TEKST Marcel van Rijnbach | **FOTOGRAFIE** Holland Storage Solutions

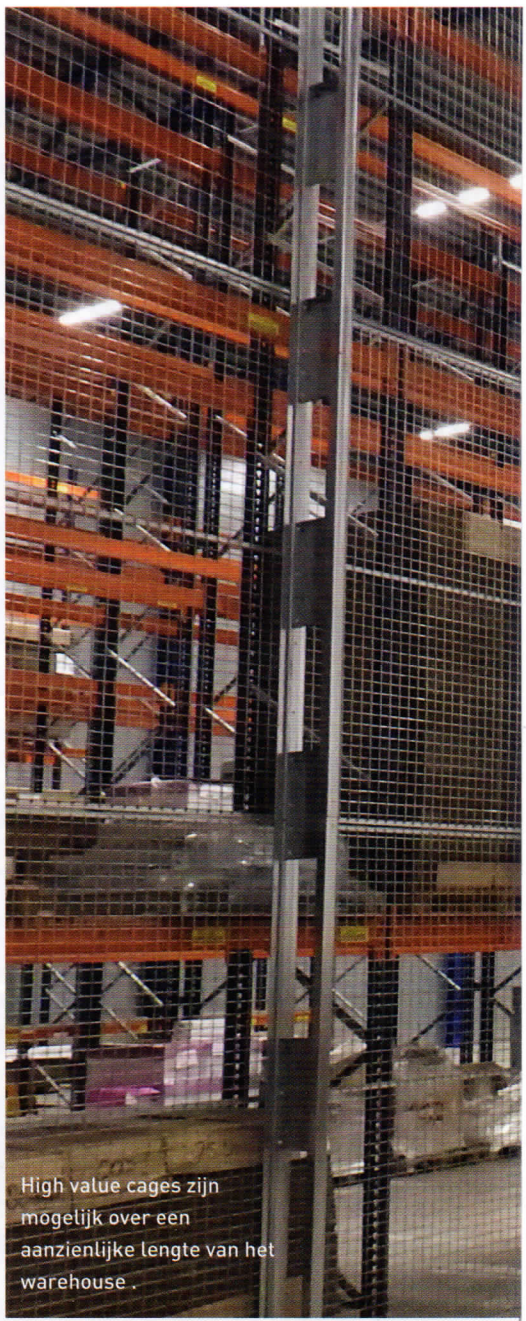
Hoe beveilig je een warehouse tegen diefstal?

Regelmatig worden voor duizenden of zelfs miljoenen euro's spullen ontvreemd uit warehouses en distributiecentra's. Inbraakbeveiliging is niet alleen een kwestie van elektronische en bouwkundige maatregelen, maar het komt vooral aan op het opstellen en naleven van een veiligheidsprotocol.

Daar schort het nogal eens aan in de logistieke branche, zeggen veiligheidsadviseur Ernesto Vanblarcum van AKE Beveiliging en directeur Hans de Graaf van magazijninrichter Holland Storage Solutions. Volgens Vanblarcum komen de meeste aanvragen voor een (aanvullende) beveiliging van het warehouse voort onder druk van de verzekeringsmaatschappij of opdrachtgever (degene die voorraad onderbrengt bij een logistiek dienstverlener). Deze partijen verlangen een bepaalde beveiligingsgraad van de voorraad om zich te wapenen tegen inkomstenderving door goederendiefstal. Directeur De Graaf van Holland Storage Solutions knikt. "Bij opslag van waardevolle goederen stijgt de verzekerde waarde. Zonder aanvullende beveiligingsmaatregelen stijgt de premie relatief nog meer. Dat zet de marges van de onderneming onder druk."

Welke hiaten in de inbraakbeveiliging treffen Vanblarcum en de veiligheidsadviseur van Holland Storage Solutions het meest aan in warehouses? Dat blijkt heel verschillend. Het ene warehouse heeft alleen een alarmsysteem geïnstalleerd en voldoet daarmee aan een basale verzekeringsvoorwaarde, terwijl het andere dc van top tot teen is beveiligd met toegangscontrole, beveiligde kooiconstructies en digitale goederendetectie en alles wat daar tussen in zit.

Wat Vanblarcum met name opvalt, is dat de handhaving van het veiligheidsprotocol vaak te wensen overlaat. "Dat begint bij de toegangscontrole. Als het systeem niet goed is ingericht of niet zorgvuldig wordt beheerd, heb je niets aan allerlei elektronische of bouwkundige veiligheidsmaatregelen. Ik noem als eenvoudig voorbeeld de schoonmaker die in plaats van acht uur volgens zijn pasje 24 uur toegang heeft tot bepaalde ruimten. Wat ik ook tegenkom is dat na een uitgebreide screening de toegang op een nooddeur niet is aangesloten op het alarmsysteem. Dat is namelijk gedaan om de logistieke medewerkers een tijdelijke uitgang te geven voor een rookpauze. Tja, dat kan natuurlijk niet de bedoeling zijn..."



High value cages zijn mogelijk over een aanzienlijke lengte van het warehouse .

Toegangsbeheer niet in orde

Volgens De Graaf is het toegangsbeheer bij menig logistiek object niet in orde. Ofwel, je kunt als externe bezoeker de magazijnvloer betreden zonder enige vorm van controle. Of het toegangsbeheer is niet goed ingericht, waardoor medewerkers ongeautoriseerd toegang kunnen krijgen tot waardevolle spullen in de opslag. "Er moet altijd iemand zijn die het personeel en bezoekers registreert en checkt voordat het magazijn wordt betreden. Toegangsbeheer en met name het handhaven ervan is een basisvereiste voor een goede beveiliging tegen diefstal."

Gebrek aan screening tijdelijk personeel

AKE Beveiliging gaat gedegen te werk bij het ontwikkelen van een beveiligingsoplossing. Het bureau werkt volgens het zogeheten CRIME securitymanagementsysteem. Onder andere het maken van een risicoprofiel en een uitgebreide inventarisatie van de beveiligingsrisico's en genomen preventieve maatregelen maken deel uit van deze aanpak. Maar ook het stimuleren van het veiligheidsbewustzijn in de organisatie kan een aandachtspunt zijn. Beveiligingsmaatregelen kunnen divers van aard zijn: organisatorisch en/of bouwkundig (kooiconstructies of compartimentering) en elektronisch/digitaal. Een maatregel die werkgevers vaak over het hoofd zien, is een screening van het (tijdelijke) personeel. "Zo gebeurt het vaak niet dat er een Verklaring Omtrent het Gedrag wordt opgevraagd, waardoor de werkgever geen inzicht heeft in een mogelijk strafbaar verleden van een medewerker", vertelt Vanblarcum. ■

VIJF BEVEILIGINGSTIPS OP EEN RIJ

- **Bespaar niet op beveiliging!**
- **Zorg voor een regelmatige security-check**
- **Werk met gecertificeerde beveiligingsbedrijven met een keurmerk**
- **(Rest)risico's kunnen worden afgekocht of verzekerd**
- **Beveilig je IT-systemen tegen hackers**