningsfase en een overzicht van mogelijke maatregelen die getroffen kunnen worden. Het document is Amerikaans en dus niet specifiek gespitst op Nederland. Wel kan dit document gebruikt worden om een overzicht van maatregelen te creëren.

Voor een interview is dhr. H. Houter benaderd, door zijn rol als security supervisor en zijn betrokkenheid bij projecten omtrent het security gereed maken van de nieuw gebouwde Eindhoven en Utrecht locaties is hij zeer goed op de hoogte van de mogelijke maatregelen en de huidige toegepaste maatregelen. Ook kan dhr. Houter een beter inzicht verschaffen over het huidige security beleid van UPS Nederland. Tot slot zijn een aantal UPS package centra bezocht (Utrecht, Eindhoven, Amsterdam, Rotterdam en Apeldoorn) om de verschillende maatregelen te observeren en in kaart te brengen welke maatregelen bij welk centrum zijn toegepast. De checklist die hiervoor is gebruikt staat in *bijlage 5*.

4.1.2. Security beleid UPS Nederland

Op het gebied van security beleid bestaat er op dit moment geen document dat zich primair richt op Nederland. In het interview met dhr. Houter kwam naar voren dat ieder land waar UPS actief is er een eigen security beleid op na houdt, dat weer onder het corporate beleid van UPS valt. In het geval van Nederland wordt er dus gekeken naar het corporate security beleid, dat zoveel mogelijk wordt aangehouden en als een soort leidraad werkt. Dit is echter niet altijd mogelijk aangezien er rekening gehouden zal moeten worden met lokale wetten en regelgeving en ondernemingsraden. Het corporate security beleid word omschreven als ruw en andere documenten zoals bijvoorbeeld de eerder genoemde security assessments worden hierop geënt. Een Nederlands UPS security beleid gespitst op de Nederlandse markt en omgeving is dus niet aanwezig. Hierdoor bestaat er ook geen Nederlandse maatstaaf wat betreft fysieke beveiliging van UPS centra in Nederland. Hiervoor zal dan ook een advies worden gegeven.

4.1.3. Corporate security beleid

Het corporate security beleid richt zich niet primair op Nederland en is dus een leidraad die waar mogelijk wordt aangehouden. Het corporate security beleid bevat vooral technische informatie en richtlijnen die aangehouden kunnen worden bij het plannen van een nieuwe UPS locatie. Hoewel de verschillende maatregelen die het document noemt helder zijn staat er verder geen toelichting hoe deze toe te passen en wanneer. Ook bevat het document een security Matrix met aanbevelingen, deze is terug te vinden in *bijlage 6*. Wederom is de gegeven informatie over waar en wanneer deze toe te passen zeer beperkt en dus lastig toe te passen in de praktijk.

4.1.4. Overzicht mogelijke maatregelen

Hieronder volgt een overzicht van de maatregelen, een korte beschrijving van de maatregel en het doel van de maatregel. In de laatste kolom is te zien bij welke centra/centrum een bepaalde maatregel is toegepast, hierbij betekent **Groen** dat de maatregel is geïmplementeerd en **Rood** dat de maatregel niet is geïmplementeerd. De inventarisatie van de huidige maatregelen is gebeurd aan de hand van observaties door middel van een checklist (*bijlage 5*) per center en gesprekken met dhr. Houter,

Maatregel	beschrijving	Doel	Geïmplementeerd in de volgende centra
Card Access Systems	Kaartlezer systemen zorgen ervoor dat bepaalde individuen toegang hebben tot van tevoren bepaalde gebieden binnen een locatie zonder dat er een sleutel nodig is.	Kaartlezers zijn een nuttig hulpmiddel om bepaalde groepen werknemers of leveranciers toegang te geven tot bepaalde gebieden. Ook kan er doormiddel van kaartlezers gemonitord worden wie bepaalde gebieden heeft betreden.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Tourniquet	Een tourniquet is een twee-, drie- of vierarmig draaihek dat wordt geplaatst voor de toegangscontrole of geleiding van personen. Tourniquets worden gebruikt voor de toegangscontrole bij gebouwen, bedrijven	Het doel binnen UPS zou zijn om onbevoegde personen te weren van panden en terreinen en het monitoren wie binnen treed en wie uittreed.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Sloten	Sloten zijn al eeuwen één van de meest gebruikte vormen van fysieke beveiliging. De effectiviteit van sloten hangt af van verschillende factoren zoals ontwerp, kwaliteit, installatie en onderhoud. Aanvullend is een goed sleutelplan ook van levensbelang voor een goed werkend sleutel systeem.	Sloten zijn in het geval van UPS bedoeld om ramen, deuren, hekken af te kunnen sluiten en het daarmee moeilijker te maken voor kwaadwillende individuen zich toegang te verschaffen tot terreinen en ruimten. Kritieke deuren hebben binnen UPS een gecertificeerd slot.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Hekwerk	Hekwerken worden al jaren gebruikt in zowel private als corporate omgevingen. Een hekwerk is een fysieke barrière en in veel gevallen ook voordeliger in verhouding met andere type barrières.	Met een hekwerk kan een UPS terrein worden afgebakend waarmee het duidelijk is voor externe dat het om privéterrein gaat. Verder is een hekwerk een effectieve eerste linie om mogelijke indringers af te schrikken of te vertragen. De noodzaak van hekken word op dit moment per locatie bepaald.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**

Verlichting	Goede verlichting in UPS vestigingen verbeterd de veiligheid van werknemers en verhoogd de efficiëntie van de aanwezige processen. Daarbij kan verlichting ook bijdrage aan een verbetering van de beveiliging van een locatie.	Verlichting kan worden gezien als een integraal onderdeel van beveiliging. Licht kan worden gebruikt om insluiping te vermijden of af te schrikken en eventuele insluipers sneller te detecteren. Tot slot zal het ook het veiligheidsgevoel van medewerkers verbeteren.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Metaal detector(en)	Screenen van werknemers doormiddel van metaal detectoren en X-Ray machines word al toegepast binnen UPS en UPS Nederland. De voornaamste redenen hiervoor zijn de veiligheid van UPS haar medewerkers en het beschermen van de waren van de klant. Deze screening kan op meerdere manieren plaatsvinden. Hierbij moet gedacht worden aan visitatie, metaal detectoren of X-Ray machines. Zowel metaal detectors als X-Ray's worden op dit moment op verschillende UPS locaties binnen UPS Nederland dagelijks gebruikt.	Screening heeft in essentie twee doelen. Ten eerste het voorkomen dat gevaarlijke en verboden voorwerpen (bijv. wapens, drugs) het desbetreffende UPS pand binnen komen. Ten tweede het voorkomen van dat medewerkers goederen van klanten of UPS bezit meenemen/stelen. De noodzaak om te screenen kan afhangen van meerdere factoren, namelijk: aantal werknemers, screeningtijd, aantal incidenten en de kosten van het screenproces.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
X-Ray machines			**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
CCTV systeem	CCTV is tegenwoordig een vrij gangbare tool voor bedrijven. Bij UPS Nederland zijn camera's in haar panden ook vrij standaard.	CCTV systemen hebben meerdere voordelen. Ten eerste schikt het crimineel of ander ongewenst gedrag af. Ten tweede kunnen terreinen en ruimtes worden gemonitord. Ten derde word er beeldmateriaal van incidenten en ongelukken vastgelegd wat gebruikt kan worden indien nodig.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Electronic Alarm Systems/IDS	Net als CCTV zijn elektronische alarmsystemen tegenwoordig vrij gangbaar. Ook UPS Nederland maakt gebruik van deze systemen.	Het doel van een alarmsysteem is het detecteren van ongeautoriseerde binnendringen van een gebouw of ander gebied. Door het detecteren kunnen hulpdiensten of andere alarmopvolgers zich naar de plaatst van detectie bewegen. Door het detecteren is het de bedoeling om diefstal en inbraak tegen te gaan. In het geval is het alarmsysteem aangesloten bij Securitas	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Kluis (cashcow machines)	Kluizen zijn een onderdeel van bijna ieder securityplan. UPS beschikt ook over kluizen om waardevolle goederen op te slaan en te beschermen.	Inbraakvrije kluizen zijn gemaakt om de inhoud te beschermen tegen geforceerde binnendringing van personen. In het geval van UPS wordt het geld dat chauffeurs meenemen na een rit in de zogenaamde cashcow gestort waarbij het bedrag gelijk word	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**

		geteld en de chauffeur een stortbevestiging krijgt.	
High value cage	UPS centra hebben over het algemeen een holdcage in een centrum. In deze ruimte worden waardevolle goederen gestald tot dat deze verder worden vervoerd.	Het hoofddoel van de holdcage is het opslaan van waardevolle en belangrijke goederen om diefstal en vermissing tegen te gaan.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Fysieke beveiliger(s)	Bij meerdere UPS locaties in Nederland worden er op dit moment particulier beveiligers ingezet om het package center te beveiligen. Denk hierbij aan de twee nieuwe locaties: Utrecht en Eindhoven.	Beveiligers houden toezicht en controleren bezoekers en medewerkers, dat zijn de voornaamste taken als particulier beveiliger. Dit doe je door te surveilleren, de wacht te houden en eventueel bezoekers te begeleiden.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Passief infrarood 'gordijn'	Op dit moment is er in het centrum in Utrecht een infrarood gordijn. Dit gordijn loopt achter de dokdeuren langs en zal buiten de operatie worden aangezet om insluipers te detecteren.	Het doel van de infrarood gordijnen is het detecteren van insluipingen en andere soorten van ongeoorloofde binnentreding van een UPS pand via een dokdeur. Het infrarood gordijn word dan ook na de operatie ingeschakeld	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**
Magneet contacten (dokdeuren)	Een magneetcontact bestaat uit twee delen: een compacte sensor (“reedcontact”) en een magneetje. Zodra deze meer dan ongeveer een centimeter van elkaar worden verwijderd, dan activeert dit het alarmsysteem.	Door roldeuren en deuren te beveiligen met een magneetcontact kan UPS haar belangrijke deuren en roldeuren simpel en effectief beveiligen.	**Apeldoorn** **Utrecht** **Heereveen** **Amsterdam** **Rotterdam** **Eindhoven** **Tilburg**

4.1.5. Security audits

De physical security assessments die intern door UPS kunnen worden uitgevoerd geven ook een beeld van de verschillende fysieke beveiligingsgebieden die UPS hanteert. De assessments onderscheiden 6 verschillende categorieën van fysieke beveiligingsmaatregelen, namelijk:

- Perimeter security
- Perimeter Access
- Yard security
- Facility-Building security
- Internal security
- CCTV overview

Deze assessments geven een goed beeld van waar corporate naar kijkt bij het beoordelen van de fysieke beveiliging van de verschillende UPS centra. Hierdoor ontstaat een beeld van de minimale eisen die corporate stelt en een minimale standaard op corporate niveau, deze kan vervolgens worden meegenomen in de aan te bevelen minimale fysieke security eisen.

4.1.6. Uitwerking interview dhr. Houter

Dhr. Houter maakt deel uit van de UPS security afdeling in Nederland. Hij is medeverantwoordelijk voor de fysieke beveiliging van de UPS package centra in Nederland. Op dit moment is hij veel betrokken bij de bouw en verbouwing van centra in Nederland (Utrecht, Rotterdam en Eindhoven), om dit zo goed en snel mogelijk uit te voeren.

Elk land voert zijn eigen security beleid wat weer onder het corporate security beleid valt. Dit komt omdat er rekening gehouden zal moeten worden met lokale regelgeving en omdat er tussen landen uiteraard verschil zit. De grote lijnen van het corporate security beleid worden aangehouden, maar er is geen specifiek document gericht op Nederland.

Door de verschillende bouwprojecten en verbouwingen van UPS in Nederland is er wel enigszins een beleid aan het ontstaan omdat er door de bouw en verbouw projecten steeds meer wordt ingezien dat er een soort minimale maatstaaf moet worden gehanteerd. Hiervoor is onder andere de security matrix gebruikt. Ook worden hiervoor de verschillende security audits gebruikt die ook van corporate afkomstig zijn. Deze zijn echter ook meer toegespitst op de Verenigde Staten en komen hierdoor in sommige gevallen niet overeen met de Nederlandse wensen en voorkeuren.

Een andere shift is toewerken naar een situatie waarin er fysieke beveiligers aanwezig zijn op de verschillende faciliteiten. Hun voornaamste taken zullen dan voornamelijk entree en exit toezicht inhouden en het begeleiden van bezoekers en in de avond het begeleiden van chauffeurs (in samenwerking met de feeder afdeling). Ook kunnen de beveiligers visitatie uitvoeren of eventueel een detectie poort bedienen.

Op het gebied van camera's wordt er uitgegaan van het volgende: waar mensen werken wil UPS toezicht en dus camera's, dit komt omdat dit risico plekken zijn. In Utrecht bijvoorbeeld hangen er voornamelijk camera's waar mensen aan het werk zijn. Voorbeelden hiervan zijn de smalls, load en unload. Ook de dokdeuren worden standaard voorzien van camera's. In praktijk is dit één camera per twee dokdeuren of zelfs één camera per dokdeur. Camera's hebben ook aantoonbaar effect, zo zijn er al meerdere mensen betrapt op stelen.

Ambitie voor de toekomst is om Utrecht en Rotterdam vanuit Eindhoven te monitoren en access control te reguleren. Dit zal gedaan worden door middel van de elektrische poort voor vrachtwagens te openen, dit spaart weer kosten doordat er minder beveiligers nodig zullen zijn.

In het kort kan er worden gesteld dat de minimale eisen omtrent fysieke beveiliging in Nederland hekken, camera's en access control door middel van badges is. Een minimale norm hiervoor is zeer welkom.

4.1.7. Voorlopige conclusie

Nu de verschillende maatregelen die UPS kan treffen en gebruikt in kaart zijn gebracht kunnen deze later in het document worden gebruikt voor de security standaard. Ook kan er worden geconstateerd dat er op dit moment geen document is voor welke maatregelen er bij Nederlandse UPS centra moeten worden gebruikt, er zijn echter wel corporate documenten beschikbaar maar deze zijn primair gefocust op de Verenigde Staten en hebben hierdoor minder relevantie voor Nederland. Het afwezig zijn van een security beleid gericht op Nederland kan gezien worden als een gemis, hierdoor is er ook geen fysieke security standaard voor UPS centra in Nederland, hierdoor lopen de verschillen tussen het beveiligingsniveau van de verschillende centra ook zeer uit één.

Ook is vastgesteld dat een alarmsysteem en acces control (door middel van badges) die minimale corporate security eisen zijn. We kunnen ook concluderen dat deze eisen redelijk mager zijn. Dhr. Houter gaf bovendien aan dat camera's en hekwerken om het terrein heen ook tot standaard gerekend kunnen worden in Nederland.

4.2. Resultaten deelvraag 2

"Wat zijn de belangrijkste security incidenten bij huidige UPS centra in Nederland?"

4.2.1. Inleiding

In het volgende hoofdstuk zal er worden gekeken naar de verschillende incidenten die zich voordoen bij de verschillende centra in Nederland. Het doel hiervan is een goed beeld te krijgen van welke incidenten het vaakst voorkomen en welke incidenten zelden tot nooit voorkomen. Met deze informatie kan er extra worden gekeken naar incidenten die veelvuldig voorkomen en dus mogelijk meer schade aanrichten aan UPS.

Voor het beantwoorden van deze deelvraag zal worden gekeken naar de verschillende incidenten registraties van de zeven UPS package center locaties in Nederland. Deze zullen vervolgens in een tabel worden verwerkt om een overzichtelijk overzicht van het type incidenten en het aantal keer dat deze voorkomen te creëren. Tot slot zullen er intern een aantal interviews worden gehouden waarin zal worden gesproken over incidenten, welke maatregelen hiervoor zijn getroffen, welke schadepost deze incidenten met zich mee brengen en welke incidenten de meeste indruk hebben gemaakt op de geïnterviewde.

Door middel van de combinatie van deskresearch en interviews wordt er een goed beeld weergegeven van welke incidenten het meest schadelijk zijn voor UPS. Ook kan er op deze manier worden gezien of het beeld van het type incidenten en hoe vaak deze voorkomen strookt met de realiteit.

4.2.2. Incident definities

In de documenten: "facility statistics worksheets" is in kaart gebracht per locatie welke incidenten er voorkomen en de frequentie waarin deze voorkomen. Binnen UPS word een aantal typen security incidenten onderscheden en in kaart gebracht. Hieronder zullen de primaire typen incidenten worden toegelicht.
Diefstal uit een pakket: het stelen van goederen of de poging tot het stelen uit een pakket dat aan UPS is toevertrouwd.
Diefstal van een pakket: het stelen of poging tot het stelen van een pakket dat aan UPS is toevertrouwd.
Diefstal van geld: het stelen of poging tot het stelen van valuta dat aan UPS is toevertrouwd.
Diefstal van bedrijfsmateriaal: het stelen of poging tot het stelen van bedrijfsmiddelen en andere goederen die aan UPS zijn toevertrouwd.
Diefstal van personen: het stelen van persoonlijke eigendommen van een UPS medewerker, leverancier, klant of bezoeker op een door UPS beheerd gebied.
Agressie: iedere handeling die de UPS Professional Conduct and Anti-Harassment Policy of de UPS Workplace Violence Policy overtreedt.
Werknemers discipline: waarschuwingen die aan een werknemers worden gegeven om zijn of haar gedrag bij te stellen en te corrigeren.
Vandalisme: het moedwillig beschadigen of vernietigen van objecten die aan UPS toebehoren of aan UPS zijn toevertrouwd.
Drugs en alcohol: overtredingen van het UPS drugs en alcohol beleid.
Medeweten van schuld: het verantwoordelijk zijn of het weten van feiten die hebben bijgedragen aan het plegen van een overtreding of misdrijf dat UPS beleid overtreed.

Fraude met labels: het feit van het veranderen of bedekken van een origineel shipping label om zo het aflever adres te veranderen met het oogmerk om het pakket te stelen.
Onbevoegd openmaken van een pakket /onbevoegde handelingen met pakketten: het onbevoegd openmaken van een pakket.
Diefstal van voertuigen: het stelen van een UPS voertuig of een voertuig dat aan UPS is toevertrouwt.
Inbraak in voertuigen: het geforceerd binnendringen van een UPS voertuig met als oogmerk diefstal of vandalisme te plegen.
Inbraak in een UPS locatie: het geforceerd binnendringen van een UPS locatie met als oogmerk diefstal of vandalisme te plegen.
Informatie diefstal: het stelen van informatie, logo's, personeelsgegevens, procesinformatie, klantinformatie etc.
LDI onderzoeken: onderzoeken naar vermiste pakketten.
Gewapende overval: het stelen van goederen van UPS doormiddel van geweld en intimidatie.

4.2.3. Overzicht van incidenten in Nederland

In de onderstaande tabel is te zijn welke incidenten in de periode 2017 tot en met 2018 hebben plaatsgevonden binnen UPS centra in Nederland. Voor Tilburg is geen informatie meer beschikbaar aangezien dit center zal sluiten door de opening van de nieuwe locatie in Eindhoven.

Type incident	Categorie incident	Aantal x in Apeldoorn	Aantal x in Utrecht	Aantal x in Heereveen	Aantal x in Amsterdam	Aantal x in Eindhoven	Aantal x in Rotterdam
Diefstal uit een pakket	Oneerlijkheid	10	12	1	16	2	27
Diefstal van een pakket	Oneerlijkheid	20	10	1	35		3
Diefstal van geld	Oneerlijkheid				1		
Diefstal van bedrijfsmiddelen	Oneerlijkheid						
Diefstal van prive eigendommen	Oneerlijkheid						
Agressie	Oneerlijkheid						
Werknemers discipline	Oneerlijkheid						
Vandalisme	Oneerlijkheid						
Drugs en alcohol	Oneerlijkheid						
Medeweten van schuld	Oneerlijkheid						
Fraude met labels	Oneerlijkheid						
Onbevoegd openmaken van een pakket	Oneerlijkheid		6				5
Diefstal van voertuigen	Anders						

Inbraak in voertuigen	Anders						
Inbraak in een UPS locatie	Anders						
Informatie diefstal	Anders						
LDI onderzoeken	Anders	2	2	1	24		6
Gewapende overval	Anders						
Security bezorgdheden	Anders			1			1
Totaal:		32	30	4	76	2	42

Met het bovenstaande overzicht kunnen we aflezen dat de meest voorkomende incidenten zijn:

- Diefstal uit een pakket
- Diefstal van een pakket
- Werknemers discipline
- Onbevoegd openmaken van een pakket
- LDI onderzoeken

Ook valt op dat inbraken, vandalisme, overvallen en andere incidenten die vaak een extern karakter hebben niet of nauwelijks voorkomen. Qua maatregelen op basis van de incidenten zal de focus dan ook moeten liggen op diefstal en interne risico's.

4.2.4. Uitwerking interview met dhr. van Beusekom

Aanvullend is er bij deze deelvraag een interview afgenomen. Tijdens dit interview werd dhr. A. van Beusekom geïnterviewd. Dhr. van Beusekom is werkzaam bij de afdeling loss prevention (LP), deze afdeling onderzoekt en handelt de verschillende security incidenten af en registreert deze in de verschillende facility statistics sheets.

De meest schadelijke incidenten binnen UPS zijn inbraken in de verschillende voertuigen van UPS en diefstal van en uit pakketten binnen UPS package centra. De genoemde incidenten gebeuren regelmatig. Diefstal en inbraak uit bezorg voertuigen gebeurt wanneer de voertuigen zich buiten het center bevinden, dit kan zowel intern als extern zijn. Deze incidenten vallen niet onder de scope van het onderzoek maar geven wel een indicatie waar de risico's liggen, namelijk vooral diefstal.

Diefstal uit en van een pakket in de verschillende UPS package centra is ook een probleem en schadepost. Dit soort incidenten komt vaak voor en in het onderzoeken en het identificeren van de daders van deze incidenten gaat veel tijd zitten. Het voorkomen van deze incidenten is dan ook een belangrijk doel. Dhr. Beusekom gaf aan dat maatregelen om deze incidenten te voorkomen ook zijn geïmplementeerd binnen UPS. Voorbeelden van deze maatregelen zijn camera's, visitatie en een hoge waarden kooi (highvalue cage).

Camera's hebben een afschrikkend effect en kunnen bijdragen aan de opsporing van daders. Visitatie schrikt ook af en kan gestolen goederen onderscheppen, echter is dit wel een duurde maatregel aangezien er mankracht voor vrijgemaakt worden. De hoge waarden kooi wordt gebruikt om hoge risico goederen met veel waarde van grotere klanten op te slaan (denk aan Apple en Dell), op deze

manier hoeven goederen met hogere waarde waar een risico factor aan zit niet over de lopende baan en wordt het risico's dat het pakket word gestolen minder.

Andere maatregelen zoals een hekwerk, access control en een alarmsysteem staan buiten kijf en zullen dus tot minimale eisen moeten behoren.

Incidenten met hogere impact zoals bedreigingen en geweld komen zelden tot nooit voor en het is tevens lastig hier maatregelen tegen te treffen. Grote incidenten, zoals het naar buiten smokkelen van hele pakketten komen ook voor, hier zijn wel maatregelen tegen te treffen.

Verder gaf dhr. Beusekom aan dat in de nieuwe vestigingen (Utrecht en Eindhoven) meer wordt geïnvesteerd in nieuwe maatregelen. Vooral op het gebied van visitatie worden er gekeken wat er mogelijk is, aangezien er wel ruimte voor moet zijn binnen een nieuw center. Dit sluit aan bij wat dhr. Houter vertelde, namelijk de ambitie om op iedere locatie een beveiliger te hebben die visitatie kan uitvoeren indien nodig.

Tot slot is besproken dat er geen incidenten zijn als inbraak in een UPS pand zelf, hierop werd bevestigd dat dit al heel lang niet is voorgekomen. Ook zijn er geen containers opengemaakt die geparkeerd stonden op de yard. Wel zijn er organisatorische maatregelen omtrent het stallen van containers, deze worden namelijk zoveel mogelijk binnen gezet, geparkeerd op een beveiligde yard of zodanig geplaatst dat het bijna onmogelijk wordt om een volle container te stelen.

4.2.5. Voorlopige conclusie

Er kan, gekeken naar de incidenten en het interview met dhr. van Beusekom, worden geconcludeerd dat de incidenten die zich voordoen binnen UPS package centra in Nederland vooral diefstal en loss incidenten omvat. Hierdoor kan er worden gesteld dat het terugdringen en voorkomen van deze incidenten als prioriteit kan worden gezien. Doordat veel van deze diefstal intern gebeurt zal er aanvullend gekeken kunnen worden naar organisatorische maatregelen omtrent het verwerven van nieuw personeel.

4.3. Resultaten deelvraag 3

"Wat zijn de beveiligingsrisico's voor huidige en toekomstige UPS centra?"

4.3.1. Inleiding

Tijdens de vorige deelvraag zijn er al een aantal incidenten en dus risico's naar voren gekomen waarmee rekening gehouden zal moeten worden. Bij deze deelvraag zal er worden gekeken naar de risico's die de package centers van UPS nog meer lopen. Hierbij zal worden gekeken naar de risico analyses/risk assessments die UPS intern heeft uitgevoerd, door middel van deze risico analyses kan er worden gekeken welke risico's moeten worden meegenomen en vervolgens gemitigeerd in de uiteindelijk aanbevolen security standaard.

Aanvullend zal er door middel van interviews worden gekeken naar welke beveiligingsdoelen er zijn in een UPS package center. Beveiligingsdoelen zijn over het algemeen afhankelijkheden. Gezocht wordt naar die elementen van de organisatie die bij emissie, uitval, manipulatie of iets dergelijks de organisatie of de omgeving van de organisatie (grote) schade berokkenen. Daarbij kan het gaan om verschillende soorten schade: economische schade (geld, uren uitval), schade aan personen (doden of gewonden), schade aan het milieu (bijvoorbeeld door het lekken van een buisleiding) en schade aan imago (NAVI,2008).

4.3.2. Riskassessments

UPS Nederland heeft interne riskassessments, deze worden jaarlijks uitgevoerd door de security afdeling. De UPS riskassessments hebben veel overlapping met de Waarschijnlijkheid-impact-matrix uit de NAVI handreiking (NAVI, 2008). Zo kijken beide naar de impact en waarschijnlijkheid van verschillende risico's die UPS heeft vastgesteld. Door te kijken naar de reeds vastgestelde risico wegingen en het maken van een algemene risico analyse die alle package centra behelst kunnen dreigingen en beveiligingsdoelen worden vastgesteld, deze kunnen vervolgens in het advies worden verwerkt.

In het kort: UPS heeft een aantal scenario's vastgesteld, per scenario word gekeken hoe waarschijnlijk het is dat het zich voordoet, dit kan uitlopen van onwaarschijnlijk tot bijna zeker. Vervolgens wordt gekeken naar de impact dat het desbetreffende incident zou kunnen hebben, wat kan uitlopen van onbelangrijk naar catastrofistisch. Vervolgens wordt er in de hiernaast afgebeelde tabel afgelezen wat het risico van het scenario is en wordt een cijfer toegekend, hoe hoger het cijfer des te meer reden om maatregelen te treffen om het te voorkomen. In de bijlage een overzicht van de verschillende riskassessments.

Facility Assessment Scoring Guide

		Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
Probability / Likelihood	Remote	1	2	3	4	5 (Low)
	Rare	2	3	4	5 (Low)	6 (Low)
	Unlikely	3	4	5 (Low)	6 (Low)	7 (Moderate)
	Possible	4	5 (Low)	6 (Low)	7 (Moderate)	8 (Moderate)
	Likely	5 (Low)	6 (Low)	7 (Moderate)	8 (Moderate)	9 (High)
	Almost Certain	6 (Low)	7 (Moderate)	8 (Moderate)	9 (High)	10 (Extreme)

Hieronder zijn de 15 scenario's te zien die UPS heeft opgesteld in haar riskassessment, ook is af te lezen welk cijfer deze risico's scoren en tot slot is af te lezen wat het gemiddelde cijfer is van alle centra bij elkaar. In *bijlage 7* zijn de losse riskassessments per center terug te vinden.

	Pilferage	Package theft	Currency theft	Theft of company assets	Assault on employee with weapon	Assault on employee with without weapon	Building break in	Vehicle theft	Trailer theft	Cargo theft	Organiz-ed crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Amsterdam	7	7	2	4	6	7	8	8	8	8	6	5	7	7	3
Apeldoorn	7	8	2	4	7	6	8	8	8	8	8	7	7	7	5
Eindhoven	7	6	3	4	5	5	6	5	7	7	5	3	9	7	3
Heerenveen	4	4	3	1	1	1	7	8	8	7	5	6	6	8	6
Rotterdam	7	7	2	4	7	7	8	8	8	8	5	6	7	8	5
Utrecht	7	8	2	4	7	6	8	8	8	8	8	7	7	7	5
Gemiddelde	6.5	6,7	2,3	3,5	5,5	5,3	7,5	7,5	7,8	7,7	6,2	5,7	7,2	7,3	4,5

4.3.3. Algemene risico analyse

Aanvullend is er een algemene risico analyse uitgevoerd die op alle package centra in Nederland is toegespitst. Hierbij is wederom gekeken naar de waarschijnlijkheid en de impact.

Risk	Probabillity/likelyhood		Impact		Rating
Pilferage	Almost Certain	Als we kijken naar de facility statistics kan er worden geconcludeerd dat de kans dat er diefstal uit een pakket zeer hoog is.	Moderate	Kleine meetbare impact op het merk UPS, operaties, aansprakelijkheid. Kan impact hebben op de lokale operatie, door toename van kosten en management aandacht. En kan een negatief effect hebben op klanten in de regio (imago schade)	8
Package theft	Almost Certain	Als we kijken naar de facility statistics kan er worden geconcludeerd dat de kans dat er diefstal van een pakket zeer hoog is.	Moderate	Kleine meetbare impact op het merk UPS, operaties, aansprakelijkheid. Kan impact hebben op de lokale operatie, door toename van kosten en management aandacht. En kan een negatief effect hebben op klanten in de	8

				regio (imago schade)	
Currency theft	Possible	Is eerder voorgekomen, mogelijkheid dat dit weer zou kunnen gebeuren.	Moderate	Geen tot weinig impact op het merk UPS, mogelijke verstoring van de operatie en verlies van omzet.	6
Theft of company assets	Possible	De mogelijk bestaat dat vijandige actoren bedrijfsmiddelen van UPS stelen.	Moderade	Geen tot weinig impact op het merk UPS, mogelijke verstoring van de operatie en kosten voor het vervangen van de gestolen assets.	6
Assault on employee with a weapon	Unlikely	Geweld tegen medewerkers (door buitenstaanders of collega's) is altijd een mogelijkheid. De kans dat dit met een wapen gebeurt is echter klein.	Major	Gevaar voor medewerkers, verstoring van de lokale operatie, slechte publiciteit voor het merk UPS, eventuele juridische kosten en aandacht.	6
Assault on employee without weapon	Possible	Geweld tegen werknemers (door buitenstaanders of collega's) is altijd een mogelijkheid.	Moderate	Gevaar voor medewerkers, verstoring van de lokale operatie, eventuele juridische gevolgen.	6
Building break in	Possible	Inbraak is altijd een gevaar, in UPS centra liggen genoeg goederen en assets om te stelen. Hierdoor is inbraak een mogelijkheid.	Major	Impact op de lokale operatie door extra kosten (reparatie, vermiste goederen, verstoring van processen) wat leidt tot verlies van omzet. Ook kan het merk UPS imago schade oplopen.	7
Vehicle theft	Possible	Het is mogelijk voor een	Major	Grote impact op de operatie,	7

		insluiper om een UPS voertuig te stelen.		aansprakelijkheid en omzet. Verlies van goederen en bedrijfsmiddelen. Negatief effect op klanten en dus imagoschade.	
Trailer theft	Possible	Net als bij voertuigen is het ook mogelijk voor potentiele aanvallers een trailer met goederen van een UPS terrein te stelen.	Catastrophic	Grote impact op de operatie, aansprakelijkheid en zeer hoog verlies omzet. Verlies van goederen en bedrijfsmiddelen. Negatief effect op klanten, mogelijk ook grote klanten wat leidt tot imagoschade en mogelijk verlies van klanten.	8
Cargo theft	Possible	Het is mogelijk dat er goederen die in een center staan worden gestolen wanneer er onvoldoende toezicht is op welke personen komen lossen.	Major	Verlies van bijvoorbeeld een pallet of andere grote hoeveelheden goederen zal leiden tot een groot verlies van omzet, aansprakelijkheid en hoogst waarschijnlijk een ontevreden grote klant.	7
Organized crime theft	Possible	De bovenstaande drie risico's kunnen allen uitgevoerd worden door georganiseerde bendes aangezien de waarde snel kan oplopen. Hierdoor kan er worden geconcludeerd dat dit risico mogelijk is.	Major	Grote impact op de operatie, aansprakelijkheid en zeer hoog verlies omzet. Verlies van goederen en bedrijfsmiddelen. Negatief effect op klanten, mogelijk ook grote klanten wat leidt tot imagoschade en mogelijk verlies van klanten.	7

Vandalism to facility or vehicles	Possible	Uit de facility statistics komen geen gevallen van vandalisme naar voren. Wel bestaat de kans dat dit gebeurt mocht iemand de kans krijgen op het terrein of zelfs in het gebouw te komen.	Moderate	Meetbare impact op de dagelijkse operaties. Kan impact hebben op de lokale operatie, door toename van kosten en dus afname van winst en kan aanvullende management aandacht innemen.	6
Terrorism	Remote	Hoogst onwaarschijnlijk dat terroristen een UPS package center zullen aanvallen.	Catastrophic	Verlies van levens, grote verstoring van de operatie, grote imagoschade voor UPS in zijn geheel.	5
Armed Robbery	Rare	Onwaarschijnlijk dat er een gewapende overval op een UPS center zal worden gepleegd. De mogelijkheid is echter niet uit te sluiten aangezien er veel cash geld in het gebouw is na kantooruren en er in sommige gevallen goederen met veel waarde in het pand aanwezig zijn.	Major	Gevaar voor medewerkers, verlies van omzet, Verstoring van de operatie, imageschade.	5
Other Property Compromise	Likely	Diefstal van medewerkers binnen UPS is altijd een mogelijkheid.	Minor	Geen tot weinig impact op het merk UPS, operaties, aansprakelijkheid.	6

Aan de riskassessments per center en de algemene riskassessment is af te leiden dat de primaire risico's pilferage, package theft, building break in, vehicle theft, trailer theft, cargo theft en armed robbery zijn, deze scoren boven zes en hebben dus een gemiddeld of hoger risico. Andere risico's waar rekening gehouden mee moet worden zijn: assault on employees, organized crime en vandalism, deze hebben een laag risico maar moeten wel in acht genomen worden.

4.3.4. Uitwerking interviews beveiligingsdoelen

Aanvullend zijn er bij deze deelvraag een aantal interviews afgenomen. Tijdens deze interviews zal er worden gesproken over de verschillende processen binnen een UPS package center om een goed beeld te krijgen van de verschillende assets die hiervoor nodig zijn. Ook zal er worden gekeken naar de kritieke assets, dit zijn assets die UPS nodig heeft om haar primaire proces door te laten gaan. Tot slot wordt er naar de persoonlijke mening omtrent een aantal aanvullende topics, met name persoonlijke ervaringen en inzichten gekeken. Hieronder zullen kort de belangrijkste punten uit de gesprekken worden benoemd.

Interview Dhr. Bliek

Het eerste interview was met dhr. Bliek, de UPS centrum manager van het center in Rotterdam. Zijn functie houdt in dat hij ervoor moet zorgen dat zijn werknemers een goede en veilige werkomgeving hebben en dat de gestelde management doelen worden bereikt, dit doet hij uiteraard samen met zijn team.

De primaire processen van een UPS package center zijn te verdelen in twee groepen, namelijk de pre-load en de re-load. De pre-load is het ochtend proces en start om 4 uur. Volume komt binnen van de verschillende hubs en worden vervolgens onderverdeeld over de verschillende UPS voertuigen om bezorgd te worden. De re-load begint aan het begin van de avond en verwerkt het externe volume. Dit volume wordt gesorteerd aan de hand van de postcodes en doorgestuurd naar het volgende package center of hub.

De assets die hiervoor nodig zijn de metro's, bij uitval van de metro's zal het hele sorteer proces ernstige vertraging oplopen omdat alles dan met de hand naar de containers getild zal moeten worden. Werknemers zelf zijn natuurlijk assets. DWS machine is een asset, deze meet het gewicht en afmetingen van pakketten op de baan. Dit zorgt ervoor dat klanten niet kunnen sjoemelen met gewicht en afmetingen. Dit maakt de DWS machine de cashcow van UPS. Scanners om het volume te tracken dus weten waar een pakket zich bevindt. De kluis voor de chauffeurs waar ze het cash geld afgeven is ook een belangrijke asset aangezien het geld dat de chauffeurs mee terug nemen hierin wordt opgeslagen en geteld. De kluis word iedere dag door een geldtransporteur opgehaald. Ook is de kluis belangrijk om fraude tegen te gaan door het geld te tellen en te controleren op echtheid.

Binnen een center zijn ook ondersteunende processen, deze zijn:
Centerteam - behandelt alle klachten/zorgen die binnenkomen van klanten
Personal Complaints - behandelt klachten over werknemers
Dispatcher - zorgt voor de planning van de chauffeurs
Finance - betalen van rekeningen en het verwerken van andere financiële transacties
Hold-cage - verwerkt en corrigeert gegevens die foutief op pakketten staan of waarvan de klant een wijziging heeft verzocht
Automotive - verzorgt onderhoud van de verschillende voertuigen
Export - verzorgt de documenten die nodig zijn voor het versturen van een pakket naar niet EU lidstaten.
Health and safety - verzorgt veiligheid binnen een center

Voor de ondersteunde processen zijn vooral de telefoon en de computer zeer belangrijk, zonder deze kun je immers niet je klanten bereiken of wijzigingen doorvoeren in het systeem, kortom kantoorassets zijn van belang.

Interview dhr. P. Peters
Dhr. (Paul) Peters is de operations supervisor van de re-load in het UPS center in Apeldoorn. Dit houdt in dat hij de sortering in de avond monitort en verantwoordelijk is voor het verloop hiervan.

Dhr. Peters gaf, net zoals zijn collega in Rotterdam, aan dat het primaire proces binnen de UPS operatie het verwerken van pakketten is zodat deze op tijd bij de klant aankomen. Dit houdt in dat deze verwerkt moeten worden tijdens de pre-load en re-load om de pakketten naar het volgende center of hub te krijgen.

De assets die hiervoor cruciaal zijn het personeel en de lopende baan. En zelfs zonder lopende baan zou het proces kunnen doorgaan al dan niet met veel moeite en vertraging. Over de DWS machine en scanners geeft dhr. Peters aan dat de operatie zonder deze ook door zou kunnen gaan, dit zal wel ten koste gaan van service richting de klant en de omzet. Omdat UPS zonder te scannen geen duidelijk beeld heeft waar pakketten zich bevinden en de afmetingen en het gewicht van de pakketten niet kan worden gecontroleerd.

Ondersteunende processen zijn wederom de kantoor processen die de operatie ondersteunen zoals HR, PE, LP, finance en de automotive shop. Hier zijn uiteraard de benodigde kantoorartikelen voor nodig. Ook de cashcountermachine is hier ondersteunend in, deze hoeft echter niet als kritiek asset gezien te worden omdat er back up plannen voor bestaan en het geld tel proces gewoon doorgang kan vinden wanneer de machine niet zou functioneren.

Dhr. Peters gaf in het interview aan dat hij fysieke beveiligers zou toe juichen. Dit omdat er op dit moment weinig controle is wie het centrum betreden, mede door het grote verloop van uitzendkrachten is er weinig zicht op wie het pand binnenkomt en met welke reden. Hierbij komt het feit dat er regelmatig pakketten verdwijnen wat in veel gevallen als oorzaak diefstal heeft. Ook hierbij zou een beveiliger kunnen helpen dit probleem terug te dringen door middel van bijvoorbeeld visitatie om zo diefstal tegen te gaan. Tot slot heeft een beveiliger een afschrikkend effect. Dhr. Peters gaf aan dat hij dit uit eigen ervaring weet door zijn tijd als supervisor bij het centrum Tilburg dat een beveiliger aantoonbaar effect heeft.

Het gebrek aan security awareness word ook gezien als een probleem. De combinatie van het verhogen van awareness en het inzetten van een fysieke beveiliger verhoogd het niveau van beveiliging.

Interview met dhr. R. Kinds
Er is ook een interview gehouden met dhr. (Rudy) Kinds. Hij is Aviation Security Officer binnen de BeNeLux UPS Aviation Security Department, dit houdt in dat hij zich bezig houdt met de luchtvracht die gesorteerd wordt binnen de Benelux. Het doel van dit gesprek was meer te weten te komen over de luchtvracht, screening hiervan en de eisen die hiervoor gelden omtrent het screening gebied ook wel de Keulenkooi genoemd.

UPS is erkend vluchtwacht agent, wat inhoudt dat UPS vracht mag screenen, deze vracht mag vervolgens via de lucht worden vervoerd. Deze screening gebeurt in de verschillende designated screening area's van UPS. De eisen die hieraan zijn verbonden worden door de Europese Unie vastgesteld en zijn terug te vinden in de verordeningen EU 300/2008, EU 272/2009 en EU 2015/1998.

Ook is er Nederlandse regelgeving, deze is te vinden in de luchtvaart wet art 37 en de uitvoering beveiliging burgerluchtvaart uit 2010.

In 2010 is UPS opgeschrikt door een incident waarbij terroristische actoren twee pakketten die explosieven bevatten probeerden te versturen om daarmee passagiersvliegtuigen op te blazen. Gelukkig konden de twee pakketten worden onderschept. Dit is voor UPS een reden geweest om pakketten beter te screenen.

Screening van pakketten gebeurt gescheiden van de rest van de vracht, dit houdt in dat er een scheiding word gemaakt tussen standaard vracht en luchtvracht. Een erkend luchtvaartagent mag deze scheiding zelf invullen. Het doel van de screening is het voorkomen van manipulatie en het onderscheppen van explosieven. Dit gebeurt doormiddel van X-Ray en honden.

Op dit moment mag de erkend luchtvaartagent zelf bepalen hoe de scheiding tussen standaardvracht en luchtvracht worden gegarandeerd. Dit zou in theorie een krijtstreep op de grond kunnen zijn. UPS acht dit echter niet wenselijk en daarom worden hiervoor kooi constructies geplaatst om zo een fysiek gescheiden screening area te creëren.

Dhr. Kinds gaf ook aan dat het toevoegen van een tourniquet aan de kooiconstructies een goede additie zou zijn. Dit zou min of meer garanderen dat het screeningproces niet wordt verstoord door personen die geen toestemming hebben om de screening area te betreden. Wanneer dit zou gebeuren is de screening keten doorbroken wat zou betekenen dat alle pakketten opnieuw moeten worden gescreend, hetgeen weer tijd en geld kost.

4.3.5. Voorlopige conclusie

De primaire processen van UPS zijn in het package center de pre-load en re-load. Deze vinden in de loods plaats en daar bevinden de verschillende assets die hiervoor nodig zijn zich ook. Bijvoorbeeld de lopende band en DWS machine. Aanvullend op de primaire processen zijn de ondersteunende processen. Deze processen vinden voornamelijk plaats in het kantoor gedeelte van een package center. Aanvullend op deze processen heb je nog de luchtvracht screening en cashcounting ruimte, hier zijn aanvullende eisen gesteld omtrent beveiliging en deze zullen dan ook apart moeten worden bekeken.

Omtrent dreigingen zijn diefstal van en uit pakketten een groot risico dat aandacht verdient, dit komt overeen met het beeld dat in de vorige deelvraag werd geschetst. Een goede manier om deze risico’s tegen te gaan is exit controle, om zo diefstal terug te dringen. Ook kunnen camera’s bijdragen aan het pakken van daders zoals dhr. van Beusekom aangaf. Aanvullende risico’s zijn inbraak en diefstal van een trailer of ander UPS voertuig. Om deze risico’s te mitigeren zal er dan ook moeten worden gekeken naar goede beveiliging van de buitenschil van het terrein en de buitenschil van het center zelf. Andere risico’s met een hoge impact maar lage waarschijnlijkheid zijn terrorisme en een gewapende overval. Deze risico’s zijn echter lastiger te mitigeren.

4.4. Resultaten deelvraag 4

"Welke maatregelen moeten uit deze risico's en incidenten voortkomen om deze te mitigeren?"

4.4.1. Inleiding

In dit hoofdstuk zal worden gekeken naar welke maatregelen voort moeten vloeien uit de verschillende security assessments risico's en incidenten om deze hierdoor zo goed mogelijk te kunnen mitigeren en zo trachten te voorkomen dat een ongewenste gebeurtenis zich voor doet. Hiervoor zal gebruikt worden gemaakt van de Bow-Tie methode.

Zoals eerder is toegelicht is de Bow-Tie methode een kwalitatieve methode waarmee op een systematische wijze een beeld kan worden geschetst van de risico's die in een organisatie aanwezig zijn en van de preventieve- en beschermingsmaatregelen die hierop (kunnen) worden ingezet. In het model staan de risico's, bedreigingen en maatregelen. In het midden staat het incident, links hiervan de oorzaken en rechts mogelijke gevolgen. De Maatregelen die tegen het incident kunnen worden getroffen staan als barrières.

Ook zal naar aanleiding van de observaties, gesprekken en literatuurstukken een verdeling gemaakt worden van secties en zones binnen een package center. Door deze verdeling te maken kan er per zone gekeken worden waar behoefte aan is. Vervolgens zal er worden aangegeven welke security maatregelen minimaal geïmplementeerd zullen moeten worden, wat aanbevolen wordt en wat uitmuntend zou zijn. Om vervolgens te toetsen of deze maatregelen de risico's mitigeren zullen Bow-Ties opgesteld worden.

4.4.2. Security zones

Een package center kan in verschillende zones worden verdeeld, door dit te doen kan er specifiek gekeken worden naar welke fysieke maatregelen er bij een bepaalde zone kunnen worden geïmplementeerd en welke nodig zijn. Zo is het bijvoorbeeld niet logisch camera's in een kantoor te hangen maar wel bij de entree. De onderverdeling komt er als volgt uit te zien:

- Outside
  - Omheining
  - Yard
- Indoors
  - Entrée
  - Kantoor
  - Loods
    - Dokken
    - Smalls-sortering
    - Unload-posities
  - Opslagruimten/opslagkooien
  - Serverruimte
  - Hold-cage
  - Value-cage
  - Customs-cage
  - Automotiveshop

- Speciale zones
    - Cashcounting room
    - Screening area

4.4.3. Outside

De eerste scheiding tussen het UPS terrein en de openbare weg is natuurlijk de **omheining**. Het is zaak ervoor te zorgen dat onbevoegden niet het terrein op kunnen komen. De manier om dit tegen te gaan is natuurlijk het implementeren van een goed hekwerk met een poort die afgesloten kan worden.
Minimaal: hekwerk dat het terrein afsluit met een poort voor UPS voertuigen, sloten op de verschillende ingangen
Aanbevolen: goede verlichting, elektrische/automatische poort, camera toezicht op de poort en eventueel andere ingangen, acces control op de poort en andere eventuele ingangen (elektrische poort met access control sluit aan bij de genoemde ambitie om toegangscontrole aangaande de feeders te monitoren vanuit Eindhoven)
Uitmuntend: CCTV die de hele omheining monitort

De **yard** is ook een te beschermen gebied. Hier staan doorgaans containers en UPS voertuigen. Goed toezicht is belangrijk en daarvoor zal er CCTV aanwezig moeten zijn.
Minimaal: CCTV toezicht, verlichting
Aanbevolen: Active infrarood detectie
Uitmuntend: n.v.t.

4.4.4. Indoors

De **entrée** is waar werknemers en bezoekers binnenkomen en vertrekken. Een cruciale plek als het gaat om monitoren wie er naar binnen gaat en wie weer vertrekt. Hier kunnen onbevoegden worden tegengehouden en kan er visitatie worden gedaan om diefstal tegen te gaan. Op dit moment wordt er in een aantal centers goed geregistreerd wie het pand binnenkomen, dit zijn: Utrecht, Eindhoven en sinds kort Rotterdam. Door middel van observaties en gesprekken kan er worden geconcludeerd dat de toegangscontrole in Apeldoorn en Amsterdam een wassen neus is, dit was voorheen ook het geval in Rotterdam maar sinds de verbouwing is de situatie verbeterd. Het verschil tussen Utrecht, Eindhoven, Rotterdam, Apeldoorn en Amsterdam is dat er bij de eerstgenoemde een fysieke beveiliger aanwezig is. Hierdoor is er een veel beter beeld van wie er binnenkomt en vertrekt. Ook draagt dit aantoonbaar bij aan het verminderen van diefstal door middel van visitaties. Een mogelijkheid is dan ook om bij alle package centra in Nederland met een beveiliger te gaan werken. Dit heeft zoals eerder genoemd meerdere voordelen en verhoogt de algemene veiligheid van een center.
Minimaal: CCTV, Access control doormiddel van een kaartlezer op de deur, IDS, sloten op buitendeuren
Aanbevolen: fysieke beveiliger, tourniquet met kaartlezer
Uitmuntend: X-Ray of metaal detector voor exit controle

Het **kantoor** is de plek waar de meeste ondersteunende processen plaatsvinden. Het is dan ook zaak om ervoor te zorgen dat hier geen personen binnentreden die daar niets te zoeken hebben. De simpelste oplossing hiervoor is een kaartlezer op de deur(en) te plaatsen.
Minimaal: Access control door middel van een kaartlezer op de deur, IDS indien een ruimte in het kantoor gebied aan de buitenmuur grenst en er een raam of andere zwakke plek aanwezig is.
Aanbevolen: CCTV gericht op de ingang van het kantoorgebied
Uitmuntend: n.v.t.

Loods, de loods is de plaats waar de primaire processen plaatsvinden en waar tijdens uren dat er niemand in het pand aanwezig is volle containers of andere UPS voertuigen kunnen staan. Daarom is het van belang te zorgen dat er geen onbevoegden de loods binnenkomen en dat inbraak onmogelijk wordt gemaakt.
Minimaal: Access control door middel van een kaartlezer op de ingangen die naar de loods leiden, CCTV gericht op de verschillende ingangen en posities waar regelmatig mensen aan het werk zijn. IDS rond de buitenmuur bij ramen en andere zwakke punten, magneet contacten op de roldeuren.
Aanbevolen: Active infrarood detectie
Uitmuntend: n.v.t.
In de loods bevinden zich ook de verschillende dokken, smalls-sortering en andere unload-posities Voor de **smalls-sortering** en **unload-posities** is het verstandig hier camera's te plaatsen om zo toezicht te houden, diefstal te kunnen voorkomen en te gebruiken als hulpmiddel bij het onderzoeken van diefstal wanneer dit zich voordoet. Ook is het verstandig om te zorgen voor goede verlichting in verband met toezicht en verhoogde kwaliteit van camera beelden.
Aangaande de **dokken**.
Minimaal: magneet contacten op de verschillende dokdeuren, IDS, CCTV gericht op de dokdeuren en op het dok zelf voor meer overzicht, goede verlichting op het dok en gericht op de containers voor beter toezicht en betere camera beelden.
Aanbevolen: actieve of passieve infrarood detectie
Uitmuntend: n.v.t.

Opslagruimten/kooien worden gebruikt om assets op te slaan. Hierbij is het van belang dat niet iedereen toegang heeft tot deze ruimtes.
Minimaal: sloten op de deuren
Aanbevolen: kaartlezers op de deuren
Uitmuntend: CCTV toezicht indien mogelijk wanneer het gaat om een openkooi constructie of gericht op de ingang van de desbetreffende kooi of deur, passieve infrarood detectie

Serverruimte, het is natuurlijk van belang dat een serverruimte goed is afgesloten en niet toegankelijk is voor onbevoegden.
Minimaal: kaartlezer op de deur
Aanbevolen: IDS in de serverruimte
Uitmuntend: n.v.t.

Hold-cage, in de holdkooi worden pakketten vastgehouden en indien nodig aangepast. Hierdoor kan het voorkomen dat er waardevolle pakketten in de ruimte aanwezig zijn. Wederom is het van belang dat de toegang tot deze ruimte zoveel mogelijk gecontroleerd wordt.
Minimaal: sloten op de deur
Aanbevolen: kaartlezer op de deur, CCTV toezicht op de ingang
Uitmuntend: IDS in de ruimte

Value-cage
Minimaal: sloten op de deur
Aanbevolen: kaartlezer op de deur, CCTV toezicht op de ingang
Uitmuntend: IDS in de ruimte

Customs-cage, in de customscage worden pakketten vastgehouden die bestemd zijn voor de douane. Hierdoor kan het voorkomen dat er waardevolle pakketten in de ruimte aanwezig zijn. Ook hier is het van belang dat de toegang tot deze ruimte zoveel mogelijk gecontroleerd wordt.

Minimaal: sloten op de deur
Aanbevolen: kaartlezer op de deur, CCTV toezicht op de ingang
Uitmuntend: IDS in de ruimte

Automotiveshop, is de plek waar onderhoud aan de verschillende UPS voertuigen plaatsvindt. Dit gebied is vaak inpandig maar kan ook in een apart gebouw plaatsvinden.
Minimaal: n.v.t.
Aanbevolen: CCTV toezicht
Uitmuntend: n.v.t.

4.4.5. Speciale zones

Cashcounting ruimte, hier wordt het geld dat de chauffeurs overdag ontvangen geteld en opgeslagen totdat het wordt opgehaald door G4S. De eisen die aan deze ruimte worden gesteld komen van G4S en zullen dan ook meegenomen worden in de fysieke security standaard.
Minimaal: inpandige kamer niet grenzend aan een buitenmuur, geen ramen, slagvaste (binnen) muren gemetseld/gelijmd van gasbeton blokken of van minimaal 18mm dik houtplaat materiaal op stevig geraamte, CCTV t.b.v. process bewaking alsmede veiligheid van de mensen in de kamer, verlichting, deur die vanaf de binnenzijde afsluitbaar (schuifslot) is, spion in de deur om naar buiten te kunnen, IDS

Screeningarea hier wordt de screening van de luchtvracht uitgevoerd. Dit kan zijn door middel van getrainde honden of X-Ray's. Hiervoor zijn buiten een scheiding tussen normale vracht en luchtvracht geen regels aangaande fysieke eisen. Wel is er uit het gesprek met dhr. Kinds gebleken dat hij wel graag een aantal maatregelen zou zien.
Minimaal: kooiconstructie, deur met kaartlezer, CCTV toezicht
Aanbevolen: tourniquet met kaartlezer
Uitmuntend: n.v.t.

4.4.6. BowTies

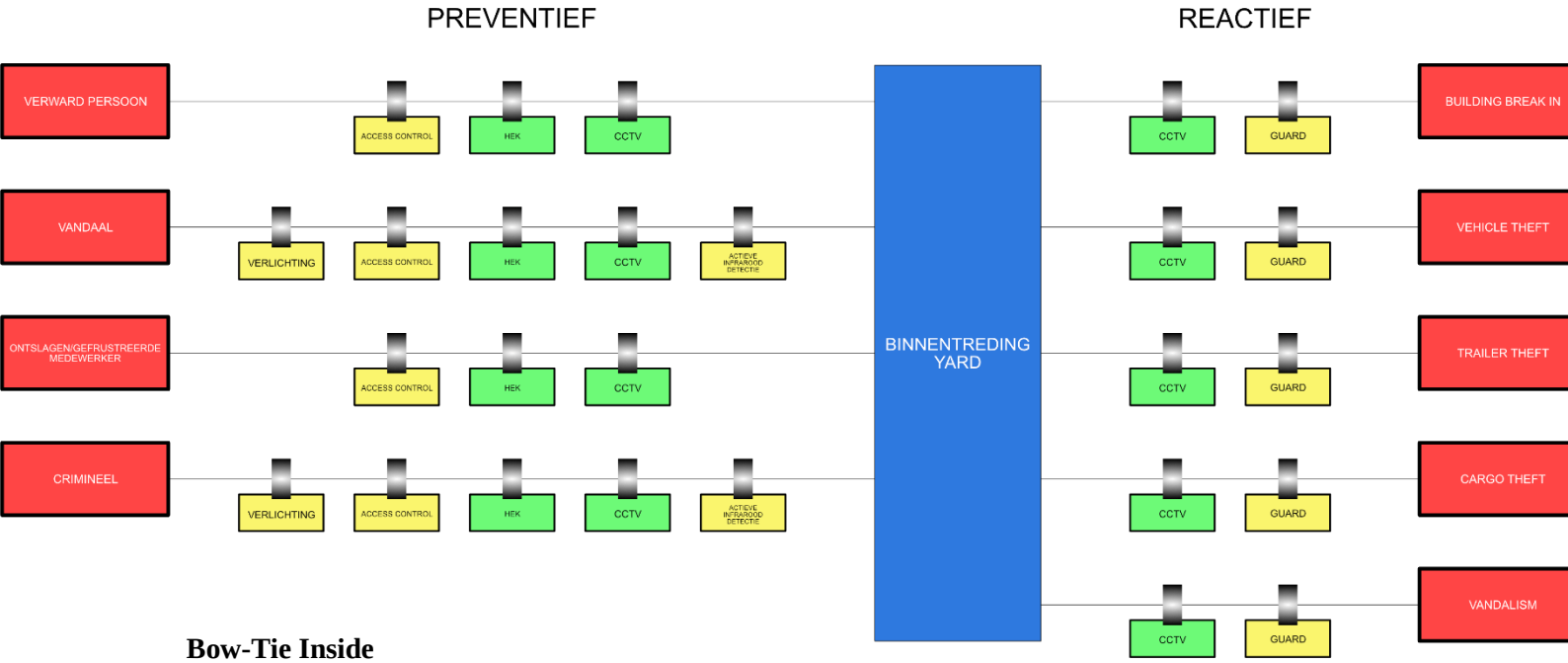
Hieronder zijn door middel van de Bow-Tie methode een aantal mogelijke dadergroepen en risico's weergegeven. Vervolgens is gekeken welke preventieve maatregelen kunnen worden getroffen om te voorkomen dat deze dadergroepen binnen kunnen treden binnen UPS. En, wanneer dit toch gebeurt, welke reactieve maatregelen hiervoor getroffen kunnen worden. Op deze manier kan een ongewenste gebeurtenis voorkomen worden.

De eerste Bow-Tie focust zich op de toegang van de yard. Hierbij is een aantal mogelijke dadertypen geselecteerd en zijn er een aantal gevolgen die het betreden van de yard zou kunnen hebben. Hierbij is het van belang om barrières op te werpen om onbevoegden van het terrein te weren. Zoals te zien is lukt dit door middel van hekwerken, en CCTV. Aanvullend is er access controle en infrarood detectie. Mocht iemand toch het terrein kunnen betreden is er CCTV om deze persoon te monitoren en te detecteren. Ook zou er een beveiliger kunnen worden ingezet om deze persoon gelijk te kunnen verwijderen.

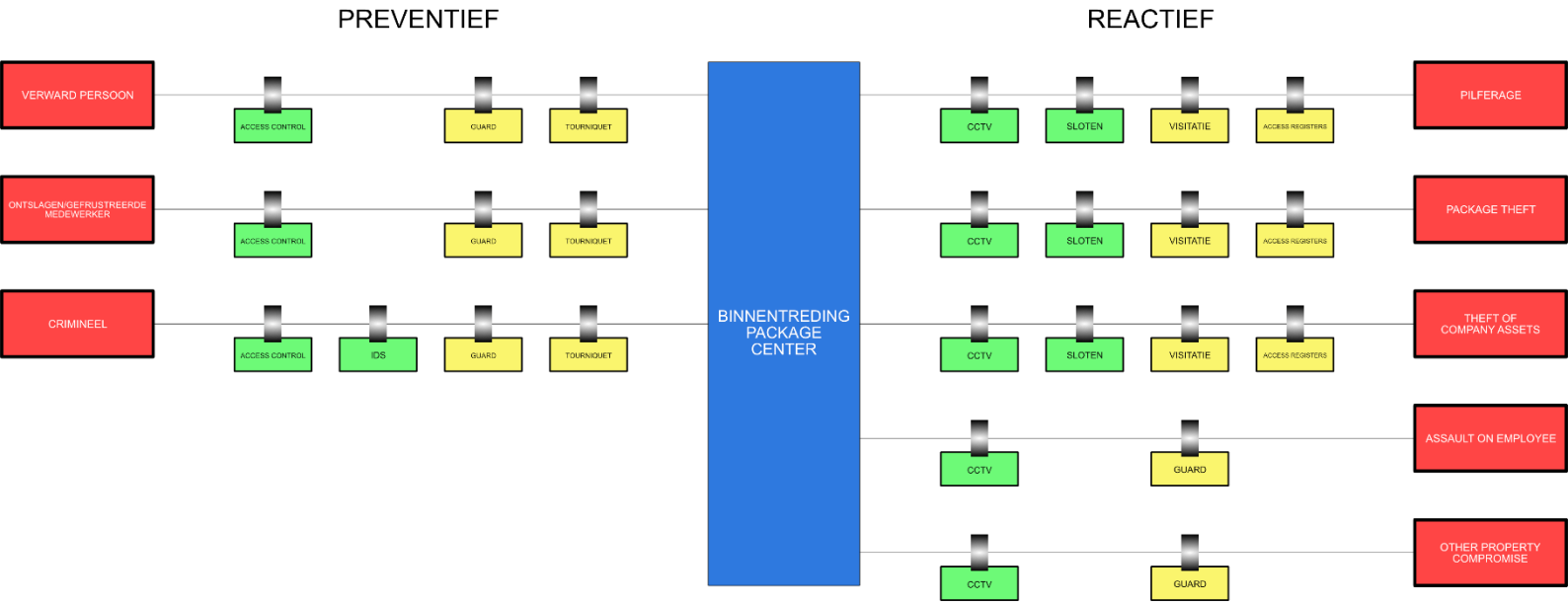
De tweede Bow-Tie focust zich op binnentreding van het pand zelf, ook hier is een aantal dadergroepen en mogelijke gevolgen vastgesteld. Wederom zijn er maatregelen geschetst die dit tegen moeten gaan. Zo is te zien dat access control en IDS de hoofdmaatregelen zijn om onbevoegden te weren. Ook zou een beveiliger hierbij kunnen ondersteunen om insluiping te ontmoedigen en access

controle uit te voeren. Mocht iemand toch binnen weten te treden, dan zijn CCTV, access control en registratie, sloten en exit visitatie mogelijke maatregelen om schade aan en voor UPS te voorkomen.

Bow-Tie Yard



Bow-Tie Inside



Deze twee Bow-Tie modellen tonen aan dat met de voorgestelde maatregelen zowel de buitenschil van het terrein als het pand zelf beveiligd zijn tegen het binnentreden van onbevoegden. Op deze manier is de security van het pand gewaarborgd en is de kans op incidenten minimaal.

5. Conclusie

5.1. Inleiding

In dit hoofdstuk zal antwoord worden gegeven op de onderzoeksvragen en probleemstelling. Deze conclusies zorgen ervoor dat er aanbevelingen gedaan kunnen worden en er een gedegen advies geleverd kan worden. Het advies is verder uitgewerkt in het advies hoofdstuk.

5.2. Antwoorden op de onderzoeksvragen

"Zijn er op dit moment standaard maatregelen op het gebied van fysieke beveiliging binnen UPS Nederland en wat houden deze maatregelen in?"

Op dit moment bestaat er geen Nederlandse standaard omtrent maatregelen die zich richten op de fysieke beveiliging van UPS package centra in Nederland. Wel bestaat er een corporate security beleidsdocument dat een aantal security maatregelen geeft. Dit is gedaan aan de hand van de corporate security matrix, deze matrix is ook toegevoegd aan de bijlage. Het corporate beleid van UPS wordt echter omschreven als ruw en gericht op security behoefte van de Verenigde Staten. Hierdoor wordt het corporate beleid dan ook meer gezien als een richtlijn in plaats van een bindende standaard.

Door de recente nieuwbouw projecten in Utrecht en Eindhoven en de uitbreiding van het center in Rotterdam is wel de behoefte aan een minimale fysieke standaard omtrent fysieke beveiliging naar voren gekomen. Ook is er al deels een minimaal security niveau toegepast.

Binnen UPS kunnen wel een aantal fysieke beveiligingsmaatregelen worden geïdentificeerd die bij alle of een aantal centra aanwezig zijn. Deze zijn: card access systemen, tourniquet, sloten, hekwerk, verlichting, metaal detectoren, X-Ray machines, CCTV, alarmsystemen, kluizen, beveiligers en magneet contacten. Van deze maatregelen zijn card access systemen, sloten, hekwerken, verlichting, CCTV, alarmsystemen en magneet contacten op de dokdeuren bij alle centra toegepast. Deze zouden kunnen worden gezien als de minimale standaard maatregelen.

"Wat zijn de belangrijkste security incidenten bij huidige UPS centra in Nederland?"

Uit de interviews en de bestudeerde literatuur in de vorm van de verschillende facility statistics die inzicht geven in de incidenten die voorvallen binnen de verschillende UPS centra in Nederland kan er worden geconcludeerd dat zich voornamelijk incidenten voordoen die betrekking hebben op diefstal uit en van pakketten. Ook kan er worden geconstateerd dat het aantal loss damage incidenten eruit springt, deze incidenten hoeven niet perse diefstal te behelzen.

Verder kan worden geconcludeerd dat incidenten die in bijna alle gevallen een extern karakter hebben zoals inbraak, vandalisme, overvallen en geweld zelden tot nooit voorkomen. Dit betekent echter niet dat dit geen risico's zijn voor UPS.

Concluderend kan er worden gesteld dat in de op te stellen minimale standaard rekening gehouden moet worden met interne risico's. Deze risico's behelzen vooral interne diefstal en verlies van pakketten.

“Wat zijn de beveiligingsrisico’s voor huidige en toekomstige UPS package centra?”

Voor de analyse van de beveiligingsrisico’s en beveiligingsdoelen is er gekeken naar de UPS riskassessments en is er intern gesproken met meerdere personen. Uit de verschillende risico analyses kan worden geconcludeerd dat de primaire risico’s pilferage, package theft, building break in, vehicle theft, trailer theft, cargo theft en armed robbery zijn. Andere risico’s waar rekening gehouden mee moet worden zijn: assault on employees, organized crime en vandalism. Bij de algemene risico analyse die vervolgens is uitgevoerd kwamen dezelfde resultaten naar voren. Deze risico’s zullen dus moeten worden gemitigeerd door middel van maatregelen, in dit geval fysieke maatregelen.

Door middel van gesprekken en interviews met supervisors en centermanagers is ook vastgesteld dat er twee primaire kern processen zijn te onderscheiden binnen een UPS package center, dit zijn de re-load en pre-load. De primaire assets die hierbij gebruikt worden zijn de metro/lopende baan, scanners en de DWS machine. De operatie kan echter wel doorgang vinden mochten deze assets wegvallen, dit gaat wel ten koste van de productiviteit. Voor de ondersteunde processen zijn vooral kantoor assets van belang. Er kan worden geconstateerd dat het risico dat de primaire en ondersteunende processen worden onderbroken klein is, wel is het gewenst om verstoring en verhoging van de werkdruk door het wegvallen van assets te mitigeren.

Tot slot is gebleken uit observaties en de verschillende gesprekken dat de security awareness binnen UPS centra niet altijd even hoog is bij medewerkers. Bij meerdere centra kon er zonder badge naar binnen worden gelopen of werd de onderzoeker zelfs binnengelaten, vervolgens werd er door niemand gevraagd wat de reden van mijn aanwezigheid in het pand was. Dit betekent niet dat niemand security aware is, maar het is wel goed om dit te benoemen. Tijdens de interviews werd het gebrek aan security awareness nogmaals door verschillende personen genoemd en bevestigd. Hoewel dit onderwerp niet onder het onderzoek valt is het wel goed om te benoemen, ook omdat dit een risico vormt voor UPS.

“Welke maatregelen moeten uit deze risico’s en incidenten voortkomen om deze te mitigeren?”

Nadat de verschillende dreigingen en risico’s voor UPS zijn geanalyseerd is er gekeken naar welke maatregelen hieruit voort moeten komen. Hierbij is een verdeling gemaakt van verschillende zones die in een UPS package centra te onderscheiden zijn, vervolgens is er per zone gekeken welke maatregelen minimaal aanwezig moeten zijn en welke maatregelen gewenst of aanbevolen zijn.

Er kan gesteld worden dat de minimale maatregelen die hieruit voorvloeien als volgt zijn:

- Hekwerk
- Verlichting
- CCTV
- Access control mechanismen
- Verlichting
- IDS
- Magneet contacten
- Sloten

Ook zijn er aan de hand van het onderzoek een aantal aanvullende aanbevolen maatregelen te onderscheiden, deze luiden als volgt:

- Actieve infrarood detectie
- Tourniquets
- Fysieke beveiliging

5.3. Antwoord op de probleemstelling

"Welke fysieke security maatregelen kunnen worden gestandaardiseerd om tot een nieuwe minimale securitystandaardisatie voor UPS package centra in Nederland te komen om zo de beveiliging te kunnen waarborgen?"

Overwegende dat er op dit moment fysieke security maatregelen bestaan die worden aangedragen door het corporate beleid, er verscheidene maatregelen bij alle package centra in Nederland zijn geïmplementeerd, er meerdere beveiligingsrisico's voor UPS package centra bestaan en verschillende security incidenten zich voordoen binnen de verschillende centra. Kan de conclusie worden getrokken dat er verschillende fysieke security maatregelen kunnen worden gestandaardiseerd om tot een minimale security standaard te komen en zo het security niveau van de verschillende centra op een minimaal niveau te brengen en te behouden.

Voor de buitenschil van een package centra is het volgende minimaal vereist: voldoende verlichting, hekwerk met een poort, afsluitbare in/uitgangen en CCTV toezicht.

Voor het pand zelf zijn de volgende maatregelen minimaal vereist: CCTV, access control mechanismen, IDS, magneet contacten op kritische deuren en op dok- en roldeuren. Tot slot is adequate verlichting vereist.

Deze maatregelen zijn het absolute minimum en zullen de beveiliging van UPS package centra in Nederland waarborgen wanneer deze worden geïmplementeerd. Wel houden de minimale maatregelen veel ruimte voor verbetering, daarom is er bij de aanbevolen minimale standaard een aanbevolen security niveau meegenomen.

6. Aanbevelingen

De aanbevelingen die gedaan worden aan de hand van het onderzoeksrapport zullen in de paragrafen hieronder toegelicht worden. De aanbevelingen zijn in feiten adviezen van de onderzoeker aan de opdrachtgeven om een fysieke security standaard te creëren en deze toe te passen om de beveiliging van UPS package centra te verbeteren.

Aanbevolen algemene security regels:

- kritieke deuren, roldeuren en dokdeuren worden voorzien van magneetcontacten
- ruimten met ramen grenzend aan de buitenmuur worden voorzien van bewegingsmelders/IDS
- verplichting om UPS badges en bezoekers badges te dragen
- aanwezigheid van fysieke beveiligers bij UPS panden

Een aanbeveling is om met fysieke beveiligers te gaan werken. Dit kan op 24/7 basis, maar gezien het type incidenten en de reeds voorgestelde maatregelen is dit niet perse nodig. Logischer zou zijn om tijden operatie uren met fysieke beveiligers te werken, dit omdat er tijdens deze uren het grootste verloop is van arbeidskrachten en de meeste kans op diefstal. Het inzetten van beveiligers sluit ook aan bij de ambitie van de security afdeling van UPS en straalt meer professionaliteit uit. Ook is er geconstateerd dat een aantal supervisors en centermanagers deze ontwikkeling zouden toejuichen. Het implementeren van fysieke beveiligers bij de verschillende centra heeft meerdere voordelen, zo zal de toegangscontrole worden verbeterd, zal diefstal verminderd kunnen worden door middel van visitaties en zal het algehele security niveau stijgen. Het nadeel is natuurlijk de kosten. Hierin zal UPS een afweging moeten maken.

6.1. Nederlandse UPS package centra security standaard

De op de volgende pagina te vinden fysieke security standaard is aanbevolen, hierbij is zoals eerder in het document aangeven wat minimaal, aanbevolen en uitmuntend is. Er moet hierbij nogmaals vermeld worden dat minimaal echt de ondergrens is.

Outside	**Minimaal**	**Aanbevolen**	**Uitmuntend**
Omheining	·Hekwerk ·Poort ·Sloten op de verschillende toegangspunten	·Verlichting ·CCTV toezicht op toegangspunten ·Automatische poort ·Access controle bij toegangspunten	·CCTV toezicht op de gehele omheining
Yard	·CCTV toezicht ·Verlichting	·Active infrarood detectie	
Indoors			
Entrée	·CCTV toezicht ·Access control d.m.v. een kaartlezer ·IDS ·Sloten	·Fysieke beveiliger ·Tourniquet met kaartlezer	·X-Ray of metaaldetector
Kantoor	·Access control d.m.v. een kaartlezer ·IDS	·CCTV gericht op de toegangspunten	
Loods	·Access control d.m.v. een kaartlezer ·Magneetcontacten op de roldeuren ·CCTV gericht op de toegangspunten en drukke posities ·IDS	·Active infrarood detectie	
Smalls-sortering	·CCTV toezicht ·Verlichting		
Unload-posities	·CCTV toezicht ·Verlichting		
Dokken	·Magneetcontacten op de dokdeuren ·IDS ·CCTV toezicht ·Verlichting	·Active of passieve infrarood detectie	
Opslagruimten/kooien	·Sloten	·Access control d.m.v. een kaartlezer	·CCTV toezicht ·Passieve infrarood
Serverruimte	·Access control d.m.v. een kaartlezer	·IDS	

Hold-cage	·Sloten	·Access control d.m.v. een kaartlezer ·CCTV gericht op de toegangspunten	·IDS
Value-cage	·Sloten	·Access control d.m.v. een kaartlezer ·CCTV gericht op de toegangspunten	·IDS
Douane-kooi	·Sloten	·Access control d.m.v. een kaartlezer ·CCTV gericht op de toegangspunten	·IDS
Automotiveshop		·CCTV toezicht	
Speciale zones			
Cash counting ruimte	·Inpandige ruimte ·Geen ramen ·Slagvaste binnenmuren ·CCTV toezicht in de ruimte ·Verlichting ·Afsluitbare deur (van binnenuit) ·Spion in de deur ·IDS		
Screeningarea	·Kooiconstructie ·Access control d.m.v. een kaartlezer ·CCTV toezicht	·Tourniquet met kaartlezer	

7. Evaluatie en methodologische verantwoording

Tijdens het onderzoek zijn er punten geweest die goed zijn gegaan en die minder zijn gegaan. Vooral het begin van het onderzoek en de periode voor mijn operatie liepen stroef. Hieronder zijn de punten die goed en minder gingen toegelicht.

Het beantwoorden van de eerste onderzoeksvraag verliep in het begin zeer moeizaam door gebrek aan informatie en literatuur. Later werd dit beter na mate meer centra werden bezocht en meer stukken aangeleverd werden. Ook verschafte het interview veel goede bruikbare informatie. Uiteindelijk is de vraag goed beantwoord door middel van deskresearch, interviews en gesprekken en observaties.

Voor het in kaart brengen van de incidenten in kader van de tweede onderzoeksvraag is ook een afspraak gemaakt voor een interview en is er gekeken naar de verschillende documenten die er bestaan binnen UPS. Hierdoor is een goed beeld ontstaan van de verschillende type incidenten. Het was echter niet mogelijk om tot een goed beeld van de schade posten te komen omdat hier geen informatie over beschikbaar was. Wel is dit onderwerp naar voren gekomen in het interview. Uiteindelijk is geconcludeerd dat de schade van de incidenten geen invloed heeft op de minimale security maatregelen die een package center zou moeten hebben. Er kan echter wel naar gekeken worden wanneer men aanbevolen maatregelen zoals een fysieke beveiliger wil implementeren, op dat moment wordt het een kosten/baten analyse.

Voor de derde deelvraag werd gekeken naar dreigingen en beveiligingsdoelen. In de interviews kwam naar voren dat er weinig echt kritieke assets zijn, en dus minder primaire beveiligingsdoelen. Hierdoor kan worden geconcludeerd dat een goede buitenschil en goed beveiligd pand zouden volstaan als minimaal standaard. Ook qua dreigingen die in de risico analyses naar voren kwamen viel dit te concluderen. Door het spreken met de juiste personen binnen UPS en het bestuderen van up to date risico analyses en een algemene risico analyse uit te voeren is ook deze deelvraag goed beantwoord.

Bij laatste deelvraag lag te focus op welke maatregelen uit de incidenten en dreigingen voort zouden moeten komen. Hierbij werd vooral terug gevallen op de informatie uit de vorige deelvragen. Het verdelen van een UPS center in zones was een aanvulling die later werd gedaan om zo tot een betere aanbeveling te kunnen komen, een dergelijke verdeling bestond nog niet. Deze verdeling is gedaan aan de hand van gesprekken en observaties. Hierna is gekeken welke zone welke maatregelen vereiste, hierover zijn meerdere momenten van sparren geweest.

8. Literatuurlijst

Appelman, A. (2010). *Intergrale beveiliging.* Alphen aan den Rijn: Kluwer.

Biggelaar, S. v. (2004). Standaardisatie van alles: de laatste trend? *Compact*, 6.

Einstein, S., & Philpott, D. (2006). *The Integrated Physical Security Handbook.* St. Marys: Government Training Inc.

Finch, P. (2004). *Supply chain risk management.* Bingley: Emerald Group Publishing Limited.

GHOR Nederland. (2009, November 5). *Handreiking regionaal risicoprofiel.* Opgehaald van Instituut fysieke veiligheid: https://www.ifv.nl/kennisplein/Documents/20091105-Politie-NVBR-GHORNL-Coordinerend-Gemeentesecretarissen-Handreiking-Regionaal-Risicoprofiel.pdf

Harris, S. (2013). *CISSP*. Maidenhead: Mcgraw-Hill Education.

Homeland Security. (2013). *Partnering for Critical Infrastructure.* Opgehaald van Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

International Foundation for Protection Officers (IFPO). (2010). *The Professional Protection Officer.* Burlington: Elsevier Science & Technology.

Ivanovic, A. (2007). *CPTED: wat is het en hoe werkt het?* Opgehaald van Veilig ontwerp beheer: http://www.veilig-ontwerp-beheer.nl/publicaties/cpted-wat-is-het-en-hoe-werkt-het/view?searchterm=CPTED

Jakeman, & Talbot. (2009). *Security Risk Management Body of Knowledge.* New Jersey: Wiley.

Janicijevic, S., Claes, P., & Lengkeek, R. (2016). *Risicomanagement.* Groningen: Noordhoff Uitgevers.

Landoll, D. (2006). *The security risk assessment handbook.* New York: Auerbach Publications.

M. Verbart, R. G. (2013). *Risico's en risicobeheersing - Bouwstenen voor beleid.* Nijmegen: PO-Raad.

Marcus, J., & van Dam, N. (2012). *Een praktijkgerichte benadering van organisatie en management.* Groningen: Noordhoff Uitgevers B.V.

Mittelmeijer, M., & van Stratum, R. (2014). *Kijk op bedrijfsprocessen.* Groningen: Noordhoff Uitgevers B.V.

Nationaal Adviescentrum Vitale Infrastructuur (NAVI) . (2008). *Handreiking Risicoanalyse*. Nationaal Adviescentrum.

The Business Continuity Institute (BCI). (2018). *Good Practice Guidelines.* Berkshire: BCI.

van Alphen, W., & Verhage, D. (2015). *Handboek risicobeheersing; een stappenplan voor het maken van een RI&E.* Zeist: Kerckebosch.

9. Bijlage

Bijlage 1. Interview topics voor het gesprek met dhr. Houter (security afdeling)

1. Kunt u om te beginnen wat vertellen over de afdeling waar u werkt en wat u doet?
2. Bestaat er op dit moment bij UPS Nederland security beleid gericht op alleen UPS Nederland en wordt dit beleid ook actief gebruikt bij u werkzaamheden?
3. Recent zijn er twee nieuwe UPS locaties geopend, Eindhoven en Utrecht. Kunt u me vertellen over de rol die de security afdeling daarbij speelt en welke stappen daarbij worden doorlopen?
4. De afdeling word ingelicht dat er een nieuwe locatie komt, hoe wordt er vervolgens beslist welke security maatregelen voor deze nieuwe locatie getroffen gaan worden?
5. Is er op dit moment een fysieke security standaard die security maatregelen voordraagt of eisen stelt aan bestaande en toekomstige UPS centra in Nederland die word gebruikt?
6. Zo nee, zou zo'n document van nut kunnen zijn in de toekomst?
7. Naar welke factoren word er gekeken bij het plannen en nemen van fysieke maatregelen?
8. Worden er vanuit UPS duidelijke eisen gesteld op het gebied van fysieke beveiliging?
9. Op welke manier wordt er gekeken of de huidige maatregelen nog wel voldoen?
10. Wat zou verbeterd kunnen worden volgens u bij het security gereed maken van een UPS centra in de toekomst?
11. Zijn er dingen waar u tegenaan bent gelopen tijdens het security gereed maken van Eindhoven en Utrecht?

Bijlage 2. Interview topics voor het gesprek met dhr. A. van Beusekom (afdeling Loss Prevention)

1. Kunt u om te beginnen wat vertellen over de afdeling waar u werkt en wat u doet?
2. Wat voor soort incidenten ziet u veel binnen UPS centra in Nederland?
3. Kunt u kort toelichten wat deze incidenten inhouden?
4. Welke incidenten zijn het meest schadelijk voor UPS?
5. Welke incidenten zijn minder schadelijk voor UPS?
6. Uit cijfers blijkt dat diefstal van en uit pakketten veel voorkomt, ziet de security afdeling dit ook als grootste risico?
7. Welke maatregelen worden hiertegen getroffen?
8. Wat zijn grote security incidenten die u binnen UPS heeft meegemaakt?
9. Wat waren de voornaamste oorzaken van deze incidenten?
10. Wat is er na deze incidenten veranderd? Of is er niets veranderd?
11. Wat kunt u vertellen over de schade die de security incidenten bij de UPS package centra veroorzaken?
12. Welke schade word geaccepteerd en bij wat voor schade worden er extra stappen genomen?
13. Welke risico's die UPS package centra lopen worden geaccepteerd door de security afdeling?

Bijlage 3. Interview topics voor de gesprekken met dhr. A. Bliek (centrummanager Rotterdam) en dhr. P. Peters (operations supervisor Apeldoorn)

1. Kunt u om te beginnen iets vertellen over uw functie en wat uw functie inhoudt?
2. Kunt u kort vertellen welke processen er dagelijks plaatsvinden binnen een UPS package center?
3. Welke processen hiervan kunnen als primair worden aangeduid?
4. Welke assets/middelen zijn van vitaal belang voor deze processen? (Denk aan scanners, servers etc.)
5. Welke impact zou het hebben als deze primaire processen worden onderbroken? (verlies van inkomsten, reputatie schade etc.)
6. Welke processen kunnen als ondersteunend/secundair worden gezien?
7. Welke assets zijn van vitaal belang voor deze processen?
8. Welke impact zou het hebben als deze processen worden onderbroken?
9. Overlegt u met de security afdeling over de risico's voor uw centrum? Zo ja, heeft u ook een aandeel in de security risk assessment die wordt opgesteld?
10. Wat zijn in uw ogen de grootste beveiligingsrisico's voor de dagelijkse operatie?
11. De belangrijkste bedrijfsprocessen mogen natuurlijk niet worden verstoord en dit is dan ook een beveiligingsdoel, welke beveiligingsdoelen kunnen er in uw ogen nog meer gesteld worden?

Bijlage 4. Interview topics voor het gesprek met dhr. R. Kinds (aviation security officer)

1. Kunt u om te beginnen iets vertellen over uw functie en wat uw functie inhoudt?
2. Kunt u kort vertellen wat luchtvracht behelst binnen UPS?
3. Welke regelgeving geldt er voor de luchtvracht en screening van die vracht?
4. Welk orgaan stelt die regelgeving op?
5. Aan welke security eisen moet het screeninggebied ofwel Keulenkooi voldoen?

Aanvullende vragen kunnen tijdens het interview gesteld worden.

Bijlage 5. Checklist fysieke security maatregelen UPS centra.

Met deze checklist is per package center gekeken welke fysieke maatregelen er zijn geïmplementeerd, de resultaten zijn terug te vinden in de resultaten van deelvraag 1.

Center:			
Maatregel:	Aanwezig ja/nee	Opmerkingen:	
Card Access Systems			
Tourniquet			
Sloten			
Hekwerk			
Verlichting			
Metaal detectoren			
X-Ray machines			
CCTV systeem			
Electronic Alarm Systems			
Safes (cashcow machines)			
High value cage			
Beveiligers			
Passief infrarood 'gordijn'			
Magneet contacten (dokdeuren)			

Aanmerkingen die naar voren kwamen tijdens de observaties

-Rotterdam zal in maart metaaldetectoren krijgen.
-het alarmsysteem is aangesloten bij Securitas.
-tourniquets worden meegenomen in de planning wanneer er een center wordt verbouwd of wanneer er nieuwbouw plaatsvindt, mits er ruimte is om een tourniquet te plaatsen.
-deuren die als kritiek zijn aangemerkt hebben sloten met een veiligheidscertificaat of zijn voorzien van access controle.
-Amsterdam heeft geen moderne cashcow machine aangezien hier geen ruimte voor is in het pand.
-de UPS security technologie groep, gevestigd in Duitsland, ondersteunt in het technische aspect van de verschillende fysieke maatregelen. De afdeling onderhoudt bijvoorbeeld contracten met leveranciers van bijvoorbeeld camera's en alarmsystemen. Deze afdeling is hierdoor goed op de hoogte van de eisen die corporate stelt aan de verschillende security hardware.
-de laatste jaren is er een shift om fysieke beveiligers op locaties te krijgen, nadeel hiervan zijn de hoge kosten waardoor het moeilijker wordt om het management hierin mee te krijgen.

Bijlage 6. Corporate security matrix.

Corporate Security
Matrix Criteria

Print Date: 09 May 2018

REQ = Required
RCMD = Recommended
(blank) = Not Required

Facility Size	Facility Category	Hard Wall Constructed	Intrusion Alarm	CCTV (Camera System)	Access Control	High Value Cage	Walk-through Metal Detector Entrance	Walk-through Metal Detector Exit	Employee Lockers	Security Guard(s)	Perimeter Fence	Employees Own UPS ID	Drivers Own UPS ID	X-ray System	Fire Panel
SCS															
0 < 50,000 ft² / 0 < 5,000 m²	< = $250,000	REQ	REQ								REQ	REQ			REQ
0 < 50,000 ft² / 0 < 5,000 m²	$250,001 < = $1,000,000	REQ	REQ			REQ					REQ	REQ			REQ
0 < 50,000 ft² / 0 < 5,000 m²	$1,000,000 +	REQ	REQ	REQ		REQ					REQ	REQ			REQ
50,001 < 99,999 ft² / 5,001 < 10,000 m²	< = $250,000	REQ	REQ								REQ	REQ			REQ
50,001 < 99,999 ft² / 5,001 < 10,000 m²	$250,001 < = $1,000,000	REQ	REQ			REQ					REQ	REQ			REQ
50,001 < 99,999 ft² / 5,001 < 10,000 m²	$1,000,000 +	REQ	REQ	REQ		REQ					REQ	REQ			REQ
100,000+ ft² / 10,001+ m²	< = $250,000	REQ	REQ								REQ	REQ			REQ
100,000+ ft² / 10,001+ m²	$250,001 < = $1,000,000	REQ	REQ								REQ	REQ			REQ
100,000+ ft² / 10,001+ m²	$1,000,000 +	REQ	REQ	REQ		REQ		REQ			REQ	REQ			REQ
Container Freight Station (CFS)		REQ	REQ								REQ	REQ			REQ
Office Space ONLY Facility		REQ	REQ								REQ	REQ			REQ
PUDO		REQ	REQ	REQ							REQ	REQ			REQ
Transportation Hub		REQ	REQ	REQ							REQ	REQ			REQ
UPS															
	< = 249 people	REQ	RCMD							RCMD	REQ	REQ			REQ
	250 < = 749 people	REQ	REQ			REQ	REQ			REQ	REQ	REQ			REQ
	750 < = 999 people	REQ	REQ	REQ		REQ	REQ			REQ	REQ	REQ			REQ
	1000 < = 1999 people	REQ	REQ	REQ		REQ	REQ			REQ	REQ	REQ			REQ
	> = 2000 people	REQ	REQ	REQ		REQ	REQ			REQ	REQ	REQ	REQ		REQ

Bijlage 7. Facility Risk Assessments

Facility Assessment Scoring Guide

Probability / Likelihood		Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Remote	1	2	3	4	5 (Low)
	Rare	2	3	4	5 (Low)	6 (Low)
	Unlikely	3	4	5 (Low)	6 (Low)	7 (Moderate)
	Possible	4	5 (Low)	6 (Low)	7 (Moderate)	8 (Moderate)
	Likely	5 (Low)	6 (Low)	7 (Moderate)	8 (Moderate)	9 (High)
	Almost Certain	6 (Low)	7 (Moderate)	8 (Moderate)	9 (High)	10 (Extreme)

Facility Risk Assessment Scores

Facility Name: AMSTERDAM
Facility Mnemonic: AMS/3439
Facility Address: Deccaweg 8
1042 AD
AMSTERDAM

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**7**	**7**	**2**	**4**	**6**	**7**	**8**	**8**	**8**	**8**	**6**	**5**	**7**	**7**	**3**

Facility Name: Apeldoorn
Facility Mnemonic: NLAPO
Facility Address: Kleine Fluitersweg
251
7316 MX Apeldoorn

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**7**	**8**	**2**	**4**	**7**	**6**	**8**	**8**	**8**	**8**	**8**	**7**	**7**	**7**	**5**

Facility Name: UPS Eindhoven (SP)

Facility Mnemonic: NLEON

Facility Address: De Keten 2

5651 GJ Eindhoven

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**7**	**6**	**3**	**4**	**5**	**5**	**6**	**5**	**7**	**7**	**5**	**3**	**9**	**7**	**3**

Facility Name: UPS HEERENVEEN

Facility Mnemonic: NLHEE

Facility Address: VENUS 106 8448 GW

Heerenveen The Netherlands

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**4**	**4**	**3**	**1**	**1**	**1**	**7**	**8**	**8**	**7**	**5**	**6**	**6**	**8**	**6**

Facility Name: Rotterdam/Schiedam

Facility Mnemonic: idem NLRTT

Facility Address: Fortunaweg 70-72

3113 AN Scheidam/Rotterdam

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**7**	**7**	**2**	**4**	**7**	**7**	**8**	**8**	**8**	**8**	**5**	**6**	**7**	**8**	**5**

Facility Name: UTRECHT

Facility Mnemonic: NLUHT

Facility Address: Reactorweg 23-A

Utrecht NL

	Pilferage	Package Theft	Currency Theft	Theft of Company Assets	Assault on employee w/ weapon	Assault on employee w/o weapon	Building Break-in	Vehicle Theft	Trailer Theft	Cargo Theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Score	**7**	**8**	**2**	**4**	**7**	**6**	**8**	**8**	**8**	**8**	**8**	**7**	**7**	**7**	**5**

Gemiddelden van alle UPS package centra in Nederland

	Pilferage	Package theft	Currency theft	Theft of company assets	Assault on employee with weapon	Assault on employee without weapon	Building break in	Vehicle theft	Trailer theft	Cargo theft	Organized crime theft	Vandalism to facility or vehicles	Terrorism	Armed Robbery	Other Property Compromise
Amsterdam	7	7	2	4	6	7	8	8	8	8	6	5	7	7	3
Apeldoorn	7	8	2	4	7	6	8	8	8	8	8	7	7	7	5
Eindhoven	7	6	3	4	5	5	6	5	7	7	5	3	9	7	3
Heerenveen	4	4	3	1	1	1	7	8	8	7	5	6	6	8	6
Rotterdam	7	7	2	4	7	7	8	8	8	8	5	6	7	8	5
Utrecht	7	8	2	4	7	6	8	8	8	8	8	7	7	7	5
Gemiddelde	6.5	6,7	2,3	3,5	5,5	5,3	7,5	7,5	7,8	7,7	6,2	5,7	7,2	7,3	4,5