LIVRE BLANC

La numérisation et la cybersécurité du contrôle d'accès physique

Une exploration des systèmes et protocoles permettant aux entreprises d'exploiter tout le potentiel du contrôle d'accès et de créer un monde plus intelligent et plus sûr.

Juillet 2021

AXIS COMMUNICATIONS

Table des matières

1 Avant-propos

Le développement de la connectivité cloud change l'aspect du secteur de la sécurité physique et oblige les installateurs à s'adapter pour rester en activité. Le contrôle des systèmes d'accès semble passer dans le camp des entreprises technologiques globales, ce qui suscite l'espérance d'une plus grande valeur de la part des systèmes eux-mêmes, à mesure qu'ils deviennent de plus en plus intelligents, évolutifs et périphériques.

Cette évolution, ainsi que son potentiel d'intégration avec d'autres systèmes d'entreprise, signifie également que la cybersécurité doit jouer un rôle encore plus important dans le développement et le déploiement du système, en particulier dans les cas où il s'appuie sur une infrastructure existante. Surmonter les obstacles techniques tels que l'architecture en série, l'absence d'adresses MAC, etc., est une étape cruciale dans la transition vers des systèmes de contrôle d'accès numériques capables de répondre aux exigences actuelles et futures.

Mettre en œuvre et sécuriser un système numérique de contrôle d'accès, c'est aussi suivre les meilleures pratiques pour assurer la meilleure sécurité possible. Nous devons évaluer et tester chaque composant impliqué dans le système, qu'il s'agisse d'un dispositif, d'un fournisseur ou d'un protocole : tous doivent être dignes de confiance et fiables. Nous devons également être constamment conscients du champ des menaces et de la manière d'atténuer les dangers présentés par les vulnérabilités et les défauts récemment trouvés.

Les fournisseurs, en particulier, doivent faire l'objet d'une attention particulière, car vous autorisez leurs appareils à entrer dans votre réseau. Un fournisseur sérieux devrait fournir et faire connaître ses propres processus de sécurisation de ses offres, par exemple en publiant un guide de durcissement, en fournissant des outils de gestion dédiés qui simplifient la gestion et la sécurisation des périphériques réseau, etc. En outre, il est préférable qu'un fournisseur soit ouvert et honnête en ce qui concerne sa stratégie de gestion des vulnérabilités et des failles découvertes.

2 Introduction: L'avenir du contrôle d'accès

La connectivité cloud a offert au secteur de la sécurité physique une nouvelle façon de déployer et d'utiliser les systèmes. Les utilisateurs et les acheteurs exigent des solutions plus intelligentes, intégrées et plus axées sur l'entreprise, avec des capacités de surveillance et de contrôle d'accès qui vont bien au-delà de celles offertes par les technologies traditionnelles.

De nombreux fournisseurs ont construit un modèle économique solide autour de leur expertise, de leur service et de leur connaissance de la sécurité physique Cependant, la connectivité réseau et l'Internet des objets (IoT) sont en constante évolution, ce qui oblige le vendeur et l'installateur traditionnels de sécurité physique à apprendre le langage informatique des plateformes ouvertes, de la connectivité IP et de l'intégration logicielle, afin de s'adapter aux changements du marché et de rester pertinents.

Il semble que le contrôle passe rapidement des fournisseurs de systèmes d'accès électroniques aux entreprises technologiques mondiales, qui ont désormais le pouvoir de façonner la sécurité dans une direction qui remet en cause son fonctionnement traditionnel. Les bâtiments et les villes intelligents offrent de grandes opportunités, et beaucoup prévoient une croissance rapide du marché du contrôle d'accès moderne, car la facilité de déploiement et la sophistication des technologies actuelles apportent de nombreux avantages à l'environnement intelligent.

Il n'est pas surprenant que l'adoption d'un contrôle d'accès hébergé soit une tendance qui s'impose, car les géants de la technologie ont démontré le succès des technologies cloud, dont on a tant dépendu pendant la pandémie mondiale de COVID-19. Ces entreprises ont la capacité, la taille et l'imagination nécessaires pour provoquer un changement radical. La sécurité physique sera également transformée car les entreprises, réalisant la valeur du cloud, se tournent vers des solutions hébergées pour prendre en charge toutes leurs exigences en matière de sécurité et d'activité.

Toutefois, à l'heure actuelle, de nombreux fabricants ne sont tout simplement pas prêts à s'adapter à ce marché en mutation et continuent à suivre des modèles économiques fondés sur des conceptions rigides et exclusives. L'évolution vers des solutions de sécurité physique intelligentes s'oppose directement à cette approche traditionnelle, qui risque d'être fortement remise en question. Le changement ne se fera pas du jour au lendemain et les nouvelles solutions d'hébergement cloud doivent encore se généraliser, mais ce nouveau monde prometteur est néanmoins dans les mains des nouveaux ingénieurs qui rejoignent notre secteur en ce moment.

L'avenir du contrôle d'accès et de la sécurité physique dans son ensemble sera donc fondé sur des attentes d'une plus grande valeur. Les systèmes de contrôle d'accès deviendront des points de collecte de données et les contrôleurs de porte des dispositifs d'entrée/sortie intelligents. Les codes QR pour la gestion des visiteurs et la reconnaissance biométrique des visages pour le contrôle d'accès sans contact seront de plus en plus gérés à la périphérie, sous forme de données dans une caméra ou un capteur. L'avenir du contrôle d'accès constitue une période passionnante et stimulante pour ceux qui sont prêts à l'accepter et à contribuer à le mettre en forme, une véritable opportunité d'innover pour un monde plus intelligent et plus sûr.

Dans cet article, nous explorons les aspects qui sont particulièrement pertinents pour le contrôle d'accès, y compris plusieurs des caractéristiques fondamentales de ces systèmes. Nous examinerons également les considérations relatives aux meilleures pratiques pour les fournisseurs et donnerons des informations et des suggestions aux clients afin de leur donner la confiance nécessaire pour défier leurs fournisseurs et prendre des décisions d'achat plus avisées.

3 Les enjeux d'un marché du contrôle d'accès en pleine évolution

Lorsque nous nous intéressons aux systèmes de contrôle d'accès physique (PACS), nous avons tendance à aborder les facteurs de risque en termes de considérations concernant l'autorisation ou le blocage de l'entrée physique. L'adoption d'une approche équilibrée pour la conception d'un système de contrôle d'accès physique est une considération importante basée sur l'évaluation de la menace potentielle.

Aujourd'hui, alors que les locaux sont davantage protégés par des solutions de contrôle d'accès électronique de plus en plus sophistiquées, ces systèmes constituent un moyen rapide et efficace de gérer l'accès dans l'ensemble de l'entreprise, en laissant une empreinte numérique qui peut être examinée et contrôlée si nécessaire, et qui peut être totalement intégrée à d'autres systèmes tels que la gestion des RH et des visiteurs.

Cette unification des systèmes produisant des informations puissantes pour faciliter la prise de décision en matière de sécurité et de gestion, ainsi que de contrôle de l'accès, il devient crucial d'évaluer en détails la cyber-maturité du système. Les criminels devenant de plus en plus sophistiqués et le champ des menaces continuant d'évoluer, le défi consiste à atténuer le risque de clonage d'identifiants d'accès, de menaces internes ou de cyberattaques lancées à distance.

Cependant, l'architecture elle-même pose un problème. De nombreux systèmes de contrôle d'accès reposent sur des infrastructures obsolètes. Les technologies de sécurité convergentes utilisant couramment cette infrastructure, le défi pour les fournisseurs est d'une part d'adapter leur matériel pour qu'il puisse se connecter à ces réseaux d'entreprise, et d'autre part de prendre conscience de l'importance de la sécurité informatique et de l'évolution du champ de la sécurité, qui impose d'évaluer en profondeur les nombreux risques auxquels une entreprise est exposée et de l'en protéger.

Les questions de cybersécurité doivent être un facteur clé du développement de nouveaux systèmes de sécurité. Les technologies de contrôle d'accès font partie intégrante de toute solution de sécurité physique et doivent donc être réalisées conformément aux principes reconnus de cybersécurité, au signalement des

incidents et aux meilleures pratiques. Il est important de reconnaître que le niveau d'intégrité d'un système est celui de son maillon le plus faible. **Un système qui n'est pas prêt à l'accepter** constitue un risque potentiel d'exposition. S'il ne peut pas démontrer qu'il est prêt à accepter, à informer et à mettre en place des mesures de récupération reconnues publiquement, cela aura en fin de compte un impact négatif sur sa capacité à fournir les niveaux nécessaires de sécurité physique pour lesquels il a été déployé.

3.1 Identifiants de cybersécurité (cyber-maturité)

L'implication croissante du secteur informatique commence à changer la façon dont les technologies sont évaluées, déployées et entretenues. L'évaluation des identifiants de cybersécurité de l'entreprise, en mettant l'accent sur les connaissances des fournisseurs en la matière, est un élément essentiel pour les acteurs de l'informatique. Ces connaissances sont également appelées « cyber-maturité ». Être cybermature suppose de bien comprendre le champ des menaces et l'atténuation des risques. La documentation et les instructions détaillées en matière de cybersécurité déjà élaborées pour les caméras réseau peuvent également être appliquées au contrôle d'accès physique, car les défis, les évaluations et les explications concernant le risque cybernétique et le danger d'attaque sont tout aussi pertinents pour ces produits.

3.2 L'avenir de l'architecture des systèmes de sécurité

Les dispositifs actuels de contrôle d'accès sont connectés via des câbles réseau et des connecteurs RJ45. Les réseaux fournissent l'alimentation des contrôleurs d'accès, ainsi que la communication entre les dispositifs et les systèmes de gestion centraux. L'évolution du contrôle d'accès se fera par la transition vers des systèmes basés sur le protocole TCP/IP. Depuis l'introduction du premier contrôleur de porte sur IP (AXIS A1001) en 2013, le contrôle d'accès a continué à évoluer, offrant désormais un large éventail de fonctionnalités avancées qui n'auraient jamais été possibles en s'appuyant uniquement sur la technologie existante.

Parmi les exemples de cette innovation, citons les lecteurs de codes QR pour faciliter le contrôle d'accès sans contact, la reconnaissance faciale par l'intégration de caméras en réseau et la lecture de plaques d'immatriculation, qui interagissent tous avec les bases de données de contrôle d'accès pour prendre des décisions sur la base des résultats relatifs à l'autorisation ou au refus d'une admission. Les principaux avantages des systèmes IP sont les faibles coûts d'installation, la simplicité de la configuration et de la gestion des appareils. L'intégration facile à d'autres dispositifs se traduit par une solution durable, qui permet la connectivité plug-and-play des nouvelles technologies et des améliorations de sécurité dès qu'elles sont disponibles.

3.3 IP ou contrôle d'accès traditionnel ?

Les avantages de l'IP se concrétiseront dans les conceptions nouvelles et modernes de contrôle d'accès, en particulier dans les systèmes sans contact que les utilisateurs finaux attendent en standard. Les utilisateurs voudront également que le contrôle d'accès s'adapte à l'utilisation des smartphones et des tablettes, et pas uniquement à partir d'une carte d'identité portable. Comment le secteur va-t-il fournir de meilleurs systèmes de contrôle d'accès, plus utiles, plus économiques et permettant de gagner du temps ? Comment pourra-t-il suivre le rythme des cycles d'innovation menés par les grandes entreprises technologiques ? Ce sont les défis qui se posent du côté des fournisseurs du secteur.

Jusqu'à présent, ces possibilités n'ont pas été exploitées, peut-être parce que les anciens systèmes de contrôle d'accès dépendent de contrôleurs de porte installés dans une architecture en série et reliés par un câblage RS-485 à une unité centrale ou un serveur. La plupart des systèmes sont également propriétaires, ce qui signifie que le contrôleur de porte est « verrouillé » pour n'autoriser sa gestion que par le logiciel

désigné par le fournisseur. Cela limite l'utilisateur final à un seul fournisseur de matériel et de logiciels, et la complexité de ces systèmes nécessite souvent un personnel expert pour l'installation et la configuration.

Lors de l'extension des systèmes d'accès traditionnels, le processus est compliqué par le fait qu'un contrôleur central standard est conçu pour s'adapter à un certain nombre de portes, les configurations non standard entraînant des coûts élevés en raison de la flexibilité limitée du système. Par exemple, ajouter une seule porte supplémentaire peut entraîner des coûts beaucoup plus élevés, rendant l'ajout injustifiable du point de vue économique.

Les réseaux IP ont permis d'introduire une architecture de système de contrôle d'accès physique beaucoup plus simple et facile à installer, présentant une flexibilité et une personnalisation plus poussées. Les professionnels de l'informatique ont une préférence marquée pour les véritables dispositifs IP et leur utilisation dans les systèmes de contrôle d'accès en réseau. Il est essentiel d'inclure ces personnes dans le futur processus de conception, car elles garantiront l'utilisation de ces dispositifs IP, eux-mêmes essentiels pour réduire le coût de l'expansion et seront une exigence pour les futures conceptions de contrôle d'accès.

3.4 Protocoles ouverts

L'avenir du contrôle d'accès est lié à la volonté des fabricants de partager leurs compétences et leurs capacités dans un forum à protocole ouvert. La résistance à cette ouverture est évidente. De nombreux développeurs de systèmes d'accès semblent privilégier un processus qui lie les utilisateurs finaux à leurs propres solutions, garantissant ainsi de futurs revenus. Mais cette approche n'a aucune valeur à long terme. Les utilisateurs exigent davantage de leurs solutions et sont heureux de partager leurs données pour y parvenir.

Les concepteurs de systèmes et les fournisseurs d'accès ont rarement les ressources ou le savoir-faire informatique pour offrir toutes les solutions que demandent les utilisateurs dans le cadre d'un système de sécurité physique complet. Bon nombre d'entre eux ne semblent pas avoir conscience que leurs offres sont rapidement éclipsées par de nouvelles solutions innovantes qui menacent à la fois leur modèle économique et leur position sur le marché du contrôle d'accès. Les capacités des systèmes les plus récents et la rapidité de l'innovation actuelle sont telles que nous sommes maintenant sur le point de ne plus avoir besoin du tout de contrôleurs d'accès, évidemment remplacés par des unités E/S intelligentes.

Les protocoles ouverts permettent aux vendeurs de réaliser des dispositifs adaptés aux systèmes d'accès de petite taille, pour lesquels la simplicité est essentielle et les coûts d'achat et d'installation doivent être compétitifs. Ces mêmes dispositifs peuvent ensuite être adaptés à des opérations plus importantes et plus complexes sur le plan technique et selon les besoins. Cette flexibilité est la caractéristique de la sécurité moderne et garantit que les systèmes achetés aujourd'hui seront toujours pertinents à l'avenir, au fur et à mesure du développement de l'activité de l'utilisateur et de l'évolution de ses exigences.

Vous trouverez plus d'informations sur l'ouverture et la technologie ouverte sur le site de l'ONVIF *www.onvif.org*, un organisme industriel créé pour conduire le développement vers des normes ouvertes.

4 Barrières techniques à l'adoption

Il y a beaucoup de choses à considérer en termes de connexions techniques, interfaces et dispositifs qui rendent le contrôle d'accès numérique possible. Le passage des systèmes traditionnels aux systèmes cloud peut avoir des conséquences. Les paragraphes suivants détaillent les points à prendre en compte pour éviter que la technologie existante et les processus qui lui sont associés, ne deviennent un obstacle à la mise à niveau et à l'adoption de nouvelles solutions.

4.1 Contrôleurs RS-485

L'une des considérations est le déploiement du contrôleur RS-485 et le risque potentiel d'installer des dispositifs semi-intelligents qui possèdent rarement, voire jamais, une adresse MAC, ce qui les rend difficiles à identifier. RS-485, également appelé TIA-485(-A) ou EIA-485, est une norme définissant les caractéristiques électriques des pilotes et des récepteurs, destinés à être utilisés dans les systèmes de communication série. Les signaux électriques sont équilibrés et les systèmes multipoints sont pris en charge. Mais la norme RS-485 ne spécifie que la couche physique, le générateur et le récepteur. Elle ne régit pas la couche vitale des communications.

Notez bien que l'absence d'adresse MAC ou l'adoption d'une architecture série ne signifie pas en soi des problèmes de fiabilité ou des effets néfastes sur le fonctionnement d'un système de contrôle d'accès : ce sont les piliers du contrôle d'accès depuis plus de 30 ans. Cependant, il est difficile d'imaginer des avancées en matière de sécurité si chaque dispositif de contrôle d'un système de contrôle d'accès n'est pas intelligent et ne peut être traité individuellement. Nous postulons que seuls des systèmes totalement intelligents et des dispositifs complètement accessibles peuvent apporter la valeur future attendue. Notez que « complètement accessibles » ne signifie pas que les dispositifs sont dépourvus de cybersécurité, bien au contraire.

4.1.1 Open Supervised Device Protocol (OSDP)

Une nouvelle méthode de communication, acceptée par la Commission électrotechnique internationale (CEI) et qui offre la possibilité d'accroître la sécurité des communications d'accès, est le protocole OSDP (Open Supervised Device Protocol). C'est une norme de communication de contrôle d'accès développée par la SIA (Security Industry Association) pour améliorer l'interopérabilité des produits de contrôle d'accès et de sécurité. L'OSDP utilise un cryptage de 128 bits, prend en charge les installations multipoints et supervise les connexions pour signaler les problèmes de lecteur. Il convient également de noter que l'OSDP prend en charge les lecteurs de cartes, les gâches de porte, les contacts d'alarme et les fonctions de demande de sortie en utilisant seulement 2 fils, au lieu des multiples connexions qui étaient auparavant nécessaires pour chaque porte. Le site de la SIA rapporte : « La norme OSDP a été approuvée comme norme internationale par la Commission électrotechnique internationale en mai 2020 et publiée sous le nom de CEI 60839-11-5 en juillet 2020. La norme OSDP de la SIA est en constante amélioration afin de conserver sa position de leader du secteur ».

4.2 La valeur des dispositifs avec adresse MAC

L'adresse MAC est l'adresse matérielle unique au monde d'une seule carte réseau ou d'un seul périphérique. En ce qui concerne les réseaux informatiques, l'adresse MAC est tout aussi importante que l'adresse IP. Les adresses MAC identifient de manière unique un ordinateur sur le réseau local et sont nécessaires au fonctionnement des protocoles réseau tels que TCP/IP. L'adresse MAC est codée en mémoire dans le périphérique et, bien qu'il soit possible de la copier via le système d'exploitation, ce n'est bien sûr pas conseillé, et l'adresse doit être protégée par votre solution de sécurité.

TCP/IP et d'autres architectures de réseau courantes adoptent généralement un modèle d'interconnexion de systèmes ouverts (OSI), dans lequel la fonctionnalité du réseau est subdivisée en couches. Les adresses MAC fonctionnent au niveau de la couche de liaison des données (couche 2 du modèle OSI) et permettent aux ordinateurs de s'identifier de manière unique sur un réseau. Le filtrage des adresses MAC ajoute une couche supplémentaire de sécurité. Avant d'autoriser un périphérique à rejoindre le réseau, le routeur vérifie son adresse MAC dans une liste d'adresses approuvées. Si l'adresse du client se trouve dans la liste du routeur, l'accès est autorisé, sinon il est refusé.

4.2.1 Alimentation par Ethernet (PoE)

PoE offre deux avantages qui se retrouvent dans toutes les applications : des économies de coûts et une flexibilité dans le positionnement des périphériques. PoE transporte les données et l'alimentation électrique sur le même câble, ce qui permet la simplification de l'architecture des dispositifs par rapport aux conceptions traditionnelles. Il est intéressant de noter que de nombreux systèmes de contrôle d'accès sont présentés comme des systèmes sur IP.

5 Les caractéristiques des meilleures pratiques

La gestion du contrôle d'accès est un élément important pour gérer efficacement le flux de personnes et contrôler l'accès. Bien plus que le simple verrouillage d'une porte ou la mise en place d'une barrière, les entreprises ont besoin de meilleures options de contrôle pour améliorer leur service à la clientèle et offrir des niveaux élevés de sécurité et de sûreté à tout moment. L'adoption d'une approche par les meilleures pratiques pour réaliser un contrôle d'accès exhaustif ne se limite pas à choisir les bons outils. Il s'agit de mettre en place la bonne architecture, d'intégrer des technologies de haute qualité, de suivre les bonnes procédures et les bons protocoles, et d'encourager le personnel et les acteurs en jeu à adopter les attitudes et les comportements adéquats.

5.1 Gestion des acteurs et convergence de l'approche sécurité

De même que l'environnement technologique converge vers une infrastructure commune pour fournir les technologies opérationnelles nécessaires au bon fonctionnement de ces sites, le processus décisionnel doit être le fruit d'une convergence de vues. Nous avons déjà vu des exemples réussis où une démarche de convergence de la sécurité a décloisonné les services et permis une meilleure collaboration entre les différentes équipes. Cette convergence revêt aujourd'hui une importance cruciale, alors que des solutions de sécurité physique et électronique traditionnelles disparates coexistent sur les réseaux.

Les équipes chargées de la sécurité physique doivent pouvoir compter sur des technologies qui soutiennent leurs besoins opérationnels et éliminent les risques associés, mais qui respectent en même temps les politiques de sécurité informatique et veillent à empêcher que les dispositifs physiques deviennent une porte dérobée d'intrusion sur le réseau. Avec la collaboration de tous les acteurs, il est possible d'aboutir à un environnement informatique et physique sécurisé.

5.2 Partenaires, fournisseurs et prestataires : attentes

Il est important de s'assurer que les acteurs tiers comprennent l'importance de maintenir les meilleures pratiques de sécurité au premier plan de tout ce qu'ils font, et qu'ils opèrent pour répondre à des besoins spécifiques. Les relations avec les prestataires sont essentielles à l'établissement d'une chaîne d'approvisionnement saine et d'un lien de confiance fort.

L'évaluation des prestataires et de leur impact sur la chaîne d'approvisionnement porte sur plusieurs aspects importants : Ils comprennent et reconnaissent les risques associés à la cybersécurité > Ils peuvent démontrer une approche mature de la cybersécurité et disposent de processus et d'outils adéquats > Ils comprennent l'impact de leur offre sur les réglementations et la législation > Ils peuvent démontrer comment ils soutiendront les exigences de conformité d'un utilisateur > La cybersécurité est un processus et pas seulement une technologie. Ils peuvent prouver l'existence d'une gestion du cycle de vie de la cybersécurité pour protéger l'entreprise d'un utilisateur.

5.3 La gestion de la sécurité : Gouvernance et processus fournisseurs

Comme toute sécurité efficace, la cybersécurité porte sur la profondeur de la défense. Il s'agit de protéger convenablement le réseau de caméras IP à tous les niveaux, depuis les produits et partenaires retenus jusqu'aux conditions définies.

5.3.1 Normes et directives

ISO 27001 – ISO/IEC 27001 est un système de gestion de la sécurité de l'information qui requiert :

- L'examen systématique des risques de sécurité informatique de l'entreprise, tenant compte des menaces, des vulnérabilités et de leurs conséquences ;
- L'élaboration et la mise en œuvre d'une suite complète et cohérente de contrôles de sécurité informatique et/ou d'autres formes de gestion du risque (comme le contournement ou le transfert du risque) pour traiter les risques jugés inacceptables ;
- L'adoption d'un processus global de gestion pour s'assurer que les contrôles de sécurité informatique restent en permanence conformes aux besoins en sécurité informatique de l'entreprise.

5.3.2 Cyber Essentials Plus

Cyber Essentials est un programme gouvernemental britannique soutenu par les acteurs du secteur pour aider les entreprises à se protéger des menaces courantes en ligne. Cyber Essentials est un indicateur efficace pour les entreprises qui comprennent les défis posés par la cybersécurité. Il s'agit d'une évaluation de ses politiques et de ses processus. Il examine plusieurs facteurs particuliers :

- Sécurité des configurations
- Administration et contrôle des accès
- Protection contre les malwares
- Gestion des correctifs
- Pare-feu et passerelles Internet

Pour les fabricants technologiques, la première ligne de défense doit jouer sur l'atténuation du risque associé à leurs propres systèmes. Depuis le 1er octobre 2014, le gouvernement britannique impose à tous les fournisseurs répondant aux appels d'offres impliquant la manipulation de certaines informations personnelles et sensibles d'être certifiés selon le programme Cyber Essentials.

5.3.3 Secure by Design, Secure by Default

Lancé par le Surveillance Camera Commissioner en 2019, le principe **« Secure by Design, Secure by Default » (sécurisé dès la conception, sécurisé par défaut, abrégé SD2)** définit une exigence minimale pour les fabricants de systèmes de caméras de surveillance et leurs composants. Ce principe consiste à adopter une approche holistique de la résolution des problèmes de sécurité au niveau de la cause d'origine plutôt qu'à en traiter les symptômes, en agissant à pleine échelle pour réduire le préjudice global à un système ou un type de composant.

Ce principe couvre l'effort technique de long terme pour s'assurer que les principes de sécurité adéquats sont intégrés aux logiciels et aux matériels. Il porte également sur la tâche tout aussi exigeante de s'assurer que ces principes sont disponibles et exploitables pour que le marché puisse les adopter immédiatement.

Pour renforcer ses technologies, Axis a aligné le principe SD2 sur le code de conduite de la stratégie britannique de cybersécurité :

- Demande d'un mot de passe
- Indicateur de complexité du mot de passe
- Chiffrement HTTPS
- 802.1x
- Accès distant DÉSACTIVÉ (parcours NAT)

6 Guides et outils (processus fournisseurs)

Lorsqu'il s'agit de sécuriser un réseau, les entreprises déploient souvent plusieurs contrôles techniques pour créer une approche de « défense par couche » qui permet de limiter les points de défaillance et d'exposition uniques. Néanmoins, un processus crucial est souvent négligé, le « durcissement du système », qui suppose notamment de changer les paramétrages par défaut du système pour mieux le protéger des menaces de sécurité informatique. Ce processus contribue de plus à réduire le nombre de vulnérabilités inhérentes à tous les systèmes.

6.1 Guide de durcissement de la fabrication

Un processus de durcissement système doit être appliqué à tous les dispositifs connectés à un réseau, notamment les station de travail, les serveurs et autres dispositifs réseau. Comme le fournisseur est celui qui connaît le mieux les paramétrages et la configuration de son système, la responsabilité doit lui revenir de fournir à ses partenaires et utilisateurs les informations nécessaires pour protéger l'intégrité des dispositifs et de l'installation de l'utilisateur final. Un guide de durcissement doit fournir des recommandations techniques à tous les acteurs impliqués dans le déploiement de solutions de vidéosurveillance. Il doit définir une configuration de référence et fournir également des informations détaillées sur les mesures prévues face à l'évolution du champ des menaces.

Tous les fournisseurs doivent s'efforcer d'appliquer les bonnes pratiques de cybersécurité au cours de la conception, du développement et du test de leurs dispositifs. L'objectif est de réduire le risque d'un défaut qui pourrait être exploité lors d'une attaque. Cependant, la sécurisation d'un réseau, de ses dispositifs et des services qu'il prend en charge exige la participation active de l'ensemble de la chaîne d'approvisionnement et de l'entreprise de l'exploitant. La sécurité d'un environnement dépend de ses utilisateurs, de ses processus et de sa technologie. Un bon guide de durcissement doit suivre les usages de base des Contrôles CIS - Version 6.1, appelés auparavant les 20 contrôles de sécurité critiques SANS. Dans le présent document, les CSC (contrôles critiques de sécurité) sont notés CSC suivi d'un numéro.

6.2 Gestion des périphériques

Un gestionnaire de périphériques est un outil sur site qui offre un moyen simple, rentable et sécurisé de gérer des périphériques connectés. Il offre aux installateurs de sécurité et aux administrateurs système une solution très efficace pour gérer toutes les tâches majeures d'installation, de sécurité et de maintenance des dispositifs.

Système d'inventaire des dispositifs/gestion des ressources :

- Politique appliquée aux comptes et aux mots de passe

- Installation efficace des mises à jour de firmwares et d'applications
- Applications des contrôles de cybersécurité : gestion de HTTPS et chargement des certificats IEEE 802.1x, gestion des comptes et des mots de passe
- Gestion du cycle de vie des certificats : gestion de toutes les tâches d'installation, de sécurité et d'exploitation
- Configuration rapide et facile des nouveaux dispositifs : sauvegarde et restauration des paramètres
- Applicable aux sites de toutes tailles : installations sur un ou plusieurs sites

6.3 Défis associés aux OEM / ODM

Les fabricants d'équipements d'origine ou OEM (Original Equipment Manufacturer) sont des fabricants qui revendent le produit d'une autre entreprise sous leur propre marque. Un fabricant de concepts d'origine (ODM, Original Design Manufacturer) est une entreprise qui conçoit et fabrique un produit spécifié par une autre entreprise, laquelle lui appose sa marque pour le vendre. Ces sociétés permettent à l'entreprise qui donne la marque de s'engager en production sans avoir à créer ou à gérer une usine.

L'adoption d'un modèle OEM ou ODM comporte de nombreux avantages pour une marque. Le premier est l'élimination de tout risque et des coûts de fabrication. La marque peut dès lors se recentrer sur l'aspect vente et marketing. C'est l'une des principales raisons pour laquelle de nombreuses marques de caméras du marché recourent aux OEM ou ODM pour leurs produits. On a relevé jusqu'à 96 fournisseurs qui revendent actuellement des caméras d'un fabricant OEM ou ODM.

Ce modèle pose plusieurs problèmes difficiles, le plus évident étant celui de la cybersécurité. Si un fabricant présente une vulnérabilité sur ses produits, cela peut avoir un impact sur tous les autres revendeurs et partenaires de la chaîne d'approvisionnement. D'autre part, la visibilité complète de la chaîne d'approvisionnement peut être très délicate à atteindre. Du fait du nombre important de fabricants OEM et ODM en activité, même un utilisateur final ayant appliqué une vigilance renforcée et refusé des technologies d'un fabricant donné, pourrait au final utiliser ces mêmes technologies sans le savoir sous une forme reconditionnée d'une autre marque.

6.4 Microprocesseur

Il s'avère que des microprocesseurs génériques équipant les dispositifs sont la cible des hackers du fait du grand nombre de vulnérabilités identifiées. La cause principale de cette situation est l'effet d'échelle qu'une seule vulnérabilité identifiée peut produire. Parmi les exemples récents, citons les failles « Meltdown » et « Spectre », deux attaques par canal latéral contre les microprocesseurs des CPU modernes, qui permettent d'accéder illégalement à des données à l'aide d'un code non privilégié.

La plupart des appareils y sont vulnérables d'une manière ou d'une autre, depuis les smartphones jusqu'aux équipements des datacenters. Les principaux éditeurs de systèmes d'exploitation ont produit des correctifs permettant d'atténuer les problèmes, mais certaines parties doivent être installées par le fabricant OEM car ils contiennent des éléments propres à la plateforme. Le Centre britannique de cybersécurité (NCSC) préconise d'appliquer les correctifs le plus vite possible.

6.5 Stratégie de firmware

La signature du firmware est importante pour les utilisateurs finaux et réduit certains risques potentiels de sabotage des dispositifs au cours du processus logistique ou de distribution. Parfois dénommée hachage,

cette signature est ajoutée au firmware lors de sa distribution. Un processeur calcule son propre hachage et ne chargera qu'une image du firmware dont le hachage correspond à celui signé par un certificat auquel il fait confiance.

6.6 La gestion des vulnérabilités

La hausse ininterrompue de la cybercriminalité et des risques correspondants oblige de nombreuses entreprises à se concentrer davantage sur la sécurité des informations. Un processus de gestion des vulnérabilités doit faire partie des initiatives de l'entreprise pour atténuer les risques liés à la sécurité des informations. Ce processus lui donnera une vue d'ensemble complète des vulnérabilités de son environnement informatique et des risques associés qu'elle encourt. Ce n'est que par l'identification et l'atténuation des vulnérabilités de son environnement informatique qu'une entreprise peut se préserver de l'intrusion de cybercriminels dans ses réseaux et du vol d'informations.

Les fournisseurs doivent impérativement garantir l'application de processus de gestion des vulnérabilités dans leurs opérations, notamment pour détecter et remédier aux vulnérabilités dans tous leurs systèmes, et pour éviter l'introduction de nouvelles vulnérabilités au cours de changements et de déploiement de nouveaux systèmes. Toutes les questions liées au risque que le fournisseur accepte de prendre doivent être communiquées et convenues avec l'utilisateur final. Si ce principe n'est pas mis en œuvre, des cybercriminels pourraient lancer des attaques contre une entreprise et ses fournisseurs.

Les correctifs de sécurité et les actualisations de vulnérabilités doivent être installés en temps utile selon un processus formalisé pour empêcher les violations de sécurité. Les fournisseurs exploitant des systèmes qu'il n'est pas possible de mettre à jour, quelle qu'en soit la raison, doivent mettre en place des mesures pour protéger ces systèmes vulnérables. Tous les changements entrepris doivent respecter le processus de conduite du changement du fournisseur.

6.7 Notifications d'alertes de sécurité

Les alertes de sécurité aident à réduire les risques dus à des vulnérabilités connues. L'alerte de sécurité peut faire référence aux rapports officiels CVE (Common Vulnerability and Exposure) ou à d'autres rapports sur les vulnérabilités. Il comprend une description de la vulnérabilité, une évaluation des risques, des recommandations et des informations sur la date de disponibilité d'une version du service. La plupart des fournisseurs sont régis par un modèle de vente indirecte et s'appuient sur un programme de partenaires.

Les notifications d'alertes de sécurité permettent aux clients n'appartenant à aucun programme de partenaires du fabricant de recevoir des notifications de cybersécurité dès que possible lorsqu'elles sont transmises au réseau de distribution. C'est un outil précieux pour les utilisateurs finaux chez lesquels des équipements sont installés mais qui n'ont pas souscrit de contrat auprès de l'installateur d'origine.

6.8 Modèle BSIMM

Le BSIMM est un cadre de mesure de la sécurité logicielle établi pour aider les entreprises à comparer leur sécurité logicielle avec d'autres initiatives et à savoir où elles en sont. Le BSIMM aide à évaluer les processus, les activités, les rôles et les responsabilités dans le domaines suivants :

- Examen de la conception et de l'architecture
- Examens des codes
- Essais des vulnérabilités connues

- Exécution d'un outil standard d'analyse de détection des vulnérabilités CVE dans les logiciels open source

6.9 Assistance long terme (LTS)

L'assistance de long terme (LTS en anglais) est une politique de gestion du cycle de vie d'un produit, dans laquelle une version logicielle est maintenue stable pendant plus longtemps que son édition normale. Le firmware LTS doit inclure uniquement des correctifs relatifs à la stabilité, la performance et la sécurité. Les fournisseurs fournissent leur firmware LTS pendant 10 ans à partir de la commercialisation d'un produit.

Il est prévu que l'assistance LTS existe en parallèle à l'assistance active existante, mais indépendamment. L'assistance LTS a pour principal avantage de préserver l'intégration à des tiers liés à la version du firmware d'origine.

6.10 Formation et collaboration

L'un des critères essentiels à évaluer dans la sélection d'un fournisseur de technologies concerne la formation et l'assistance qu'il fournit. Comme les problématiques de la filière et du secteur évoluent, particulièrement en matière de cybersécurité, les fabricants doivent s'emparer du sujet et proposer au marché du contenu et de la documentation en rapport. En voici quelques exemples :

- Des cours de cybersécurité en présentiel et gratuits
- Formation en ligne la cybersécurité
- Test rapide en ligne de cybersécurité
- Guide de durcissement
- Politiques sur les vulnérabilités
- Meilleures pratiques de cybersécurité
- Concepts et termes employés en cybersécurité

7 Création d'un profil de cyberhygiène : prochaines étapes et considérations

Une bonne cyberhygiène implique l'identification, la hiérarchisation et la réponse aux risques pour les principaux services et produits de l'entreprise. La mise en œuvre des meilleures pratiques de sécurité en matière de cyberhygiène contribuera à prévenir les violations de données et les configurations incorrectes des systèmes, ainsi qu'à minimiser les risques associés pour l'entreprise. Il est également important d'obtenir l'accord des parties prenantes sur les principaux domaines de menace, afin de se concentrer sur les objectifs essentiels de la gestion des risques.

Bien qu'il ne s'agisse pas d'une liste exhaustive, les considérations suivantes contribueront à améliorer l'efficacité de la gestion des cyber-menaces.

7.1 Fournisseurs

Vérifier les homologations et les certifications

Examinez les homologations et les certifications, comme celle d'ISO 9000 ou autres certificats de qualité. Déterminez si les produits du fournisseur ont été conçus pour fonctionner sur un réseau d'entreprise.

Rechercher des preuves d'application des meilleures pratiques

Veillez à ce que le fournisseur choisi puisse démontrer qu'il applique les meilleures pratiques en matière de cybersécurité. Il doit proposer un guide de durcissement qui décrive les mesures de cybersécurité et de sécurité physique, ainsi que les meilleures pratiques visant à sécuriser le réseau.

Faire l'audit du fournisseur

Réalisez un audit approfondi avant de vous engager dans un achat. Vérifiez bien les conditions commerciales pour vous assurer de leur clarté et de leur transparence. D'un point de vue financier, il est important de se demander ce qu'il adviendrait du produit et de l'assistance en cas de difficulté de l'entreprise.

Déterminer les ressources pour un soutien continu

Vérifiez que votre fournisseur dispose bien des ressources nécessaires pour continuer à créer les solutions dont vous pensez avoir besoin à l'avenir. Vérifiez que votre fournisseur est d'une taille, d'une envergure et d'une capacité suffisantes pour répondre aux besoins de votre entreprise à l'avenir.

Définir les besoins de l'activité future

Concentrez-vous sur vos besoins à l'avenir. Les dispositifs et solutions intelligents ont la capacité de développer l'activité et de préparer l'avenir d'une entreprise. Vous devez donc être certain que le fournisseur répondra à vos attentes, voire les dépassera, en vous proposant des contrats de maintenance et une assistance permanente.

Chercher à vérifier l'éthique des pratiques commerciales

Recherchez des preuves de pratiques durables et éthiques. Un partenariat fondé sur la confiance et des objectifs communs constitue une base solide pour sa pérennité. Le fournisseur a-t-il mis en place des systèmes de gestion environnementale, un programme de responsabilité sociale des entreprises (RSE) ou une politique d'approvisionnement éthique ?

7.2 Produits et systèmes

Réaliser un contrôle préalable

Effectuez un contrôle technique préalable du système et de ses éléments de base pour vous assurer qu'il apporte de la valeur et qu'il n'existe pas de facteurs sous-jacents susceptibles d'affecter son fonctionnement. Veillez à ce que les informations sur l'évaluation et l'atténuation des risques soient disponibles et claires.

Vérifier le contrat de maintenance

Vérifiez ce qui est inclus dans le contrat, par exemple si le contrat de service et de maintenance comprend les mises à jour des logiciels du fabricant et les mises à niveau des firmwares.

Sécuriser les dispositifs connectés

Assurez-vous que votre système de sécurité physique connecté au réseau est bien sécurisé. Les systèmes de sécurité doivent être déployés en tenant compte de la cybersécurité : changement du nom d'utilisateur et du mot de passe par défaut, installation du dernier firmware, utilisation du cryptage (idéalement HTTPS), désactivation de l'accès à distance.

Demander une déclaration de sécurité de conception des produits

Votre fournisseur doit être en mesure de présenter une déclaration de sécurité de conception prouvant la cybersécurité de tous les dispositifs connectés.

Évaluer l'intelligence du système

Les dispositifs connectés qui sont pleinement intelligents sont ceux qui sont mis en réseau avec une adresse MAC et font partie intégrante de l'architecture du système. Les dispositifs sans adresse MAC ne sont pas considérés comme intelligents et ne peuvent être identifiés, gérés ou protégés individuellement.

Évaluer la conformité au RGPD / Data Protection Act

Le RGPD est entré en vigueur en 2018, en même temps que la mise à jour du Data Protection Act de 1998. Assurez-vous que les produits et les systèmes sont conformes au RGPD et au Data Protection Act 2018.

T10168631/FR/M1.7/2107

À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader technologique de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès, l'interphonie et les systèmes audio. Axis emploie plus de 3 800 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été créée en 1984 et son siège social se situe à Lund, en Suède.

Pour plus d'informations sur Axis, rendez-vous sur notre site Web *axis.com*.