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 ziekenhuis willen ontwerpen of evalueren. De raadgevingen zijn geschreven in achtneming van de ziekenhuis situatie en niet in functie van maximale veiligheid zoals in een instituut waar hoge veiligheid noodzakelijk is.

Geïntegreerde veiligheid in ziekenhuizen

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:

I. Algemene begrippen.
II. Het operatief centrum.
III. Audio & video.
IV. Toegangscontrole.
V. Ontwerp tips.
VI. Onderhoud en aanpassingen.
VII. Algemene informatie en normeringen.

Robert Verhulst

Revisie 4.1. April 2024

I. Algemene begrippen

Voorwoord:

In dit werk bespreken we het beveiligen van ziekenhuizen in het algemeen ter bescherming van de werking volgens West-Europese omstandigheden. In deze context wordt een ziekenhuis site beschouwd als een open instelling waar iedereen op gelijk welk uur op minstens een plaats toegang krijgt.

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 en personen.

Voor ziekenhuis of verzorgingsinstellingen maakt men een afwijkende risicoanalyse met een ander oog op de proportionaliteit naar de gekozen oplossing. (de factor slaagkans is veelal hoog) De bewegingsvrijheid beperken zou zonder twijfel lijden tot nieuwe risico’s. Een volgend aspect is de zorg tot interventie gericht naar proactieve oplossingen.

Meest voorkomende risico’s:
- Toegang tot afdelingen of middelen die een risico vormen voor personen, instelling en operationele werking
- Aanwezigheid van kostbaarheden.
- Diefstal
- Ontvoering, gijzeling
- Sensatiepers
- Agressie en neurologische problemen
- Parkeer problemen
- Cyberaanval, datalek

Gelukkig op dit ogenblik is geweld onder vorm van “active shooter” nog niet aanwezig in onze westerse instellingen.

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

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.*

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 ?

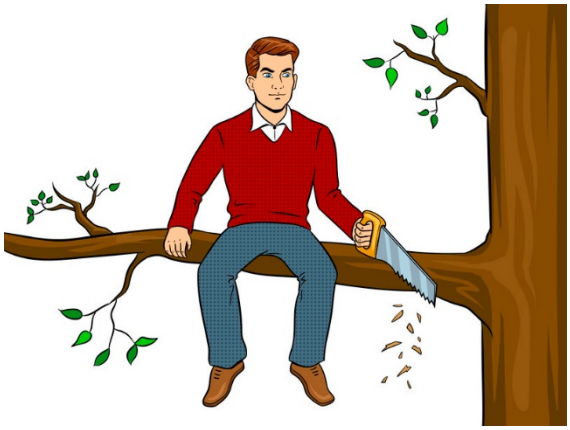
Is blijkbaar geen Nederlands woord. Toch kies ik ervoor om dit woord te gebruiken omdat dit woord een beter beeld geeft. Overwaking in de betekenis van een vorm van volledige observatie en controle. Dit is niet alleen een alarm bekijken en actie ondernemen, maar ook proactief een evolutie volgen, een 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 dokter of verpleegster kan haar activiteit niet verlaten voor een niet medisch event!



- 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 niet toegestaan vermits steeds de fysieke kabel en apparatuur door anderen toegankelijk zijn en niet aan dezelfde veiligheidsvoorschriften voldoen. Door de aard en risico vorm van toepassingen in ziekenhuizen kan dit als een proportioneel risico toegestaan worden maar wees waakzaam en zeker met cloud applicaties ten opzichte van NIS2 regeling! Denk ook aan de aanzienlijke bandbreedte die op continue basis wordt ingenomen door video en audio over het netwerk.

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!

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.

Nooddeuren :

Ziekenhuis nooddeuren hebben zeker een camera nodig maar geen toegangscontrole. De camera detecteert de nooddeur opening en moet een alarm vormen naar de veiligheidsdienst. (normaal gebruik of patiënt in gevaar)

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 uitwendige 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 .