Geïntegreerde veiligheidssystemen.

Veiligheidssystemen kunnen niet bestaan uit één zelfde standaard oplossing!

Geïntegreerde veiligheidssystemen.

Een veiligheidsinstallatie is niet hetzelfde als een algemene elektrische installatie die gebouwd is volgens noodwendigheden en normen. Dit werk is er onder meer gekomen na tientallen jaren het gebrek aan gezond boerenverstand te zien ontbreken in realisaties!

Robert Verhulst

Robert Verhulst

ISBN: 9789464051384

Met dank voor de foto overname:
HTC parking & security bv Nederland
Dormakaba België
Idemia Frankrijk
Proton Data USA
Axis communications Zweden

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

www.rcms.expert

Doel van dit werk:
Met dit werk wil ik iedereen die betrokken is bij het ontwerpen van een geïntegreerd veiligheidssysteem met vernieuwende technologische beveiliging een leidraad geven en naar een nieuw tijdperk brengen qua technologie.

Het werk bevat zes hoofdstukken:
I. Algemene begrippen.
II. Geïntegreerde veiligheid.
III. Toegangscontrole.
IV. Audio en video.
V. Andere middelen.
VI. Afstandsoverwaking
VII. Onderhoud en aanpassingen
VIII. Cybersecurity
IX. Algemene informatie en normeringen

Robert Verhulst

Revisie 9.0. Mei 2021

Veiligheid het begin!

In werkelijkheid haast nooit aanwezig is een veiligheidsstudie van plaats, omgeving, structuur, terrein,… van een nieuw te bouwen gebouw of site! Nochtans hoort een veiligheidsoverweging voor het ogenblik dat de architect een potlood op papier zet. Samen met de eerste lijnen van een ontwerp moet de belangrijke fysieke inplanting gevolgd worden met veiligheidsadvies. Risico's achteraf oplossen met elektronische middelen is vaak moeilijk en een dure ingreep.

I. Algemene begrippen

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 of safety
- Brandveiligheid
- Rampspoed
- Noodsituatie
- 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

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.

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 zijn.

Overwaking:

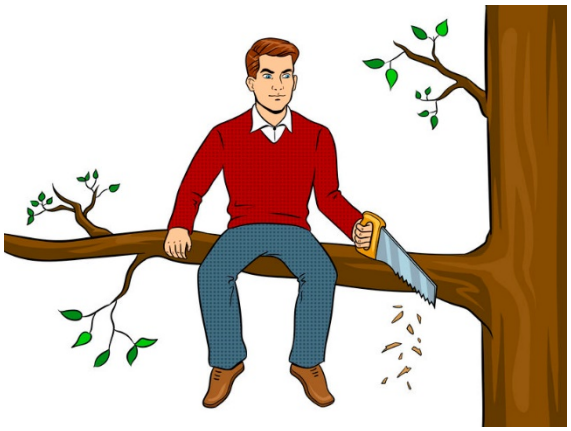
Is blijkbaar geen Nederlands woord. Toch kies ik ervoor om dit woord te gebruiken omdat dit woord een beter beeld geeft. Overwaking in de betekenis van een vorm van volledige observatie en controle. Dit is niet alleen een alarm bekijken en actie ondernemen, maar ook proactief een evolutie volgen, een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



worden. Gebruik van VLAN op een bestaand netwerk is niet toegestaan vermits steeds de fysieke kabel en apparatuur door anderen toegankelijk zijn en niet aan dezelfde veiligheidsvoorschriften voldoen.
- 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.

Bunker?

De plaats waar in reële tijd beslissingen worden genomen inzake veiligheid moet gehuisvest zijn op een veilige en goed beschermde plaats. Een aanval zal meestal gericht zijn op een directe wijze naar het target en in deze omstandigheden moet de veiligheid in werking blijven. Mocht een aanval gelijktijdig of vooraf toch gericht zijn naar de veiligheid overwaking dan moet deze voldoende versterkt zijn om uitwendige interventietijd mogelijk te maken.

Praktisch gezien moet het centrale systeem en controle zich op een veilige plaats bevinden dewelke afgeschermd is met fysieke middelen, toegangscontrole en onzichtbaar van buitenaf. Te dikwijls wordt een overwaking aanzien als een nachtportier job.

Binnen veiligheidsgrenzen:

Een geïntegreerd systeem maakt meestal tal van verbindingen met andere technieken. Echter mag men de aandacht van een operator niet onttrekken door niet veiligheid gebonden meldingen. Achter elke niet veiligheid gebonden opdracht kan een kritische veiligheidstoestand schuilgaan. Kritische technische toestanden die niet direct verbonden zijn met veiligheid kunnen eventueel gemeld worden en doorgegeven worden aan andere bevoegde personen, deze uitzondering met korte afhandeling moet echter beperkt blijven. Het is

evenmin de taak van de veiligheid beambte om de temperatuur van een lokaal te gaan aanpassen, daar tegenover kan een waterlek wel een veiligheidsrisico vormen.
Maak een onderscheid tussen security en non-security, vermijd ingewikkelde constructies als PSIM (Physical security information management) waarin eveneens technische overwaking en besturing gebeurt. BCS (Building Control Systems) zijn een must voor complexe systemen, maar vereisen andere vaardigheden en kunnen gemakkelijk op afstand worden bediend.

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)
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.

Bepaalde instellingen hebben hiervoor een sleutel management software, systeem of een beambte. Een nieuwe aanpak met nieuw technologie kan leiden tot een belangrijke ROI met hogere veiligheid.

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.

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.

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. Daarbij vraagt een PIR een voeding terwijl de camera gevoed wordt langs PoE. In het algemeen zou een detectie niet langer een alarm moeten geven zonder het bewijs te hebben van de oorsprong van het alarm.

Wetten en reglementering:

In de laatste decennia zijn reglementering, standaarden, wetten, verordeningen,… ontstaan die niet altijd de zaak vergemakkelijken. Nog erger gesteld is het met de opvatting dat een systeem hierdoor kan aanzien worden als conform. Deze regelgevingen moeten echter aanzien worden als een fundament van een veiligheid systeem en niet als het eind objectief. Franse, Duitse en Engelse nationale instituten voor de veiligheid spreken op een moderne manier van "*guides*", "*guidelines*", "*richtlinien*" in gepubliceerde documenten.

Voedingen:

Elk toestel heeft een voeding nodig, een tabel moet opgemaakt worden en een bepaling over welke autonomie elk apparaat moet beschikken. Ga na van welke factoren de algemene netvoeding afhankelijk is en welke aardlekken een onderbreking kunnen veroorzaken. As built documenten moeten een ééndraadschema van netvoeding aansluitingen bevatten voor alle aansluitingen in het systeem van elektrische aankomst tot elk toestel. Laag spanning voedingen van toestellen moeten een afgewogen autonomie bezitten.

Interventie, evacuatie, invacuatie:

Deze drie 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.