Hoe voorkom je gaten in de beveiliging van het warehouse?

Op 11 september 2001 werd de wereld opgeschrikt door vier terroristische aanslagen in de Verenigde Staten. Sindsdien zijn de beveiligingseisen wereldwijd flink opgeschroefd, met name in onze wereldwijd opererende supply chains. Twintig jaar later bestaat daarover nog altijd veel onduidelijkheid in de logistieke sector. Beveiligingsexperts Stijn Belt van logistiek adviesbureau Groenewout en Pascal Verbaten van Verbaten Security Consultancy geven aan hoe bedrijven alle beveiligingseisen kunnen vertalen naar concrete eisen waaraan hun warehouse moet voldoen.

Neem als voorbeeld een logistiek dienstverlener die aan een projectontwikkelaar vraagt om een nieuw warehouse te bouwen. De eerste vraag van de projectontwikkelaar gaat over de eisen waaraan het warehouse moet voldoen, onder meer op het gebied van beveiliging. Tegelijkertijd krijgt de logistiek dienstverlener van andere stakeholders vragen over de beveiliging van het nieuwe warehouse. Vragen van opdrachtgevers, van overheden, van verzekeraars, van douane-autoriteiten en van andere partners in de supply chain. Die vragen gaan over FSR, TAPA-A, -B of -C, over luchtvrachtbeveiliging, over het BORG-certificaat of over de AEO-status. Waar staan die termen voor? En wat betekenen die voor de concrete eisen waaraan het nieuwe warehouse moet voldoen?

Overzicht van beveiligingsstandaarden

De genoemde termen zijn voorbeelden van Nederlandse, Europese of wereldwijd geldende beveiligingsstandaarden. Wat zijn de belangrijkste beveiligingsstandaarden waarmee bedrijven in de logistiek te maken krijgen? Hieronder volgt een overzicht:

- TAPA (Transport Asset Protected Association): Internationale beveiligingsstandaard voor supply chains. Onderscheid in 3 certificeringen:
    - TSR TAPA (Trucking Security Requirements) 1, 2 of 3
    - FSR TAPA (Facility Security Requirements) A, B of C
    - PSR TAPA Parking Security Requirements level 1, 2- 3 of TAPA Partner

- BORG: Nederlandse standaard voor inbraakbeveiliging
- AEO (Authorised Economic Operator): Europese standaard voor douanegoederen
- GDP (Good Distribution Practice): Internationale standaard voor farmacie
- IATA (International Air Transport Association): Internationale standaard voor luchtvrachtbeveiliging
- ISPS (International Ship & Port Facility Security): Internationale standaard voor zeehavenbeveiliging
- FM / Marsh (eisenpakketten geformuleerd door grote verzekeraars)

Al deze standaarden zijn opgesteld door verschillende instanties met elk hun eigen insteek. Specialisten in inbraakbeveiliging hebben bijvoorbeeld onder de naam BORG richtlijnen geformuleerd, die aangeven hoe bedrijven zich kunnen wapenen tegen inbraak. De douane stelt eisen aan de logistieke keten die dienen als entrepot om zeker te stellen dat bedrijven de juiste importheffingen afdragen. De IATA hanteert weer andere verplichtingen om te voorkomen dat foute goederen in het vliegtuig belanden. En in de GDP staan aanvullende eisen aan de distributie en opslag van farmaceutische producten.

Fouten in de beveiliging

Wat beveiliging in de logistiek complex maakt, is dat de meeste standaarden alleen maar iets zeggen over een deel van de totale beveiliging. Zo eisen verzekeraars vaak een BORG-certificaat in de veronderstelling dat een pand volledig beveiligd is. Maar BORG zegt niets over toegangscontrole of camerabewaking. Soms spreken standaarden en regelgeving elkaar zelfs ronduit tegen. Een voorbeeldcase: een warehouse waarin de sleutel naast de vluchtdeur hing, simpelweg omdat de brandweer dat nu eenmaal eiste. Misschien is dat veilig in geval van een brand, maar het helpt niet om diefstal te voorkomen. De markt biedt andere oplossingen die aan alle eisen voldoen.

Omdat veel bedrijven het totaalplaatje van eisen en standaarden niet overzien, ontstaan fouten in de beveiliging. De facilitair manager denkt bijvoorbeeld dat hij het pand goed heeft beveiligd, maar heeft vaak geen grip op de dagelijkse operatie. Dan is de toegang voor bezoekers bijvoorbeeld afgeschermd met een tourniquet, maar staat twintig meter verderop de overheaddeur wagenwijd open. Ook ontbreekt vaak het overzicht over de hele keten. Met als gevolg dat het warehouse misschien goed beveiligd is, maar de supply chain zo lek is als een mandje. Veel standaarden zijn juist gefocust op beveiliging van de hele keten. Neem bijvoorbeeld luchtvracht: de zwakste schakel is vaak niet het vliegveld, maar het warehouse waarin de luchtvrachtcontainer wordt geladen.

De basis: het beveiligingsconcept

Hoe krijg je nu de beveiliging op orde? Als eerste is het zaak om de eisen en wensen van de hoofdrolspelers binnen het bedrijf met behulp van een (interne of externe) beveiligingsexpert te inventariseren. Daartoe horen niet alleen de logistiek directeur, maar ook de facilitair manager, de operationeel leidinggevende, de kwaliteitsbeheerder en de security manager. Op basis van hun input ontstaat een eerste beeld van de beveiligingsbehoefte. Waar gaan bijvoorbeeld de goederen naar binnen en naar buiten? Liggen in het warehouse douanegoederen of farmaceutische goederen? Wordt gebruik gemaakt van luchtvracht? Moeten alle goederen even goed beveiligd worden?

Op basis van de antwoorden kan een voorlopig beveiligingsconcept worden opgesteld. Dat concept moet vervolgens getoetst worden bij externe belanghebbenden zoals opdrachtgevers, verzekeraars, lokale overheden, brandweer, etc. Met hun input kan het beveiligingsconcept worden verbeterd en kan worden gestart met de uitvoering.

Vier essentiële elementen in het beveiligingsconcept

Hoe ziet een dergelijk beveiligingsconcept eruit? In hoofdlijnen kunnen we vier essentiële elementen onderscheiden:

1. **Organisatorische maatregelen.** Hieronder vallen alle benodigde procedures. Mag een vrachtwagen bijvoorbeeld zomaar het terrein oprijden of moet de chauffeur zich eerst melden? Wie mag hem toegang verlenen? Welke papieren moet hij controleren? En mag de chauffeur zelf laden en lossen of mag hij alleen toekijken?
2. **Bouwkundige maatregelen.** Die betreffen de eisen waaraan het gebouw zelf moet voldoen. Waar komen wel en geen deuren en ramen? Welke ramen kunnen wel of niet open? Zijn dikke betonnen muren nodig en hoe hoog moeten die dan zijn? Moet er een hek rondom het pand? De uitvoering van de bouwkundige maatregelen kan het bedrijf in handen leggen van de projectontwikkelaar of het bouwbedrijf.
3. **Elektronische maatregelen**. Denk aan inbraakbeveiliging, intercom, camerasystemen en toegangscontrolesystemen. Komen medewerkers binnen via een tourniquet of hebben ze een pasje nodig? Hoe wordt vastgelegd wie wel of niet toegang krijgt? En welke mensen op welk moment in het warehouse zijn geweest? De installateur is het aanspreekpunt voor de elektronische maatregelen.
4. **Management-maatregelen.** Uiteindelijk staat of valt beveiliging met het gedrag van mensen. Een warehouse beveiligen als een bunker helpt niet als mensen de deur open laten staan. Het management moet toezien op naleving van alle procedures en afspraken, medewerkers aanspreken op ongewenst gedrag en uiteraard zelf het goede voorbeeld geven.

TAPA als uitgangspunt

In de praktijk kan het handig zijn om het beveiligingsconcept op te hangen aan een bestaande beveiligingsstandaard zoals TAPA. Het voordeel van TAPA is dat het een brede, veelomvattende standaard is die internationaal wordt geaccepteerd. Maar TAPA alleen is niet voldoende. Deze standaard geeft bijvoorbeeld wel aan wat moet worden beveiligd – zoals de toegang tot het pand – maar niet precies op welke manier dat moet gebeuren. TAPA biedt dus net te weinig houvast voor bouwbedrijven en installateurs. Daarvoor is extra informatie nodig.

Bovendien: TAPA biedt een goede basis voor beveiliging van het warehouse, maar is niet allesomvattend. Voor warehouses met bijvoorbeeld luchtvrachtgoederen, douanegoederen en farmaceutische goederen gelden soms aanvullende eisen die niet in TAPA zijn opgenomen. Per warehouse moet dus worden onderzocht of elementen uit bijvoorbeeld de BORG-, IATA-, GPD- of AEO-richtlijnen moeten worden toegevoegd aan het beveiligingsconcept.

Uitvoering en audit

Als het beveiligingsconcept definitief is en de uitvoering is gestart, is het werk nog niet klaar. Toezicht is nodig om te waarborgen dat alle maatregelen correct worden uitgevoerd. Ook hier kunnen standaarden helpen, zoals de NEN 1010 waarin de Europese installatievoorschriften zijn vastgelegd. Tijdens de bouw is het dus raadzaam om iemand in het projectteam te hebben die het beveiligingsconcept begrijpt en tot op spijker- en schroefniveau weet hoe dat gerealiseerd moet worden.

De laatste stap is de audit die nodig is om definitief het TAPA-, AEO-, GDP- of andere standaard te ontvangen. Voor bijvoorbeeld het TAPA-certificaat komt een auditeur langs van een geaccrediteerde inspectie instelling die het hele warehouse aan een onderzoek onderwerpt. Aan het eind van de inspectie zijn er twee mogelijkheden: het bedrijf ontvangt de informatie dat alles voldoet aan de standaard of het krijgt binnen tien dagen een rapport met de bevindingen (Security Corrective Action Requirement (SCAR). De SCAR's dienen binnen zestig dagen verholpen te zijn.

Dan toetst de auditeur of dat inderdaad is gebeurd op basis van de toegestuurde bewijslast in de vorm van procesbeschrijvingen en/of foto's. Of hij komt opnieuw langs voor een inspectie. Pas als hij akkoord is, ontvangt het bedrijf het TAPA-certificaat.

Blijvend aandacht

Met een goed beveiligingsplan dat correct is uitgevoerd, is het heel goed mogelijk om een warehouse waterdicht te beveiligen. De certificaten vormen het bewijs daarvan richting klanten, verzekeraars en andere stakeholders. Maar zoals met alles geldt ook dat beveiliging een onderwerp is, dat blijvend aandacht verdient. Niet alleen om ongewenst gedrag door managers en medewerkers te voorkomen, maar ook omdat het warehouse en de activiteiten die daarin plaatsvinden voortdurend veranderen. Bij elke verandering is het zaak om te checken of het beveiligingsplan nog steeds voldoet.

Over de auteurs

Stijn Belt
Senior Facility Consultant
Groenewout

Groenewout is een vooraanstaand onafhankelijk logistiek adviesbureau gericht op het ontwikkelen en implementeren van logistieke en supply chain operaties, waaronder op security gebied.

Groenewout begeleidt bedrijven bij het definiëren en implementeren van hun supply chain security beleid.

Stijn Belt is dagelijks betrokken bij beveiligingsprojecten van logistieke operaties. Hij is gespecialiseerd in supply chain security, (brand)veiligheid & beveiliging oplossingen, systeem integratie en technische installaties.

E: belt@groenewout.com
T: +31 6 2122 0414

Pascal Verbaten
Directeur-eigenaar
Verbaten Security Consultancy

Verbaten Security Consultancy is een onafhankelijke adviesorganisatie gespecialiseerd in Supply Chain Security, die zich bezighoudt met het opzetten van beveiligingsconcepten, het uitvoeren van pre-audits en het bieden van ondersteuning bij de aanschaf en implementatie van beveiligingsconcepten. Ook verzorgen wij Security Awareness trainingen voor magazijnmedewerkers en vrachtwagenchauffeur op basis van de laatste regelgeving, zoals TAPA, AEO, C-TPAT, ISPS en bekende afzender lucht. Als bedrijf kunnen wij u bijstaan in het proces voor certificering op basis van TAPA, AEO, C-TPAT, ISPS en bekende afzender lucht.

E: pascal@verbatensecurity.com
T: 31 6 1331 2308