SMART BUILDINGS ALLIANCE
FOR SMART CITIES

LA CYBER SÉCURISATION DES BÂTIMENTS TERTIAIRES

LIVRE BLANC

La commission Cyber Building

Animée par Alain Kergoat, co-fondateur d'Urban Practices et directeur des Programmes de la SBA, et par Jean-Christophe Denis, directeur Urbanisation et responsable Cyber Building chez WALLIX Groupe, la commission Cyber Building fait partie des commissions du pilier Smart Building de la SBA.

Lancée en 2021, la commission réunit aujourd'hui plus de 60 membres issus de toutes tailles d'entreprises, de la TPE au grand compte, qui représentent l'ensemble des corps de métiers de la filière : maîtrise d'ouvrage, maîtrise d'œuvre, exploitation, fourniture de solutions. Elle intègre également des représentants d'organismes publics ou parapublics.

Sa feuille de route consiste à sensibiliser à la démarche de cybersécurité, en réunissant tous les acteurs concernés par la sécurité et les données du bâtiment, pour ensemble poser les enjeux, principes et cadres d'action d'une démarche de Cyber Building. Ensuite, l'ambition de la commission est de travailler sur une extension cybersécurité du cadre de référence R2S (Ready2Services) pour les bâtiments dits sensibles.

La commission Cyber Building a vocation à définir une vision partagée et un langage commun de l'ensemble des acteurs des différents thèmes de la cybersécurité appliquée au bâtiment.

La SBA remercie chaleureusement les personnes qui ont contribué à ce livre blanc :
ACOME, Julien Leroy • ACTIVUS GROUP, Laurent Fraimont et Cédric Thevenot • ACS-2I, Gilles Trojani • AFNOR, Brice Gilbert • ALLIANZ, Sébastien Chemouny • ANITEC, Lilian Caule • AN2V, Virgile Augé • ANSSI, Éric Hazane • ARCOM, Philippe Raynaud • CAISSE DES DÉPÔTS, Aymeric Buthion • CNPP, Nathalie Labeys et Ronan Jezequel • CYBERHUB, Philippe Hubert • DALKIA SMART BUILDING, Jean-Christophe Clément • ENGIE, Loïc Mouëzy et Gilles Courtes • ENOCEAN, Emmanuel François • GATEWATCHER, Karim Mazoir • HPE, Vincent Blavet • HYVILO, Damien Couval • ICADE, Frédéric Caufriez et Alexandre Masraff • IGNES, Anne-Sophie Perrissin-Fabert • INGETEL, Nicolas Le Net et Gilles Genin • IMAPROTECT, Henri Morawek • KARDHAM DIGITAL, Pascal Zerates • MOBOTIX, Patric Ferrant • OCCITALINE, Daniel Zotti • ONEPOINT, Sophie Lérault • ORANGE, Nicolas Joulain et Grégory Levilain PICHET, Julien Ohayon • PATRIARCHE, Maxime Favre-Mercuret • POLESTAR, Christian Carle • SIA PARTNERS, Ronan Mac Farlane • SIEMENS, Mathieu Demont • SIGNIFY, François Darsy • SPAC, Mickaël Wajnglas • STID, Sandrine Castillo et Baptiste Dupart • SYLVANIA LIGHTING, Pierre Taing • SYS ET COM, Stéphane Rigolet • TWO-I, Ariane Truffert • URBAN PRACTICES, Alain Kergoat • WALLIX Groupe, Jean-Noël de Galzain et Jean-Christophe Denis • WAVESTONE, Gérôme Billois.

Nous voulons également remercier les membres du Club CyberOT du GIMELEC pour leurs apports et la qualité des échanges qui nous ont permis collectivement de faire grandir notre vision de la cybersécurité du bâtiment : Marc Coutelan, NOZOMI Networks • Rodolphe de Beaufort, GIMELEC • Yoann Delomier, WALLIX Groupe • Vincent Nicaise, STORMSHIELD • Bernard Piqueras, WEIDMULLER • Stéphane Potier, ADVENS • Jocelyn Zindy, EIFFAGE Énergie Systèmes.

Lidia Zerrouki : Direction de la publication
Alain Kergoat : Direction des programmes
Jean-Christophe Denis (WALLIX Groupe) : Direction éditoriale
Pierre-Marie Pacaud : Direction Marketing et communication
Conception graphique et illustrations © Les 5 sur 5
Dépôt légal : janvier 2023. ISBN 978-2-491340-22-3

ÉDITO

Les deux grands défis du monde dans lequel nous vivons sont ceux de la transition environnementale et de la transformation numérique. En cela, le bâtiment intelligent est un projet passionnant puisqu'il réunit ces deux aspects pour révolutionner l'immobilier. Avec le « Smart Building », le bâtiment devient une plateforme d'objets connectés et de services numériques destinée à assurer la sécurité des occupants et leur mobilité totale, l'optimisation des espaces avec des applications servicielles, l'interconnexion des équipements informatiques et des capteurs pour améliorer l'efficacité énergétique et la sûreté. Ces dispositifs numériques rendent également les bâtiments plus bavards, générant des données et des contenus à protéger contre les cyberattaques et les fuites de données, conformément à la réglementation RGPD en vigueur depuis 2018.

Pour rendre le bâtiment à la fois plus économique, plus écologique et plus serviciel, le Smart Building implique une approche responsable et l'usage de technologies numériques viables et fiables. Le bâtiment opère sa transformation numérique avec des innovations technologiques qui décuplent sa valeur immobilière et son attractivité, dans un contexte où les cyberattaques deviennent le premier risque auquel doivent faire face les organisations et les entreprises. Ces défis nécessitent une approche de la cybersécurité intégrée par conception (Security by Design), dans tous les systèmes de gestion du bâtiment, les capteurs, la gestion des accès et des services offerts, l'interconnexion avec les équipements mobiles, et ce que l'on appelle le « smart office ».

Concevoir et investir dans les bâtiments intelligents est donc aujourd'hui un enjeu vital et un atout stratégique en termes d'écologie, de sécurité et de bien-être des occupants. Mais cette transformation numérique de l'immobilier s'accompagne en conséquence d'une approche holistique de la cybersécurité, de manière à protéger les utilisateurs et leurs données personnelles de risques numériques, et des menaces internes ou externes auxquelles ils sont exposés. Mettre en place une stratégie pour prévenir les risques inhérents à la numérisation des bâtiments est ainsi devenu incontournable. Mais par où commencer ? Comment s'y prendre ? Vers quels acteurs se tourner ?

La tendance « Security by Design » dans l'immobilier est récente. Elle est rendue nécessaire à chaque cahier des charges pour la construction de nouveaux bâtiments intégrant des systèmes intelligents. L'objectif de ce livre blanc est de permettre à tous ceux qui s'intéressent à ce sujet d'en comprendre les concepts et les cas d'usage, de découvrir les solutions disponibles qui permettent de répondre à ces enjeux, et d'intégrer la dimension cybersécurité au cœur de la réussite d'un projet de Smart Building.

Foncières, bailleurs, collectivités, industriels, experts et dirigeants d'entreprises se sont réunis au sein de la commission Cyberbuilding de la SBA, pour partager un langage commun, allier technologies, usages et métiers pour relier le meilleur des deux mondes.

Une nouvelle page s'ouvre pour l'immobilier, l'avènement des Cyber Smart Buildings…

Jean-Noël de Galzain, fondateur et CEO, WALLIX Groupe
Benjamin Ficquet, Vice-Président Smart Buildings, SBA

SOMMAIRE

INTRODUCTION

Nous entrons dans un monde hyper connecté dans lequel tout citoyen, tout bâtiment, tout équipement, toute mobilité, toute infrastructure, seront connectés et interagiront entre eux en temps réel. Cette tendance de fond semble inéluctable pour répondre aux grands enjeux de société actuels tant environnementaux, qu'économiques et sociétaux. Face à cette évolution majeure de notre société, une condition s'impose: la confiance. Sans confiance, cette (R)évolution n'aura pas lieu sereinement.

Cela sous-entend de disposer de systèmes résilients répondant à des critères de cybersécurité toujours à la pointe. La cybersécurité devient dès lors la pierre angulaire de cette révolution numérique avec des enjeux tant sur les données que sur les équipements et systèmes parmi lesquels émergent deux grands ensembles: l'informatique (IT: Information Technology) et les systèmes industriels (OT: Operational Technology).

Avec l'avènement de la cybersécurité, d'autres problématiques émergent autour de la confidentialité des données, questionnant l'éthique numérique et les libertés individuelles, mais aussi autour des enjeux d'intégrité et de disponibilité de la donnée. À ce jour, les experts s'accordent à dire «*qu'il est déjà minuit bien passé et que le risque est omniprésent*» (Interview d'Emmanuel François, ancien président de la Smart Buildings Alliance). Quand on sait que près de 90% des objets connectés aujourd'hui ne répondent pas aux règles minimales de cybersécurité, il est urgent de s'interroger et d'agir. La Commission européenne a d'ailleurs saisi l'importance du défi de la cybersécurité et a posé les premiers jalons pour un «Cyber Resilience Act».

Ce livre blanc répond lui aussi à cette urgence d'une meilleure prise en compte de la cyber résilience appliquée au bâtiment en général et au Smart Building en particulier. Il fait le point sur l'état à date des outils et des méthodes à disposition des professionnels pour renforcer la cybersécurité de leur projets bâtimentaires et les éclaire sur les bonnes pratiques à mettre en œuvre en s'appuyant sur des exemples concrets.

1

ENJEUX, DÉFIS ET CHAMP D'ACTION

Relier le monde des systèmes industriels (OT : Operational Technology) et celui de l'informatique (IT : Information Technology) soulève d'emblée un différentiel dans leurs temporalités et leurs éléments de langage. Cela implique d'opérer une démarche de sensibilisation des différentes parties prenantes d'un projet de bâtiment intelligent et sécurisé.

Les équipementiers doivent être accompagnés dans leur capacité à réaliser les intégrations avec les solutions de cybersécurité. Les architectes du bâtiment et les architectes des systèmes d'information doivent plus que jamais travailler de concert. Les mainteneurs et exploitants doivent être sensibilisés aux bonnes pratiques à déployer et les inclure dans leurs plans de sécurisation. Enfin, pour favoriser l'adoption des solutions de cyber sécurisation du bâtiment, les personnels opérationnels doivent être formés à leur utilisation.

DÉFINITION D'UN SYSTÈME D'INFORMATION BÂTIMENTAIRE (SIB)

Face à la numérisation croissante des métiers et à l'hybridation des usages du bâtiment, il convient de définir ce que nous appellerons un Système d'information bâtimentaire (SIB) afin de fonder de manière pérenne la stratégie de cybersécurité.

Nous proposons ainsi de considérer trois familles de systèmes :
- les systèmes d'information techniques bâtimentaires ;
- les services digitaux du bâtiment aux usagers ;
- les systèmes de gestion du bâtiment.

Les systèmes d'information techniques bâtimentaires sont définis comme les systèmes d'information dont tout ou partie des éléments actifs essentiels sont présents physiquement dans le bâtiment et qui concourent à la maintenance, la sécurité, la sûreté, la connectivité, aux objectifs RSE de l'immeuble et à son exploitation. Cette définition englobe notamment le système de sûreté (contrôle d'accès, vidéo surveillance, détection anti-intrusion…), la gestion technique du bâtiment (GTB, les infrastructures GSM indoor et le WiFi, les ascenseurs, les systèmes IoT, les infrastructures de recharge des véhicules électriques (IRVE), le système de comptage des places de parking, l'arrosage automatique, la gestion de la performance énergétique (GTPE), la visiophonie/interphonie.

Les services digitaux du bâtiment aux usagers comprennent des applications locales ou SaaS (Software as a Service) liées à des services comme notamment le restaurant d'entreprise, la conciergerie, l'espace de coworking, la gestion des salles de réunion, les mini-boutiques, l'imprimante partagée, la réservation de places de parking… Ce sont des systèmes ayant une interface avec l'usager du bâtiment.

Les systèmes de gestion du bâtiment comprennent par exemple les outils de gestion immobilière, l'outil de ticketing de la maintenance, le BIM (Building Information Modeling), le BIM-GEM (BIM-Gestion exploitation maintenance), le BOS (Building Operating System)/Jumeau numérique, la GMAO (Gestion de maintenance assistée par ordinateur), la main courante informatique du poste de sécurité. En d'autres termes, ce sont des applications destinées aux gestionnaires et exploitants du bâtiment.

« Faire de la sécurité, c'est poser des questions qui peuvent "fâcher" ou faire peur ; c'est ingrat et indispensable. Il est crucial de trouver un terrain d'entente qui (ré)concilie les différents personnels à impliquer dans le processus. »
ANSSI

Cette définition permet ainsi de définir les limites de compétences dans la gestion de cybersécurité du bâtiment. Nous distinguons un ensemble de systèmes physiquement très ancré dans le bâtiment dont les caractéristiques le rapprochent des systèmes industriels, et un ensemble d'applications qui, bien que destiné à contribuer au fonctionnement du bâtiment, reste proche des systèmes informatiques que connaissent les DSI.

ORGANISATION DE LA CYBERSÉCURITÉ DES SIB

Il est difficile de réduire les bâtiments à un profil type tant les situations de gestion, exploitation et occupation des bâtiments sont diverses : propriétaire occupant, monolocataire, multilocataires, bâtiment exploité en code du travail, en ERP ou de manière mixte, maintenance et gestion internalisée ou externalisée, etc.

Malgré tout, pour un système d'information bâtimentaire, on peut considérer trois types d'utilisateurs :
- **l'intégrateur** qui conçoit et installe le système ;
- **le mainteneur** qui en assure le maintien en condition opérationnelle ;
- **l'opérateur** qui l'exploite dans le cadre de sa mission.

Que ces utilisateurs soient un ou plusieurs, internes ou externalisés, il convient de fixer le cadre de leur contribution dans le dispositif de cybersécurité du système.
Le sujet étant émergeant, cette démarche implique un effort notable d'acculturation des prestataires. Cela commençant par l'adaptation du contrat pour y inclure des exigences et objectifs à atteindre.

➔ *Il appartient au donneur d'ordre d'exprimer ses objectifs de cybersécurité en termes de gestion des actifs informatiques, de gestion des accès physiques, de gestion des accès logiques, de durcissement, de gestion des vulnérabilités et des correctifs, de maintien en condition de sécurité, de maintenance et de gestion des incidents. Les utilisateurs externes peuvent, pour leur part, formaliser leur contribution par l'intermédiaire d'un plan d'assurance sécurité.*

LE FINANCEMENT DE LA CYBERSÉCURITÉ BÂTIMENTAIRE

En fonction du schéma d'exploitation de l'immeuble, le financement de la cybersécurité peut se révéler un véritable sujet en soit. Sur un patrimoine existant, le déploiement d'une démarche cybersécurité implique plusieurs étapes : une évaluation de l'état des SI existants, des mesures correctives pour porter la cybersécurité au niveau souhaité, la mise en place d'un maintien en condition de sécurité et ponctuellement des audits de contrôle.

Dans cette démarche, les dépenses induites peuvent s'apparenter à des dépenses de maintenance et d'exploitation. Le bailleur pourra être légitimement tenté de traiter ces dépenses en charges refacturables aux locataires. Malheureusement, le budget à allouer à la cybersécurité est relativement décorrélé de la surface locative. Ainsi, pour un immeuble de petite surface, l'aspect financier peut contraindre les ambitions de sécurité.

Sur un nouveau projet immobilier, les aspects de cybersécurité doivent être pris en amont et intégrés aux exigences des cahiers des charges des lots techniques et des contrats d'exploitation – maintenance. Ainsi l'impact économique de la cybersécurité est maîtrisé et fait partie intégrante du projet, comme toute autre qualité associée aux équipements et solutions livrés, la cybersécurité du bâtiment est donc conçue «by design» .

LES OBJECTIFS DE LA CYBERSÉCURITÉ

La cybersécurité des systèmes d'information dans le bâtiment concourt à plusieurs objectifs selon la nature du SI concerné :
- protéger les usagers de l'immeuble ;
- garantir la disponibilité de l'immeuble conformément à sa finalité ;
- empêcher que les systèmes d'information du bâtiment ne soient le vecteur d'une attaque contre les usagers et leurs SI de gestion ;
- assurer la sécurité des données personnelles des usagers et des données sensibles des entreprises locataires.

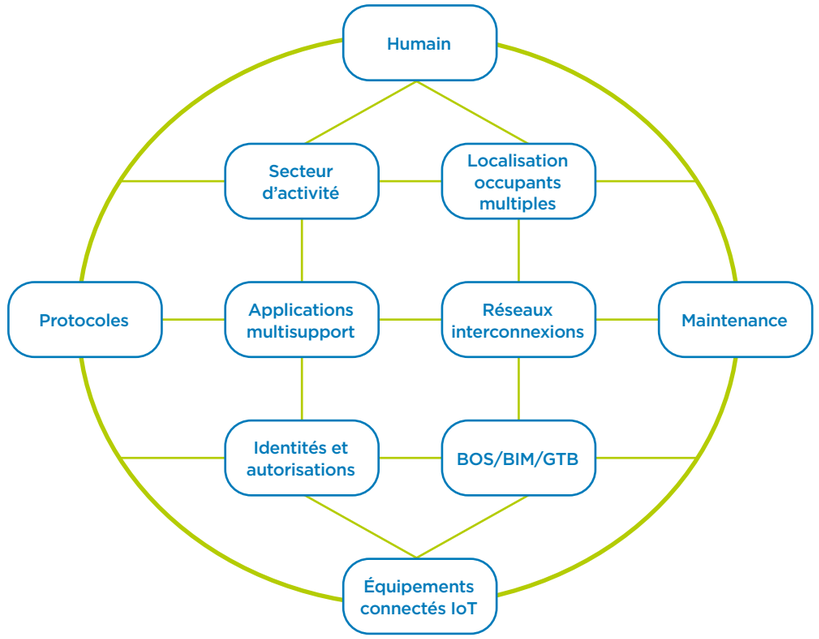
2

VECTEURS DE RISQUE ET IDENTIFICATION DES CIBLES À PROTÉGER

CYBERATTAQUES : DES DOMMAGES VIRTUELS MAIS AUSSI MATÉRIELS

Le développement du Smart Building, mais aussi de la Smart City, induit un développement du risque cyber. En effet, l'interconnexion de bâtiments, véhicules et objets implique l'utilisation de logiciels qui ne respectent pas forcément le principe de Security by Design. L'interconnexion augmente significativement le nombre de points d'entrée (appelés aussi surfaces d'attaque) dans des systèmes issus d'écosystèmes différents à la maturité cybersécurité variable.

Les vecteurs de risque sont nombreux et varient selon les activités du ou des occupants, l'emplacement du bâtiment, et d'autres critères qui seront abordés dans la gestion des risques. Ces risques peuvent provoquer des dommages aussi bien « immatériels » (vol de données, demande de rançons, paralysie du SI) que matériels.



CYBERRISQUE : LA PARALYSIE DE L'ENSEMBLE DE L'ÉCOSYSTÈME URBAIN

Non contentes de provoquer des dommages matériels d'ampleur, les futures cyberattaques dirigées contre les systèmes Smart pourraient également entraîner une paralysie de l'ensemble de l'écosystème urbain. En effet, dans un monde de milliers d'équipements interconnectés, une cyberattaque risque de créer une réaction en chaîne, ou effet domino, à partir d'une intrusion depuis un seul point d'accès.

L'enjeu est d'autant plus important que les services critiques des Smart Cities seront massivement digitalisés. Par exemple, les feux rouges pourront être interconnectés à différents fournisseurs, pour des raisons d'optimisation (gestion du trafic, redirection en temps réel, création de voies d'urgence…). Un réseau privé d'électricité pourra par exemple engendrer un arrêt momentané de la production dans les usines ou perturber les réseaux de transport. Ces réseaux seront entièrement ouverts, avec des API de communication (notamment pour l'open data).

Pour mieux appréhender ces nouveaux risques, il convient donc de se pencher sur des cas de piratage industriel aux conséquences similaires (voir annexe 2, des exemples de piratages et leurs conséquences).

MENACES A L'ÉCHELLE DU BÂTIMENT, PANORAMA DES RISQUES

La menace cyber pour un bâtiment n'est pas qu'un sujet de récupération de données pour les chiffrer ou les revendre. Les données de température, de bilan énergétique ou de parcours clients ou utilisateurs sont en effet peu intéressantes à monnayer. En réalité, chaque système d'information, selon sa fonction dans le bâtiment, selon son degré d'ouverture et d'interconnexion et selon l'activité des occupants, engendre des scenarii de menace qui lui sont propres. Une analyse de risque contextualisée est donc nécessaire pour chaque immeuble.

L'attaquant peut utiliser un biais physique ou digital/logique, ou bien une combinaison des deux. Il commencera par tenter l'attaque la plus facile à mettre en œuvre, qui nécessite le moins de compétences. Mais il saura s'adapter… et changer ses plans pour atteindre son objectif. Lors d'attaques hybrides, l'attaquant peut par exemple profiter d'un poste non verrouillé pour rebondir sur le réseau, récupérer des données, falsifier une identité, augmenter ses droits sur le réseau. Les attaques, qu'elles soient physiques ou digitales, sont liées et l'accès à l'une peut donner accès à l'autre. Il faut savoir par exemple, qu'un badge non sécurisé peut être copié en quelques secondes grâce à un équipement acheté une vingtaine d'euros sur des sites Internet.

L'attaquant prend toujours la voie la moins sécurisée, il cherche le maillon faible. Cela peut venir des applications, d'un défaut de configuration sur un firewall, d'un spam, de la crédulité et du social engineering, d'un «rogue point WiFi» ou accès sauvage WiFi… Mais cela peut venir aussi d'une erreur, d'une fausse manipulation, ou d'une défaillance dans le processus de vérification.

Quelques idées peuvent être développées à titre d'exemple :

- **un système vidéo protection ou de contrôle d'accès** peut être visé pour en dérober les données personnelles ou pour le mettre hors service. L'impact pourra être soit une perte de données sensibles, soit une brèche dans le dispositif de sécurité physique du bâtiment ;
- **un système GTB** peut être visé pour le mettre hors service ou le rendre déficient et ainsi induire des dommages matériels (température excessive dans un local serveur, par exemple) ou une gêne opérationnelle aux locataires (température trop élevée ou trop faible pour la présence des occupants, par exemple) ;
- **la maquette numérique du bâtiment** peut être ciblée soit pour en connaître les détails complets avant d'y réaliser une intrusion (et à l'extrême d'y mener une attaque terroriste), soit, de manière malicieuse, pour y corrompre les données, induire une perte de confiance dans l'outil et perturber plus ou moins fortement l'exploitation des équipements de l'immeuble et leur maintenance ;
- **les badges d'accès** peuvent être dupliqués ou volés ;
- **un lecteur de contrôle d'accès** peut être attaqué : *Rejeu* (Replay Attack) de trames échangées sur un protocole de communication entre un lecteur et un système de gestion.

L'attaque peut être également menée en utilisant un capteur de température, un système d'affichage connecté, ou en utilisant les faiblesses des protocoles de communication eux-mêmes.

➔ ***Le risque prend sa source dans les activités liées au bâtiment et à ses occupants, mais pas seulement. Il faut donc veiller à séparer les SI. Dans le cadre d'occupants multiples, il est crucial de cloisonner les activités des locataires et celles du bâtiment (GTB, sûreté, maquette numérique, flux et activités de maintenance…).***

Les risques peuvent aussi être liés à la situation géographique du bâtiment (zone citadine, industrielle, proximité de fleuve et risques d'inondations, etc.).

La proximité des bâtiments avec d'autres (dont on ne sait rien de la sécurité), et avec des infrastructures publiques (passage de personnes, véhicules etc.), le tissage de plus en plus dense des SI (partenariats, filiales internationales, franchises etc.) et leurs interactions, voire leurs dépendances, l'inférence des activités, la montée en puissance des attaquants vis-à-vis du nouvel or, les données, les enjeux économiques et sociaux induits, tout ceci, crée ou amplifie très fortement les risques. Ce sont des risques qui, à l'instar des organisations, sont en cascades.

L'objectif de l'attaquant peut être un rebond vers les SI des locataires. **La compartimentation entre le SI bâtimentaire et les SI des locataires est un aspect crucial**.

Cela peut également aller plus loin et notamment dans le domaine de l'énergie. En effet, il est avéré qu'une variation brusque de consommation énergétique de l'ordre de 3 gigawatts, soit l'équivalent de la prise de contrôle d'un million de logements ou 10 000 bâtiments tertiaires, pourrait entraîner un *blackout* énergétique à l'échelle de l'Europe !

3

CONCEPTS FONDATEURS

Le risque est inhérent à toute activité… et l'informatique n'y déroge pas. Le système d'information des bâtiments (GTB, gestion énergétique, supervision sûreté, BOS, maquette numérique…) en tant que système interconnectant des ressources et des données pouvant être critiques, est lui aussi concerné. Les données sont convoitées, c'est l'or invisible, immatériel qu'il faut protéger.

Il faut alors savoir (mesurer) ce qu'on risque, pour chaque équipement, chaque action. Pour cela, il faut établir une liste exhaustive indiquant la valeur de l'asset, ses vulnérabilités et sa criticité et la réévaluer régulièrement et donc avoir un plan cyclique de management du risque.

ÉVALUATION DES RISQUES

- Indicateurs mesurés : valeur, gravité, impact, probabilité
- Traitement du risque : acceptation, transfert, refus, risque résiduel

QUELQUES POINTS D'ATTENTION À PRENDRE EN CONSIDÉRATION :

1. Afin de protéger les personnes il faut être capable de **protéger leurs données.**
2. On ne peut pas protéger les données sans **sécuriser les personnes** qui les manipulent.
3. Chaque équipement connecté doit être connu, monitoré et accessible à travers un **système de contrôle d'accès** (IAM : Identity Access Management) évolué et régulièrement évalué. Les comptes à privilège (PAM : Priviledge Access Management) doivent avoir une sécurité renforcée.
4. Tous les comptes doivent faire l'objet d'une **politique de mots de passe** performante.
5. Le **Least privilege** : le juste privilège et son traçage (Traçabilité, non-répudiation).
6. Les mesures se complètent, se renforcent mutuellement, et la complexité inhérente doit être maîtrisée à travers un SOC (**Security Operation Center**) et toutes les données doivent être analysées dans un SIEM (**Security Incident and Event Management**), toujours en utilisant des solutions éprouvées, et les standards cybersécurité du marché.
7. La complexité amplifie les surfaces d'attaque et est porteuse de risques et d'erreurs. Simplifier n'est pas aisé, car les SI ont chacun un historique, et sécuriser un existant nécessite des plans parfois à long terme. C'est pourquoi, dans le cadre de la construction des nouveaux bâtiments, il faut **adopter les mesures et les intégrer en concertation avec les constructeurs et équipementiers à la conception**.
8. Le propriétaire doit donc avoir préalablement élaboré sa **politique de sécurité des SI du bâtiment**, afin d'inclure dans ses différents cahiers des charges l'expression de principes et/ou de règles. Ce n'est qu'en connaissance des attentes cybersécurité du propriétaire en phase d'exploitation que les intégrateurs seront en mesure de concevoir des SI conformes. À défaut, il est à craindre que les SI ne soient pas paramétrés conformément à la politique cybersécurité, ou pire, ne puissent pas permettre l'application des règles de cybersécurité du propriétaire.
9. La sécurité à 100 % n'existe pas, mais nous devons atteindre l'exhaustivité en termes de mesures de sécurité, sur la base de la liste des assets (équipements, process,

données, rôles…) réalisée lors de l'analyse de risque. Pour cela, il existe des **outils et des méthodes** basés sur des cadres de référence, des normes et des standards reconnus et déjà éprouvés en informatique de gestion (conformité ANSSI, ISO, RGPD, PCI-DSS, HIPAA…).

10. **Savoir en temps réel** ce qui se passe en termes de cybersécurité (qui fait quoi avec quelles données) et être capable **d'alerter** et **d'agir** (contrer l'attaquant, scénario de crise), mais aussi **d'anticiper**.
11. Les solutions déployées ne sont optimales que lorsqu'elles sont pleinement adoptées : il faut donc accompagner ces déploiements en intégrant **sensibilisation, transfert de compétences et conseil** (technologique, organisationnel, appui de gouvernance, exploitation).
12. Un système complexe n'est jamais qu'un ensemble de systèmes moins complexes et moins difficiles à appréhender.

EN SYNTHÈSE

N'autoriser que le nécessaire, s'assurer que c'est la bonne personne, (re)vérifier et tracer…

Least Privilege « POLP »	Firewalling, PEDM
Défense en profondeur	L'oignon, l'hiver… Additionner les solutions (sans recouvrement) et diminuer les surfaces d'attaque
Contrôle des accès	IdM, IAM, PAM, SSO
Traçage et analyse	Logs, monitoring, SOC-SIEM, CTI (failles, preuves, actions, assurance)
Compétences, sensibilisation	Sensibilisation, formation, « Due care, due dilligence », expertise externe
Vision holistique, gouvernance	Études, mises en concurrence, benchmarks POCs, partenariats, accompagnement
Usage des standards	TCP/IP, solutions reconnues, communautés
Principe de Kerckhoffs	Pas de sécurité par l'obscurité, seule la clé est secrète

… et toujours faire preuve de bon sens !

Les solutions ne manquent pas, et en se référant aux standards, on peut s'assurer qu'elles sont éprouvées. Les solutions open source permettent un niveau de mise à jour plus rapide, étant donné qu'elles sont suivies de près par des communautés souvent très dynamiques et nombreuses. Attention toutefois à toujours suivre le niveau de conformité afférent à l'activité menée dans le bâtiment. Dans le cas d'OSE (Opérateurs de services essentiels) ou d'OIV (Opérateurs d'importance vitale), la conformité passera par un choix de composants certifiés (par exemple CSPN de l'ANSSI).

4

LES **RÉFÉRENTIELS** EXISTANTS

Le sujet des réglementations est large et à chaque infrastructure, il convient de réaliser une étude de risques, un zonage, un profilage des types d'attaquants et des types d'attaques, puis d'adopter les bonnes réglementations.

LES RECOMMANDATIONS NATIONALES

L'ensemble des agences nationales de cybersécurité comme l'ANSSI définit un cadre réglementaire qui pose des recommandations permettant de lutter contre l'ensemble des cyberattaques. On peut notamment citer les guides de recommandations nationales de l'ANSSI en France, de la BSI (*Bundesamt für Sicherheit in der Informationstechnik*) en Allemagne, ou d'autres entités en Espagne et aux Pays-Bas. Ceux-ci définissent :

- les recommandations pour la protection des systèmes d'information essentiels ;
- les recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection ;
- les bonnes pratiques de l'informatique.

Ces guides, à vocation de sensibilisation aux bonnes pratiques de sécurité liées aux usages du numérique, visent à accompagner les entreprises pour la mise en œuvre des mesures de sécurité nécessaires au maintien de l'intégrité, l'authenticité et de la disponibilité des services et des données. Ils font partie d'un catalogue listant les guides ainsi que des notes techniques.

LES CERTIFICATIONS NATIONALES

En parallèle, pour sécuriser certaines entités critiques (OIV, OSE), l'ANSSI, la BSI, les Pays-Bas, l'Espagne, et l'UE recommandent de faire certifier les différents sous-systèmes qui composent les solutions déployées (en IT et en OT).

Alliance SPAC

SPAC fédère l'écosystème de la sécurité physique pour construire un marché de la sécurité physique fort, interopérable et intelligent, correspondant aux nouveaux usages de nos infrastructures. Le but est d'augmenter le niveau de sécurité de notre marché et de vous donner la possibilité de sécuriser les infrastructures les plus critiques.
Pour cela, l'alliance SPAC utilise le cadre réglementaire national et européen et le protocole de communication SSCP, certifié CSPN.

CNPP

Le Centre National de Prévention et de Protection (CNPP) a développé des compétences en cybersécurité des systèmes d'information pour faire face au risque cyber. Il a créé un laboratoire d'évaluation de la cybersécurité des objets connectés, permettant au CNPP de se positionner comme un acteur pour la maitrise du risque cyber sur les niveaux de risque intermédiaires (« Substantial Assurance Level » du Cyber Act).

CNPP Cert., organisme certificateur, propose des certifications de services (marque APSAD) et de produits (marques A2P, CNPP Certified). Il a intégré la dimension cybersécurité depuis 2017 au sein des programmes de certification en électronique de sécurité.

Dans le cadre de la certification de services selon le référentiel NF 367-I80, les installateurs certifiés dans le domaine de l'électronique de sécurité intègrent ainsi dans leurs prestations, les bonnes pratiques méthodologiques pour la conception, la réalisation, l'exploitation et la maintenance des systèmes de sécurité/sûreté, au regard du risque cyber, en appui du référentiel APSAD D32 dédié à la Cybersécurité de ces installations.

Dans le cadre des certifications de produits d'électroniques de sécurité, le critère « robustesse aux attaques numériques »/cybersécurité est évalué en complément de l'évaluation des caractéristiques fonctionnelles sécurité/sûreté des produits certifiés.

Ces certifications s'appuient sur un socle d'exigences techniques adaptées aux niveaux de risque numérique et rédigées en cohérence avec les recommandations de l'ANSSI, permettant de garantir un niveau de robustesse global cohérent pour les niveaux intermédiaires.

CNPP Cybersecurity, qualifié PASSI par l'ANSSI, propose des prestations d'accompagnement et de formation pour la cybersécurité des systèmes d'informations.

4.3. LES RECOMMANDATIONS EUROPÉENNES

Les recommandations et réglementations nationales sont souvent différentes et il est difficile pour des fournisseurs de solutions d'appliquer des réglementations différentes en fonction des clients et pays qu'ils adressent. Les actions sont donc « fragmentées ». C'est dans le but d'harmoniser les réglementations et aussi dans un but de souveraineté européenne que l'Union européenne définit un cadre réglementaire commun. Ce cadre est fondamental pour l'ensemble des états, et les recommandations sont reconnues par les 27 membres.

Directive NIS

Adoptée par les institutions européennes le 6 juillet 2016, la directive Network and Information System Security (NIS) poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. La version 2 de cette directive qui est en cours de définition prévoit aussi de prendre en compte le contrôle d'accès physiques. Elle a une vision plus transverse d'une attaque potentielle. Les recommandations pourront mettre en application des actes délégués comme la certification européenne.

Cybersecurity Act

Géré par l'ENISA, le règlement européen « Cybersecurity act » a été adopté par le Parlement européen le 12 mars 2019 puis par le Conseil de l'Union européenne le 7 juin. Il marque une véritable avancée pour l'autonomie stratégique européenne. Il poursuit un double objectif : l'adoption du mandat permanent de l'ENISA, l'Agence européenne pour la cybersécurité, et la définition d'un cadre européen de certification de cybersécurité, essentiel pour renforcer la sécurité du marché unique numérique européen. Cette certification ouvrira des marchés aux fournisseurs de solutions. Elle permettra un choix de solutions de confiance européennes.

Cyber Resilience Act

Un premier jalon du Cyber Resilience Act a été posé et est en cours d'élaboration au niveau de la Commission européenne. Il consiste en une proposition de règlement sur les exigences de cybersécurité pour les produits comportant des éléments numériques, et renforce les règles de cybersécurité afin de garantir des produits matériels et logiciels plus sûrs. Quatre objectifs ont été définis :

- veiller à ce que les fabricants améliorent la sécurité des produits comportant des éléments numériques dès la phase de conception, de développement et tout au long du cycle de vie ;
- assurer un cadre de cybersécurité cohérent, facilitant la conformité des producteurs de matériel et de logiciels ;
- améliorer la transparence des propriétés de sécurité des produits comportant des éléments numériques ;
- permettre aux entreprises et aux consommateurs d'utiliser les produits contenant des éléments numériques en toute sécurité.

LES NORMES INTERNATIONALES

Norme ISO/IEC 27001

La norme ISO/IEC 27001 – Système de management de la sécurité de l'information (SMSI) constitue le modèle international d'organisation pour répondre aux enjeux de cybersécurité. Elle définit comment les organismes privés et publics doivent s'organiser et les moyens qu'ils doivent mettre en œuvre pour assurer la sécurité des informations numériques et non-numériques.

Assurer la sécurité d'une information revient à préserver :

- sa confidentialité : seules les personnes autorisées doivent pouvoir accéder à cette information ;
- son intégrité : l'information doit rester exacte et complète ;
- sa disponibilité : l'information doit rester accessible et utilisable à la demande par les personnes autorisées.

4 LES RÉFÉRENTIELS EXISTANTS

La norme ISO/IEC 27001 décrit un socle minimal de 114 mesures de sécurité (qui sera réduit à 93 lors de la révision de la norme) à mettre en œuvre et à prioriser au regard des risques (de niveaux forts, moyens, faibles) qui pèsent sur les actifs (serveurs, logiciels, informations sensibles…) d'un organisme. L'appréciation des risques, qui est l'élément central de cette norme, va dépendre du contexte d'un organisme : stratégie, exigences clients, exigences réglementaires applicables…

➔ *La norme ISO/IEC 27001 s'applique à tout secteur d'activité et sa popularité l'a amené à servir de modèles à des déclinaisons sectorielles de référentiels en lien avec la cybersécurité. L'ISO Survey estimait le nombre de certificats ISO 27001 en 2020 à 44 499 dans le monde dont 396 en France.*

La popularité de la norme ISO/IEC s'intensifie en Europe depuis la mise en application du RGPD (Règlement général sur la protection des données personnelles) en mai 2018 car elle offre une réponse possible aux enjeux de cybersécurité des données personnelles. La croissance de popularité est accélérée en France où le décret HDS oblige les hébergeurs de données de santé à caractère personnel à être certifié ISO/IEC 27001 depuis avril 2018.

Norme IEC 62443

Les contraintes du monde industriel sont différentes de celles du secteur tertiaire. La nécessité de produire sans interruption et l'importance des risques humains et environnementaux ont motivé l'élaboration d'une norme qui prend en compte les spécificités de l'OT alors que l'IT était traité dans la norme ISO/IEC 27001.

Dans cette perspective, la norme IEC 62443 concerne la cybersécurité des systèmes d'automatisation et de commande industrielles. Elle apporte une vraie valeur ajoutée pour la sécurisation des bâtiments intelligents qui utilisent de nombreux automates. Elle est composée de plusieurs documents regroupés en quatre parties, dont notamment des déclinaisons sectorielles de la norme ISO/IEC 27001 et d'autres normes de la série ISO 27000, ce qui en fait une norme très complète :

	Exigences organisationnelles	Guide d'implémentation	Analyse des risques cyber
Générique tout secteur	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005
Industrie	IEC 62443-2-1	IEC 62443-2-5	IEC 62443-3-2

- **Partie IEC 62443-1** – Général : cette partie regroupe les documents destinés au concepts généraux, à la terminologie et aux méthodes.
- **Partie IEC 62443-2** – Politiques et procédures : cette partie spécifie les mesures organisationnelles, et s'adresse aux exploitants et mainteneurs des solutions d'automatisation. Il contient également des recommandations dans le cadre des corrections et mises à jour des composants du système.
- **Partie IEC 62443-3** – Systèmes : cette partie est dédiée aux moyens opérationnels de sécurité des Systèmes d'Automatisation et de Commande Industrielles. Il fournit une évaluation actuelle des différents outils de cybersécurité, décrit la méthode et les

moyens pour structurer leur architecture en zones et conduits, et dresse un état des lieux des techniques de protection contre les cyberattaques.
- **Partie IEC 62443-4** – Composants : cette partie est destinée aux équipementiers de solutions de contrôle-commande (automates, éléments de supervision, stations d'ingénierie et autres équipements de commutation). Cette partie décrit d'une part les exigences de sécurité pour ces équipements et présente les bonnes pratiques de développement d'un produit.

Norme ETSI 303 645

La norme ETSI 303 645 – Cybersécurité pour les objets connectés grand public a été la première norme reconnue au niveau européen sur ce sujet. Elle spécifie des dispositions pour la cybersécurité des appareils grand public connectés à Internet et de leurs services associés.

1. Dispositions relatives aux mots de passe.
2. Dispositions relatives à la gestion des rapports de vulnérabilités.
3. Dispositions relatives aux mises à jour de sécurité des logiciels.
4. Dispositions relatives au stockage sécurisé des paramètres sensibles de sécurité.
5. Dispositions relatives à la sécurité des communications.
6. Dispositions relatives à la minimisation des surfaces d'attaque exposées.
7. Dispositions relatives à l'intégrité des logiciels.
8. Dispositions relatives à la protection des données personnelles.
9. Dispositions relatives à la résilience face aux pannes.
10. Dispositions relatives à l'examen des données de télémétrie du système.
11. Dispositions relatives à l'effacement des données d'utilisation par l'utilisateur.
12. Dispositions relatives à l'installation et à la maintenance des systèmes.
13. Dispositions relatives à la validation des données d'entrée.

Plusieurs des produits IoT concernés par cette norme sont fréquemment utilisés dans les bâtiments intelligents, comme :

- les produits connectés liés à la sécurité tels que les détecteurs de fumée et les serrures de porte, les caméras intelligentes ;
- les systèmes domotiques et d'alarme connectés ;
- les assistants domestiques intelligents ;
- d'autres produits grand public concernés par cette norme correspondent à d'autres usages :
  - les appareils électroménagers connectés comme les machines à laver et les réfrigérateurs ;
  - les téléviseurs et les haut-parleurs ;
  - les jouets connectés pour enfants et les moniteurs pour bébé ;
  - les trackers de santé portables.

4 LES RÉFÉRENTIELS EXISTANTS

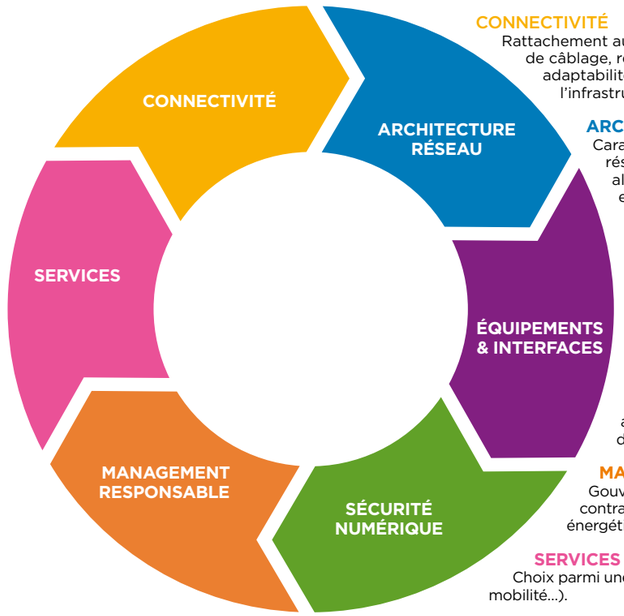
Devant le besoin de sécurisation pour tous les objets connectés et la pluralité des technologies disponibles, d'autres référentiels ont été développés afin de répondre à tous les besoins de sécurisation. Par exemple, le référentiel du label IQS offre une alternative à la norme ETSI 303 645 en s'adressant à tous les types d'objets connectés. Ce label exigeant mais en accord avec les moyens des fabricants porte sur 25 exigences de sécurité permettant à toute solution IoT d'atteindre un premier niveau de résistance aux attaques.

LE RÉFÉRENTIEL R2S ET LA SÉCURITÉ NUMÉRIQUE

Lancé en juin 2018 et révisé en juin 2022, R2S (Ready2Services), le référentiel expert coconstruit par la SBA et l'organisme de certification Certivea, signe la qualité des infrastructures numériques des bâtiments d'activité.

Ce référentiel définit le niveau d'exigence attendu d'un Smart Building. Il s'agit d'un bâtiment qui possède une infrastructure de communication pérenne, reposant sur des standards ouverts, qui facilite l'accès centralisé aux données des équipements connectés en assurant un niveau de sécurité élevé au réseau bâtimentaire et aux systèmes qui lui sont rattachés. Au-delà des aspects techniques, l'objectif est d'accompagner les bâtiments en conception, réalisation et exploitation dans une démarche de management transversal et responsable et favoriser l'accès à une large gamme de services pour le bâtiment et ses usagers.

Il est structuré autour de 6 piliers :



CONNECTIVITÉ
Rattachement aux réseaux opérateurs, mise en œuvre de l'infrastructure de câblage, réseaux radio (mobile WiFi, IoT, géolocalisation), adaptabilité et redondance du câblage, alimentation électrique de l'infrastructure réseau, sécurisation de l'infrastructure réseau.

ARCHITECTURE RÉSEAU
Caractéristiques du réseau Smart, survivance des fonctions réseau (management, résilience, protection, QoS…), alimentation des terminaux en PoE, gestion de domaine et adressage dynamique, continuité de services Internet.

ÉQUIPEMENTS & INTERFACES
Périmètre du réseau Smart, survivances des fonctions, liste et documentation des API, caractéristiques des API, exigences spécifiques pour les API terrain et l'API centrale, maquette numérique (statique et dynamique).

SÉCURITÉ NUMÉRIQUE
Sécurisation du réseau Smart et des systèmes connectés (accès au réseau, cloisonnement et routage, surveillance de trafic…), procédures de sécurité réseau (gestion des événements, mise à jour, sécurité d'accès aux services, accès aux applications, gestion des risques) et protection des données personnelles.

MANAGEMENT RESPONSABLE
Gouvernance du projet, propriété immobilière, cadre de contractualisation des services, commissionnement, sobriété énergétique et qualité environnementale.

SERVICES
Choix parmi une liste non exhaustive de services (énergie, espaces, santé, mobilité…).

Au cœur du référentiel, l'on retrouve quelques principes fondamentaux qui structurent la démarche R2S :

- le modèle d'architecture en 3 couches indépendantes : équipements terrain, infrastructure numérique de communication, applications et services ;
- l'existence d'un réseau fédérateur du bâtiment conforme aux standards IP : le réseau Smart ;
- l'interopérabilité des systèmes pour favoriser l'ouverture et l'évolutivité des services ;
- la sécurité numérique renforcée du réseau, des systèmes et des données ;
- la gouvernance du projet intégrant pleinement la dimension numérique.

Le volet spécifiquement dédié à la sécurité numérique a pour objectif de traiter des thèmes couvrant la sécurité des réseaux et systèmes du bâtiment et des procédures de gestion des risques et de protection des données. On retrouve dans ce volet les critères d'évaluation suivants :

- SE1.1 – Sécurisation des accès au réseau Smart ;
- SE1.2 – Cloisonnement du réseau Smart et routage ;
- SE1.3 – Sécurisation de la supervision des systèmes ;
- SE1.4 – Mécanismes de surveillance des trafics et de protection contre les logiciels malveillants ;
- SE2.1 – Collecte et traitement des événements ;
- SE2.2 – Mise à jour et lutte contre l'obsolescence ;
- SE3.1 – Sécurisation de l'accès aux applications ;
- SE3.2 – Prévention et gestion des risques ;
- SE4.1 – Conformité au Règlement général sur la protection des données.

Au-delà des critères dédiés à la sécurité numérique, l'on y trouve également des points de renforcement concernant une prise en compte systémique sur la protection, la résilience et les mesures de gouvernance qui complètent les critères listés ci-dessus, à noter en particulier :

Sur la connectivité

- CO1.2 – Redondance de rattachement du bâtiment aux réseaux externes ;
- CO5.1 – Capacité de redondance des câblages du bâtiment ;
- CO5.4 – Contrôle des accès et protection des infrastructures.

Sur l'architecture réseau

- RE2.1 – Capacité de résilience du réseau Smart ;
- RE2.2 – Détection d'anomalies et protection du réseau Smart ;
- RE3.1 – Administration du Réseau Smart et de leurs équipements.

Sur le management responsable

- MA1.2 – Administration du réseau Smart et des systèmes du bâtiment ;
- MA3.1 – Contrats de services (SLA) avec des fournisseurs ;

➔ *Avec plus du tiers des points totaux du référentiel qui portent sur la sécurité dans son ensemble, R2S propose un ensemble de critères de référence pour intégrer la cybersécurité au sein de son projet bâtimentaire.*

5

MÉTHODE

La lutte contre les cybermenaces ne peut s'inscrire que dans une approche globale impliquant l'ensemble des acteurs de la chaîne de valeur, d'où une certaine complexité à mettre en œuvre des mesures efficaces et durables. S'il existe, à ce jour, des normes et des règles sur les produits, l'installation et l'exploitation, il n'existe pas de référentiel incluant à la fois les équipements, les infrastructures, leur mise en œuvre et leur maintenance. De fait, l'une des ambitions de la SBA avec son référentiel R2S (Ready2Services) qui comprend déjà un haut niveau d'exigences, est d'apporter des premiers éléments de réponse à un cadre sur la cybersécurité des bâtiments.

Afin d'être pleinement sécurisé et serein, que ce soit vis-à-vis des connexions depuis le réseau interne au bâtiment ou depuis Internet (Clouds, mainteneurs et leurs VPNs, etc.), il faut établir un plan global, qui repose sur une stratégie. Cette stratégie doit incorporer les différents aspects du projet (techniques, besoins métiers, organisationnels, financiers, besoins en conformité…) et définir un chemin vers le but final. Ce chemin peut être segmenté en différentes phases. Pour des raisons englobant tous les aspects du projet, le but peut changer. Il convient donc de bien choisir son architecture et ses composants afin d'être en mesure de s'adapter au contexte, en réévaluant pour chacune de ces adaptations les risques induits par les évolutions et adaptations du projet et en mettant à jour le plan de risques.

Éléments à prendre en compte pour établir une stratégie de cybersécurité :
- analyse de risque, plan de gestion des risques, gouvernance et management ;
- mise en place d'une méthode qui assure la prise en compte :
  - des enjeux liés aux données personnelles ;
  - aspects préventifs : communication, « évangélisation » ;
  - aspects dissuasifs : sécurité physique ;
  - aspects correctifs : technologies, organisation (processus, validation, management, compétences) ;
- gestion de crises : processus testé et validé ;
- réponse à attaque (ciblée), PRA, PCA, sauvegardes, secours ;
- surveillance, SOC SIEM.

ANALYSE DE RISQUE

Au même titre que pour les SI de gestion ou SI industriels, la réalisation d'une analyse de risque sur les SI bâtimentaires est une étape incontournable dans le management du risque numérique au sein d'une organisation. L'objectif reste l'identification et le traitement des risques du SI au regard d'un niveau de sécurité à atteindre.

Afin de permettre de structurer l'approche et également d'obtenir des résultats reproductibles dans le temps, le choix de la méthodologie d'analyse de risque est indispensable. Il peut être envisagé d'utiliser la même approche et la méthodologie d'analyse de risque utilisée au sein de l'organisation mais il faudra l'adapter au SI bâtimentaire, les référentiels étant différents. L'objectif de cette approche est notamment d'obtenir des résultats comparables avec les autres SI de l'organisation et ainsi faciliter la compréhension des risques par les instances dirigeantes. Cependant il conviendra d'intégrer dans cette méthode, les éléments spécifiques aux bâtiments (automates, capteurs, sûreté…).

À défaut de démarche d'analyse de risque mise en place au sein de l'organisation, la méthode EBIOS Risk Manager élaborée par l'ANSSI en 2018 peut s'appliquer sur un SI bâtimentaire. Cependant c'est une démarche qui peut s'avérer longue et plus adaptée aux SI de gestion traditionnels où le degré de maturité en cybersécurité sont plus importants. On peut citer ici la méthode MEHARI, qui est plus légère, et semble plus adaptée.

La difficulté régulièrement rencontrée dans la réalisation d'une analyse de risque sur un SI bâtimentaire est l'hétérogénéité des briques applicatives et techniques. Ainsi, la phase de cadrage est indispensable à l'identification des services métier composant son SI. Il faudra par exemple s'intéresser à la valeur « Contrôler son espace de travail » plutôt que réaliser un découpage entre application mobile, solutions techniques et équipements IoT. L'analyse de risque sera ainsi réalisée sur l'ensemble de la chaîne de valeur et les mesures de sécurité identifiées à la fin du processus permettront l'atteinte d'un niveau de sécurité cohérent avec le besoin métier.

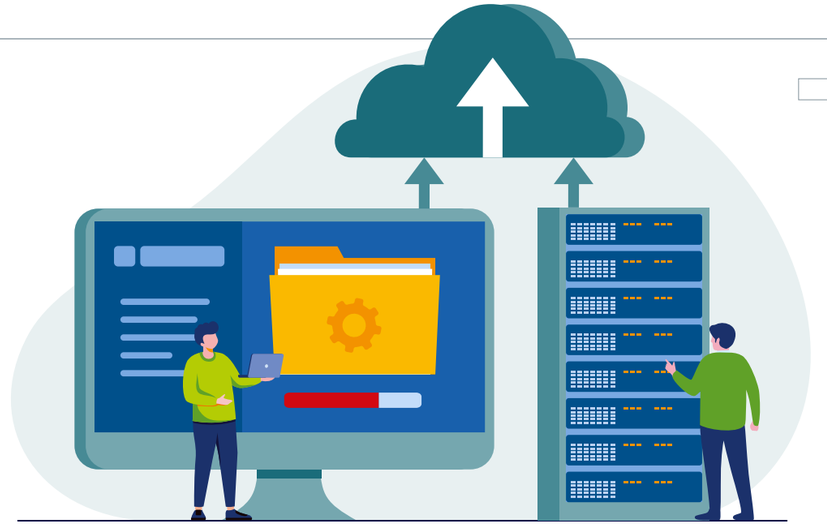
➔ *Le choix dans la granularité des valeurs métier est également structurant pour le reste de la démarche. Une analyse de risque englobant un ensemble trop important d'éléments sera complexe à maintenir dans le temps. En revanche, rester à un niveau trop haut ne permettra pas d'identifier clairement des mesures efficientes dans le traitement des risques. Ce curseur doit être pris au niveau de chaque organisation notamment au regard du besoin en sécurité du système et du niveau de maturité de l'organisation.*

Dans un objectif d'instaurer la confiance dans un SI, l'analyse de risque d'un SI bâtimentaire peut être intégrée dans une démarche plus globale d'homologation de sécurité. Cette démarche permet à ce qu'un responsable d'une organisation puisse obtenir une vision suffisante du niveau de sécurité de son système, lui permettant ainsi de décider s'il souhaite accepter les risques résiduels pesant sur son SI. Pour un certain nombre de systèmes, la réalisation d'une homologation de sécurité est rendue obligatoire par des textes, tels que le NIS, la LPM, l'instruction générale interministérielle n° 1300, le référentiel général de sécurité (RGS) et la politique de sécurité des systèmes d'information de l'État (PSSIE).

ENJEUX SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Une fonctionnalité essentielle du Smart Building est de faciliter l'interaction entre un individu et un bâtiment. Dans ce cadre, une multitude de services est mise à la disposition d'utilisateurs, essentiellement à travers d'outils numériques, qui nécessitent la manipulation de données personnelles. Ces données doivent être collectées et traitées conformément au Règlement général sur la protection des données (RGPD).

Ainsi, il est indispensable d'intégrer dans tout projet Smart Building une prise en compte des exigences RGPD. La réflexion doit être lancée au plus tôt notamment à travers la mise en place d'une démarche de Privacy by Design qui s'attachera à adopter dès la phase de conception un ensemble de mesures organisationnelles et techniques appropriées pour garantir la protection de la vie privée des individus.



Un point de vigilance doit toutefois être observé concernant les données à prendre en compte dans le cadre de cette mise en conformité RGPD. Il est à rappeler que le règlement définit une donnée personnelle comme toute information se rapportant à une personne physique identifiée ou identifiable. Ainsi dans certains cas de Smart Building, un nombre important de données brutes collectées par des objets connectés du Smart Buiiliding peuvent se rapporter à une personne clairement identifiable.

Prenons par exemple un hôtel connecté ou une résidence étudiante nouvelle génération. Différents capteurs de présence et de température sont installés au sein de chaque logement afin d'apporter de nouveaux services aux habitants. Une relève en temps réel de la puissance appelée est également mise en place pour assurer un meilleur pilotage de la consommation électrique de l'occupant. Les données traitées dans le cadre de ces cas d'usage permettent de suivre le comportement d'un individu et sont donc à considérer comme une donnée personnelle au sens du RGPD.

➔ *Dès la phase de conception d'un nouveau service Smart Building, il est donc indispensable d'identifier les données pouvant être considérées comme donnée personnelle selon le RGPD. L'erreur trop souvent commise est de considérer uniquement les données d'identification (ex : nom, prénom) comme donnée personnelle et d'omettre que les données concernant une personne physique identifiable sont également à considérer comme telle. L'une des clés de Security by Design consiste également à ne collecter des données associées aux individus eux-mêmes qu'en cas de stricte nécessité. Par exemple, le suivi du nombre de personnes dans une pièce pour optimiser le chauffage ne nécessite pas de savoir qui est présent. Les données collectées sont ainsi moins sensibles et leur criticité en cas d'attaque est moindre.*

SÉCURITÉ PRÉVENTIVE

La sécurité préventive ou sécurité périmétrique consiste à filtrer les informations qui transitent par le réseau du Smart Buiiliding. De même, on peut y tracer les demandes d'accès, les contrôler et alerter le cas échéant en cas de tentative d'intrusion. Le contrôle d'accès est un point crucial en cyber. À lui seul, bien implémenté, il permet de réduire considérablement les surfaces d'attaque.

Cela peut être complété par des « pentests » ou tests de pénétration, qui sont en fait des tentatives d'intrusion, réalisées par des sociétés spécialisées dans la cybersécurité. Ces sociétés font l'objet de certifications et les tests sont fortement encadrés avec des procédures.

Ensuite, il convient d'effectuer ce que l'on appelle des « scans de vulnérabilité » de la plateforme Smart Builiding. L'objectif étant de s'assurer que les versions installées de tous les softwares déployés, soient les dernières (les patches de sécurité) et de faire remonter les vulnérabilités ou les brèches des systèmes scannés, afin de les traiter. Il est crucial de connaitre l'état des systèmes pour prendre les bonnes décisions, et de les documenter.

SÉCURITÉ PRÉDICTIVE

Ce domaine encore complètement étranger au sujet du Smart Building, consiste à modéliser le comportement du bâtiment afin d'en identifier les comportements déviants, comme cette fameuse augmentation de température au 10e étage d'un bâtiment, dont les ascenseurs et les portes sont bloquées…

Cette sécurité consiste à modéliser, sur la base de machine learning et grâce à la collecte exhaustive des logs de tous les systèmes, le comportement quotidien du bâtiment. Cette modélisation dure en général deux à trois semaines.

Une fois que le modèle existe, il sert de base à un centre de supervision, ou Security Operation Center « SOC » du bâtiment, auquel on adjoint un SIEM (centralisation et analyse de logs) pour identifier un comportement déviant, et engager un processus de remédiation. Dans l'exemple donné, cela consiste à forcer la GTB à remettre une température à 18 degrés et débloquer portes et ascenseurs.

Les SOC sont aujourd'hui des solutions largement déployées sur nos SI d'entreprise. Ils seront amenés à l'être dans l'industrie, dont le Smart Building avec l'accélération de la digitalisation des bâtiments.

MINIMISER LA SURFACE D'ATTAQUE

La multiplication des objets connectés dans les systèmes d'information du bâtiment, de la ville… engendreront nécessairement une recrudescence de failles si aucune mesure n'est prise. En effet, la plupart du temps, ces équipements sont nombreux et leur prix unitaire est extrêmement bas, ce qui implique une faible Security by Design. Au niveau hardware ou software, ces objets connectés n'ont généralement qu'une couche sécuritaire minimum. Dans certains cas, leur chiffrement est même désactivé, faute de puissance. De plus, leur surface d'attaque est potentiellement élevée puisqu'ils exposent de nombreuses informations pour échanger des données avec différentes applications.

Pour chacun des systèmes du SI bâtimentaire, des mesures/configurations sont à appliquer afin de minimiser la surface d'attaque au maximum et aussi d'éviter les mouvements latéraux des attaquants. La mise en place d'un réseau segmenté en VLANs est un bon exemple de mesure.

FÉDÉRER L'ENSEMBLE DES OBJETS CONNECTÉS

Pour éviter une cyberattaque paralysante pour l'ensemble d'un écosystème bâtimentaire ou urbain (effet domino cité plus haut), il convient d'apporter une réponse technologique adaptée en fédérant l'ensemble des objets connectés. À l'échelle des entreprises, il s'agit de mener des travaux de sensibilisation (développement de la culture IT et OT), tandis qu'à l'échelle nationale et internationale, il s'agit de définir des normes et un cadre réglementaire. En priorisant le concept de Security by design, la défense contre les futures cyberattaques sera ainsi prise en compte dès la conception des produits : une manière efficace de prévenir le risque cyber. Pour cela, les acteurs industriels doivent accompagner les fournisseurs d'IoT et autres systèmes techniques du bâtiment afin de faciliter l'intégration de solutions de sécurité dans les produits, en proposant des interfaces et des API sécurisées.

DÉFINIR DES NORMES DE SÉCURITÉ ET DES CERTIFICATIONS

Les certifications garantissant un niveau de sécurité minimum seront nécessaires pour renforcer le niveau global de sécurité. Pour rappel, en France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) délivre une certification pour attester de la robustesse d'un produit selon des critères de conformité. À l'échelle européenne, l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) est chargée d'évaluer la conformité des produits selon leurs exigences en matière de cybersécurité.

Bien que ces normes et certifications s'adaptent à la réalité des menaces, tous les systèmes d'information ne les suivent pas. Il est donc nécessaire de faire un travail de sensibilisation aux risques et d'assurer que ces systèmes respectent la notion de conformité. *De facto*, l'enjeu des prochaines années sera d'adapter les normes existantes au Smart Builiding – et d'en établir de nouvelles – afin de prévenir le risque au niveau du bâtiment, mais aussi plus généralement de la ville.

Un certain nombre de normes s'adaptent effectivement à la réalité des menaces mais il faut encore que les systèmes mis en place les suivent systématiquement, ce qui n'est pas vraiment le cas, d'où le risque… Il faut à ce titre une vraie prise de conscience de tous les acteurs de la chaîne de valeur et ceci au niveau même de la gouvernance des entreprises impliquées.

MATRICE DE PRIVILÈGES

Afin d'appliquer les bons droits («Need to know», moindre privilège…), il convient d'avoir une cartographie des utilisateurs et de leur(s) rôle(s). Il faut lister les utilisateurs et leurs privilèges permettant de les regrouper et de leur attribuer les bons niveaux de droit:

- utilisateurs finaux;
- comptes applicatifs;
- comptes de service;
- responsables d'applications et de bases de données;
- administrateurs.

Afin de pouvoir maîtriser ces différents profils et leurs droits sur les systèmes, il faut disposer d'une solution de gestion des utilisateurs dont la plus connue est l'annuaire!

DÉFINITION D'UN PROGRAMME

La définition du programme et son contenu génère des actions dans différentes catégories ou couches. Le traitement de ces actions peut être d'ordre hardware (appliance spécialisée par exemple), logiciel (déploiement d'une solution de cybersécurité), organisationnel, ou la mise en place d'un processus. Cela peut aussi être une formation, du recrutement ou la mise en place d'un partenariat technologique. Quels que soient les moyens, il faut définir un plan, une roadmap d'implémentation «collant» à celle de la construction du bâtiment ou sa rénovation.

LA GESTION DE PROJET CYBERSÉCURITÉ

Une approche cybersécurité dans un environnement Smart Building ou Smart City résulte d'une stratégie qui est souvent spécifique en raison du contexte et des risques. Si les briques d'un projet sont souvent assez proches, leur mise en œuvre répond souvent à des objectifs différents et peut s'appliquer à des systèmes retenus dans le plan de déploiement en fonction de leur criticité. Pour aider les décideurs à construire leur stratégie, les entreprises spécialisées dans la cybersécurité industrielle définissent généralement un plan d'action comprenant les étapes suivantes:

Exemples de briques techniques pouvant être mises en œuvre dans un projet de cyber sécurisation du bâtiment

GESTION DES RISQUES, ACCOMPAGNEMENT, SENSIBILISATION
- Analyse des risques (BIA)
- Définition des règles de sécurité, compliance (R2S, RGPD)
- Identification des contre-mesures (solutions, org, process)
- Pentest (pilotage et correctifs)
- Risk Assessment Program (cyclique)
- Documentation

SÉCURITÉ PÉRIMÉTRIQUE DU RÉSEAU SMART
- Architecture du réseau (Ethernet, TCP/IP, services)
- Segmentation du réseau (Switches, VLANs, routage)
- Accès distant sécurisé (VPN site et nomades)
- Filtrage réseau (Firewalling, contrôle inter VLANs)
- Inspection des paquets (IDS/IPS)
- Fonctions essentielles au réseau (DHCP, DNS, NTP)
- Authentification réseau
- Redondance du réseau (multi-WAN, résilience des liens)
- Prody, reverse Proxy

GESTION DES IDENTITÉS, AUTHENTIFICATION CENTRALISÉE
- Service centralisé de gestion des identités et des droits
- Authentification forte avec token et smartphone
- SSO

GESTION DES ACCÈS À PRIVILÈGE – INFRA, BOS, BIM
- Management des accès à privilège en haute disponibilité (administrateurs, BOS, firewalls, DBA, applications…)
- Gestion avancée des mots de passe/certificats
- Enregistrement des sessions (preuves, assurance, debug)
- EPDM: durcissement des postes SIB
- Sécurisation BIM (transport des documents sensibles personnels mobiles)

GESTION DES INCIDENTS DE SÉCURITÉ – SOC-SIEM

Gestion des logs
- Collecte, agrégation, normalisation, transformation et enrichissement des logs
- Maîtrise des règles et des seuils d'alertes
- Reporting multiniveaux: technique, pilotage, gouvernance
- Détection, qualification et signalement des incidents de sécurité

Prendre conscience, passer à l'action
- Sensibilisation du management via la communication des équipes, des autorités et des associations.
- Prise de conscience suite à des attaques de concurrents ou partenaires.
- Échanges entre équipes IT et OT sur la stratégie cybersécurité.
- Rédaction d'un avant projet et d'un cahier des charges pour un premier accompagnement

Cadrer, diagnostiquer, planifier
- Établir une cartographie initiale du système industriel.
- Réaliser un audit organisationnel et technique.
- Mener une analyse de risque pour caractériser les ratios risques/vulnérabilités.
- Faire réaliser des tests d'intrusions sur l'OT.
- Réaliser des POC Cyber-OT.
- Mettre en place une stratégie cybersécurité industrielle globale et priorisée.
- Planifier son implémentation.
- Faire évoluer l'organisation IT/OT sur la gouvernance cyber.

Réduire les risques
- Déployer une campagne de sensibilisation, de formation et de conduite du changement sur les processus IT/OT.
- Durcir les systèmes OT:
  - mise à jour ou isolement des systèmes obsolètes;
  - segmentation réseaux OT;
  - sécurisation des accès et des droits utilisateurs;
  - gestion et durcissement de tous les périphériques;
  - rédaction des procédures;
  - gestion des sauvegardes;
  - paramétrage sécurité… .
- Durcir la sécurité physique des sites industriels.
- Tests, Commissioning.
- Certification ISO et IEC.

Maintenir en condition de sécurité
- Réaliser des audits réguliers du niveau de sécurité des sites OT.
- Veille sur les vulnérabilités et le niveau de menace.
- Coordination entre maintenance prédictive et gestion des patchs pour optimiser la disponibilité.
- Maintien des cartographies à jour sur les systèmes OT.
- Surveillance des installations, planification et remédiation (management des logs, analyse du trafic réseau et des données opérationnelles…).
- Valorisation des données collectées et de la sécurisation pour optimiser les performances opérationnelles.

Anticiper et gérer les incidents
- Préparation du plan de continuité de l'activité.
- Tests de reprise après incidents.
- Sécuriser une capacité ponctuelle de réponse à incidents, de gestion et de résolution de crise.
- Entretien des canaux avec les partenaires cybersécurité (ANSSI, SOC, CSIRT).
- Supervision des mesures de sécurité.

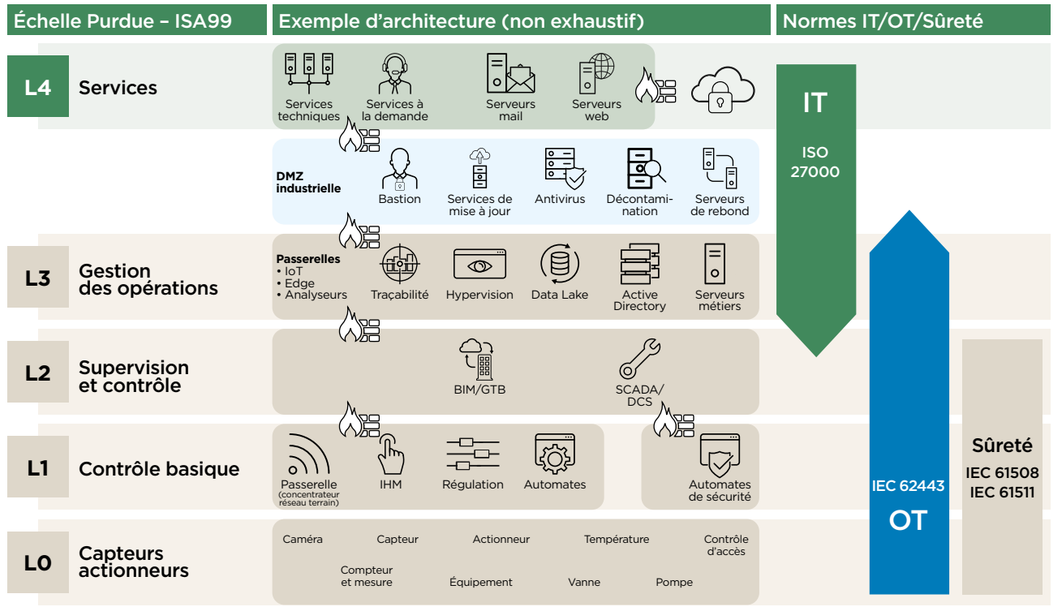
6

SPÉCIFICITÉS OT ET IT

Les équipementiers sont en pleine mutation et il est crucial que cette évolution se renforce. Leurs produits se doivent aujourd'hui de pouvoir communiquer avec des protocoles standard et être capables de s'interfacer avec les solutions informatiques standard du marché. Ces solutions ont l'avantage d'être connues et éprouvées, et bénéficient d'une solide expérience.
Par exemple un contrôle d'accès permettant de s'interfacer via des APIs ou des connecteurs à des annuaires, permettant du SSO (Single Sign On) ou encore capable d'envoyer ses logs sur un SIEM (Security Information and Event Management). La maîtrise des systèmes passe par la connaissance de ce qui transite sur le réseau, de ce qu'on risque, de ce qui est craint. Pour arriver à cette connaissance, il faut des outils qui intègrent des fonctionnalités de collecte, de normalisation et d'analyse.

DÉFINITION

L'OT (Operational Technology) est la technologie opérationnelle qui traite les systèmes opérationnels qui ont un impact sur un environnement physique et permettent le bon fonctionnement des équipements techniques et leur pilotage opérationnel. Si l'OT est naturellement présente dans l'industrie (pilotage de process industriels, des lignes robotisées…), elle est aussi très présente en dehors de l'industrie pour les systèmes d'information techniques (gestion des utilités et des infrastructures, monitoring énergétique…). La norme IEC 62443 sur la sécurité des systèmes industriels est d'ailleurs applicable à la sécurité des systèmes de gestion technique du bâtiment. À ce titre, il est possible de décrire l'architecture informatique d'un système d'information de Smart Building selon l'échelle Purdue qui est le standard pour décrire les systèmes industriels.



ADAPTATION DU MODÈLE DE PURDUE POUR LES SI DU BÂTIMENT

COMPOSITION D'UN SI TECHNIQUE BÂTIMENTAIRE

Les différents composants associés aux environnements de type Smart Builiding se déclinent de la façon suivante :

- des outils orientés service tel que logiciel de maintenance, de configuration et de pilotage positionnés sur le réseau IT et accessibles la plupart du temps en distanciel ;
- des composants de supervision tel que BMS (Building Management System) ou SCADA qui permettent de centraliser les échanges et de superviser les équipements de contrôle au service des différents composants OT que l'on retrouve en couche terrain ;
- des équipements d'automatisme et de régulation ;
- des composants terrains qui permettent d'assurer le contrôle :
  - des fluides (Eau/Air) ;
  - de l'énergie ;
  - des sous-systèmes tel que
    - le contrôle d'accès ;
    - la détection incendie ;
    - la vidéosurveillance ;
    - la détection d'intrusion ;
    - l'éclairage et les ouvrants ;
    - les ascenseurs ;
    - les bornes de recharge pour véhicules électriques.

Attention, il est nécessaire de bien cartographier et de faire l'inventaire des différents composants communicant, des différents sous-réseaux techniques. Il ne faut, par exemple, pas négliger les sous-réseaux sans fil présents dans le bâtiment qui servent de supports à différents capteurs. De même les systèmes réputés « Air Gap » doivent également être vérifiés.

➔ *L'ensemble de ces composants et des flux de données associés doivent être sécurisés selon les grands principes de cyber sécurisation OT :*
- cartographie des composants ;
- segmentation par process ;
- segmentation réseau et contrôle des flux montants et descendants ;
- sécurisation des accès distants ;
- gestion des mots de passe et des identités ;
- contrôle des droits associés.

DESCRIPTION DES PRINCIPAUX SOUS-SYSTÈMES TECHNIQUES DU SIB

Le système d'information technique d'un bâtiment assure le contrôle et la supervision de l'ensemble des installations techniques à usage tertiaire. Ce système d'information est constitué de sous-réseaux dédiés à des fonctions précises décrites ci-après.

Sous-réseau technique utilities

Le réseau utilities assure le monitoring de l'énergie électrique dans le bâtiment pour la haute et basse tension afin que l'énergie soit distribuée dans le bâtiment sans coupure (délestage et reconfiguration de boucle en cas de surtension). Il permet également la bonne ventilation de l'air ainsi que la production et distribution de l'eau froide, l'eau chaude à destination du chauffage ainsi que l'eau chaude sanitaire (robinet, toilette, entretien…). Le réseau utilities permet également de gérer l'éclairage, les stores électriques ainsi que l'ensemble des IoTs assurant le confort des personnes.

Sous-réseau technique sécurité/sûreté

Le réseau sécurité/sûreté est dédié à la vidéo protection et au contrôle d'accès ainsi qu'à la prévention et la gestion d'incendie. Pour le contrôle d'accès, il permet l'identification et l'authentification des personnes et le verrouillage/déverrouillage d'un point d'accès pour autoriser ou empêcher le passage des personnes en fonction de leurs droits. Pour la vidéo protection, il permet de protéger un bâtiment avec des moyens d'acquisition, de transmission, de gestion et d'enregistrement d'images. Enfin, pour la sécurité incendie, il permet de détecter un départ de feu et de mettre en sécurité le bâtiment et les personnes.

Sous-réseau technique communication

Le sous-réseau communication assure les moyens de pouvoir communiquer avec et dans le bâtiment. Il correspond notamment au réseau VDI, à la téléphonie pour les communications internes et externes ainsi qu'au réseau informatique et au WiFi, au réseau mobile indoor.

Sous-réseau technique mobilité

Les ascenseurs, monte-charges et escaliers mécaniques sont contrôlés et supervisés par le réseau mobilité. Pour assurer le bon fonctionnement des zones de parking le réseau mobilité gère les accès véhicules et notamment l'accès au parking (barrière, ouverture de porte…), la reconnaissance d'immatriculation, la signalétique d'occupation ainsi que le fonctionnement des recharges.

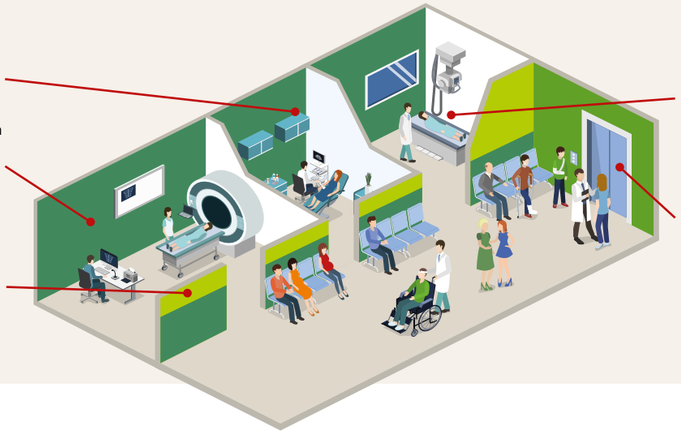
Sous-réseau technique d'administration et de maintenance

La gestion de la maintenance des équipements du système d'information technique est assurée par le réseau d'administration. Ce sous-réseau gère les flux des utilisateurs à privilèges du BIS et héberge les outils d'administration. Il contient notamment les éléments relatifs à la documentation et notamment l'inventaire des équipements, les ordres de travaux, les interventions de maintenance programmée. Sur les aspects des ressources d'énergie et de l'eau, il prévoit la comptabilisation et l'analyse des consommations. Enfin, il centralise l'ensemble des documentations techniques du système d'information technique du bâtiment.

ILLUSTRATION DE RISQUES LIÉS AUX CYBERATTAQUES SUR LE SI TECHNIQUE DU BÂTIMENT

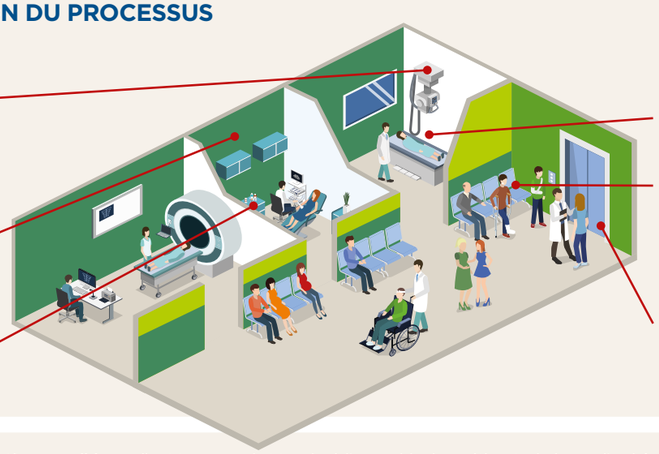
Risques liés au système de gestion de la sécurité incendie

CYBERATTAQUE : PRISE DE CONTRÔLE DU SYSTÈME DE GESTION DU BÂTIMENT



Risques liés au système de gestion technique des bâtiments (GTB)

CYBERATTAQUE : PRISE DE CONTRÔLE DU SYSTÈME DE GESTION DU BÂTIMENT + MODIFICATION DU PROCESSUS



L'organe GTB est un système sensible, car il est transversal et touche à l'ensemble des métiers techniques d'un hôpital. De plus, certains métiers plus critique comme la gestion des blocs opératoires peuvent impacter la sécurité et la prise en charge des patients.

Risques liés au système de gestion technique de l'énergie (GTE)

CYBERATTAQUE : PRISE DE CONTRÔLE DU SYSTÈME DE GESTION ÉLECTRIQUE + DÉCLENCHEMENT D'UN INCIDENT ÉLECTRIQUE + COUPURE DE L'ALIMENTATION DU BÂTIMENT + MISE EN ÉCHEC DU DÉMARRAGE DU GROUPE DE SECOURS

Le maintien en sécurité du système GTE est particulièrement critique: une interruption prolongée de l'électricité déclenche un plan blanc sur toute la zone concernée avec le déplacement de tous les patients et de risques importants pour la santé de certains.

NORMES DE L'OT

Les normes applicables sont les mêmes que pour les systèmes industriels, que ce soit la norme ISO 27000 liée au système de management de la sécurité de l'information (SMSI), à la norme IEC 62443 décrivant les aspects techniques et les aspects liés aux processus de la sécurité informatique industrielle, et aux référentiels normatifs IEC 61508 et IEC 61511 sur la sécurité fonctionnelle des systèmes instrumentés de sécurité. On retrouve des référentiels dédiés pour la Cybersécurité des sous-systèmes bâtiment tel que l'APSAD D32 (voir chapitre sur les normes).

Mesures générales de l'ANSSI

Le guide de recommandations de l'ANSSI regroupe les thèmes des différentes mesures de sécurité organisationnelles et techniques portant sur la sécurisation des systèmes industriels. Ces mesures techniques s'adressent à l'ensemble des acteurs impliqués sur les systèmes industriels (chefs de projet, acheteurs, automaticiens, intégrateurs, développeurs, équipes de maintenance, RSSI, etc.).

Elles sont décrites de façon générique afin de couvrir l'ensemble du monde industriel. Cependant il est nécessaire d'adapter ces mesures au contexte, à l'environnement, au métier ainsi qu'aux besoins et contraintes de fonctionnement du système cible.

Ces mesures organisationnelles et techniques permettent de répondre aux exigences et objectifs de sécurité établis lors de l'analyse de risque préliminaire du système.

Cependant, elles ne peuvent se suffire à elles-mêmes et entrent dans une démarche globale de sécurisation.

Les mesures techniques participent à la défense en profondeur du système mais ne peuvent pas être décorrélées des mesures organisationnelles associées permettant leur mise en œuvre ainsi que leur maintien dans le temps.

Mesures de sécurité organisationnelles

Les mesures de sécurité organisationnelles détaillées par l'ANSSI sont regroupées en cinq thèmes :

- connaissance du système industriel ;
- maîtrise des intervenants ;
- intégration de la cybersécurité dans le cycle de vie du système industriel ;
- sécurité physique et contrôle d'accès aux locaux ;
- réaction en cas d'incident.

➔ *Zoom sur les spécificités organisationnelles de l'OT.*

- *Environnement réglementaire exigeant :*
  - *obligations réglementaires (OIV, ...) ;*
  - *normes organisationnelles.*
- *Pérennisation de systèmes obsolètes :*
  - *maintien en condition opérationnelle à moindre coût ;*
  - *gestion des vulnérabilités : équipements en production et pièces de rechange.*
- *Objectif et nombre des intervenants :*
  - *équipes en 3/8 ;*
  - *exploitant, fournisseur, intégrateur ;*
  - *opérateur, mainteneurs...*
- *Optimisation des coûts par l'externalisation :*
  - *perte de la maîtrise d'installation ;*
  - *pas ou peu de prise en compte de la cybersécurité dans les plans d'extension ou de rénovation.*

Mesures de sécurité techniques

Les mesures de sécurité techniques sont quant à elles regroupées en quatre thèmes :

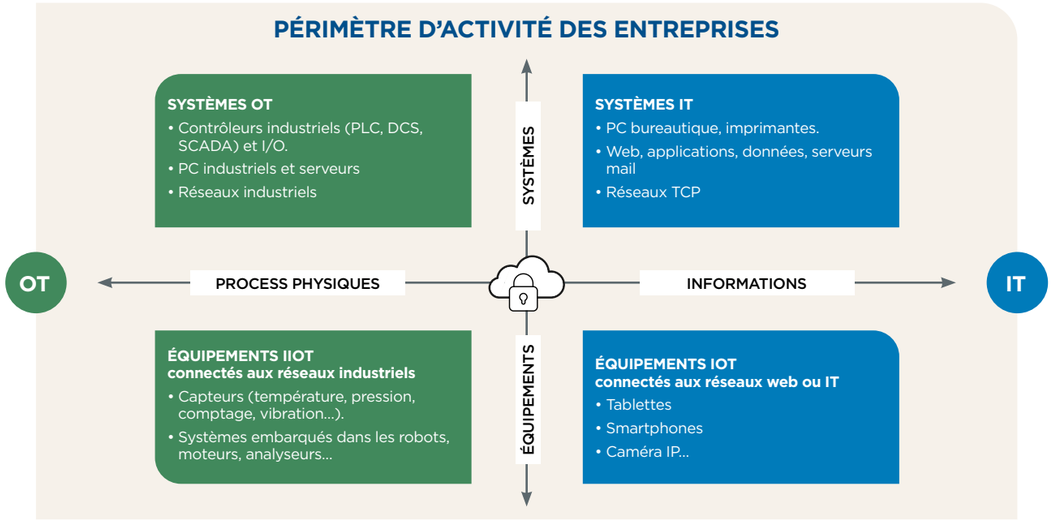
- authentification des intervenants : contrôle d'accès logique ;
- sécurisation de l'architecture du système industriel ;
- sécurisation des équipements ;
- surveillance du système industriel.

➔ *Zoom sur les spécificités techniques de l'OT.*

- *Des installations à longue durée de vie :*
  - *rentabilisation sur plusieurs dizaines d'années ;*
  - *obsolescence des composants ;*
  - *difficultés à pérenniser la maintenance.*
- *Des composants vulnérables :*
  - *pas ou peu de mécanismes de cybersécurité intégrés ;*
  - *patch management complexe à mettre en œuvre.*
- *Une utilisation continue :*
  - *considération physique et économique ;*
  - *disponibilité 24/7 ;*
  - *fenêtre de maintenance réduite.*
- *Hétérogénéité et empilement technologique :*
  - *besoins variés/spécificités constructeurs ;*
  - *différents intégrateurs et gestion par lot ;*
  - *rénovations et extensions favorisant l'empilement de produits de générations et technologies différentes.*
- *Contraintes environnementales :*
  poussière, humidité, chaleur, rayonnement électromagnétique...
- *Utilisation de protocoles de communication :*
  - *normés ou spécifiques ;*
  - *pas ou peu de mécanismes de sécurité.*
- *Flux de communication :*
  - *difficultés à maîtriser les matrices de flux et la visibilité des échanges.*

LES SPÉCIFICITÉS DE L'OT PAR RAPPORT À L'IT EN MATIÈRE DE CYBERSÉCURITÉ

Le monde de l'OT comporte de nombreuses spécificités par rapport aux enjeux de l'IT, mais malgré des différences métiers fortes, on observe une convergence progressive des technologies et de la gouvernance entre l'IT et l'OT. Les enjeux de réduction de consommation énergétique, de digitalisation des environnements (connectivité à tous les étages, digitalisation des salles, composants IoT...), de confort, de personnalisation du parcours utilisateur... sont autant de vecteurs de convergence technique et favorisent une gouvernance commune. Cette dernière doit prendre en comptes les différences métiers, et adapter son approche en conséquence.



6 SPÉCIFICITÉS OT ET IT

ÉLÉMENTS CLÉ DE CYBER SÉCURISATION DES SIB*

Certains de ces éléments ont déjà été abordés dans la définition de la cybersécurité. Cependant, sont regroupés ici les points importants dans le domaine de l'OT. Celui-ci est particulièrement concerné par les attaques hybrides, qui utilisent un système physique défaillant pour accéder à un système logique ou inversement, et ainsi rebondir afin d'obtenir le résultat recherché par l'attaque.

Contrôle d'accès physique aux équipements et aux bus de terrain

Il faut sensibiliser à l'ensemble des acteurs ayant une interaction avec ces équipements et préconiser :

- de fermer les armoires où se trouvent les équipements et de sécuriser les clés d'accès ;
- de rendre inaccessible tous les accès aux câbles réseau et/ou aux bus terrains ;
- de mettre en place un système de contrôle d'accès physiques pour ces équipements.

Cloisonnement des réseaux

La cartographie des flux est un élément indispensable aux systèmes industriels, car il permet d'évaluer très rapidement les vulnérabilités du système. Une fois cette cartographie effectuée, il est nécessaire de séparer les réseaux par des équipements dédiés ou des VLANs.

Il faut également filtrer les flux au moyen de pare-feu. Les systèmes de pare-feu doivent être inhérents à chaque matériel afin de sécuriser au mieux les installations.

Comme indiqué à plusieurs reprises dans ce livre blanc, les équipements doivent être en mesure de tracer les flux rejetés et de les analyser ou de les transférer à un SIEM (Security Information and Event Management).

Gestion des médias amovibles

Il est fortement recommandé de désactiver l'utilisation de ces médias ou d'appliquer une politique forte de discrimination de ces périphériques.

Gestion des comptes (accès logique, authentification)

Définir une politique de gestion des comptes utilisateur et des comptes d'application ET ne pas oublier de changer régulièrement les mots de passe. Une politique de gestion de mots de passe doit être mise en place sur les sites industriels avec une forte incitation à une intégration automatique des contrôles d'accès dans le SI.

Les équipements industriels doivent être inclus dans cette politique, ce qui exclut de fait les mots de passe par défaut de ces équipements.

La gestion des autorisations est également primordiale pour éviter que certains utilisateurs aient accès à des ressources ou des opérations non souhaitées. Les objets connectés disposent en général de peu de capacités à intégrer des systèmes d'autorisation, il est donc préférable de les agréger à du Edge Computing permettant ainsi cette gestion d'autorisation.

➔ *Rappel des mesures à prendre :*
- durcissement des configurations ;
- gestion des journaux d'événements et d'alarmes ;
- gestion des configurations ;
- sauvegardes/restaurations ;
- documentation ;
- protection antivirale ;
- mise à jour des correctifs (planification) ;
- protection des automates (PLC) ;
- stations d'ingénierie, postes de développement.

LES ENJEUX DE L'OT DANS LE SMART BUILDING

Les enjeux du Smart Building restent très tournés vers la notion de continuité de service. En effet, il est indispensable de maintenir opérationnel des équipements tel que les ascenseurs, la climatisation ou le contrôle d'accès, en particulier dans des infrastructures critiques comme les hôpitaux.

Néanmoins, on observe un cloisonnement des corps de métiers qui interviennent dans ce type d'environnement, et chacun y associe sa propre vision et connaissance de la sécurité. Il est donc essentiel d'homogénéiser cette approche et d'y adjoindre une stratégie de sécurité commune, prenant en compte les spécificités organisationnelles et techniques décrites précédemment.

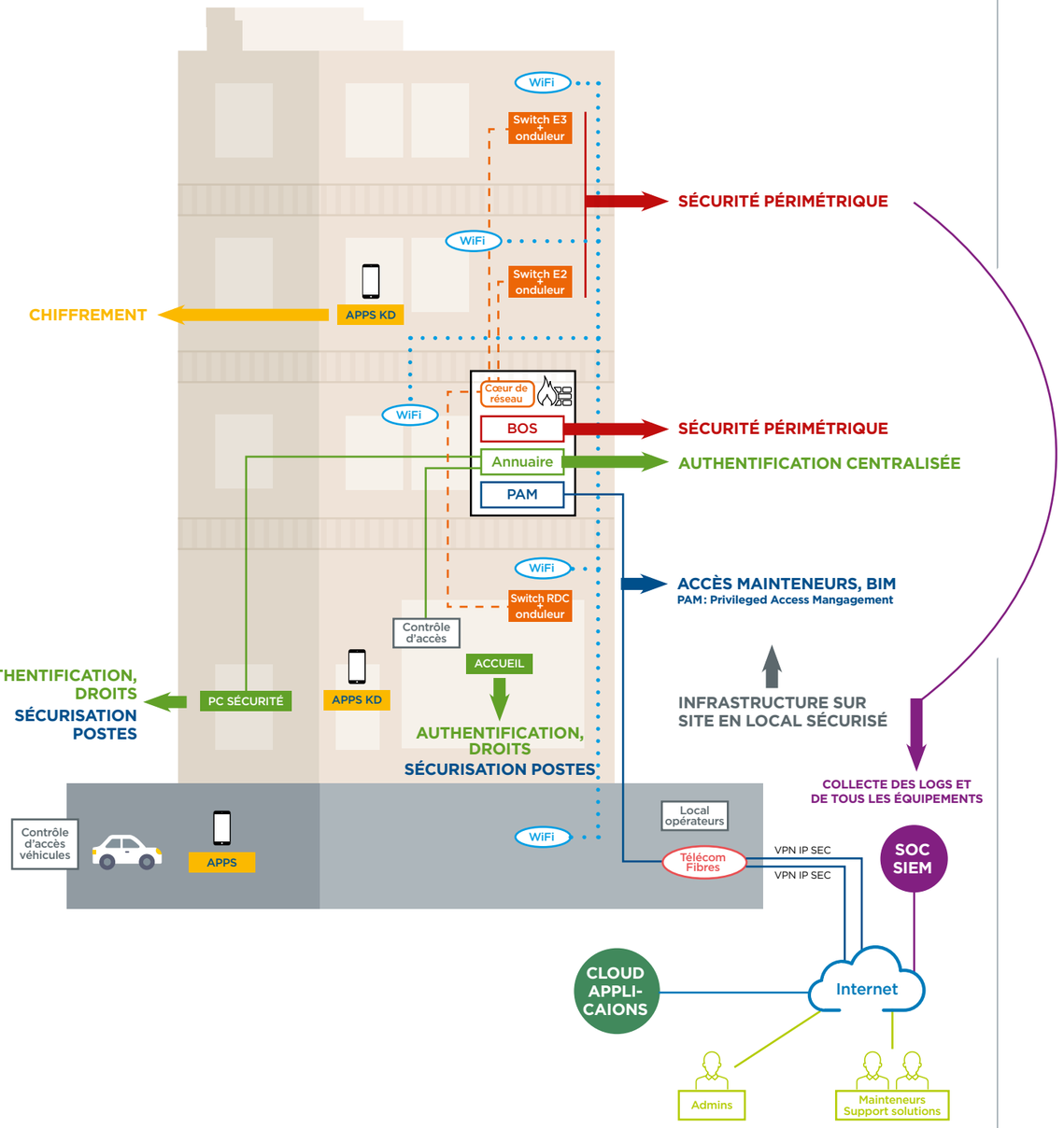
Les systèmes existants, installés depuis des années (Brown Field), sont intrinsèquement vulnérables, à cause des spécificités techniques et organisationnelles des systèmes « OT ». C'est pour cette raison que des nouvelles offres sont proposées comme le diagnostic des systèmes existants, l'analyse de risque, ou encore pour ceux soumis à des obligations, un audit. Il faudra réaliser un inventaire et une cartographie de l'existant, avec éventuellement selon la taille de l'installation et le nombre d'équipements raccordés, l'utilisation d'outils adaptés.

Les nouveaux systèmes (Green Field) sont conçus en Secure by Design. Cela signifie que le risque et la sécurité sont intégrés lors de sa conception et tout au long du cycle de vie. Le maintien de leur niveau de sécurité dans le temps est réalisé au travers de prestation de Maintien en conditions de sécurité (MCS) qui peut être adossée à un contrat de maintenance ou à une prestation de type MCO (Maintien en conditions opérationnelles). Là aussi, c'est une nouvelle offre spécifique à la cybersécurité.

* NDLR : l'ensemble des têtes de chapitres correspondent aux bonnes pratiques de l'ANSSI.

7 LES SOLUTIONS DE CYBER-SÉCURITÉ APPLIQUÉES AU BÂTIMENT

Au même titre que toute autre construction, la cybersécurité requiert à la fois la mise en place d'un projet et nécessite la mise en œuvre de « briques » (Solutions, switches, bastions, sondes…), des liants (réseaux, interfaces, APIs…) et du savoir-faire. De l'expérience à la fois technique en cybersécurité mais également une connaissance métier de l'environnement du bâtiment.



7 LES SOLUTIONS DE CYBERSÉCURITÉ APPLIQUÉES AU BÂTIMENT

SÉCURISER LES ACCÈS À DISTANCE

La multiplicité des acteurs fabricants d'objets connectés conduit à la multiplicité des accès sur ces objets qu'il faut sécuriser avec des solutions cyber spécifiques. Il devient alors possible de faire du contrôle d'accès à ces objets connectés et du suivi des opérations réalisées à distance par les tierces parties en charge de la maintenance des objets connectés. Ces solutions sont combinées à des solutions d'authentification forte multifacteurs (MFA) qui permettent de s'assurer de l'identité de la personne qui se connecte à la caméra embarquée, au capteur de température ou à n'importe quel objet connecté pour en réaliser la maintenance.

SÉCURISER LES ACCÈS À PRIVILÈGES

Les datacenters stockent les données sensibles et hébergent des outils qui pilotent le fonctionnement des objets connectés. Ce sont des cibles attirantes pour les opérateurs malveillants car s'ils parviennent à accéder au cœur de ces systèmes et à en prendre le contrôle, ils peuvent occasionner des dommages significatifs comme par exemple pirater les données sensibles des utilisateurs d'un service numérique ou faire tomber des services digitaux. Les conséquences vont de la rupture du service à la perte de crédibilité du système et de son infrastructure, et des personnes qui en assurent la gestion.

La sécurisation des accès à privilèges à ces datacenters est une composante essentielle au succès des services du Smart Buiilding et de la Smart City et les solutions de traçabilité, d'audit et de contrôle de type Privileged Access Management (PAM) sont la réponse à cette problématique. Ces solutions permettent de garantir que seuls les administrateurs autorisés auront accès aux services adéquats du datacenter et de tracer les opérations – par nature sensibles - qu'ils conduiront sur ces datacenters.

AUTHENTIFIER LES UTILISATEURS ET GÉRER LEURS ACCÈS AUX SERVICES

Pour que les services digitaux se développent rapidement, il est nécessaire de faire en sorte que les utilisateurs de ces services aient confiance dans la sécurité des données qu'ils échangent avec leurs opérateurs de services. Il est aussi nécessaire de permettre à ces opérateurs de proposer des innovations numériques dans des conditions économiquement viables à long terme. Pour ces deux raisons au moins, l'authentification des utilisateurs est un enjeu essentiel pour le développement du Smart Buiilding, en adressant le risque d'usurpation d'identité avec des mécanismes avancés reposant le plus souvent sur les smartphones des utilisateurs. Avec des solutions proposées de plus en plus souvent en mode SaaS, l'authentification forte multifacteurs (MFA) permet de façon simple de créer le bon niveau de confiance pour l'utilisateur du service sans nuire à son expérience qui doit rester fluide et simple pour accéder au service et le consommer dans le temps. Ces mêmes solutions permettent à l'opérateur de service de contrôler que seuls ses abonnés auront accès aux services payant par exemple, une exigence minimale sur laquelle repose leur viabilité.

SÉCURISATION DES ACCÈS DES PRESTATAIRES D'EXPLOITATION

Les fonctions vitales d'un bâtiment exigent une continuité de service sans faille, pilotées et maintenues par de nombreuses équipes internes et externes à l'environnement. Les accès à ces ressources sont donc clefs et doivent être sécurisés.

Le plus grand défi pour les équipes IT/OT aujourd'hui est sans aucun doute la centralisation et le contrôle de ces accès internes ou externes. Les constructeurs ont imposé leurs outils d'accès à distance jusqu'à présent, et le résultat est une multitude de solutions VPN plus ou moins sécurisées, disséminées dans les salles techniques.

De nombreuses cyberattaques dans le domaine des technologies de l'information commencent par l'exploitation d'un outil d'accès à distance non sécurisé. Il est donc impératif de centraliser ces portes ouvertes et d'en assurer le contrôle, la visibilité et la traçabilité.
La sécurisation du système d'information OT d'un bâtiment nécessite une double approche :

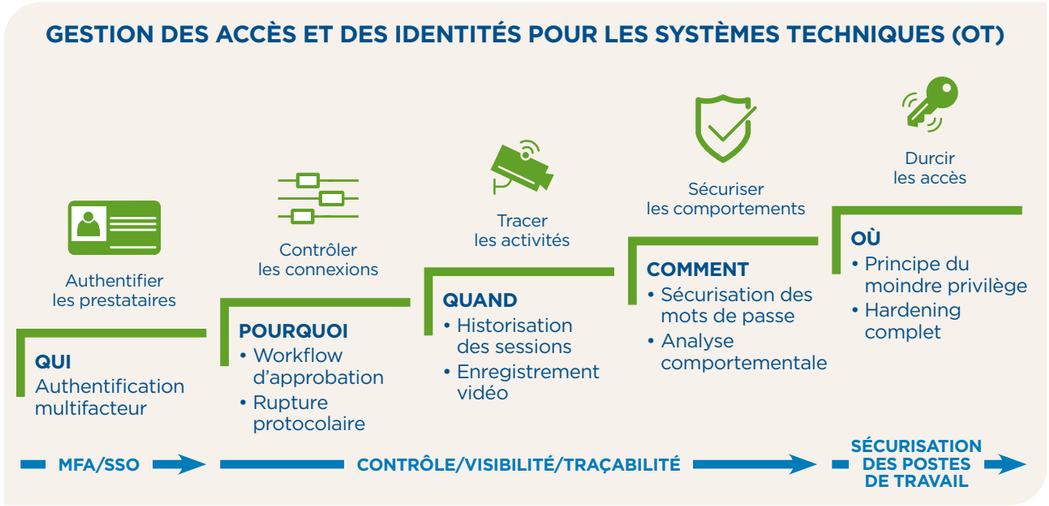
La défense en profondeur

En raison de leur criticité, les accès aux composants que l'on retrouve dans les environnements OT doivent être soumis à une approche de sécurité à tous les niveaux. Authentification des utilisateurs, contrôle et sécurisation des sessions, suppression des droits, durcissement des postes d'ingénierie et des consoles de gestion et de supervision.

Zero Trust

Il est crucial de prendre en compte les droits et les autorisations des prestataires tout au long de leur parcours de connexion. Les cyberattaques s'appuient de plus en plus sur l'ensemble de la chaîne d'approvisionnement. Il est donc très important de considérer que tout utilisateur externe ou interne est une menace potentielle. Les solutions bastions permettent un contrôle fin des droits et des comportements des utilisateurs (découpage du protocole, analyse comportementale, workflow d'approbation, etc.).

➔ *Avec les solutions de « Bastion », ou de PAM (Privileged Access Management), les prestataires accèdent simplement et efficacement à leurs équipements sans risque de contamination. L'activité est enregistrée et tracée, les mots de passe sécurisés et la continuité de service assurée.*



GÉRER LES SYSTÈMES HÉTÉROGÈNES DE FAÇON SIMPLE ET SOUVERAINE

De nombreuses solutions de cybersécurité doivent être combinées pour offrir une réponse globale au nécessaire besoin de confiance des utilisateurs. Or, le déploiement de solutions de sécurité hétérogènes et non interopérables peut mener à des complexités des systèmes d'information qui finissent par favoriser les cyberattaques.

L'approche consiste donc à déployer des solutions capables de fournir une vue globale aux équipes de supervision, au-delà des différentes composantes cyber fournies par chacun des acteurs du marché. En créant un lien entre plusieurs de ces différents outils et en leur permettant d'interagir entre eux, les solutions souveraines comme SCAR (Service commun d'administration et de reporting) permettent aux structures intelligentes de fédérer et d'administrer des solutions hétérogènes à partir d'une interface commune, de remonter rapidement des KPI cyber pertinents de manière à accélérer la prise de décision, et de vérifier simplement que chaque brique cyber d'un système se comporte conformément aux attentes.

GESTIONS DES LOGS

SOC

Un SOC (Security Operation Center) est une plateforme de services composée de personnes, de softwares, de processus, visant à assurer la sécurité d'un SI. Le SOC réagit aux alertes en provenance d'un SIEM ou du monitoring, ou d'un appel client. C'est une organisation.

SIEM

Un SIEM (Security Information and Event Management) est une solution logicielle qui permet la collecte, le tri et la normalisation, ainsi que l'analyse des logs d'un système. Il met en œuvre des patterns comportementaux, des listes et des algorithmes permettant la détection d'erreurs ou d'actions malveillantes, ou encore des tentatives d'intrusion. Le SIEM ne s'arrête pas aux événements de sécurité. Il peut également servir comme plateforme analytique des données du bâtiment et ainsi établir des rapports sur l'efficacité énergétique, l'usage des ascenseurs etc.

XDR

Le eXtended Detection and Response (XDR) est une solution logicielle visant à augmenter le SIEM et via des analyses croisées diminuer fortement les faux positifs (points noirs d'un SIEM) et donc accroître la pertinence des indicateurs et alertes, l'objectif étant également de diminuer les temps d'analyse et d'apporter une réponse plus rapide.

ÉTENDRE LA SUPERVISION AVEC DES SONDES RÉSEAUX

Les sondes améliorent la visibilité sur les ressources industrielles, informatiques, de l'IoT, à la périphérie et dans le Cloud, pour accélérer la sécurité et la transformation digitale. Elles permettent de mettre en œuvre un triptyque voir/détecter/unifier et de compléter la gestion des logs.

Voir

Les sondes permettent de « voir » toutes les ressources et tous les comportements des systèmes industriels et de l'IoT sur les réseaux pour une connaissance exhaustive.

Inventaire temps-réel des ressources :

- améliore la cyber résilience et le gain de temps grâce à l'inventaire automatisé des ressources ;
- identifie toutes les ressources communicantes ;
- fournit des informations complètes sur les nœuds, notamment le nom, le type, le numéro de série, la version du micrologiciel et les composants, ainsi que sur les risques, les alertes de sécurité et de fiabilité, les correctifs manquants et les vulnérabilités.

Évaluation automatique des vulnérabilités :

- identifie les appareils des fournisseurs qui sont vulnérables et utilise la base de données des vulnérabilités maintenue par le gouvernement américain.

Surveillance continue :

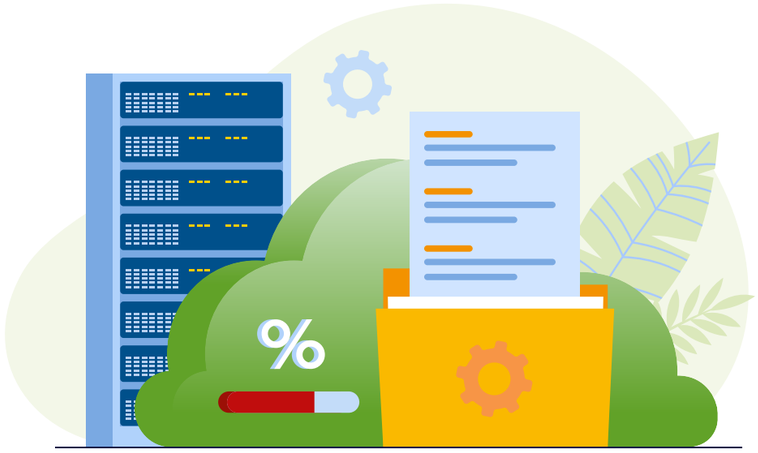
- surveillance continue de tous les protocoles pris en charge : industriels, informatiques et IoT ;
- pas d'angles morts critiques dans la protection causée par une surveillance limitée ou une prise en charge inadéquate des protocoles.

Détecter

Les sondes permettent de détecter à partir des informations collectées les cybermenaces, les vulnérabilités et les risques et anomalies pour un traitement plus rapide.

Réduction des risques grâce à la visualisation du réseau :

- fournit une compréhension instantanée du réseau industriel/IoT et de ses schémas d'activité ;
- présente des données clés telles que le débit du trafic, les connexions TCP et les protocoles ;
- améliore votre compréhension des activités « normales ».



Détection des menaces :
- identifie les menaces pour la cybersécurité et la fiabilité des processus ;
- détecte les menaces avancées et les cyber risques à un stade précoce et avancé.

Unifier

La sécurité, la visibilité et la supervision de l'ensemble des ressources pour une meilleure résilience.

Infrastructure de sécurité intégrée :
- optimise les processus de sécurité informatiques/industriels ;
- facilite l'harmonisation des données de sécurité pour un traitement cohérent ;
- comprend des intégrations prédéfinies avec des systèmes de gestion des ressources, des tickets et des identités, et des SIEM.

SERVICES DE DIAGNOSTIC CYBERSÉCURITÉ ET ANALYSE DE RISQUE

Chaque système existant de gestion technique de bâtiment avec ses différents sous-systèmes et équipements qui le composent est différent et nécessite un diagnostic personnalisé sur l'état des lieux et la vulnérabilité. Ce diagnostic constitue la première étape vers la sécurisation de vos systèmes.

Cela consiste à réaliser l'inventaire, à identifier les vulnérabilités, à analyser les risques, à détecter les failles de sécurité, et à proposer un plan d'action pour renforcer la sécurité.

Les différentes étapes de mise en œuvre :
- analyse de risque ;
- évaluation niveau de sécurité par rapport aux référentiels ;
- analyse des mesures cybersécurité en réduction de risque ;
- inventaire et cartographie physique, logique, technique et fonctionnelle ;
- rapport et restitution ;
- proposition d'un plan d'action ;
- support à l'homologation LPM (Loi de programmation militaire) ;
- analyse de vulnérabilité ;
- tests d'intrusion ;
- formation et sensibilisation.

SERVICES DE MCS (MAINTIEN EN CONDITION DE SÉCURITÉ)

Pour maintenir le niveau de sécurité à un niveau acceptable et permettre à vos systèmes d'assurer la continuité du service fourni, la mise en place de services de MCS permet une gestion maîtrisée et pérenne des risques liés aux vulnérabilités logicielles et matérielles.

Bénéfice en matière de sécurité :
- garantie d'une base saine et performante ;
- meilleure maîtrise des installations pour les évolutions futures ;
- augmentation de la disponibilité opérationnelle ;
- optimisation des coûts globaux de possession.

Les différentes étapes de mise en œuvre :
- veille de vulnérabilité et détection/qualification de nouvelles menaces ;
- application des correctifs de sécurité sur les équipements et les logiciels déployés ;
- gestion d'obsolescence ;
- formation de sensibilisation, amélioration continue ;
- simulation d'attaques ;
- réponse sur incidents.

EXEMPLE D'INTÉGRATION : LE CONTRÔLE D'ACCÈS

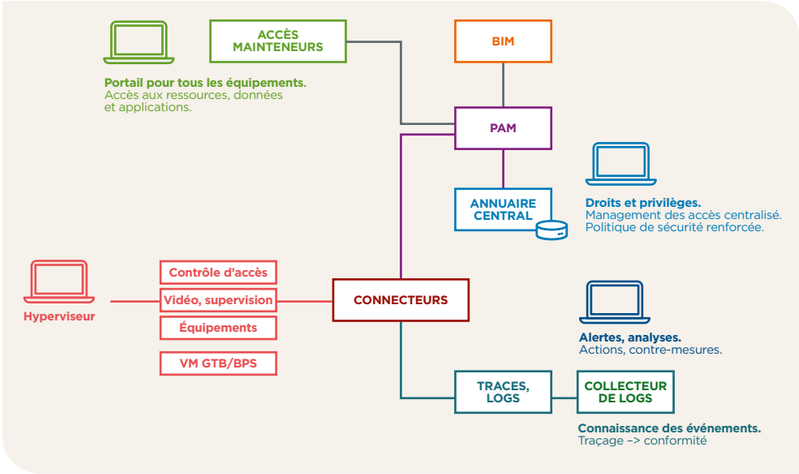
La mise en place de mesures de sécurité en profondeur nécessite de pouvoir s'interfacer, échanger des informations avec les équipements. Pour pouvoir faire cela, les équipements doivent disposer d'APIs ou d'interface de programmation exposant des fonctions comme l'annuaire, les logs ou encore du SSO (Single Sign On). Ces connecteurs permettent de se raccrocher aux standards reconnus et éprouvés du marché et d'offrir des solutions qui seront utilisables pour tous les équipements et solutions logicielles disposant de ces connecteurs.

Cette infrastructure permet en outre la mise en place d'une gouvernance ainsi que l'application des règles de conformité.

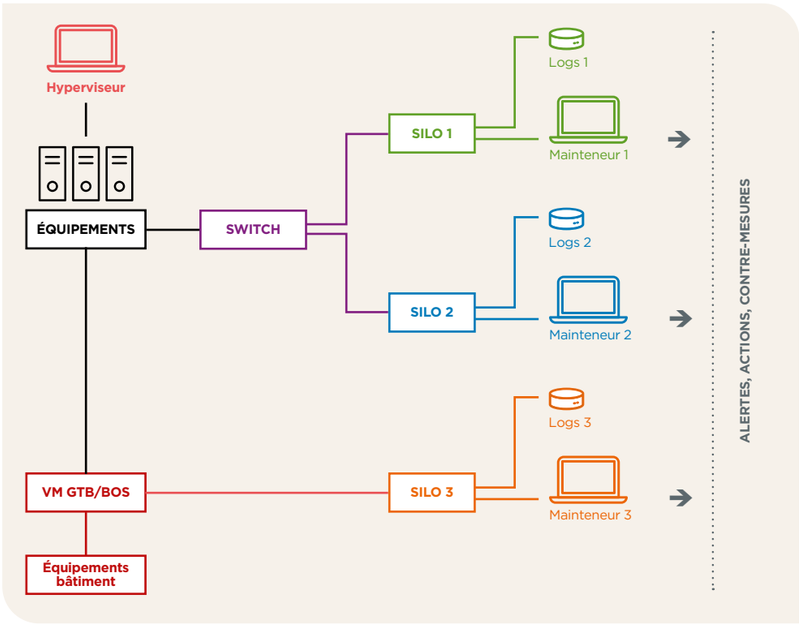
Le schéma ci-après montre l'intégration d'un système de contrôle d'accès disposant de connecteurs. Il indique également la réutilisation des briques déployées pour les autres composantes du système. Dans notre cas, on dispose d'un connecteur LDAP (Annuaire) et syslog (Logs). Dans cette architecture, on utilise également une brique de PAM (Privileged Access Management) permettant de centraliser tous les accès munis d'un niveau élevé de droits et de tracer toutes les opérations réalisées (voir chapitre : Sécuriser les accès à privilèges). Le BIM et le contrôle d'accès comme le PAM sont connectés à l'annuaire central. Cette centralisation permet de déployer des politiques de sécurité globales plus efficaces et maîtrisables.

La capacité à centraliser les différents logs des systèmes permet de réaliser des analyses, notamment via un outil de SIEM (Security Incident and Event Management). Un système de SIEM est capable de fournir des tableaux de bord plus faciles à manipuler et permettant de prendre des décisions et d'intervenir beaucoup plus rapidement, mais aussi d'avoir des infos croisées et d'avoir une vue d'ensemble, ce qui est très important pour la pertinence des mesures de sécurité déployées.

7 LES SOLUTIONS DE CYBERSÉCURITÉ APPLIQUÉES AU BÂTIMENT



Sans ces connecteurs, les données (comptes, privilèges, accès etc.) sont éclatées en silos qui ne « discutent pas » (voir schéma suivant). L'effet est une gestion beaucoup plus compliquée des accès aux systèmes et un monitoring global de la sécurité difficile et tout aussi complexe. Au final, on n'a pas la maitrise réelle des systèmes et on ne sait pas ce qui se passe sur son réseau. Ou bien, retrouver les informations devient un travail long et laborieux (par exemple retrouver des traces d'une intervention ayant causé des problèmes et des incidents).



Les mondes du bâtiment et de la cybersécurité ne parlent pas encore le même langage aujourd'hui, ou de façon segmentée. Or, c'est bien là que tout se joue. La cybersécurité est une affaire de partenariat avec les équipementiers.

Le cadre R2S notamment, vise à relier ces deux mondes. Tout d'abord orienté Smart Building, le cadre de référence de la SBA intègre une dimension cybersécurité et réseau (au sens large) importante.

8

CONCLUSION

Dans le monde connecté que nous connaissons tous, nous sommes témoins des attaques réalisées un peu partout sur la planète (domaines de l'industrie, de l'énergie, des assurances, des banques, des sites de commerce, les gouvernements, les brevets, etc.). Elles sont souvent l'œuvre de personnes, d'organisations avec d'importants moyens. Ces personnes ou ces organisations criminelles sont déterminées, outillées et toujours en évolution. Nous pouvons voir que certaines attaques sont extrêmement dangereuses, surtout quand elles ciblent des industries critiques (sites Ceveso, centres pétroliers, traitement des eaux, usines manipulant des produits toxiques, centrales nucléaires, etc.).

Que dire alors dans un monde en passe de devenir hyper connecté ? Quand une poignée d'octets sur un automate (une centrifugeuse) suffisent pour mettre en péril nos vies par le biais des systèmes censés nous protéger, et que nous ne savons pas qu'il y a eu compromission. Nous comprenons bien que le risque est décuplé et que les enjeux sont de plus en plus stratégiques pour ces attaquants, et donc cruciaux pour nos infrastructures. Devant la multiplicité des attaques d'envergure, des sites à risque, et du 24/7/365 des attaques, nous devons bien sûr mettre en place des boucliers, mais il faut déjà comprendre les moyens et les campagnes quasi-militaires menées contre nos infrastructures et nos données, nos savoirs, nos usages. En d'autres termes, il faut être au courant de ce qui se passe sur nos systèmes informatiques (mais, pas que) et pour cela imaginer et déployer des outils, des solutions au spectre assez large, afin de surveiller ces SI de façon intelligente, exhaustive et permanente, et mettre en place des procédures sur divers plans (design, administration, mise à jour, etc.).

Nous avons parlé de matériels, de données, de maintien de la sécurité par la supervision intelligente et proactive. Il est temps de parler de ce que cela protège au final, avant les données, les serveurs, les automates, c'est-à-dire les humains. Il est crucial d'intégrer cette dimension à nos réflexions. Car, nous devons être les outils de notre propre protection.

UNE STRATÉGIE, DES OUTILS ET DES HOMMES

Il est bien connu que beaucoup d'attaques ont lieu à la suite d'une négligence d'une personne dans la chaîne, d'une inattention. Un clic sur un lien dans un spam, quelqu'un qui tient la porte d'entrée par politesse… Tout est utilisable, les attaquants se positionnent dans l'attente d'un événement de ce type pour passer, faire un pas de plus vers leur objectif, qui peut être totalement « ailleurs ». Quant à leur cheminement, il peut sembler erratique, touchant parfois à des choses estimées peu sensibles, mais il ne l'est pas, c'est juste qu'on ne voit pas l'objectif final. D'où la nécessité de traquer et tenter de « déduire » ce cheminement sur le réseau (analyse de logs, recherche de patterns…), et de définir un strict contrôle d'accès aux ressources.

Toutes ces technologies, ces outils, doivent fonctionner de manière collégiale afin d'être efficace. On comprend bien qu'il est important de relier les traces mais aussi qu'il faut pouvoir piloter nos systèmes et nos contre-mesures de manière centralisée en disposant d'un système d'alerte performant. Il faut également surveiller et sécuriser de façon drastique ces systèmes devenant par là-même extrêmement critiques.

8 CONCLUSION

Enfin, il est important de prendre conscience que la cybersécurité est un volet intégré à une approche de création de valeur par la mise en place de solutions digitalisées. Elle ne doit plus être à l'avenir une surcouche implémentée postérieurement à un projet digital mais bien une composante intégrée au modèle d'affaire global qui vient sécuriser la continuité des opérations.

➔ *Avoir une bonne connaissance (documentée) de ses actifs et des risques.*
➔ *Déterminer la cible de sécurité et prévoir les budgets adéquats.*
➔ *Savoir ce qu'il se passe sur son réseau, disposer d'alertes.*
➔ *Faire appel au bon sens, à la simplicité.*
➔ *Sécuriser par l'architecture, pas seulement par l'empilement de solutions.*
➔ *Utiliser des standards reconnus et interagir avec leurs communautés.*
➔ *Communiquer, sensibiliser, former, se certifier.*
➔ *Nouer des partenariats avec des spécialistes.*

Devant cette complexité évidente et galopante, nous devons mettre en place un cadre afin de guider et garantir la couverture des systèmes envisagés, l'exhaustivité des points de surveillance, et un système d'évaluation des menaces adapté et imaginatif. Et ne pas être naïf : de nombreux exemples prouvent que les cybercriminels n'ont pas de limites (cyberattaques d'hôpitaux, par exemple) et que leurs actions outrepassent complètement le sens commun et qu'ils n'ont cure des personnes. Or, on l'a vu, ce que nous protégeons par-dessus tout, ce sont des femmes et des hommes.

Nous pensons que les objectifs de sécurité dans le contexte actuel nécessitent une approche globale, réaliste. Disposer d'une offre intégrant toutes les couches (défense en profondeur) peut être une bonne approche :

- l'offre doit intégrer toutes les dimensions de la cybersécurité en un tout homogène et interconnecté, partageant donc les informations cruciales aux opérations (MCO, capacity planning, surveillance et alertes, gouvernance) ;
- elle doit faire l'objet d'un accompagnement complet, intégrant sensibilisation et formation ;
- elle doit s'appuyer sur des standards et être entièrement documentée.

9

TABLEAU DES ABRÉVIATIONS, GLOSSAIRE

SIGLE	DÉVELOPPEMENT	NOTES
ANSSI	Agence nationale de la sécurité des systèmes d'information	L'Agence nationale de la sécurité des systèmes d'information est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
API	Application Programming Interface	En informatique, une interface de programmation d'application ou interface de programmation applicative est un ensemble normalisé de classes, de méthodes, de fonctions et de constantes qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels (Wikipédia).
BIM	Building Information Modeling	Il désigne les outils de modélisation des informations de la construction implémentés par des applications qui permettent la modélisation des données du bâtiment, d'une structure, d'un édifice ou d'un ouvrage.
BSI	Bundesamt für Sicherheit in der Informationstechnik	Homologue allemand de l'ANSSI en France.
BOS	Building Operationg System	Le BOS permet de modéliser chaque zone du bâtiment et d'organiser des données hétérogènes en un format unifié, aisément accessible par des applications tierces de différentes marques. Sur tout un étage, par exemple, il peut gérer les flux d'informations venant d'une centrale d'air Carrier, de volets roulants Diagral, d'un ascenseur Koné et d'une GTB Schneider Electric (SBA).
CID CIDT	Confidentialité/Intégrité/ Disponibilité/Traçage	Triade ou quadriade des concepts à la base de la cyber sécurisation.
CTI	Cyber Threat Intelligence	La Threat Intelligence, ou Cyber Threat Intelligence est une discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberespace, afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (Wikipédia).
EBIOS	Expression des besoins et identification des objectifs de sécurité	Méthode d'évaluation des risques maintenue par l'ANSSI.
GTB	Gestion Technique du Bâtiment	La gestion technique de bâtiment est un système informatique généralement installé dans des grands bâtiments ou dans des installations industrielles afin de superviser l'ensemble des équipements qui y sont installés (Wikipédia).
HIPAA	Health Insurance Portability and Accountability Act	C'est une loi votée par le Congrès des États-Unis concernant la santé et l'assurance maladie. Les normes définies forment un référentiel santé.

9 TABLEAU DES ABRÉVIATIONS, GLOSSAIRE

SIGLE	DÉVELOPPEMENT	NOTES
IAM	Identity and Acess Management	En sécurité des systèmes d'information, la gestion des identités et des accès est l'ensemble des processus et des technologies mis en œuvre par une entité pour la gestion des habilitations de ses utilisateurs à accéder aux ressources du système d'information (données, applications). Il s'agit donc de savoir et gérer qui a accès à quelle information et quand.
IDaaS	IDentity As A Service	Service d'identité hébergé et géré par un fournisseur externe à l'entreprise., par exemple dans un Cloud.
IDG	Informatique de gestion	Informatique traditionnelle (Bureautique etc.) souvent opposée à l'informatique industrielle.
IDM	Identity Management	Annuaires.
IDS	Intrusion Detection System	Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions (Wikipédia).
IT	Information Technology	Informatique « traditionnelle » ou informatique de gestion. « Tout le spectre des technologies de traitement de l'information, notamment les logiciels, le matériel, les technologies des communications et les services connexes. Généralement, les technologies de l'information ne comprennent pas les technologies embarquées qui ne génèrent aucune donnée pour l'usage de l'entreprise. » (JDN).
ISO	International Standards Organization	Organisation internationale de normalisation.
LPM	Loi de programmation militaire	
MFA	Multi Factor Authentication	L' authentification multifacteur (MFA : englobant l'authentification à deux facteurs ou 2FA, ainsi que des termes similaires) est une méthode d'authentification électronique dans laquelle un utilisateur de l'appareil n'a accès à un site Web ou à une application qu'après avoir présenté avec succès deux ou plusieurs éléments de preuve (ou facteurs) à un mécanisme d'authentification : connaissance (quelque chose que seul l'utilisateur sait), possession (quelque chose que seul l'utilisateur possède) et héritage (quelque chose que seul l'utilisateur est). MFA protège l'utilisateur contre une personne inconnue qui tente d'accéder à ses données telles que des informations d'identification personnelle ou des actifs financiers. Authentification multifacteur - (xcvWiki).
NIST	National Institute of Standards and Technology	

SIGLE	DÉVELOPPEMENT	NOTES
OT	Operational Technology	« L'OT désigne le matériel et les logiciels qui détectent ou provoquent un changement par le biais de la surveillance et/ou du contrôle directs des périphériques physiques, des processus et des événements dans l'entreprise. » JDN.
PAM	Privileged Access Management	Il s'agit de la gestion des comptes à privilèges (Root, Administrator, DBAs, administrateurs d'applications etc.) « Les logiciels PAM permettent aux entreprises de sécuriser les accès sensibles aux ressources critiques, ce qui signifie que seules les personnes possédant les identifiants appropriés peuvent y accéder. Les technologies PAM devraient également aider les organisations à être conformes, via un processus de sécurisation, de gestion et de suivi des comptes à privilèges, ainsi que des accès à ces comptes. » (Zdnet).
PCA	Plan de Continuité d'Activité	
PCI-DSS	Payment Card Industry Data Security Standard	Référentiel finances. La norme de sécurité de l'industrie des cartes de paiement est un standard de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique. La norme PCI DSS est établie par les cinq principaux réseaux cartes et est gérée par le Conseil des normes de sécurité PCI (Wikipédia).
PEDM	Privilege Escalation and Delegation Management	
PLC	Programmable Logic Controler	Un contrôleur logique programmable permet de contrôler une machine, un automate.
POC	Proof Of Concept	
POLP	Principle Of Least Privilege	
PRA	Plan de reprise d'activité	
PTR	Plan de traitement des risques	
R2S	Ready to Services	
Réseau Smart		Nom donné par la SBA au réseau du SI bâtimentaire, intégrant les notions de segmentation et implémentant le protocole TCP/IP.
RGPD (GDPR)		Règlement général sur la protection des données.
SBA	Smart Buildings Alliance	
SCADA	Supervisory Control And Data Acquisition	
SIB	Système d'information bâtimentaire	
SIEM	Security Incident and Event Management	

9 TABLEAU DES ABRÉVIATIONS, GLOSSAIRE

SIGLE	DÉVELOPPEMENT	NOTES
Smart Building		Smart Building ou bâtiment intelligent. Un bâtiment est défini comme smart lorsqu'il est capable de fournir des données à des applications diverses. Ces données permettent aux applications de surveiller et modifier les équipements techniques du bâtiment (énergie, éclairage, climatisation, sécurité, parkings…).
Smart City		Définition de la CNIL : « La ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. »
SOC	Security Operation Center	
SSO	Single Sign On	
VPN	Virtual Private Network	
XDR	eXtended Detection and Response	Solution travaillant avec le SIEM.

10

ANNEXES

ANNEXE 1

DÉTAIL DES MESURES DE L'ANSSI POUR L'OT

Mesures de sécurité organisationnelles

➔ **Rôles et responsabilités**: les réseaux OT ont la réputation d'être des systèmes d'information dont il est difficile de connaitre les composants et l'environnement d'exploitation. Il est essentiel d'acquérir une connaissance précise et complète du système pour pouvoir lui appliquer les mesures de sécurité dont il fait l'objet.

Ainsi il faut pouvoir définir une chaîne de responsabilités de la cybersécurité permettant le fondement d'une bonne gouvernance. Cette chaîne vise à sensibiliser et responsabiliser les acteurs afin de:
- se tenir informer de la menace;
- planifier, acquérir et mettre en œuvre les mesures de sécurité;
- diffuser les bonnes pratiques de cybersécurité au sein de l'établissement;
- maintenir les règles et mesures de sécurité;

➔ **Cartographie**: il convient également de disposer d'une connaissance complète de l'ensemble des constituants du système d'information à travers une cartographie (*a minima*) physique, logique et applicative. Cette cartographie doit être suivie et mise à jour régulièrement. Elle s'intègre à une démarche générale de gestion des risques permettant de disposer d'une vision commune et partagée du système au sein de l'établissement afin de:
- faciliter la prise de décision;
- identifier les systèmes critiques et exposés;
- réagir et prévoir efficacement les scénarios de défense en cas d'attaque;
- identifier les fonctions nécessaires à la gestion de crise.

➔ **Analyse de risque**: une fois la cartographie du système réalisé, une analyse de risque doit être engagée. Celle-ci apportera une connaissance supplémentaire au système étudié et permettra surtout d'identifier et d'évaluer le danger au regard des probabilités d'occurrence. Elle servira ensuite pour la mise en place de mesures de sécurité techniques, physiques et organisationnelles adaptées aux risques et aux besoins. L'analyse de risque devra favoriser une approche fédérative entre la sûreté de fonctionnement et la cybersécurité. La sûreté de fonctionnement est ici vue comme l'aptitude d'un système à remplir une ou plusieurs fonctions et à ne pas présenter de dangers pour les utilisateurs et l'environnement. Les critères de cette analyse devront être ceux du risque industriel c'est-à-dire le risque sur l'information mais aussi l'investissement, la capacité de production ou de rendre le service, les personnes, l'environnement.

➔ **Gestion des sauvegardes**: un plan de sauvegarde doit être mis en place afin de disposer des données participant au bon déroulement d'un Plan de reprise d'activité (PRA) qui intervient après une attaque. Ce plan doit prendre en compte un suivi des sauvegardes à chaque modification. Les données à sauvegarder concerne les équipements

serveurs, postes informatiques, automates et équipements terrain (capteurs, actionneurs), équipements réseau, équipements de sécurité. Pour l'ensemble de ces composants, les données à sauvegarder, lorsqu'elles sont existantes, sont :

- le fichier d'installation logiciel ;
- la base de données de configuration ;
- l'historian ;
- les firmwares ;
- les programmes automates ;
- le fichier de configuration.

➔ **Gestion de la documentation** : en ce qui concerne la conception, l'exploitation et la maintenance des systèmes industriels, une documentation détaillée doit être rédigée et sauvegardée afin de maîtriser avec exactitude l'exploitation des processus. Cette documentation intègre notamment les analyses fonctionnelles, schémas d'architecture et plan d'adressage. Le plan doit prévoir une tenue à jour et une sauvegarde maîtrisée (lieu de stockage et journalisation des mises à jour) de ces documents.

Maîtrise des intervenants

➔ **Gestion des intervenants** : les intervenants sur les systèmes industriels ont des profils différents (mainteneur, responsable technique, responsable d'exploitation…). Ils peuvent être internes ou être des prestataires extérieurs (fabricants de machines, intégrateurs…). Il est essentiel de pouvoir gérer ces intervenants en fonction de leurs droits, fonctions, scope d'intervention. Cette gestion implique notamment une maitrise à jour des accès aux locaux, au réseau, aux données ainsi qu'à l'utilisation d'équipements électroniques. Ces données d'accès doivent être conformes aux bonnes pratiques de gestion des identifiants.

➔ **Sensibilisation et formation** : le facteur humain étant souvent la porte d'entrée d'une cyberattaque, il convient de sensibiliser et de former les intervenants aux bonnes pratiques de cybersécurité. Cette sensibilisation aura pour effet de diminuer fortement les négligences largement exploitées par les cyberattaquants. Les avancées technologiques ainsi que les schémas d'attaques évoluant au fil des années, cette sensibilisation devra être suivie dans le temps.

➔ **Gestion des interventions** : les interventions sur les systèmes industriels doivent faire l'objet d'une procédure organisée et tracée décrivant l'ensemble des aspects essentielles à l'intervention. Il conviendra notamment de notifier et valider avec le responsable du système l'identité de l'intervenant, la période et le périmètre d'intervention. L'ensemble des actions effectuées doivent être décrites ainsi que les équipements permettant ces actions.

Intégration de la cybersécurité dans le cycle de vie du système industriel

La cybersécurité doit être considérée comme un métier et faire partie intégrante des projets, de la phase de spécification à la phase d'exploitation notamment pour des programmes de création, extension et refonte des systèmes.

➔ **Exigences dans les contrats et cahiers des charges** : un volet sur la cybersécurité doit être intégré aux cahiers des charges et prévoir la livraison de l'ensemble des documentations nécessaires à la prise de connaissance du système sur sa constitution, sa conception et son fonctionnement. Pour les systèmes les plus critiques, le cahier des charges devra prévoir une clause exigeant la fourniture de logiciels et matériels labellisés sur le plan de la cybersécurité. Le système devra également faire l'objet d'une analyse de risque. L'intégrateur choisi devra mettre en œuvre l'ensemble des bonnes pratiques cyber dans la réalisation du projet (confidentialité du projet, environnement de développement sécurisé…)

➔ **Intégration de la cybersécurité dans les phases de spécification** : le cahier des charges devra prévoir l'ensemble des mesures techniques nécessaires à la sécurité du système ainsi que l'ensemble des procédures permettant le maintien de son niveau de sécurité. Le système devra être spécifié de tel sorte que ses fonctions soient exclusivement liées à la conduite du process.

➔ **Intégration de la cybersécurité dans les phases de conception** : une attention particulière sera portée sur la complexité du système qui devra être réduite afin de minimiser le risque cyber. Les rôles des différents intervenants seront définis et de telle sorte que les privilèges soient réduits au strict nécessaire. Les administrateurs auront des droits et des accès dissociés des autres intervenant sur le système.

➔ **Audits et tests de cybersécurité** : le maintien en condition de sécurité doit prévoir des audits réguliers du système afin de convenir de la bonne marche des fonctions de sécurité mise en œuvre ainsi que de l'organisation associée. Ces phases de tests peuvent être organisées conjointement avec les phases de maintenance.
La qualité de l'audit devra être contrôlée par le responsable du système. Sa conduite devra être réalisée par un prestataire du domaine, idéalement labellisé pour ce type d'intervention.

➔ **Transfert en exploitation** : avant la mise en exploitation du système, une vérification du niveau de sécurité est recommandée. Pour les systèmes les plus critiques, une homologation ainsi qu'une autorisation d'exploitation sont demandées.

➔ **Gestion des modifications et évolutions** : toute modification d'applications, fichier de configuration de l'ensemble des composants du système doit être tracée. Les changements entre les versions doivent être clairement identifiées.

➔ **Processus de veille** : une veille liée au risque cyber doit être organisée et suivie dans le temps. À cet effet, les CERT nationaux ainsi que ceux des fabricants et éditeurs de logiciels doivent être consultés pour permettre une application des mesures adaptées aux tendances et failles identifiés.

➔ **Gestion de l'obsolescence** : les équipements et logiciels utilisés sur le système peuvent faire l'objet d'obsolescence laissant de nouvelles portes d'accès aux cyberattaquants. Il convient de prévoir en amont cet aspect en l'intégrant dans les contrats signés avec les fournisseurs et en établissant un plan de gestion d'obsolescence des composants.

Sécurité physique et contrôle d'accès aux locaux

➔ **Accès aux locaux**: une politique de gestion des accès aux locaux doit être mise en œuvre pour permettre un accès approprié aux intervenants. Une vigilance particulière sera adressée aux prestataires et intervenants externe.

➔ **Accès aux équipements et aux câblages**: l'ensemble des composants du système seront sous contrôle d'accès et placés dans des locaux ou des armoires fermés à clé. *A minima*, les prises et moyens de connections au système ne devront pas être accessibles au public. Pour les systèmes les plus critiques, câbles et prises feront l'objet d'une sécurisation complémentaire.

Réaction en cas d'incident

➔ **Plan de reprise ou de continuité d'activité**: un plan de reprise d'activité (PRA) ou de continuité d'activité (PCA) doit être mis en œuvre. Le PRA doit permettre de prévoir par anticipation, les mécanismes pour reconstruire et relancer le système en cas de sinistre. Le PCA doit permettre de prévoir une stratégie qui limite l'impact d'un incident quitte à ce que le service soit dégradé. Dans le cas où un PRA et PCA est déjà existant pour le fonctionnement du système, il faudra y intégrer les incidents de cybersécurité.

➔ **Mode dégradé**: en cas de sinistre ou d'intervention, les procédures devront prendre en compte les aspects de cybersécurité et s'assurer de dégrader *a minima* les moyens mis en œuvre. Les procédures veilleront particulièrement à ne pas provoquer de dégâts matériel et humain.

➔ **Gestion de crise**: une procédure de gestion de crise permettant de faire face à la survenance d'une crise ainsi qu'à l'analyse *a posteriori* doit être mis en place. Cette procédure permettra de réagir au plus juste et au plus efficacement face à une menace. Elle permettra également de tirer les enseignements afin d'améliorer les procédures et les moyens techniques dans une vision prospective. Cette gestion décrira rigoureusement le plan d'action (que faire, qui alerter…) et prévoira une procédure d'escalade afin de traiter l'incident au bon niveau de responsabilité.

Mesure de sécurité techniques

Authentification des intervenants : contrôle d'accès logique

Couvre les aspects liés à la gestion de l'identification et l'authentification des utilisateurs du système. Ces catégories sont:

➔ **Gestion des comptes**: cette catégorie regroupe les différentes règles permettant d'identifier chaque utilisateur, compte et rôle associé afin de les maîtriser et limiter les privilèges associés à chacun d'eux en se donnant la possibilité de les contrôler via des audits par exemple. Une attention particulière étant portée sur les comptes à forts privilèges tels que les comptes d'administration.

➔ **La gestion de l'authentification**: cette section aborde les mécanismes inhérents à l'accès aux différents composants constituants le système (physique et logique) ainsi que la protection des secrets associés à ces mécanismes en appliquant une politique de sécurité liée aux mots de passe.

Sécurisation de l'architecture du système industriel

Aborde la structuration de l'architecture du système ainsi que la sécurisation des différentes interconnexions et échanges (communications, flux, protocoles) au sein du système lui-même et vers l'extérieur. Ce thème regroupe ainsi les catégories suivantes:

➔ **Cloisonnement des sous-systèmes techniques** : il s'agit de penser les architectures en zones cloisonnées selon les fonctions ou nécessités techniques du système. Par ailleurs il est nécessaire de prévoir les mécanismes de protection liés à ces cloisonnements (filtrage, segmentation physique ou logique le cas échéant…). Il est par ailleurs fortement recommandé que le réseau d'administration soit cloisonné des autres réseaux. Selon la sensibilité de certains systèmes il peut être demandé de maîtriser encore davantage le cloisonnement et les flux avec l'emploi d'équipements qualifiés ANSSI (emploi d'une diode labellisée par exemple).

➔ **Interconnexion avec le système d'information de gestion**: cette section reprend les éléments de la catégorie précédente en appliquant les mesures de protection (filtrage, gestion des flux…) au niveau de l'interconnexion avec le système d'information de gestion.

➔ **Accès Internet et interconnexions entre sites distants**: les interconnexions du système avec Internet ou à d'autres systèmes via Internet doivent être limitées et protégées via des mécanismes robustes voire qualifiés selon le niveau de sensibilité de l'installation.

➔ **Accès distants**: la télémaintenance/télégestion ne peut pas être déployée pour toutes les installations selon leur criticité/sensibilité. Et lorsque cela est possible les solutions mises en place devraient être labellisées et contrôlées (sonde de détection, journalisation…).

➔ **Systèmes industriels distribués** : concernant ces systèmes, ils se doivent d'utiliser des réseaux et protocoles protégés et maîtrisés, en s'appuyant sur des solutions sécurisées dédiées (passerelle VPN, sonde de détection…) en privilégiant des liaisons louées avec des ressources dédiées aux réseaux publics qui doivent être évités.

➔ **Communications sans fil**: l'usage de technologies sans fil doit être limité au strict nécessaire et les communications ainsi que les équipements doivent être cloisonnés au maximum, sécurisés et surveillés en fonction de la criticité du système. Il est indispensable de séparer physiquement et logiquement les réseaux WiFi publics des réseaux WiFi utilisés par les systèmes d'informations techniques.

➔ **Sécurité des protocoles**: lorsque c'est possible, les protocoles non sécurisés devraient être désactivés au profit des protocoles sécurisés. Sinon des mesures de protection périmétriques doivent être mises en place (Pare-feu, VPN…). Par exemple l'utilisation du protocole BACnet Secure Connect est préférable car il intègre des mécanismes d'authentification, chiffrement et contrôle d'identité.

Sécurisation des équipements

Cette section présente les aspects liés à la sécurisation des équipements utilisés au sein du système ainsi que la sécurisation de leur configuration et leur maintien dans le temps. Ces catégories sont les suivantes:

➔ **Durcissement des configurations**: il s'agit de désactiver tout ce qui n'est pas nécessaire au fonctionnement du système (comptes utilisateurs par défaut, ports physiques, services non indispensables, outils de débogage…) mais aussi de mettre en place les mécanismes permettant une sécurisation supplémentaire des accès comme la protection de l'accès au BIO, à la CPU au programme, la mise en place de liste blanche des applications autorisées à s'exécuter… Il faudrait par ailleurs pouvoir s'assurer que les logiciels, firmwares, programmes, fichiers de configuration… ne soient pas modifiés sans autorisation et soient contrôlés régulièrement.

➔ **Gestion des vulnérabilités**: ce processus s'inscrit dans une démarche globale et doit assurer la recherche de vulnérabilités en les identifiant selon leur impact sur le système et proposer les solutions correctives ou le cas échéant palliatives après validation et vérification de la non-régression du système avant leur déploiement.

➔ **Interfaces de connexion**: souvent les interfaces de connexion sont négligées car nous pensons le système isolé et non atteignable. Cependant il s'agit d'un vecteur important d'attaques. C'est pourquoi il est nécessaire de définir et mettre en place une politique de sécurité liée à: l'utilisation et la gestion des moyens amovibles et les bonnes pratiques associées à leur emploi (connexion uniquement entre les systèmes autorisés, désactivation des lancements automatiques…), le contrôle des points d'accès réseau, l'utilisation d'un sas de décontamination…

➔ **Équipements mobiles**: sur le même principe, dans le cas de l'utilisation d'équipements mobiles, leur emploi doit être maîtrisé, limité et dédié au système industriel. Et en cas de traitement de données sensibles ils doivent être sécurisés avec des mécanismes de chiffrement du stockage par exemple. Par ailleurs il est fortement recommandé que ces équipements soient résidents sur le site d'exploitation.

➔ **Sécurité des consoles de programmation**, des stations d'ingénierie et des postes d'administration: chaque équipement (programmation, ingénierie, postes d'administration) doit être réservé à leur fonction et ne pas être connecté à Internet. De plus ils doivent être installés dans des locaux maîtrisés et contrôlés et, être durcis au même titre que les autres équipements et suivre des règles d'utilisation clairement définies (mise hors tension lorsqu'ils ne sont pas utilisés, désinstallation des outils non nécessaires…).

➔ **Développement sécurisé**: dans le cadre d'une programmation, des règles de bonnes pratiques ainsi que des options ou fonctions avancées de sécurité liées à certains compilateurs doivent être appliquées. Par ailleurs il est fortement recommandé de procéder à des audits de code par un prestataire externe.

Surveillance du système industriel

Couvre la notion de traçabilité des événements sur le système industriel, au travers de la catégorie suivante:

➔ **Journaux d'événements**: afin d'assurer la traçabilité des événements sur le système, une politique de gestion doit être définie et mise en place comprenant: les événements pertinents à tracer, leur conservation (stockage, archivage), les conditions d'analyse, ainsi que les alertes à générer.
Par ailleurs des moyens de détection d'intrusion (type sonde) doivent être mis en place et selon la criticité/sensibilité du système ces mécanismes devront être labellisés.

ANNEXE 2

CAS DE PIRATAGE INDUSTRIELS, DE BÂTIMENTS ET LEURS CONSÉQUENCES

En 2000, un Australien pirate le système SCADA (Supervisory Control And Data Acquisition) de Hunter Watertech, une entreprise de traitement des eaux usées située dans le comté de Maroochy. À l'aide d'un équipement radio et d'un ordinateur, il provoque le déversement de 800 000 litres d'eaux usées brutes dans les parcs locaux, les rivières et le terrain d'un hôtel Hyatt Regency. L'attaque a un impact écologique d'ampleur : destruction de la vie marine à l'échelle locale et eau rendue impropre à la consommation pour les habitants.

Dans le même ordre d'idées, on retrouve Stuxnet, utilisé en 2010 contre une centrifugeuse du site d'enrichissement d'uranium de Natanz en Iran.

Un autre exemple éloquent est celui du malware Triton, dirigé contre un site pétrochimique d'Arabie Saoudite. Triton s'en prend au système de sécurité et au système numérique de contrôle-commande. L'attaque est stoppée à temps mais aurait pu entraîner la défaillance de l'ensemble du site industriel. Son ampleur et son retentissement médiatique permettront de réveiller les consciences des acteurs industriels internationaux.

Des exemples de ce type ont déjà eu lieu, notamment en 2016 en Ukraine où des hackers s'en sont pris au réseau électrique de la ville de Kiev. Un moment historique puisque si les cyberattaques étaient habituellement dirigées contre des entreprises, celle de ces hackers ciblait une infrastructure publique. Résultat : 1,4 millions d'habitants subirent un black-out total de plusieurs heures.

Août 2012 : Fermeture du réseau de la Saudi Aramco. L'ancien secrétaire d'État à la Défense (USA) Leon Panetta avait, de fait, déclaré que « l'attaque de 2012 [avait] été la plus destructrice de l'histoire de l'Internet », *Le point*. Le site de Jubail (Al Jubayl) est pourtant un site ultra sécurisé et l'un des plus importants au monde. Il s'agissait d'une nouvelle version du virus Shamoon. Cette action a été revendiquée par un groupe hacktiviste.

En décembre 2013, la chaîne de magasins Target a ainsi été victime d'une cyberattaque massive sur ses serveurs, conduisant à la subtilisation de 40 millions de numéros de cartes bancaires et de 70 millions d'adresses mails, coordonnées postales et numéros de téléphones de clients. L'élément marquant dans cette attaque est qu'elle a été organisée à partir du vol des identifiants d'un prestataire, qui gérait les systèmes de ventilation et de climatisation du groupe Target.

En 2008, le département informatique de San Francisco en a ainsi fait les frais, (note de la rédaction : absence de PAM). Un ingénieur du nom de Terry Childs a créé et exploité un réseau FiberWAN, crucial pour de nombreux services en ligne. Il a alors consolidé le contrôle de tous les mots de passe des administrateurs systèmes ; ce qui est *a priori* une bonne idée. Seulement, suite à un différend avec l'organisation, il a pris le contrôle total du réseau, et n'a pas voulu partager les identifiants des comptes à privilèges utilisés. Résultat ? L'infrastructure IT de San Francisco s'est arrêtée. Les employés peuvent par conséquent compromettre les comptes à privilèges pour de nombreuses raisons. Edward Snowden en est l'exemple même, *Zdnet*.

2007, Willows, États-Unis, système de dérivation de l'eau : l'attaquant a exploité une vulnérabilité relative au contrôle des droits d'accès des salariés. Un employé licencié a endommagé un système de surveillance de la dérivation d'eau. Conséquence : le système de surveillance a été hors service occasionnant 5 000 dollars de dégâts.

2013, Géorgie, États-Unis, intoxication par l'eau : il s'agit d'une vulnérabilité liée au manque de surveillance des locaux. Il est possible d'accéder au système d'eau sans aucune alerte. Des intrus ont franchi les clôtures et modifié les réglages des niveaux de fluor et de chlore. Résultat : 400 habitants privés d'eau potable.

Attaque physique contre le Capitole à Washington en 2020 et vol de données.

À PROPOS DE LA SBA

Créée en 2012, la Smart Buildings Alliance œuvre chaque jour à faire du Smart Buiilding un atout au service des territoires, des entreprises et des occupants.

Unique en son genre par sa transversalité, son ouverture et la diversité des 450 entreprises et organisations membres qui la compose, la SBA structure ses actions autour de trois piliers: Smart Home (logement résidentiel collectif), Smart Building (bâtiment tertiaire) et Smart City (ville et territoire intelligents).

Revendiquant depuis plus de 10 ans un attachement fort pour un numérique responsable, la SBA prône la neutralité technologique tout en promouvant l'interopérabilité des systèmes, la mutualisation des équipements et des infrastructures, l'ouverture, la disponibilité, la qualité, la sécurité et la gouvernance des données.

Avec plus de trente commissions et groupes de travail, elle fédère l'ensemble des corps de métiers dans une démarche collaborative de construction de cadres de références, d'approches et de solutions innovantes.

La Smart Buildings Alliance est à l'origine du cadre de référence R2S (Ready 2 Service) et de ses déclinaisons (R2S Résidentiel, R2S 4Care, R2S Connect, R2S 4Grids, R2S 4Mobility...), ainsi que du référentiel BIM for Value.

L'alliance s'appuie sur des chapitres régionaux présents au plus près des territoires et rayonne également à l'international avec des SBA pays.

SMART HOME

SMART BUILDING

SMART CITY

DEVENEZ **MEMBRE**
DE LA SBA AU CÔTÉ DES
ACTEURS RÉFÉRENTS
DU SMART **BUILDING**,
DU SMART **HOME**
ET LA SMART **CITY**

Scannez ce QR Code pour plus d'informations sur l'adhésion à la SBA.

LES ACTIONS DE LA SBA

- **RENCONTRES**
  - ▸ Fédérer la filière dans un esprit de transversalité
  Événements SBA pour le partage d'expérience et la veille autour des thématiques du bâtiment intelligent dans la ville et le territoire durables.
- **PUBLICATIONS**
  - ▸ Partager notre vision et nos recommandations
  Cadres de référence (R2S, R2S 4Mobility, R2S Résidentiel, R2S Connect, BIM4Value...), Thémas et livres blancs, baromètres, webinars.
- **COMMISSIONS**
  - ▸ Réflexions sur l'évolution du bâtiment dans la ville intelligente
  Plus de 30 commissions spécifiques actives grâce à nos 450 membres.
- **RELATIONS INSTITUTIONNELLES**
  - ▸ Sensibiliser les décideurs publics
  Ministères, institutions publiques, collectivités locales, syndicats professionnels...
- **COOPÉRATION INTERNATIONALE**
  - ▸ Rayonner au-delà des frontières
  Échanges avec les organisations internationales. Ainsi qu'une présence nationale, régionale et européenne.

UNE QUESTION ? UN PROJET ?
CONTACTEZ-NOUS...

par mail : contact@ smartbuildingsalliance.org

par téléphone : 0820 712 720

www.smartbuildingsalliance.org

www.linkedin.com

twitter.com

youtube.com

LES MEMBRES

ABB • ACCENTA • ACOME • ACR • ACS2I • ACTIVUS GROUP • AD VANTAGE • AD-STOA • ADEUNIS RF • ADVIZEO BY SETEC • AESTRIA • AFPA - TOULOUSE • AIRELIOR FACILITY MANAGEMENT • AIRTHINGS • AIRZONE FRANCE SARL • ALCANTE • ALCATEL LUCENT ENTERPRISE • ALLIANCE DU BÂTIMENT • ALLIANZ REAL ESTATE • ALPHA RLH • ALTAREA COGEDIM • ALTERNET • AN2V • ANITEC • APILOG AUTOMATION • ARC INFORMATIQUE • ARISTOTE • ARP ASTRANCE • ARTELIA • ARUBA • ASCAUDIT ÉNERGIES & FLUIDES • ASSOCIATION BACNET FRANCE • ASSOCIATION FRANÇAISE DE L'ÉCLAIRAGE • ASSOCIATION HQE • ASSOCIATION PROJET LORIAS • ASSUR & SENS • AURA DIGITAL SOLAIRE • AUTOMATIQUE ET INDUSTRIE • AV USER CLUB • AVELIS GROUP • AVELTYS • AVIDSEN • AXIANS • AZUR SOFT • B ECO MANAGER • B27 • B2AI • BARBANEL • BCC • BIMSY • BIRDZ • BNP PARIBAS REAL ESTATE • BOUYGUES CONSTRUCTION • BOUYGUES ENERGIES & SERVICES • BOUYGUES IMMOBILIER • BUREAU VERITAS CERTIFICATION • C2S BOUYGUES • CABA • CAILLOU VERT CONSEIL • CAISSE DES DÉPÔTS • CAPENERGIES • CBRE • CCI NICE CÔTE D'AZUR • CCUBE EXPERTISE • CD2E • CDC HABITAT • CERTIVEA • CINOV • CIT RED • CNAM • CNOA • CNPP • CODRA • CONNECTING TECHNOLOGY • CONNEK+ CONSEIL • CONSEIL DE DÉVELOPPEMENT MÉTROPOLE DE LYON • CONTINENTAL AUTOMOTIVE • COVIVIO • CR SYSTEM • CRESTRON EUROPE BV • CSTB • CYBERREADY • CYRISEA • DATA SOLUCE • DECAYEUX • DECELECT • DEERNS FRANCE • DELTA DORE • DEMATHIEU & BARD • DESKAPAD • DIS INGÉNIERIE • DISTECH CONTROLS • DOMOCORE • DOVOP DÉVELOPPEMENT • DREES & SOMMER • DRYAS • DTO SOLUTIONS • E-T-A • E'NERGYS • ECM RENOVBAT • ÉCOLE DE MANAGEMENT DE NORMANDIE • ECONOMIE D'ENERGIE • EFFICACITY • EFICIA • EFUTURA • EGF BTP • EGIS CONSEIL BÂTIMENTS • EIFFAGE ÉNERGIE • EMBIX • EN ACT ARCHITECTURE • ENERBEE • ENERGIE IP • ENERGISME • ENGIE SOLUTIONS • ENJOY • ENLESS WIRELESS • ENSI POITIERS • EQUANS • EY • EURECAM • EVOLIS • EXEO INGÉNIERIE • F2A SYSTÈMES • FACILITY DATA STANDARD • FARE PROPRETÉ • FEDENE • FÉDÉRATION DES ASCENSEURS • FEI • FEILO SYLVANIA • FFIE • FLOW • FORMAPELEC • G-ACTIV • GA SMART BUILDING • GA2B • GECINA • GETEO • GIMELEC • GPMSE-TN • GRIOT CONSEIL • GROUPE PROJEX • GROUPE QUALITEL • GROUPE SNEF • GROUPE TRACE • HABITAT76 • HAGER • HEINRICH ECLAIRAGE SAS • HELINK • HELVAR • HENT CONSULTING • HERVE THERMIQUE • HID GLOBAL • HOPPE FRANCE • HSBC • HUAWEI TECHNOLOGIES • HUB TEN • HXPERIENCE • HYDRAO • HYDRELIS • HYVILO • I-PORTA • ICADE • ICONICS • IDEX • IDTIQUE • IGNES • IKO REAL ESTATE • IMA PROTECT • IMMOBILIÈRE 3F • INGÉROP CONSEIL ET INDUSTRIE • INNES • INNESSENS - SCGI • INNOVATION PLASTURGIE COMPOSITES • INOVAYA • INSTALLUX • ISTA • J2 INNOVATIONS • JEEDOM • JIP CORPORATION • JOOXTER • KALIMA DB • KARDHAM DIGITAL • KIPSUM • KNX • KORUS • L'IMMOBILIÈRE IDF • LAKOUDIGITAL • LANCELOT CONSULTING • LD EXPERTISE • LE RÉSIDENTIEL NUMÉRIQUE • LEGRAND • LES COMPAGNONS DU DEVOIR • LEXCITY AVOCATS • LINKIO • LM INGENIERIE • LONMARK FRANCE • LUCIBEL • LUTRON ELECTRONICS • MAGMA • MBACITY • MEANWHILE • MEDIACONSTRUCT • MICROSENS • MOBILITY PLUS • MOBOTIX • MOVEWORK • MTCE CONSULTING • MUSEUM NATIONAL D'HISTOIRE NATURELLE • NAITWAYS • NCI • NET DISPLAY SYSTEM • NEODOMUS SOLUTIONS • NET AND YOU • NETSEENERGY • NEXITY • NOBATEK • NODON • NOVABUILD • NT CONSEIL • OCCITALINE • OKKOS • ONEPOINT • OPNA • ORANGE • ORIZON GROUP • ORLÉANS MÉTROPOLE • OVERKIZ • PALAMEDE TECHNIC EUROPE • PATRIARCHE UX • PBRAMAUD CONSEIL • PLAN BÂTIMENT DURABLE • PÔLE FIBRES - ENERGIVIE • PÔLE TES • POLESTAR • PRESTANTENNES • PRESTATERRE • PROLOGIS • PROTECT FRANCE • PULS • QWANDA • QWANZA • RABOT DUTILLEUL • RÉSEAU DEF • RÉSEAU DUCRETET • RESO • REUSITH • REXEL • ROBEAU • RT FLASH • S2E2 • S2T INGENIERIE • SAFE CLUSTER • SAINT-GOBAIN • SALTO SYSTEMS • SAMEA INNOVATION • SAS KINTSUGI-LOWCARBON (SETUR) • SATO ET ASSOCIÉS • SAUTER RÉGULATION • SBI CONSULTING • SCHNEIDER ELECTRIC • SE3M • SEDEA/HESTIA • SELUO • SERCE • SERELEC • SETEC BÂTIMENT • SIA PARTNERS • SIBCO • SIEA • SIEL 42- TERRITOIRE D ENERGIE LOIRE • SIEMENS ENERGY • SIG - SERVICES INDUSTRIELS DE GENÈVE • SIGNIFY • SIMONS VOSS TECHNOLOGIES • SLAT • SMALT • SMART BLUEDING • SMART HOME • SMART WORLD PARTNERS • SMARTHOME EUROPE • SMO VAL DE LOIRE NUMÉRIQUE • SOCOMEC • SOGEPROM • SOGETREL • SOMFY • SPAC • SPIE • SPINALCOM • SPL LYON CONFLUENCE • SQUARE SENSE • STID • SUPPLINNOV • SYLFEN • SYNOX • SYNTEC INGÉNIERIE • SYPEMI • SYS & COM • SYSTEMATIC PARIS-RÉGION • TACTIS • TECH FOR BUILDINGS • TECHNAL • TECHNILOG • TECXTEAM • TELEVES CORPORATION • TENNERDIS • TK ELEVATOR • TPF LUXEMBOURG • TRIGRR • TWYNSIS • UBIANT • ULIS • UNIVERS FIBRE • UNIVERSITÉ DE RENNES 1 • URBAN PRACTICES • URMET FRANCE • USGC • USING CITY • VAYANDATA • VELTYS • VERSPIEREN • VILOGIA • VINCI ÉNERGIES • WAGO • WAVESTONE • WEBDYN • WISE BUILDING • WIT • WITCO • WITTI • WIXALIA • WSP • XICATO • Z#BRE

LES MEMBRES **D'HONNEUR DE LA SBA**

SMART BUILDINGS ALLIANCE FOR SMART CITIES

www.smartbuildingsalliance.org