De l'auteur :

Lors de mes 40 années d'activité dans le monde de la sécurité, j'ai été frustré à plusieurs reprises par les installations, les normes ou les conceptions auxquelles j'ai été exposé. Avec ce travail, je souhaite fournir des conseils aux personnes qui souhaitent concevoir ou évaluer la sécurité dans un hôpital. L'avis est rédigé en tenant compte de la situation hospitalière et non en termes de sécurité maximale, comme dans un institut dans lequel un grand niveau de sécurité est nécessaire.

Sécurité intégrée dans les hôpitaux

Robert Verhulst

Je souhaite remercier pour l'acquisition de photos :
HTC parking & security bv Pays-Bas
Dormakaba Belgique
Idemia France
Proton Data USA
Axis communications Suède
Boon Edam bv Pays-Bas
CDVI France

Pour toute question sur ce livre:

info@rcms.expert

www.rcms.expert

L'ouvrage contient les chapitres suivants :

Robert Verhulst

Révision 6.0. août 2024

Sécurité intégrée ?

Définition:

Tous les éléments, logiciels, matériels, organisation qui forment un tout pour un système de sécurité où tous ces éléments forment la connexion nécessaire à une solution de sécurité totale.

Ce que ce n'est pas :

Atteindre cet objectif ne signifie pas nécessairement un unique système central, mais avec une connexion entre des systèmes indépendants et un fonctionnement sur la même structure de réseau, d'importantes économies peuvent être réalisées.

Jusqu'à présent, la sécurité dans les hôpitaux était appliquée de manière traditionnelle et très semblable à la sécurité d'une agence bancaire. Lors de la conception, de la rénovation ou de l'agrandissement, la sécurité n'est guère prise en compte et est généralement définie en quelques mots. C'est sans bonne définition que les installateurs commencent généralement à installer comme habituelle. Cet ouvrage a été réalisé après étude et coopération de grands hôpitaux, que je remercie sincèrement pour leur coopération.

En quoi un hôpital est-il différent d'un autre site :
- Taille du site avec un grand nombre de personnes en libre circulation.
- De longs couloirs traversent le bâtiment.
- Le contrôle des mouvements ne peut pas être obtenu fasse à la productivité.
- Les risques sont bel et bien présents.
- Limité en moyens de fonctionnement autres que médicaux.
- L'évacuation est extrêmement difficile.
- Contamination, agression,…
- L'agresseur est souvent aussi le patient.
- L'intention d'un visiteur ne se lit pas sur son visage.
- Les analyses de risques conventionnelles ne peuvent pas être appliquées où sont très difficiles à appliquer

Ce qui ne peut pas être appliqué dans un hôpital :
- Poste de garde central.
- Équipe d'intervention (trop cher, fonctionnement trop lent compte tenu de la structure du bâtiment).
- Obstacles pouvant ralentir le fonctionnement.

Ce qui est d'une importance vitale :
- Un temps d'intervention rapide est vital compte tenu des risques

Ce qui est possible dans un hôpital :
- des techniques telles que le contrôle d'accès, la surveillance par caméra, la distribution de musique et de divertissement, le système d'appel, la surveillance technique, la centralisation de l'éclairage incendie et de secours, peuvent être utilisées sur un seul réseau.

.

I. Concepts généraux

Préface:

Dans ce travail, nous discutons de la sécurisation des hôpitaux en général pour protéger leur fonctionnement dans les conditions de l'Europe occidentale. Dans ce contexte, un site hospitalier est considéré comme une institution ouverte où chacun a accès à tout moment à au moins un lieu.

Le mot sécurisé est une expression utilisée dans de nombreuses applications et très souvent dans un contexte de protection contre les accidents. Dans cet ouvrage on parle de sécurité dite « sécurité » et de protection contre les attaques ou abus contre le site et les personnes.

Pour les hôpitaux ou les établissements de santé, une analyse de risque différente est réalisée avec un regard différent sur la proportionnalité à la solution choisie. (les chances de succès sont souvent élevées) Restreindre la liberté de mouvement entraînerait sans aucun doute de nouveaux risques. L'aspect suivant est le souci d'une intervention visant à des solutions proactives.

Risques les plus courants :

- Accès aux services ou ressources qui présentent un risque pour les personnes, l'institution et le fonctionnement opérationnel.
- Présence d'objets de valeur.
- Vol.
- Enlèvement, prise d'otage.
- Presse à sensations.
- Agressivité et problèmes neurologiques.
- Problèmes de stationnement.
- Cyberattaque, violation de données.

Heureusement, la violence sous forme de « tireur actif » n'est pas encore présente dans nos institutions occidentales. Il reste cependant un risque qui, dans ces circonstances et en raison de l'accessibilité, se concentre sur la personne ciblée.

Sûreté ou sécurité ?

Dans la langue française, on parle, en général, de la sûreté. Toutefois, il existe une très grande distinction en termes de sécurité entre les secteurs suivants:

Secteur de la sécurité humaine :
- Sécurité incendie –
- Catastrophe naturelles
- Accident du travail
- Urgence
- Émeutes

Secteur de la protection des personnes et des valeurs, ou le terme exact est sûreté :
- Vols
- Contrôle d'accès
- Espionnage
- Sabotage
- Toute forme d'agression
- Cybersécurité
- Couverture générale et observation
- Détection des incendies

Avec les secteurs donnés ci-dessus en exemple, je tente surtout de couvrir la sûreté contre la malveillance. Il est clair que, dans le secteur de la sûreté, le danger imprévu ou incalculable joue un rôle important.

Trois points caractérise un système de sécurité :

Capteurs, caméras, sous-stations, ... tous les éléments qui font partie d'un système de sécurité doivent être protégés contre le sabotage, la destruction, les faux effets, les interférences de toute nature... Cela ne peut être évité dans de nombreux cas, mais il est extrêmement important que un signal d'alarme est émis. (par exemple, un tireur ou un laser tire sur une caméra de sécurité depuis l'extérieur d'une clôture)

> *Un appareil de détection qui ne peut pas générer ce signal n'est pas adapté à la sécurité !*

Une installation de sécurité ne doit pas contenir de « point de défaillance unique » !

> *Créez une matrice de tous les éléments utilisés, y compris l'alimentation électrique, et demandez à votre installateur d'afficher les conséquences qui en résultent sur chaque composant.*

Tout système de sécurité ou sureté n'est opérationnel que s'il est également capable de contrôler à tout moment son bon état de fonctionnement. Pour cela, les anomalies de toutes sortes doivent être traduites en alarmes.

> *Il n'est pas rare qu'en raison d'une rénovation, d'une campagne publicitaire, d'un événement, etc., un appareil de détection ne soit plus en mesure, involontairement ou délibérément, d'effectuer la détection souhaitée.*

Identifiant ?

Dans ce travail, on parle généralement d'identifiant quand on entend un moyen utilisé pour identifier une personne. Selon l'installation, il peut s'agir d'un badge, d'une étiquette, d'une clé électronique, d'un smartphone,...

Surveillance:

En utilisant le mot surveillance, je souhaite attirer l'attention sur une forme d'observation et de contrôle complets. Il ne s'agit pas seulement d'une alarme et d'une action, mais aussi de suivre une évolution de manière proactive, d'éviter un danger imminent et de prendre les mesures nécessaires. Cette surveillance ne peut être effectuée que par les personnes ayant une connaissance de la situation, car elle suivent jour après jour l'activité dans le domaine et ont une connaissance du passé. La surveillance à distance se limite fréquemment dans le suivi d'instructions prédéterminées et le suivi des alarmes après les faits. Elle est généralement faite par des personnes ayant peu d'affinité avec la dynamique des évènements. Dans le cas d'une surveillance sur place ou locale, le surveillant a une connaissance de l'événement et de l'environnement grâce à laquelle il peut mieux évaluer la détection et prendre des décisions proactives, tandis que la surveillance à distance devient post-événement, avec peu de connaissance de ce qui se passe sur le site et occasionnera toujours des dommages plus importants.

Indépendance:

La surveillance d'un sujet ou d'un domaine doit être indépendante de son propre fonctionnement.

Voici quelques cas qui illustrent ce principe:

- Un centre informatique est surveillé avec un certain nombre de caméras et de capteurs. Une grave erreur est de fournir l'alimentation électrique ininterrompue ou le logiciel de la surveillance dans cette même salle. En effet, une attaque pour saboter le centre informatique va

également arrêter le système de sûreté et laisser le client sans aucune preuve et sans aucun autre contrôle !

- Une caméra observe un générateur d'énergie d'urgence, mais dépend du générateur pour son alimentation.

- Un réseau doit être indépendant et géré par les services de sûreté. L'utilisation de VLAN sur un réseau existant est a évité, car le câble physique et l'équipement sont toujours accessibles par d'autres et ne répondent pas aux mêmes exigences de sûreté. Tenez également compte de la bande passante importante qui est utilisée en permanence par la vidéo et l'audio sur le réseau. En raison de la nature et de la forme de risque des applications dans les hôpitaux, cela peut être considéré comme un risque proportionnel, mais soyez vigilant et certainement avec les applications cloud. par rapport à la réglementation NIS2 ! Tenez également compte de la bande passante importante utilisée en permanence par la vidéo et l'audio sur le réseau.

- Une caméra d'observation est alimentée sur une prise locale, d'autres appareils tels qu'un réfrigérateur qui montre un défaut ou provoque une fuite de terre va désactiver la caméra.

L'Internet!

La communication Internet est désormais indispensable et, dans la plupart des endroits, une très haute fiabilité peut être atteinte. Pourtant, en cas de danger comme la guerre et le terrorisme, c'est le moyen de sabotage le plus recherché !

Wifi!

Le WiFi est aujourd'hui un moyen de communication sans fil couramment utilisé. Généralement connecté à Internet, on peut communiquer en audio et vidéo presque partout dans le monde. La communication s'effectue dans la bande 2,4 GHz ou 5 GHz. Lorsqu'il y a une connexion à Internet, tous les dangers de la cybersécurité sont également présents. Cependant, la communication est assez facilement rendue inutilisable par l'utilisation d'un brouilleur. Cependant, le WiFi peut également être utilisé de manière totalement privée dans le cadre d'un réseau OT.

Clés:

Malgré toutes les nouvelles technologies, les clés physiques n'ont toujours pas disparu. Selon la taille d'un site, il y a parfois des milliers de clés physiques inutilisées, et elles fournissent un accès malgré le contrôle d'accès électronique. Les clés physiques et les passe-partouts peuvent être recréés assez facilement et constituer une menace supplémentaire. (Ce n'est pas parce qu'un serrurier honnête fait faire une clé chez le fabricant qu'un cambrioleur ne peut pas le faire) Attention : souvent une clé avec un accès plus faible peut être ajustée en perçant et/ou en limant pour obtenir un accès plus élevé !

Un souci majeur concerne les clés des armoires techniques qui sont généralement universelles! Gardez à l'esprit que le contact d'ouverture de l'armoire provoquera une alarme, mais ne pourra pas éviter un sabotage.

Un contact anti-sabotage est un interrupteur électrique placé à l'intérieur de l'armoire de sûreté pour signaler un accès par une alarme.

Ancienneté:

La durée de vie des dispositifs de sûreté physiques est longue. Parcontre, ce n'est pas le cas des produits électroniques. Comme l'évolution des clés au cours du siècle dernier, la technologie de sûreté a pris des mesures pour se protéger contre les nouveaux défis en ligne avec l'évolution de la technologie informatique. En général, on peut dire qu'une installation vieille de 20 ans ne répond plus aux attentes actuelles en termes de sûreté et d'efficacité.

Préparation:

Une installation à la fine pointe de la technologie fonctionne de manière invisible pour superviser le bon fonctionnement de tous les composants de l'installation. Dans le passé, un bon détecteur infrarouge passif était souvent considéré comme de haute qualité parce qu'il n'avait jamais causé d'alarme! Dans la technologie actuelle, chaque capteur ou contrôle doit être connecté à un réseau et fournir suffisamment d'informations pour assurer sa sensibilité et son but . Assurez-vous que les images de la caméra sont visionnées régulièrement ! Une panne de caméra ou une mauvaise image ne mènera qu'à la frustration après avoir vérifié les faits.

Débarrassez-vous du détecteur PIR:

Les détecteurs PIR utilisés pour la détection de mouvement sont à la fin de leur vie, car les caméras peuvent effectuer une bien meilleure détection et en fournir des preuves. Un PIR peut être placé hors de direction ou saboté avec un spray. Une caméra ne peut-être saboter par cause d'analyse d'image interne et la communication constante. En outre, un PIR nécessite une alimentation pendant que la caméra est alimentée le long de PoE. En général, une détection ne doit plus donner d'alarme sans avoir la preuve de l'origine de l'alarme. Utilisez un tel détecteur pour allumer automatiquement la lumière, mais certainement pas comme capteur à des fins de sécurité.

Portes de secours :

Les portes de secours des hôpitaux ont certes besoin d'une caméra mais pas d'un contrôle d'accès. La caméra détecte l'ouverture de porte de secours et doit envoyer une alarme au service de sécurité. (usage normal ou patient à risque)

État de préparation :

Une installation de pointe fonctionne de manière invisible pour surveiller le bon fonctionnement de tous les composants de l'installation. Autrefois, un bon détecteur infrarouge passif était souvent considéré comme de haute qualité car il ne provoquait jamais d'alarme ! Dans la technologie actuelle, chaque capteur ou contrôleur doit être mis en réseau et fournir suffisamment

d'informations pour garantir sa sensibilité et son objectif d'origine. Assurez-vous que les images de la caméra sont visionnées régulièrement ! Une panne de caméra ou une mauvaise image ne mènera qu'à la frustration après avoir vérifié les faits.

Intervention, évacuation :

Ces deux concepts sont liés et ont chacun un modèle de mise en œuvre et chacun a une interrelation. Un programme prédéterminé de mise en œuvre et de raccordement doit être élaboré à cet effet. Cela nécessite une observation claire et une contrôlabilité de la part d'un centre opérationnel.

Intervention:

-Doit toujours être faite selon le plan et selon les informations relatives aux faits.

-Le centre opérationnel de sûreté, inaccessible, ne doit jamais être abandonné, sauf lorsqu'il est lui-même compromis (par exemple, incendie)
-La première intervention consiste à utiliser tous les moyens possibles télécommandés pour remédier à la situation du centre opérationnel, pour sécuriser les personnes et les ressources.
-La deuxième phase de l'intervention consiste à donner aux personnes présentes pour mener des opérations de protection. (personnel ayant une connaissance des risques et des connaissances sur le site) -La troisième phase consiste à demander un renforcement professionnel externe avec des connaissances limitées sur les risques locaux et les infrastructures. Il est important de procéder à une évaluation immédiate de la capacité extérieure d'urgence et du temps.

Évacuation:

-Un ordre d'évacuation est une entreprise dangereuse dans laquelle les gens sont exposés à une course inconnue dans un état de panique pour quitter un environnement.
-Différents outils peuvent améliorer une évacuation:
Ne pas effectuer une évacuation totale si pas nécessaire.
Utilisez des conseils audio pour mener l'évacuation. Donner des noms de pièces, couloirs, éléments de construction… Pensez aux lieux géographiques, personnages importants, propres noms de produits,….Ce sont les meilleurs à mémoriser les orientations dans le message audio.
Utiliser l'indication dynamique de direction d'évacuation.
Utiliser l'identification des personnes qui ont atteint le point de rassemblement.

Deux voies ?

Indication dynamique des issues de secours:

Comme les pictogrammes standard, les panneaux d'évacuation dynamiques ont la même figure de la personne qui franchit une porte sur un côté du panneau tandis que la seconde moitié du panneau a un pictogramme contrôlable.

Grâce à cette nouvelle technologie, une évacuation peut être orientée en fonction des informations issues de la détection incendie ou du contrôle d'accès.

Rassemblement :

Rassemblement signifie rassembler, dans des conditions de sécurité le mot est utilisé pour le système qui vérifie la présence de personnes dans un lieu particulier. C'est un moyen nécessaire pour garantir la sécurité des personnes en cas d'incidents et des personnes évacuées ainsi que des personnes en rétention et des services d'intervention.

Concrètement, un ou plusieurs points de rassemblement seront définis dans le modèle d'évacuation où les personnes impliquées se réunissent lors d'un incident ou d'un exercice. Le point de rassemblement est équipé d'un lecteur d'identifiant qui identifie la présence au point de rassemblement. En établissant une corrélation dans les données du système de contrôle d'accès en utilisant les derniers historiques d'accès dans le bâtiment et en se connectant au point de rassemblement, l'intervention peut être dirigée vers le lieu et les personnes. Assurez-vous que ces informations sont claires et consultables depuis l'extérieur de la zone de danger.

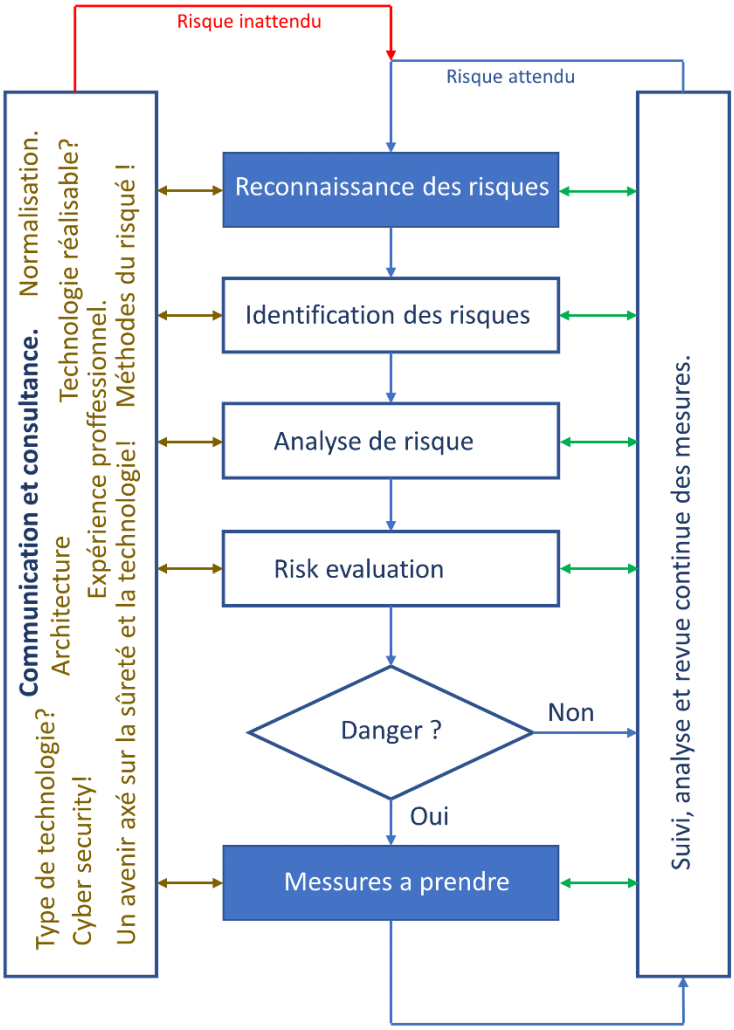
Il est conseillé de prendre les mesures supplémentaires suivantes :

1. Fournir un identifiant avec autorisation spécifique à l'équipe d'intervention afin que toute aide à l'intervention puisse avoir lieu. Peut être stocké à un point de rassemblement et validé lors de l'intervention.
2. Faire une remarque spécifique claire dans les données de contrôle d'accès pour les personnes qui ont besoin d'aide en cas d'incident.
3. Lors de la consultation des personnes impliquées dans l'incident, assurez-vous que les filtres peuvent être utilisés en fonction de la zone, du lieu de rassemblement et de l'heure.

Analyse des risques:

La plupart des analyses de risque, comme base pour travailler sur une sûreté, sont farouchement exagérées et manquent généralement d'une nouvelle approche créative. Lorsque cela produit de bons résultats pour les études de sûreté, le facteur de renseignement de l'attaquant manque souvent d'applications de sûreté. Un consultant en sûreté expérimenté devrait penser au-dessus de cette méthode trop simple d'analyse des risques dans le domaine de la sûreté.

Afin de commencer et de maintenir la gestion des risques, une consultation entre les différentes parties dans un domaine multi-champ est nécessaire. Le prochain calendrier donne une bonne vue de la façon dont chaque sujet doit être abordé.



Calcul de l'évaluation des risques par risque :

Différentes méthodes sont utilisées pour estimer un fait qui compromet la sécurité. Pour les environnements hospitaliers, je recommanderais d'utiliser la méthode la plus générale où chacun des trois facteurs est noté de 0 à 100 et la racine cubique du produit représente l'évaluation du risque.

$$\text{Risque} = \sqrt[3]{V \times W \times S}$$

Cependant, ce qui perturbe cette approche, ce sont les nombreux éléments d'improbabilité et les chances de succès qui doivent être déterminés comme probables dans leur intégralité.

Infection:

Le logiciel de contrôle d'accès peut facilement faire une liste des personnes qui sont venues dans la proximité de l'autre lors de l'identification à un accès. C'est particulièrement intéressant en cas de pandémie mais aussi dans les laboratoires où le contact mutuel peut conduire à la contamination. Dans ces derniers cas, les ouvre-portes automatiques et la technologie mains libres sont préférés comme lecteur d'accréditation et commande d'ouverture de porte (sans contacte physique) à l'intérieur.

Inspection du produit ! :

Longtemps, les inspections de produits ont été le moyen de déterminer la qualité d'un produit, mais cela est encore en partie exact. En effet, dès qu'un produit contient un firmware interne, son fonctionnement continu ne peut plus être vérifié. Seul le fabricant du produit a une idée du comportement du produit.

Quelques exemples :

- Une caméra dispose d'une porte dérobée dans le logiciel afin que l'accès puisse être obtenu de l'extérieur sans utiliser de communication de sécurité. Cela peut se faire de différentes manières, telles que : WiFi, communication

infrarouge, toutes autres formes de communication RF, temps, son, vibration, etc.

- Un produit sans communication tel qu'un capteur ou un détecteur peut être influencé tel que : télécommande infrarouge, f(time), lumière, son, vibration, ...

Proportionnalité et gestion des risques :

La première chose à considérer lors de la conception d'un système de sécurité pour un site est sa proportionnalité aux risques identifiés. Malheureusement, la normalisation, la législation, les réglementations, les inspections, etc. font que la proportionnalité n'est pas toujours réalisable.

Détection d'incendie:

Les normes actuelles sont tellement surréglementées que toute proportionnalité en termes d'analyse des risques devient impossible. Par conséquent, la meilleure option d'intégration consiste à fournir une connexion minimale à tous les panneaux de détection d'incendie lorsqu'un signal d'alarme est fourni à la sécurité centrale. Fournissez également une sorte de signal de surveillance qui vous permet de contrôler en permanence si ces panneaux sont en bon état de fonctionnement.

Secret:

Le secret d'une installation de sûreté est certainement l'un des aspects les plus importants d'un projet de sûreté. Après tout, le secret protège le propriétaire de la planification d'un vol ou d'un cambriolage. L'inattendu est l'un des facteurs les plus importants pour contrecarrer ou retarder une attaque de toute nature (lire: ralentir = ralentir ou promouvoir le temps d'intervention).
Quelques exemples d'erreurs graves dans le cas du secret:
A. Une porte ou un portail où la marque du fabricant se trouve sur la face visible.

Conséquence : l'attaquant sait à quoi s'attendre et quelles ressources il peut utiliser.
B. Un badge d'accès avec logo ou adresse à laquelle il est autorisé à accéder.

En conséquence, la clé d'accès peut être volée ou perdue, mais elle indique également où elle peut être utilisée (semblable à attacher une carte de visite à la clé de la maison).