Van de auteur:

Over de gehele 40 jaar actief bezig geweest in de veiligheidswereld ben ik vele malen gefrustreerd geweest over installaties, normen of ontwerpen die ik te zien kreeg. Met dit werk wil ik raadgevingen verschaffen aan personen die de veiligheid in een winkel omgeving willen ontwerpen of evalueren. De raadgevingen zijn geschreven in achtneming van de winkel situatie en niet in functie van maximale veiligheid zoals in een instelling waar hoge veiligheid noodzakelijk is.

Geïntegreerde veiligheid in retail

Robert Verhulst

Met dank voor de foto overname:
Idemia Frankrijk
Proton Data USA
Axis communications Zweden
CDVI Frankrijk

Heeft U vragen over dit werk:
info@rcms.expert

www.rcms.expert

Het werk bevat volgende hoofdstukken:

Robert Verhulst

Revisie 1.0. September 2024

Geïntegreerde veiligheid?

Definitie:

Alle elementen, software, hardware, organisatie die een geheel vormen voor een veiligheidssysteem waar al deze zaken de noodzakelijke verbinding vormen tot één totale oplossing van de veiligheid.

Wat het niet is:

Dit doel bereiken betekent niet noodzakelijk één centraal systeem, maar met een verbinding tussen onafhankelijke systemen en werking op eenzelfde netwerkstructuur kan een grote kostenbesparing bekomen worden.

Cijfers van inkomensverlies in de retail industrie:
Een welbekend tijdschrift in de veiligheidswereld schreef deze maand over de verliezen geboekt in de retailsector in Groot-Brittannië.
Enkele gegevens (cijfers uit GB van 2023):
- Zelfscan kassa's in warenhuizen zouden het aantal diefstallen verhogen met 122% en beteken een verlies van 4% wat enorm is voor artikelen voor dagelijkse voeding.
- 200 Miljoen pond is de ontbrekende inventaris waarde die wordt toegeschreven aan inwendige diefstal.
- 1,77 Miljard dollar in de VS, een totaal verlies aan diefstal met een toenemende verhoging van 33% sinds de COVID periode.
- Sedert jaren wordt diefstal door eigen personeel op 25% van de feiten geraamd.
- Nederland met 17 miljoen inwoners heeft actueel meer dan 400000 diefstal aangiftes per jaar aan de politie.
- België met 11 miljoen inwoners heeft actueel meer dan 300000 diefstal aangiftes per jaar aan de politie.
Deze ontzettend hoge en groeiende cijfers zijn alleen aangiftes van alle aard en houden de vele niet aangegeven diefstallen in. Veel diefstallen in de retail werden niet vastgesteld en alleen bij inventarisatie vastgesteld. Diefstallen zonder aangifte zijn deze door overwaking opgemerkt maar door machteloosheid zonder gevolg gelaten.
Volgende verontrustende factor is het gebruik van wapens, in US vuurwapens en in Europa messen.

Er is geen wondermiddel dat retailbedreigingen kan verminderen. Retailers moeten een combinatie van mensen, processen en technologie gebruiken om de beveiliging te verbeteren.
Personeel gebaseerde benadering omvatten training over herkennen en wat te doen in en na bedreigende situaties. Goede, grondige training zorgt ervoor dat de juiste reactie ingebakken en een tweede natuur wordt.
AI-aangedreven videoanalyse kan worden gebruikt om mensen te identificeren aan de hand van hun gezicht, gevechten, wapens, indringers in verboden gebieden en zelfs winkeldiefstal of diefstal door werknemers te detecteren. AI heeft geen last van vermoeidheid of afleiding. Omdat AI een nieuwe technologie is, variëren producten in effectiviteit. Het kiezen van de juiste leverancier is essentieel.

3 modellen:

De retail industrie is zo uitgebreid in organisatievormen dat we deze model per model moeten bespreken.

Model 1: het warenhuis met kassa's aan de uitgang en zelfscan kassa's.

Model 2: De department winkel met open ruimte, verschillende afdelingen en kassa's verdeelt over de oppervlakte.

Model 3: gespecialiseerde winkels met kassa's dicht bij de uitgang.

Vormen van diefstal:

- Meenemen van voorwerpen zonder intentie van betaling
- Meenemen van goederen zonder toelating

Wat diefstal in de hand werkt:

- Afwezigheid van toezicht
- Afwezigheid van camera's
- Kleine voorwerpen
- Voorwerpen met hoge waarde
- Makkelijke vluchtwegen
- Goederen met kleine waarde
- Goederen met publicitaire waarde
- Sociale leefomgeving
- Diefstal vaststelling
- Gemakkelijke herverkoop op internet
- Oproer, manifestatie, paniek

Wist je dat Wereldwijd het aantal diefstallen door eigen personeel geschat wordt op 25% van de totale ontvreemdingen!

I. Algemene begrippen

Voorwoord:

Het woord beveiligen is een uitdrukking die in veel toepassingen gebruikt wordt en heel vaak in een context van het beschermen tegen ongevallen. In dit werk spreken we over het beveiligen bekend onder de uitdrukking “security” en een bescherming bied tegen een aanval of misbruik tegen de site, goederen en personen.

Dit werk legt de nadruk op veiligheidsoplossingen in de retailsector zonder de algemene basiskennis in de veiligheid te vergeten. Daarom kan men na hoofdstuk 3 vooral de algemene vakkennis terugvinden.

Safety of security?

In de Nederlandse taal spreekt men, vrij algemeen, van veiligheid. Toch is er een zeer groot onderscheid qua veiligheid tussen de volgende sectoren:
Sector van humane veiligheid en gezondheid of safety
- Brandveiligheid en evacuatie
- Rampspoed
- Noodsituatie
- Werkomstandigheden
- Machineveiligheid
- Rellen

Sector ter bescherming van mens en waarden of security
- Inbraak veiligheid
- Toegangscontrole
- Spionage
- Sabotage
- Elke vorm van agressie
- Cyber veiligheid
- Algemene overwaking en observatie
- Branddetectie
- Overval met geweld
- Terreur

Met bovenstaande sectoren als voorbeeld tracht ik verder in dit werk het onderscheid te maken door het gebruik van de termen “security” en “safety”. Uit de aangehaalde factoren is het duidelijk dat in de security sector het onverwachte of onberekenbare gevaar een belangrijke rol spelen.

Drie essentiële punten voor een veiligheidssysteem:

Sensoren, camera's, onderstations, … alle elementen die deel uitmaken van een veiligheidssysteem moeten beschermd zijn tegen sabotage, vernieling, schijnwerking, defect, beïnvloeding van elke soort… Dit kan in veel gevallen niet vermeden worden, maar het is uiterst belangrijk dat hiervan een alarm signalering het gevolg is. (vb. een schutter of laser schiet van buiten een omheining op een beveiligingscamera)

> *Een detectieapparaat die dit niet kan is niet geschikt voor beveiliging!*

Een veiligheidsinstallatie mag geen "single-point-of-failure" bevatten!

> *Maak een matrix van alle gebruikte elementen inclusief stroom voorziening en laat uw installateur de gevolg schade op elk onderdeel weergeven.*

Elk veiligheidssysteem is pas in werking als het ook in staat is om op elk ogenblik de toestand van goede werking onder controle te hebben. Hiervoor moeten anomalieën van alle aard als alarm vertaald worden.

> *Niet uitzonderlijk dat door verbouwing, reclame campagne, gebeurtenis,… een detectieapparaat ongewild of gewild niet verder instaat is de gewenste detectie uit te voeren.*

Personeel toegang en vertrek:

Personeel moet beschikken over een middel waarbij zij zich kunnen identificeren. Toegang tot de site gebeurd bij voorkeur langs een specifieke weg en niet langs de klanten toegang. Toegang wordt verkregen met een elektronische sleutel. Meestal onder vorm van een badge of smartphone met foto, naam en voornaam zonder verdere logo of reclame. Op de achterkant wordt uitgelegd dat de vinder van de badge deze zo vlug mogelijk opstuurt naar een adres die met de betreffende retail organisatie niets te maken heeft. Aan beide zijden van de deur wordt een camera geïnstalleerd en de deur wordt vrij gemaakt door het identificeren van de persoon op een online toegangscontrole waarvan de deur onder controle wordt gehouden. Alle deurbewegingen worden in het systeem chronologische gelogd. Als de deur te lang open blijft, wordt een zoemer in werking gesteld en een alarm gecreëerd.

Opgepast autonome deursloten met bediening door een badge of tag beantwoorden niet aan de veiligheidseisen voor deuroverwaking!

Credentials?

In dit werk spreekt men meestal van credential wanneer men een middel bedoelt dat gebruikt wordt om een persoon te identificeren. Dit kan, afhankelijk van de installatie, een badge zijn, een tag, een elektronische sleutel, een smartphone, maar ook een vorm van barcode of QR-code zijn.

Overwaking of bewaking ?

Is blijkbaar geen Nederlands woord. Toch kies ik ervoor om dit woord te gebruiken omdat dit woord een beter beeld geeft. Overwaking in de betekenis van een vorm van volledige observatie en controle. Dit is niet alleen een alarm bekijken en actie ondernemen, maar ook proactief een evolutie volgen, een dreigend gevaar vermijden en hiervoor de nodige actie ondernemen. Overwaking kan alleen door mensen met kennis ter zake, mensen die dag op

dag de activiteit op het te overwaken domein kennen. Bewaken is het opvolgen van vooraf bepaalde instructies en opvolgen van alarmen na de feiten, meestal door mensen met weinig affiniteit met het dynamische gebeuren.

Onsite overwaking of remote bewaking!
Bij onsite of plaatselijke aanwezige overwaking heeft de overwaker kennis van het gebeuren en de omgeving waardoor hij detectie veel beter kan evalueren en **proactief** beslissingen nemen.
Remote bewaking is steeds post event met weinig kennis van het gebeuren op de site en zal steeds grotere schade tot gevolg hebben. Spijtig genoeg wordt deze keuze gemaakt uit kost overweging.

Onafhankelijkheid:

Een overwaking van een onderwerp of een domein moet onafhankelijk zijn van de werking van dit onderwerp.

Voorbeelden uit ervaring ter verduidelijking:
- Een computercenter wordt overwaakt met een aantal camera's en sensoren, een zware fout bestaat erin de ononderbroken voeding of de software van de overwaking in deze ruimte te voorzien.
Een aanval tot sabotage op het computercenter zal eveneens het veiligheidssysteem buiten werking stellen en de klant zonder enig bewijs laten zonder enige verdere controle!

- Een camera observeert een noodstroomaggregaat, maar is voor zijn voeding afhankelijk van het aggregaat.
- Een observatie camera wordt gevoed op een plaatselijk stopcontact, andere toestellen als een koelkast dewelke een fout vertoont of een aardlek veroorzaakt zal de camera buiten werking stellen.
-Een operationeel netwerk als een beveiliging toepassing moet in principe onafhankelijk zijn en door de veiligheidsdiensten beheerd worden. Gebruik van VLAN op een bestaand netwerk is te vermijden vermits steeds de fysieke kabel en apparatuur door anderen toegankelijk zijn en niet aan dezelfde veiligheidsvoorschriften voldoen. Denk ook aan de aanzienlijke bandbreedte

die op continue basis wordt ingenomen door video en audio over het netwerk.
- Een observatie camera wordt gevoed op een plaatselijk stopcontact, andere toestellen als een koelkast dewelke een fout vertoont of een aardlek veroorzaakt zal de camera buiten werking stellen.

Internet !

Internet communicatie is heden niet meer weg te denken, op de meeste plaatsen kan men een zeer hoge betrouwbaarheid verkrijgen. Echter, bij gevaar zoals oorlog en terrorisme is het “het” eerste en meest geviseerde middel tot sabotage!

Wifi !

Wifi is een hedendaags veel gebruikt middel om draadloos te communiceren. Meestal geconnecteerd met Internet kan men bijna overal ter wereld een communicatie voeren in audio en video. De communicatie verloopt in de 2.4GHz of de 5GHz band. Wanneer er een connectie aanwezig is met internet zijn ook alle gevaren van cybersecurity aanwezig. Anderzijds is de communicatie vrij gemakkelijk onbruikbaar gemaakt door gebruik van een jammer. Wifi is echter ook volledig privaat te gebruiken als een onderdeel van een OT netwerk.

Een jammer: is een elektronische zender met hoog vermogen die communicatie binnen een frequentieband verstoord.

Sleutels:

Ondanks alle nieuwe technologieën zijn fysieke sleutels nog steeds niet verdwenen. Afhankelijk van de grote van een site zie je soms duizenden ongebruikte fysieke sleutels, maar die ondanks de elektronische toegangscontrole toegang verschaffen. Fysieke sleutels en lopers kunnen vrij gemakkelijk nagemaakt worden en vormen een bijkomende bedreiging. (het is niet omdat de eerlijke slotenmaker een sleutel laat aanmaken bij de fabrikant dat een inbreker deze niet kan maken) Let op: veelal kan door boren en/of vijlen een sleutel met lagere toegang aangepast worden om hogere toegang te verkrijgen!

Nog grotere zorgen bestaan er voor sleutels van technische kasten dewelke meestal universeel zijn! Hou rekening dat het tamper contact van de kast een alarm zal veroorzaken maar de sabotage niet kan vermijden.

Een tamper contact is een elektrische schakelaar binnen de veiligheidskast geplaatst om een toegang tot de kast te melden als een alarm.

Ouderdom:

Wanneer fysieke veiligheidsmiddelen zeker een lange levensduur bezitten is dit niet het geval voor elektronische producten in de sector. Net als de evolutie van sleutels over de laatste eeuw, heeft de veiligheidstechnologie stappen gezet om bescherming te bieden tegen nieuwe uitdagingen in overeenstemming met de evolutie van informaticatechnologie. Men kan in het algemeen zeggen dat een installatie van twintig jaar oud niet meer beantwoordt aan de huidige verwachtingen qua veiligheid en efficiëntie.

Weg met de PIR-detector :

PIR-detectoren die worden gebruikt voor bewegingsdetectie zijn aan het einde van hun leven, omdat camera's veel betere detectie kunnen uitvoeren en kunnen bewijs leveren van detectie. Een PIR kan uit richting geplaatst worden of met een spray gesaboteerd. Een camera is sabotage vrij door interne beeld analyse en constante communicatie. Gebruik een PIR detector voor het automatisch aansteken van het licht maar zeker niet als sensor voor een veiligheidsdoel.

Paraatheid:

Een state of the art installatie werkt op een onzichtbare manier aan het overwaken van de goede werking van alle onderdelen in de installatie. Vroeger werd dikwijls een goede passief infrarode detector als kwaliteitsvol beschouwd omdat hij nooit een alarm heeft veroorzaakt! In huidige technologie moet elke sensor of besturing op een netwerk verbonden zijn en voldoende informatie verschaffen om de oorspronkelijke gevoeligheid en doel te waarborgen. Zorg ervoor dat camerabeelden regelmatig bekeken worden! Een camera uitval, of een slecht beeld zal tot frustratie leiden pas na het opzoeken van feiten.

Interventie, evacuatie:

Deze twee begrippen houden verband met elkaar en hebben zowel elk een model van uitvoering als elk een onderling verband. Een op voorhand bepaald programma van uitvoering en verband moet hiervoor opgesteld worden. Hiervoor is duidelijke observatie en bestuurbaarheid noodzakelijk vanuit een operatief centrum.

Interventie :

-Moet steeds gebeuren volgens plan in functie van de gegevens betreffende de aan de hand zijnde feiten.
-Het operatief centrum van beveiliging, die ontoegankelijk is, mag nooit verlaten worden, behalve wanneer het zelf in het gedrang komt (vb. brand)
-De allereerste interventie bestaat erin alle mogelijke op afstand bestuurbare middelen aan te wenden om vanuit het operationeel centrum de toestand te

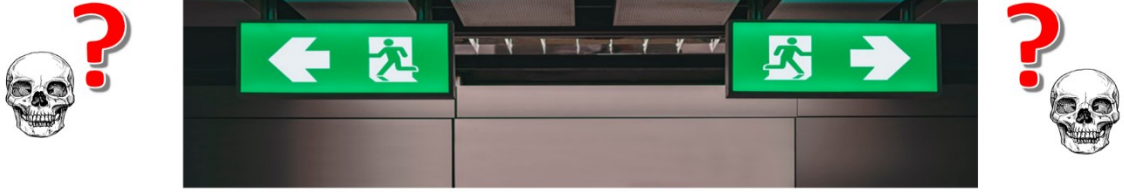
verhelpen, mensen en middelen te beveiligen.

-De tweede fase van interventie is eigen aanwezige mensen opdrachten verschaffen om handelingen uit te voeren ter bescherming. (personeel met kennis van risico's en site kennis)
-De derde fase bestaat erin professionele versterking op te roepen met gelimiteerde kennis over plaatselijke risico's en infrastructuur. Belangrijk is een onmiddellijke inschatting te maken van de noodwendige kracht en tijd . Interventie in een winkel wordt uitgevoerd door aanwezig bewakingsdienst en niet door personeel. Personeel moet immers de aandacht bijhouden, want het gebeuren kan een afleiding maneuver zijn.

Evacuatie:

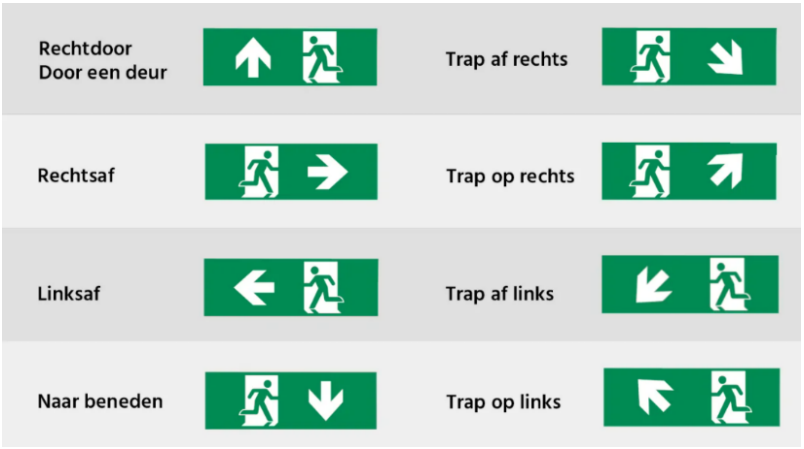
-Een bevel tot evacuatie is een gevaarlijke onderneming waarbij mensen blootgesteld worden aan een onbekende vlucht in paniek toestand om een omgeving te verlaten.
-Verschillende hulpmiddelen kunnen een evacuatie verbeteren:

- Voer geen totale evacuatie uit wanneer niet noodzakelijk.
- Gebruik audio begeleiding om de evacuatie te leiden.
  Geef namen aan vertrekken, gangen, bouwdelen…Denk aan geografische plaatsen, belangrijke personages, eigen productnamen,….Dit zijn de beste te herinneren oriëntaties in het audio bericht.
- Gebruik dynamische evacuatie richting aanduiding.
- Gebruik identificatie van personen dewelke het verzamelpunt hebben bereikt.



Twee wegen ?

Huidige standaard pictogrammen voor vluchtwegen:



Dynamische vluchtweg aanduiding:

Net zoals de standaard pictogrammen hebben dynamische vluchtweg borden dezelfde figuur van de persoon die door een deur loopt aan één zijde van het bord terwijl de tweede helft van het bord een bestuurbaar pictogram heeft. Voorbeeld:

Met deze nieuwe technologie kan men een evacuatie oriënteren in functie van informatie uit de branddetectie of de toegangscontrole.

Mustering :

Mustering betekent verzamelen, in veiligheidsomstandigheden wordt het woord gebruikt voor het systeem dat de aanwezigheid van personen op een bepaalde plaats verifieert. Het is een noodzakelijke manier om de veiligheid van personen te waarborgen bij incidenten en geëvacueerden personen als interventie diensten in veiligheid te brengen.
Praktisch zal men in het evacuatie model een of meerdere verzamelpunten definiëren waar de betrokken personen samen komen bij een incident of een oefening. Het musteringpunt is uitgerust met een credentiallezer die de aanwezigheid bij het musteringpunt identificeert. Door een correlatie te maken in de gegevens van het toegangscontrolesysteem gebruik makende van de laatste toegangshistorieken in het gebouw en het aanmelden op de verzamelplaats kan men de interventie sturen naar plaats en personen. Zorg

dat deze gegevens duidelijk zijn en van buiten de gevaren zone kunnen geraadpleegd worden.
Het is geraadzaam om volgende bijkomende maatregelen te nemen:
1. Voorzie voor de interventieploeg een specifieke credential zodat eventuele hulp bij interventie kan plaats vinden. Kan aan een mustering punt opgeslagen worden en geldig gemaakt bij interventie.
2. Maak een duidelijke specifieke bemerking in de toegangscontrole gegevens bij de personen dewelke hulpbehoevend zijn bij een incident.
3. Zorg bij het raadplegen van de personen betrokken bij het incident dat men filters kan gebruiken op basis van zone, laatste identificatiepunt, plaats van mustering en uur.