La sécurité informatique dans le domaine de l'automatisation de bâtiments

Livre blanc version 1.0

Franklin Linder

14/11/2014

SAUTER
Für Lebensräume mit Zukunft.

Résumé

Le thème de la **sécurité informatique dans l'automatisation de bâtiments** a considérablement gagné en importance ces dernières années. Cela s'explique par le développement des **technologies** utilisées. En effet, ces dernières ainsi que les technologies employées dans l'automatisation industrielle se sont de plus en plus alignées sur les **technologies informatiques** en général. Les appareils sont devenus des micro-ordinateurs dotés d'un système d'exploitation. L'utilisation du **standard IP** s'est généralisée pour la communication et **Internet** est employé dans la communication à distance. L**'ouverture et la standardisation**, établies dans le but de pouvoir utiliser des systèmes hétérogènes dans l'automatisation de bâtiments, ont encore augmenté la vulnérabilité de ceux-ci.

Contrairement aux infrastructures informatiques en général, la menace concerne cependant plus que de « simples » données dans le cas de l'automatisation de bâtiments. Du fait de la connexion du système de GTB aux installations techniques du bâtiment (ventilation, éclairage, portes, systèmes d'accès), les attaques peuvent avoir des **conséquences graves sur la sécurité-même du bâtiment**.

Le risque effectif encouru par les bâtiments est **spécifique à chaque projet** et dépend fortement de la **sensibilité** du système d'automatisation et du degré de dépendance du bâtiment vis-à-vis de ce dernier.

En principe, deux types de mesures peuvent être prises pour protéger un système de GTB : protection des **appareils/PC/logiciels** et/ou protection de l'infrastructure informatique, c'est-à-dire **des réseaux et des différents accès aux réseaux**.

L'application de mesures de protection des **appareils/PC/logiciels** commence déjà chez le **fabricant**. Les mesures de protection de l'**infrastructure informatique** et la mise en place de celles pour les **appareils/PC/logiciels** sont du ressort du fabricant de l'installation, bien que **les donneurs d'ordres, maîtres d'ouvrage et bureaux d'étude** posent à la base les exigences fonctionnelles et le cadre budgétaire (appels d'offres et listes de prestations).

Les travaux relatifs à la sécurité informatique d'une installation s'étendent tout au long du cycle de vie de cette dernière, de la fabrication des composants jusqu'à l'exploitation et la maintenance en passant par l'étude de projet et la mise en service. **Le déploiement de normes de sécurité adéquates demande la participation active de toutes les instances impliquées.** Les dispositifs de sécurité mis en place doivent être à la mesure des risques potentiels. Il est indispensable de réaliser au préalable une **analyse des risques**.

Ce livre blanc « **La sécurité informatique dans le domaine de l'automatisation de bâtiments** » décrit en détails les mesures de protection possibles. Dans les graphiques, vous trouverez des informations supplémentaires concernant les différentes menaces potentielles.

Le présent livre blanc traite exclusivement des **normes de sécurité informatique à appliquer contre toute attaque/intervention indésirable provenant de l'extérieur**. Les aspects « **disponibilité des systèmes informatiques** » et « **sécurité technique des installations CVC** » sont uniquement abordés sous l'angle de la minimisation des dommages en cas de panne de la commande.

Introduction/généralités

Ce livre blanc relatif à la **sécurité informatique dans le domaine de l'automatisation de bâtiments** traite exclusivement des **mesures de sécurité informatique protégeant contre toute attaque/intervention indésirable provenant de l'extérieur**. La **disponibilité des systèmes informatiques** (« sûrs » à comprendre par « ne tombe jamais en panne, ne plante jamais, redondance », etc.), qui est souvent perçue comme faisant partie intégrante de ce sujet, ne sera pas abordée ici. Le thème de la **sécurité de l'installation CVC** (alimentation de secours, verrouillage matériel, exécution redondante de certaines fonctions, etc.) n'est abordé que sous l'angle d'une minimisation des dommages en cas de panne de la commande.

L'intérêt croissant pour le thème de la **sécurité informatique dans le domaine de l'automatisation de bâtiments** s'explique par le développement technologique de ces dernières années. L'intelligence dont sont dotées les techniques d'automatisation atteint depuis un certain temps des niveaux de plus en plus intégrés. Les automates programmables et unités de gestion locale sont devenus depuis longtemps des **micro-ordinateurs avec système d'exploitation intégré** spécifiques à un secteur. En conséquence de cela, les **technologies informatiques générales** existantes ont été en grande partie adoptées pour la communication. En ce qui concerne les appareils autonomes, la tendance penche également vers toujours plus d'intelligence intégrée et de technologies de communication haut de gamme.

Dans l'automatisation de bâtiments, l'évolution des 10 à 15 dernières années a été en outre marquée par **la standardisation et l'ouverture**. L'intégrabilité des systèmes est devenue un argument de vente majeur pour différents fabricants. Alors que les systèmes étaient auparavant conçus différemment selon les fabricants et ne pouvaient donc communiquer que difficilement les uns avec les autres, de nouveaux **standards** ont été définis dans les années 2000 en ce qui concerne **les réseaux, les protocoles et les bâtiments**, ce qui a entraîné une ouverture des systèmes.

Comme des standards informatiques généraux ont été utilisés pour communiquer, l'**intégration** des systèmes d'automatisation de bâtiments est devenue possible dans les structures actuelles de la branche **Business IT**. L'utilisation d'**Internet** pour la communication à distance s'est imposée, ce qui a ouvert à l'automatisation de bâtiments des **possibilités de communication presque illimitées**.

Toutes ces modernisations ont apporté aux clients et exploitants de l'automatisation de bâtiments une valeur ajoutée considérable : **fonctionnalités** optimisées, **possibilités de communication** presque infinies et **liberté de choix** totale pour les nouveaux projets et les extensions de projets existants.

Ces développements, en soi réjouissants, ont cependant augmenté proportionnellement la vulnérabilité de l'automatisation de bâtiments. Cette dernière a atteint le niveau de vulnérabilité des infrastructures informatiques générales.

Du fait de la connexion des systèmes d'automatisation de bâtiments aux installations techniques du bâtiment (installations CVC, éclairage, contrôles d'accès, portes coupe-feu, etc.), les **conséquences de cette vulnérabilité ont une plus grande portée** que dans le cas des infrastructures informatiques générales. Ce ne sont plus uniquement les « simples » données qui peuvent être manipulées ou modifiées. Toute intrusion illicite peut avoir un impact

sur la **sécurité des équipements techniques du bâtiment**. Les conséquences d'une attaque criminelle peuvent être lourdes.

Le degré de vulnérabilité d'un bâtiment varie fortement en fonction du **type et de l'utilisation de ce dernier**. Tous les bâtiments ne présentent pas le même intérêt pour les criminels et n'auront pas la même sensibilité aux suites de l'attaque.

Les risques sont minimisés si « seuls » les équipements CVC (chauffage, ventilation et climatisation) sont raccordés sans **l'éclairage, les contrôles d'accès, les commandes de portes**, etc. Le risque n'est évidemment pas le même qu'il s'agisse d'un petit bâtiment privé ou d'un bâtiment central, fortement fréquenté ou **à risque particulièrement élevé pour la sécurité** (aéroports, gares, etc.). Les **menaces** auxquelles ces bâtiments sont exposés peuvent, dans les cas extrêmes, dégénérer en actes de violence ou attentats terroristes par piratage informatique.

Les dispositifs de sécurité mis en place doivent être à la mesure des risques potentiels. Il est dans tous les cas indispensable d'effectuer au préalable une analyse des risques spécifique au projet.

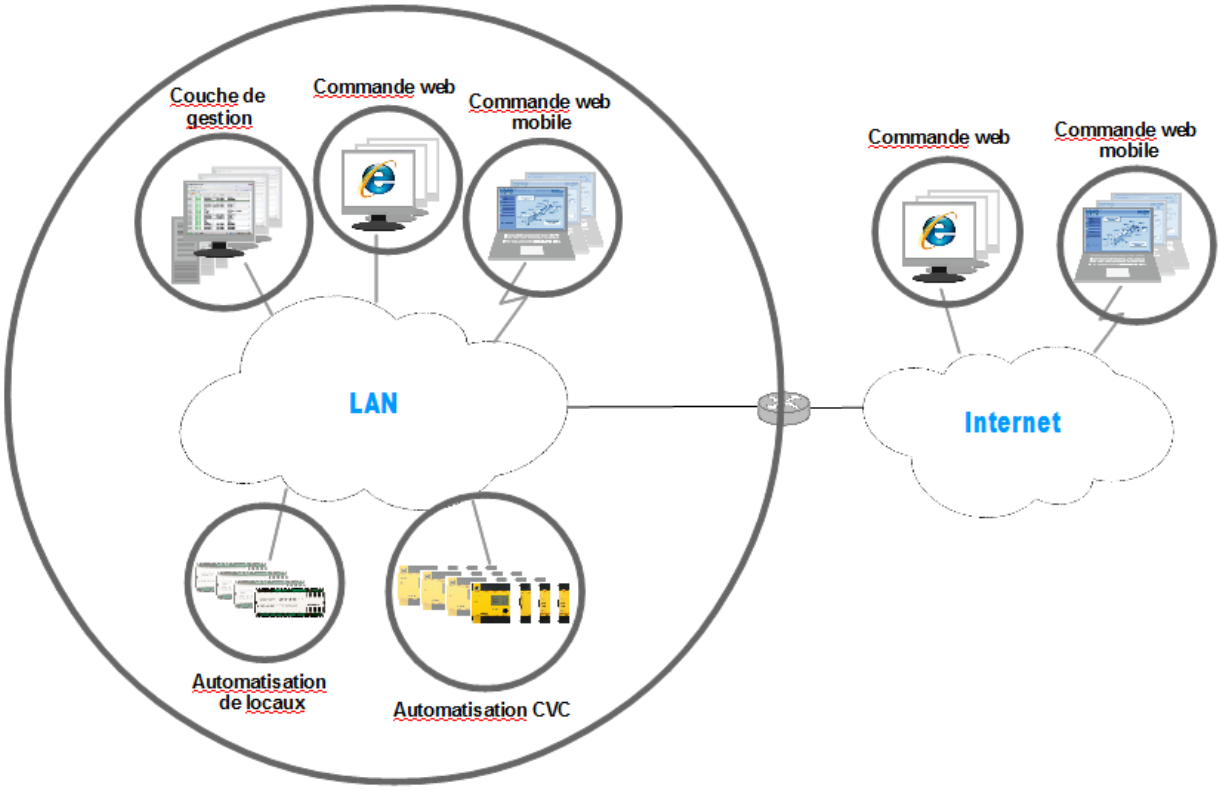
Des mesures de base indispensables doivent être prises dans toutes les installations. Un renforcement de la sécurité passe cependant toujours par des mesures coûteuses et laborieuses. Une sécurité totale et absolue dans le domaine de l'automatisation de bâtiments est, même avec ces mesures, impossible à garantir complètement.

Les éléments constitutifs de la sécurité informatique dans l'automatisation de bâtiments

La sécurité d'une automatisation de bâtiments basée sur les réseaux peut être améliorée par des **mesures de protection réparties sur deux niveaux principaux** :

De la même manière que les habitants d'une ville médiévale pouvaient être protégés par la porte de leur maison et/ou par les portes de la ville, les mesures de protection des systèmes d'automatisation de bâtiments peuvent être prises **au niveau des appareils (unités de gestion locale, PC, etc.)** et/ou **au niveau des accès aux réseaux concernés**. Comme autrefois où il s'agissait de ne pas laisser entrer le danger dans la ville et pour cela de fortifier les portes de la ville, il est **crucial** dans les systèmes d'automatisation de bâtiments de renforcer **en premier lieu la protection des accès aux réseaux**. Tout comme les portes et murs d'enceinte de la ville ne peuvent jamais être entièrement infranchissables et que des sujets dangereux peuvent également venir de l'intérieur de la ville, il est indispensable de protéger séparément les différents appareils impliqués dans l'automatisation de bâtiments.

Il n'est possible d'atteindre un résultat satisfaisant qu'en combinant des mesures à ces deux niveaux.



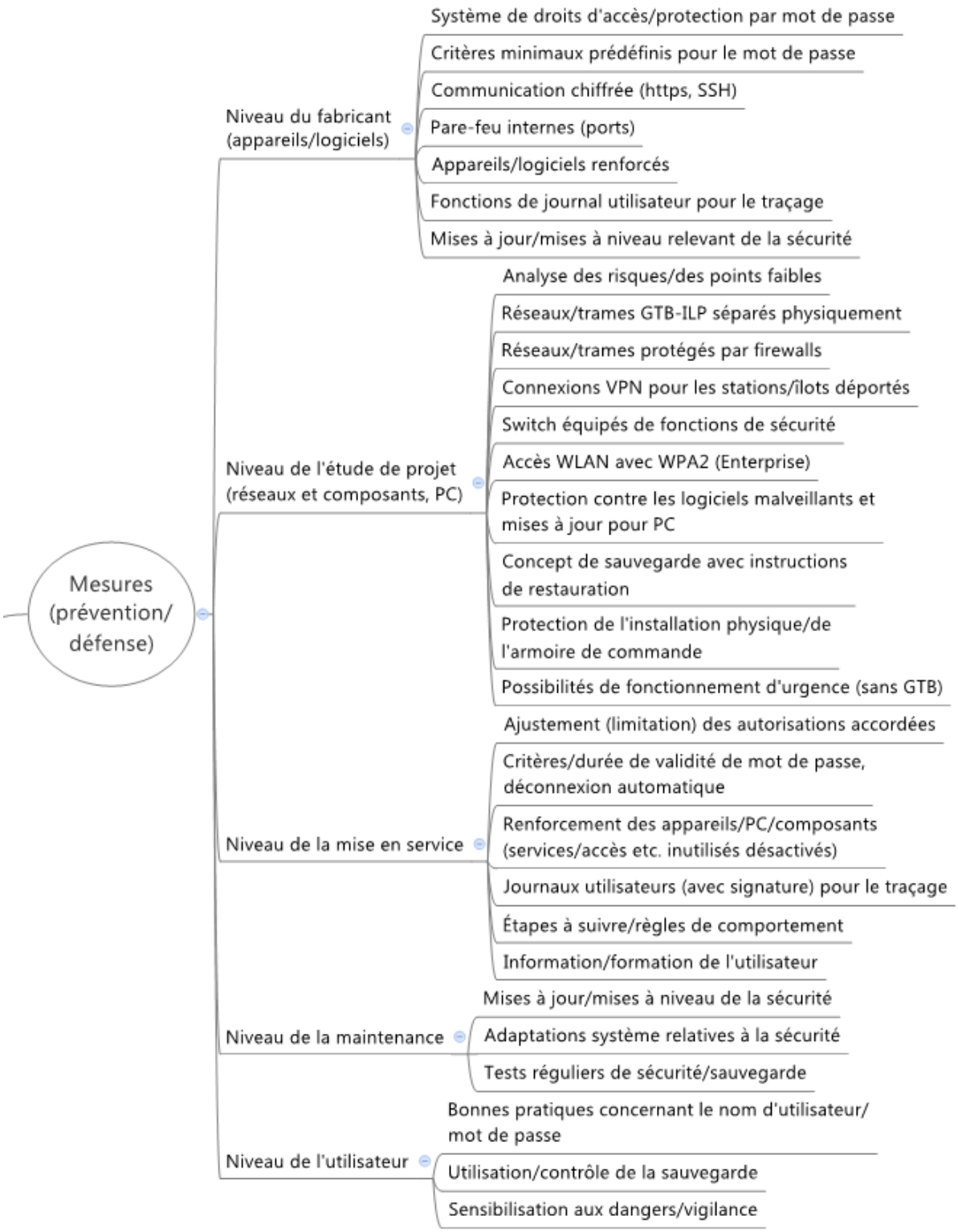
Dans le cycle de vie d'une installation d'automatisation de bâtiments, les **mesures prises au niveau des appareils/logiciels** doivent être initiées chez le **fabricant des produits**. Il intègre d'usine les mesures de sécurité les plus complètes possibles à ses produits. Cela peut inclure par exemple un système de droits d'accès avec mot de passe, la prise en charge de la communication cryptée, des pare-feu internes, etc.

Ces mesures de protection préinstallées **sur les appareils/logiciels** doivent être ensuite complétées et paramétrées lors de la **mise en place et mise en service de l'installation**. Le système de droits d'accès doit être installé, les utilisateurs par défaut supprimés, les appareils éventuellement « post-durcis ». Les PC achetés séparément doivent être équipés à ce moment-là d'une protection contre les logiciels malveillants (programme antivirus) et être « post-durcis » dans la mesure du possible.

Le fabricant du système d'automatisation de bâtiments a alors peu d'influence ou une influence seulement indirecte sur les **actions mises en œuvre au niveau de l'infrastructure informatique**, c'est-à-dire **au niveau des réseaux/trames de réseaux et de leurs accès**. Celles-ci sont prévues et réalisées par le **fabricant de l'installation d'automatisation de bâtiments** (en coopération avec le responsable IT du client/de l'exploitant du bâtiment/du maître d'ouvrage). Il détermine si l'exploitation de l'installation d'automatisation de bâtiments ou au moins de la couche d'automatisation s'effectue sur un réseau dédié, si l'utilisation d'une connexion Internet pour la communication à distance est requise, comment le réseau est segmenté, quelles mesures de sécurité sont employées (pare-feu, connexions VPN, etc.) pour les points d'accès et comment les Wi-Fi éventuels peuvent être sécurisés. Les **maîtres d'ouvrage et bureaux d'étude** fixent les exigences fonctionnelles et le cadre budgétaire.

Les travaux de sécurité informatique s'étendent tout au long du cycle de vie d'une installation. Ils commencent comme décrit plus haut chez le fabricant des appareils et des programmes utilisés et sont complétés lors de l'étude de projets, la réalisation et la mise en service de l'installation. Cependant, même pendant la phase d'exploitation, une sécurité informatique durable exige des efforts soutenus de la part des techniciens de maintenance ainsi que des exploitants/utilisateurs.

Le respect des normes de sécurité en vigueur a pour condition préalable la coopération active de toutes les instances impliquées.


Mesures (prévention/ défense)
Niveau du fabricant (appareils/logiciels)
Système de droits d'accès/protection par mot de passe
Critères minimaux prédéfinis pour le mot de passe
Communication chiffrée (https, SSH)
Pare-feu internes (ports)
Appareils/logiciels renforcés
Fonctions de journal utilisateur pour le traçage
Mises à jour/mises à niveau relevant de la sécurité
Niveau de l'étude de projet (réseaux et composants, PC)
Analyse des risques/des points faibles
Réseaux/trames GTB-ILP séparés physiquement
Réseaux/trames protégés par firewalls
Connexions VPN pour les stations/îlots déportés
Switch équipés de fonctions de sécurité
Accès WLAN avec WPA2 (Enterprise)
Protection contre les logiciels malveillants et mises à jour pour PC
Concept de sauvegarde avec instructions de restauration
Protection de l'installation physique/de l'armoire de commande
Possibilités de fonctionnement d'urgence (sans GTB)
Niveau de la mise en service
Ajustement (limitation) des autorisations accordées
Critères/durée de validité de mot de passe, déconnexion automatique
Renforcement des appareils/PC/composants (services/accès etc. inutilisés désactivés)
Journaux utilisateurs (avec signature) pour le traçage
Étapes à suivre/règles de comportement
Information/formation de l'utilisateur
Niveau de la maintenance
Mises à jour/mises à niveau de la sécurité
Adaptations système relatives à la sécurité
Tests réguliers de sécurité/sauvegarde
Niveau de l'utilisateur
Bonnes pratiques concernant le nom d'utilisateur/ mot de passe
Utilisation/contrôle de la sauvegarde
Sensibilisation aux dangers/vigilance

Éléments au niveau du fabricant

Cela concerne les **appareils dotés d'un système d'exploitation intégré** (ASn, appareils de réseau et, éventuellement, capteurs intelligents) ainsi que les **logiciels de la couche de gestion** (logiciel SCADA, logiciel d'analyse de la consommation énergétique et logiciel de gestion énergétique). Les outils logiciels d'étude de projet sont moins concernés car ils ne peuvent être généralement utilisés que pendant un temps restreint et sous la surveillance étroite du fabricant du système de GTB et du constructeur de l'installation.

Système de droits d'accès/protection par mot de passe

Tous les appareils et produits logiciels disposant d'accès utilisateur (serveur web, accès de configuration, etc.) doivent bien évidemment être équipés d'un **système de droits d'accès** configurable avec **mot de passe**.

Les **interfaces de données** qu'utilisent les appareils/produits logiciels pour la communication avec leurs sources de données doivent également être protégées de toute intrusion par un moyen d'authentification approprié. Cela concerne par exemple les sources des données des logiciels d'analyse de la consommation énergétique et logiciels de gestion énergétique.

La sécurité peut en outre être fortement renforcée lorsque la protection par mot de passe est dotée de fonctions supplémentaires, comme l'évaluation de la **complexité du mot de passe**, une **déconnexion automatique** en cas d'inactivité, un **blocage temporaire** après un certain nombre de tentatives d'entrée de mot de passe ou une **durée de validité du mot de passe**.

Critères minimaux prédéfinis pour le mot de passe

La **complexité du mot de passe**, la **déconnexion automatique**, le **blocage temporaire** et la **durée de validité du mot de passe** sont des éléments importants contribuant à une bonne protection.

Le **fabricant** doit mettre à disposition de telles fonctionnalités dans ses produits afin qu'elles puissent être fixées selon le niveau de sécurité de l'installation dès la mise en service. Si le fabricant programme de manière définitive les **critères minimaux** dans ses produits et que ceux-ci ne peuvent plus être adaptés ultérieurement au niveau de sécurité exigé par l'installation, cela signifie en général qu'ils ont été réglés sur un niveau trop élevé.

Il est cependant judicieux d'intégrer d'usine une option, voire mieux une obligation de modification de l'**utilisateur Admin et de son mot de passe standard** après la mise en service, c'est-à-dire après une certaine période de fonctionnement ou selon un critère prédéfini. Beaucoup de grands cas de piratage médiatiques se basent justement sur cette faille. Le **mot de passe standard** n'a bien souvent pas été modifié après la mise en service et a été facile à trouver parmi les listes des mots de passe de différents fabricants qui se trouvent sur Internet.

Communication cryptée (https, SSH)

Pour une bonne sécurisation de la communication, les produits doivent être en mesure d'utiliser une **communication sécurisée ssl/TLS** (**https, SSH**) pour leur serveur web et leurs interfaces de configuration. Outre le cryptage de la communication, elle permet aussi une authentification fiable des participants. Cette authentification passe par des certificats si on a recours à une Infrastructure de Gestion de Clés (Public Key Infrastructure - PKI).

Pare-feu internes (ports)

Tous les appareils compatibles réseau d'un système (en général avec le système d'exploitation Linux) doivent être sécurisés à l'aide d'un **pare-feu installé et préconfiguré d'usine**. Tous les ports qui ne sont pas utilisés pour une exploitation normale sont alors inaccessibles. Dans les produits logiciels, les ports non utilisés/non requis à la livraison, c'est-à-dire après une installation standard, doivent également être rendus inaccessibles. Pour une adaptation optimale au concept de sécurité de l'infrastructure, les numéros de port utilisés doivent rester librement configurables pour les différents services.

Appareils/logiciels « durcis »

Tous les appareils et produits logiciels concernés doivent être livrés « pré-durcis » d'usine. Cela signifie que tous les **services et accès** non requis ne doivent **pas être installés** ou doivent être désactivés d'usine. Les fonctionnalités informatiques standard comme Telnet (port 23) ou FTP (port 20) représentent pour les pirates des possibilités supplémentaires bien connues pour s'introduire dans les systèmes matériels d'automatisation de bâtiments.

Fonctions journal utilisateur (avec signature)

Pour analyser ultérieurement une vraie attaque ou même une attaque présumée (erreurs de manipulation, jeux), tous les systèmes doivent prendre en charge dans la mesure du possible les **fonctions journal utilisateur** (enregistrement des **activités de l'utilisateur**). Celles-ci aident non seulement à identifier l'agresseur/le responsable mais aussi à savoir où sont localisés les dommages et conséquences éventuels ainsi que ce qui doit être corrigé.

Pour un traçage précis des attaques graves, ces enregistrements doivent être **sécurisés à l'aide d'une signature** de sorte qu'ils ne puissent pas être modifiés intentionnellement par un agresseur rusé ou involontairement par un intervenant distrait.

Mises à jour/mises à niveau relevant de la sécurité

Comme toute technologie informatique, les techniques d'agression sur les installations informatiques se développent en permanence et très rapidement. Tous les produits concernés doivent par conséquent faire l'objet d'un entretien et d'une mise à jour périodiques. Le fabricant de produits d'automatisation de bâtiments doit effectuer des mises à jour/mises à niveau relevant de la sécurité de ses produits et mettre à disposition les canaux de distribution correspondants.

Éléments au niveau de l'étude de projet

Au cours de l'étude de projet de l'automatisation de bâtiments, **l'infrastructure informatique** et ses **éléments de sécurité** (entre autres) sont fixés. Il s'agit notamment de définir la **topologie** (des réseaux et trames de réseau), de fixer les **mesures de protection au niveau des points d'accès** et de déterminer les **programmes de sécurité qui doivent être installés sur l'ordinateur de la couche de gestion**.

Sans oublier que des mesures servant à éliminer les défauts résultant d'attaques informatiques doivent être planifiées à ce moment-là.

Le concours des **maîtres d'ouvrage et des bureaux d'étude** est décisif au cours de cette phase. C'est en fixant les **exigences techniques** et le **cadre budgétaire** dans leurs **appels d'offre et listes de prestations** qu'ils permettent d'établir les mesures de sécurité à prendre.

Analyse des risques/des points faibles

Une **analyse des risques** constitue la base de la conception d'éléments de protection adaptés. Comme le risque n'est pas le même pour tous les bâtiments, ni pour tous les systèmes d'automatisation de bâtiments, il est indispensable de procéder à une **analyse des risques spécifique au projet**. Elle détermine l'étendue des **mesures de sécurité** à mettre en place. Les facteurs à prendre en compte sont également le degré de sensibilité du bâtiment et les fonctions d'automatisation de bâtiments utilisées (CVC, éclairage, portes (coupe-feu), systèmes d'accès...).

Réseaux GTB/IP séparés physiquement/segmentation

Comme les systèmes de GTB modernes utilisent le standard IP (OSI, couche 3) comme base pour presque toute leur communication, il paraît naturellement attrayant de pouvoir utiliser également **l'infrastructure réseau IP d'un bâtiment souvent déjà existante**, solution économique en termes de coûts. Cependant, notons que ceci ne constitue **pas la meilleure option** en termes de sécurité pour le système d'automatisation de bâtiments. Indépendamment des questions de performance et de disponibilité éventuelles, la protection des réseaux ne peut pas s'adapter de manière optimale à l'automatisation de bâtiments. En effet, les contraintes posées par d'autres applications doivent être prises en compte. De plus, une utilisation commune de l'infrastructure réseau permet à **beaucoup d'utilisateurs** de pénétrer directement dans le réseau d'automatisation de bâtiments **à travers des accès supplémentaires** (porteurs de risques supplémentaires) le cas échéant.

Réseaux/trames protégés par des pare-feu

La **protection de tous les accès réseau par des pare-feu** est l'une des mesures les plus importantes et les plus efficaces pour renforcer la sécurité informatique et bloquer toute tentative d'accès illicite. Le pare-feu contrôle chaque paquet de réseau réceptionné avant son transfert, sur la base de l'**adresse d'expédition/de destination et des services utilisés**.

Les pare-feu dotés de **fonctions de contrôle supplémentaires** augmentent le niveau de sécurité. Les pare-feu de ce type vérifient non seulement les informations d'adressage des paquets réceptionnés mais également d'autres aspects. Ils analysent par exemple le contenu des paquets (**Deep Packet Inspection - DPI**) avant de leur accorder l'accès au réseau.

Il existe des pare-feu qui filtrent également les **données sortant du réseau**. Autant d'obstacles en plus pour les programmes malveillants qui ne sont pas reconnus par les machines concernées.

Une **segmentation plus fine** des réseaux concernés peut renforcer davantage leur sécurité. Cette subdivision du réseau local permet de protéger **les frontières** de chacun des sous-réseaux plus petits ainsi formés à l'aide de **pare-feu**. Il est ainsi possible de mieux limiter l'impact négatif des machines touchées par un virus à l'intérieur du réseau local.

Les pare-feu sont de nos jours souvent intégrés avec le routeur à un même appareil. Les fonctions des pare-feu sont de plus couvertes par des switch de plus en plus intelligents. **Ces trois fonctionnalités sont de plus en plus souvent combinées dans des appareils toujours plus performants.**

Connexions VPN pour les stations/îlots déportés

La connexion de stations ou îlots déportés par **VPN (Virtual-Private Network)** au système de GTB renforce la sécurité globale de manière significative.

La connexion VPN établit un **canal crypté** entre la station/l'îlot distant(e) et le réseau/la trame local(e) interne à l'installation. Comme le nom l'indique, la station/l'îlot distant(e) est intégré(e) virtuellement à ce réseau/cette trame local(e). La **communication est cryptée** et l'identité de chaque participant VPN est sécurisée par un **mot de passe**. Si un **certificat** d'authentification (à partir de la Public Key Infrastructure) est utilisé pour le cryptage **(ssl/TLS)**, les personnes non autorisées n'ont pratiquement aucune possibilité d'épier l'accès ou de l'utiliser à des fins malveillantes.

Sécuriser les stations déportées avec VPN est non seulement intéressant pour les stations distantes (sur WAN/Internet) **mais également pour les stations d'autres trames** dans des réseaux plus importants.

Switch équipés de fonctions de sécurité

Si malgré les objections émises plus haut, une infrastructure réseau déjà existante est utilisée à la fois par le système de GTB et par d'autres utilisateurs, il est recommandé d'utiliser des **switch avec fonctions de sécurité intégrées**. Ces derniers peuvent considérablement améliorer la sécurité des composants de GTB raccordés au réseau commun en filtrant les **données envoyées à chaque utilisateur**. Le switch garantit la réception exclusive par chaque utilisateur des paquets de données qui lui ont effectivement été adressés.

Des switch plus sophistiqués sont de plus en mesure de rassembler certains utilisateurs d'un même réseau (les utilisateurs du système de GTB, par exemple) dans un **VLAN**. Ceux-ci communiquent donc au sein de leur **propre réseau virtuel** et ils ne sont alors visibles et accessibles pour les autres utilisateurs du réseau que si le routeur/pare-feu utilisé le permet explicitement.

Ces switch peuvent en partie être configurés manuellement avec des filtres **« Listes blanches »/« Listes noires »**. Dans ces listes, les appareils autorisés à être raccordés et les ports auxquels ils peuvent se raccorder sont définis précisément (sur la base de l'**adresse MAC**) lors de la mise en service. Ceci prévient le raccordement d'appareils tiers au réseau de GTB.

Accès WLAN WPA2 (Enterprise)

Si des appareils (mobiles) doivent être raccordés à l'installation par **WLAN (Wireless LAN)**, seul un routeur WLAN prenant en charge le **standard WPA2 (Enterprise)** peut fournir un bon niveau de sécurité apte à répondre aux exigences modernes.

Le standard de sécurité WPA2 crypte les données de communication en s'appuyant sur le **standard AES (Advanced Encryption Standard).**

Contrairement au WPA2 sans « Enterprise », pour lequel l'authentification se fait par l'entrée du (même) mot de passe pour tous (Preshared Key), la variante « **Enterprise** » supporte des mots de passe différents, soit pour comptes utilisateur (**LDAP/Active Directory, RADIUS**), soit pour **certificats** (à partir de la Public Key Infrastructure).

Aujourd'hui, les processus **WPA2** et surtout **WPA2-Enterprise** sont considérés comme **très difficiles, voire impossibles à pirater** si des mots de passe assez longs et complexes sont utilisés et si le WPS est désactivé.

Protection contre les logiciels malveillants et mises à jour pour PC

À côté de la protection réseau, la phase d'étude de projet sert également à définir **quel type de protection contre les logiciels malveillants** doit être installé sur l'**ordinateur de gestion** concerné. Pour que celui-ci reste efficace, un **concept de mise à jour** réalisable doit également être défini.

La protection contre les logiciels malveillants annule l'action entre autres de **virus, logiciels espion, chevaux de Troie** connus et les élimine si cela est possible. Étant donné que seuls les logiciels malveillants connus peuvent être détectés, il est important d'effectuer régulièrement des mises à jour.

Concept de sauvegarde avec consignes de récupération

La présence d'un **dispositif de sauvegarde** spécialisé doit être une évidence pour tout système de GTB.

En effet, il est tout à fait probable qu'un système de GTB ne soit plus opérationnel après une attaque, ce qui a un impact sur l'exploitabilité du bâtiment concerné. La **remise en fonction** de l'installation doit alors être effectuée **dans l'extrême urgence**. Une procédure claire mise en place dès le départ avec des **consignes de récupération pas à pas** (testées et mises en pratique au préalable, voir ci-dessous) se révèle dans ce cas une aide précieuse.

Étant donné que les fichiers de sauvegarde contiennent en général également des **copies de données extrêmement sensibles**, il est crucial de prévoir dès l'étude de projet **un emplacement sûr où elles pourront être conservées**. Les éléments contenant des informations de configuration système et les données de gestion des utilisateurs pouvant présenter un grand intérêt pour un pirate avisé doivent notamment faire l'objet d'une protection spécifique.

Sécurité de l'installation physique/de l'armoire de commande

La sécurité physique de l'installation, des armoires de commande et des dispositifs de communication doit bien sûr être assurée aussi bien pour éviter toute véritable attaque mal intentionnée que pour empêcher toute personne non autorisée à accéder au système de manière inconsidérée.

Dans le contexte de la cybersécurité, il convient surtout de mentionner les **points d'accès physiques aux appareils, armoires de commande et dispositifs de communication**. En aucun cas les prises (libres ou occupées) Ethernet, USB et de configuration destinées aux ordinateurs, à ASn, aux routeurs, etc. ne doivent être rendues accessibles.

Possibilités de fonctionnement d'urgence (sans GTB)

Si une attaque devait avoir des répercussions sur le bon fonctionnement du système de GTB, **des unités de commande et de signalisation locale reliées à l'UGL et aux installations** peuvent avoir un rôle majeur à jouer dans la sauvegarde des fonctions de cette dernière.

Il en est de même pour les **systèmes de verrouillage matériels** intégrés aux installations techniques (par exemple, si un ventilateur ne peut pas fonctionner parce que le volet est complètement fermé, etc.).

Éléments au niveau de la mise en service

Pendant la phase de mise en service, les exigences en matière de cybersécurité pour l'étude de projet doivent être mises en place et complétées. Tous les **paramètres relevant de la sécurité** (autorisations, critères de mot de passe, ports, etc.) doivent être **réglés** et les mesures de protection doivent être si possible **testées** pour garantir qu'elles fonctionnent. Il convient de souscrire un **abonnement aux mises à jour** et de **former** les futurs **utilisateurs** afin d'assurer de bonnes conditions d'exploitation et de maintenance.

Ajustement (limitation) des autorisations accordées

Lors de la mise en service, les **utilisateurs/groupes d'utilisateurs** doivent être créés et leurs **droits** définis pour tous les appareils/ordinateurs et systèmes concernés. Plus les droits auront été adaptés avec exactitude aux tâches des utilisateurs/groupes (c'est-à-dire **restreints/limités**), plus le risque sera minime. À la fois le risque d'attaque ciblée et le risque d'erreur de manipulation involontaire.

L'importance de cette restriction prend tout son sens lorsqu'on songe à l'usurpation illégale de **données de connexion** (nom d'utilisateur et mot de passe) ou aux **comptes utilisateur qui restent actifs** sur certains appareils/ordinateurs.

Critères/durée de validité de mot de passe, déconnexion automatique

De nombreux appareils, systèmes d'exploitation et programmes offrent la possibilité de régler ces paramètres. Quel **niveau de complexité** doit présenter un **mot de passe** ? Quelles restrictions faut-il mettre en place ? À quelle fréquence le **mot de passe doit-il être changé** par l'utilisateur ? Après quelle durée d'inactivité l'utilisateur doit-il être **automatiquement déconnecté** ? L'analyse de risque détermine l'étendue des contraintes à fixer.

Il est cependant essentiel de garder une **vue d'ensemble** et de s'orienter sur l'**application pratique**. **Convivialité** et **sécurité** se font concurrence et il faut garder à l'esprit que plus les critères de mot de passe seront nombreux, plus **l'utilisateur aura de difficultés** à gérer ce dernier. Plus la graphie du mot de passe sera longue et compliquée, plus l'utilisateur devra le changer souvent et plus il aura de mots de passe différents à retenir, plus il ressentira la nécessité de les noter quelque part. En effet, il utilise également des mots de passe dans le privé. Certains que les membres de sa famille doivent connaître et d'autres qui doivent rester confidentiels. Chaque système possède ses propres règles de création de mot de passe. **A un moment donné, cela devient impossible à gérer** et il en résulte des **listes de mots de passe enregistrées sur le smartphone**. De même, on note des mots de passe dans des **gestionnaires de mots de passe gratuits** plus ou moins sécurisés ou inscrits sur un bout de papier caché **sous le clavier**, etc.

« Post-durcissement » des appareils/PC/composants

Une fois l'installation et la configuration de tous les éléments pertinents terminées, le **« (post-)durcissement » de tous les appareils (Linux) et des ordinateurs** renforce encore la sécurité. Cela implique l'élimination de tous les **services, accès, comptes utilisateur, processus et programmes** inutilisés ou du moins leur désactivation. Seuls les éléments effectivement nécessaires aux fonctionnalités souhaitées doivent rester sur les appareils. Plus le système sera « maigre », moins l'agresseur sera susceptible de trouver des outils utiles et plus sa tâche sera rendue difficile.

Cela vaut surtout pour les ordinateurs. Les appareils (ASn, par exemple) doivent être, dans la mesure du possible, « pré-durcis » par le fabricant (et non avoir fait l'objet d'une compilation).

Journaux utilisateur (avec signature) pour le traçage

En cas de défaut, le rôle des **journaux utilisateur**, journaux de bord toujours accessibles et actifs, prend toute son importance. Ils servent à la fois à **exercer un contrôle précis** mais également à simplifier considérablement la **récupération du système ou des données** en cas de panne.

Les journaux de bord doivent être **activés et configurés lors de la mise en service**, le cas échéant. Ils doivent au moins pouvoir enregistrer toutes les actions des utilisateurs, les modifications effectuées sur des données et évidemment toute action de réglage ou de commutation.

Ils peuvent être réglés pour les bases de données et les routeurs. Cela permet d'optimiser le contrôle.

Comme il est probable qu'un agresseur particulièrement qualifié essaie d'effacer toute trace de son attaque des journaux utilisateur, il peut être opportun de sécuriser ces derniers par un mécanisme de **signature numérique**. La signature numérique protège les données enregistrées de toute modification ultérieure grâce à une **clé de signature**.

Il convient de garder une **vision sur le long terme** lors de la configuration des journaux de bord. Comment empêcher qu'ils ne deviennent trop volumineux ? Doivent-ils être sauvegardés régulièrement ? Combien de temps faut-il conserver leur contenu ?

Étapes à suivre/règles de comportement

Les étapes à suivre/règles de comportement définitives et testées (**procédure opérationnelle permanente POP ou standard operating procedure SOP)** concernant la cybersécurité doivent être présentes dès la mise en service de l'installation sous deux aspects principaux : D'un côté, celles prévues pour une **exploitation normale**. Elles aident à garantir que tous les mécanismes de sécurité sont opérationnels sur la longue durée et tenus à jour. De l'autre, celles s'appliquant **en cas d'attaque/de défaut** et contenant toutes les informations/étapes à suivre concernant la sensibilisation, la stratégie de réduction et de réparation des dommages.

Les étapes de travail/règles de comportement (POP) établies pour une **exploitation normale** contiennent par exemple des **processus opérationnels, check-lists** et **fonctions de rappel** d'un calendrier. En respectant ces points, vous garantissez que **tous les éléments relatifs à la sécurité** sont à jour : La protection contre les logiciels malveillants a-t-elle été actualisée ? Les mises à jour de programmes et de systèmes d'exploitation relatifs à la sécurité ont-elles été installées ? Quelles mesures de sécurité doivent être mises en place sur les éléments qui viennent d'être installés/ajoutés ? Les sauvegardes ont-elles été exécutées, enregistrées correctement et comment la récupération est-elle régulièrement testée ? Le point de contrôle a-t-il exercé son rôle ? Ces étapes de travail/règles de comportement constituent **une pierre angulaire de taille dans l'effort global de prévention ou de réduction des risques**.

Si un événement venait à affecter la fonctionnalité du système de GTB, il est probable que ce dernier devienne partiellement ou complètement inopérant. Dans les cas extrêmes, cela peut avoir des **répercussions majeures sur l'exploitabilité du bâtiment**. La remise en fonction du système de GTB doit alors être effectuée dans l'extrême urgence. Des **règles de comportement** claires et pratiques avec **consignes pas à pas** se révèlent dans ce cas une aide précieuse. Outre apporter une aide concernant la récupération, elles peuvent également contenir des informations concernant les voies de signalisation, numéros d'appel, procédures d'escalade, mesures d'urgence, etc.

Information/formation de l'utilisateur

Dans une exploitation quotidienne du système de GTB, la cybersécurité ne peut être optimale que si **tous les éléments impliqués** jouent correctement leur rôle. Le **facteur humain**, c'est-à-dire non seulement les techniciens de maintenance mais surtout les exploitants/utilisateurs du système, est ici d'une importance capitale.

Si l'installation est dotée de tous les dispositifs de sécurité appropriés, les intervenants représentent alors **le plus grand risque potentiel**.

Les plus grands dangers se présentent sous la forme d'erreurs de manipulation de l'installation-même (jeux, expérimentations), mauvaise manipulation des dispositifs de sécurité, **usage inapproprié des données d'accès ou d'autres données**, utilisation abusive des **dispositifs de communication, actes involontaires malgré une bonne foi certaine** (e-mail, phishing, etc.).

Outre la **formation** des collaborateurs à ce sujet technique qui se révèle indispensable pour garantir une commande correcte de tous les dispositifs de sécurité de l'installation, il importe de les informer sur les enjeux et de les **sensibiliser aux risques et dangers potentiels**.

La mention de thèmes relevant de la cybersécurité dans une **formation spécifique** (indépendamment des autres thèmes) leur donne plus de poids. Le fait de **rafraîchir** régulièrement ses connaissances aide à maîtriser le sujet même après une longue période et à éviter les incidents. Sans oublier les séances d'information pour les nouveaux collaborateurs.

Le thème « **Comportement à adopter et récupération technique en cas de dommage** » à lui seul mériterait de faire l'objet d'une formation spécifique.

Éléments au niveau de la maintenance

Les techniques d'attaque d'installations informatiques sont en constante évolution. Les technologies de défense également. Le système de GTB peut donc également continuer à se développer.

Il incombe aux techniciens de maintenance (en ce qui concerne la sécurité informatique) **d'entretenir et de mettre régulièrement à jour tous les éléments de sécurité informatique** installés et, si nécessaire, **d'adapter l'installation aux dernières évolutions technologiques**.

Mises à jour/mises à niveau relevant de la sécurité

Tous les appareils et programmes, en particulier les ordinateurs et leur logiciel de protection contre les logiciels malveillants, les dispositifs de communication tels que les routeurs, les appareils VPN, etc. doivent être **régulièrement mis à jour** à l'aide des dernières versions disponibles. C'est là le seul moyen pour les mécanismes de protection d'être à la hauteur des techniques d'attaque qui ne cessent de se perfectionner.

Il est possible que les derniers développements techniques rendent nécessaires des **mises à niveau** vers des versions plus modernes et plus complètes.

Adaptations système relevant de la sécurité

Les éléments matériels et logiciels installés sur les systèmes de GTB ont en général des **cycles de vie bien plus longs que les installations informatiques commerciales**.

L'augmentation du nombre de menaces qui planent sur les systèmes d'information ou sur les mécanismes de sécurité de ces systèmes peut rendre nécessaire, outre les soins apportés aux mesures de sécurité déjà mises en place, l'introduction d'**adaptations système plus larges et plus complètes**.

Tests réguliers de sécurité/sauvegarde

Afin de garantir un niveau de défense élevé, les mesures de sécurité doivent faire l'objet de **contrôles à des intervalles de maintenance prédéfinis** et, dans la mesure du possible, de **tests** précis.

Il convient également de mettre périodiquement en pratique le déroulement des **actions à mener en cas d'attaque/de panne**. Cela concerne également la récupération de données sauvegardées. Il est ainsi arrivé que certaines données sauvegardées se soient révélées inutilisables après un incident.

Il convient également de contrôler à des intervalles réguliers que les exploitants/utilisateurs de l'installation **respectent** dans la pratique **les codes de sécurité informatique** dans le cadre d'un contrôle de sécurité.

Éléments au niveau de l'utilisateur

Comme cela a été maintes fois souligné, le niveau de sécurité informatique d'une installation de GTB ne peut être et rester bon que si tous les acteurs impliqués jouent leur rôle de protection durant toute la durée de vie de l'installation. Cela implique particulièrement les **utilisateurs lors de l'exploitation quotidienne** de l'installation. Ce sont les premiers à pouvoir signaler des événements anormaux.

Bonne pratiques concernant le nom d'utilisateur/mot de passe

Comme mentionné plus haut, le **niveau de complexité du mot de passe** est fixé par le fabricant ou au plus tard lors de la mise en service de l'installation et adapté le cas échéant au risque auquel cette dernière est exposée.

De plus, les utilisateurs doivent choisir un **mot de passe** difficile à cracker. Cela signifie qu'il ne doit **en aucun cas contenir des éléments faciles à deviner** comme le nom, le nom du partenaire/des enfants, la date de naissance, etc. Certains pirates (ou personnes qui jouent ou expérimentent) écrivent des algorithmes qui comparent les mots de passe avec des données personnelles en vue de les cracker.

En général, c'est surtout la **longueur** qui fait la robustesse d'un mot de passe (plus que la complexité, etc.). Par exemple, des **phrases** sont tout à fait adaptées, tant qu'il ne s'agit pas de citations célèbres par exemple. Elles présentent l'avantage d'être plus faciles à mémoriser. Par exemple : « sauter 1 jour sauter toujours » ou « un utilisateur d'Internet averti en vaut deux ».

Bien évidemment, il est également proscrit des bonnes pratiques d'**inscrire** son mot de passe où que ce soit ou de le **prêter** à quelqu'un.

Utilisation/contrôle de la sauvegarde

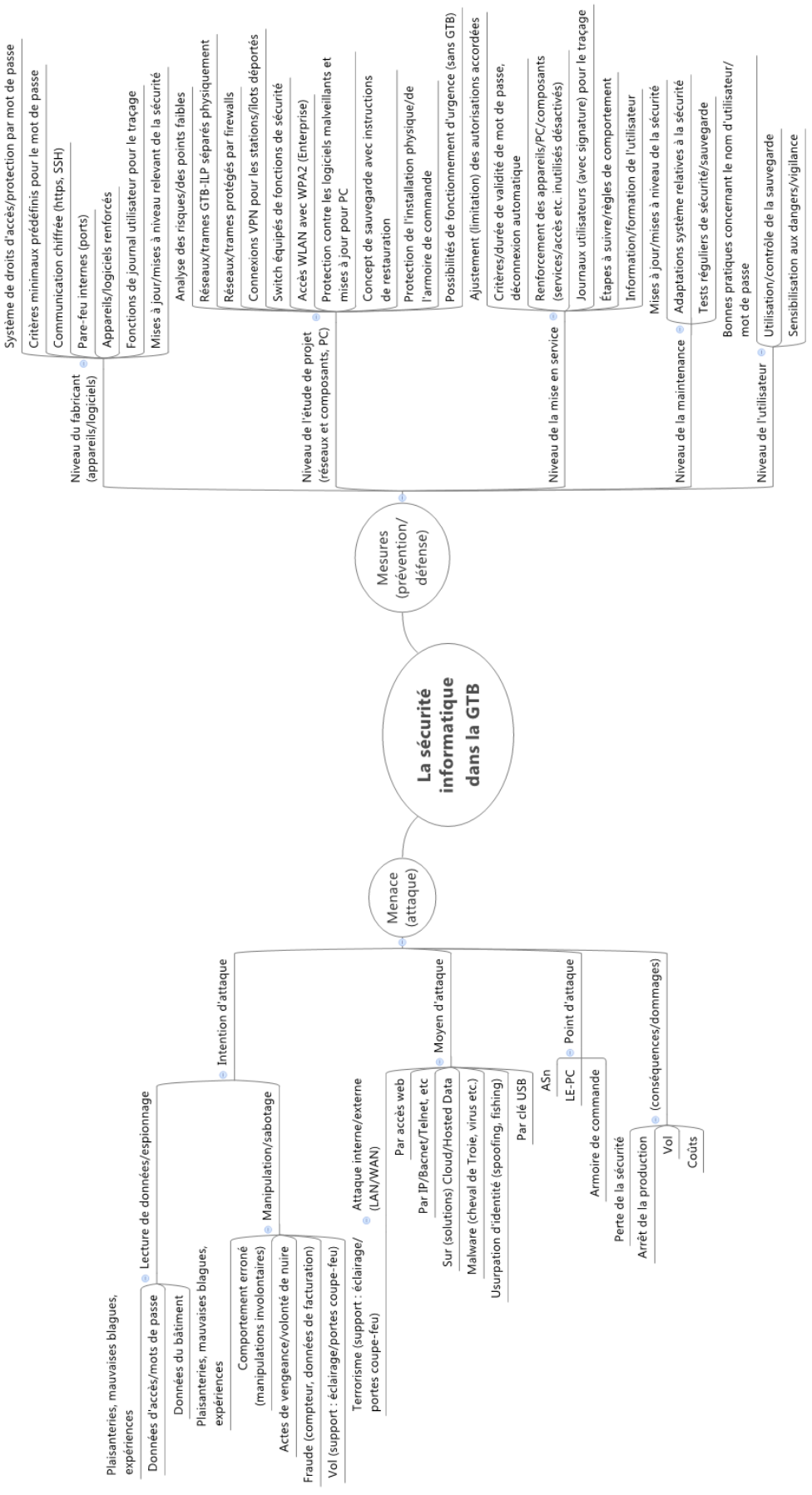
Il convient de contrôler le bon déroulement et l'exécution complète des **processus de sauvegarde** automatisés. Si nécessaire, il faut changer de support de sauvegarde externe. De plus, sa **validité** doit être régulièrement testée (voir plus haut).

Comme les **données de sauvegarde** contiennent en général des copies de données extrêmement sensibles, elles doivent être conservées à un endroit protégé de manière fiable. Les fichiers contenant des informations de configuration système et les données de gestion des utilisateurs pouvant présenter un grand intérêt pour un pirate avisé doivent notamment faire l'objet d'une protection spécifique. Les documents d'étude de projet comme les topologies système, concepts de sécurité, etc. constituent des informations très utiles pour un agresseur aux intentions hostiles et doivent être conservées ainsi que leurs copies **dans un endroit protégé à ces fins**.

Sensibilisation aux dangers/vigilance

Comme mentionné plus haut, les utilisateurs d'un système de GTB doivent suivre des formations consacrées au thème de la cyber sécurité qui les sensibiliseront aux dangers potentiels. Il est crucial de les sensibiliser et de les motiver à garder une vigilance permanente. Toute **anomalie** doit être **détectée** et **prise au sérieux**.

Comme c'est bien souvent le cas, le facteur humain constitue le principal risque. Le **phishing**, les **mises à jour de programme piégées** et même les **conversations** peuvent permettre à quelqu'un d'obtenir des données sensibles, des informations système, des noms d'utilisateur et des mots de passe avec un niveau d'autorisation le plus élevé possible.


La sécurité informatique dans la GTB
Mesures (prévention/ défense)
Niveau du fabricant (appareils/logiciels)
Système de droits d'accès/protection par mot de passe
Critères minimaux prédéfinis pour le mot de passe
Communication chiffrée (https, SSH)
Pare-feu internes (ports)
Appareils/logiciels renforcés
Fonctions de journal utilisateur pour le traçage
Mises à jour/mises à niveau relevant de la sécurité
Niveau de l'étude de projet (réseaux et composants, PC)
Analyse des risques/des points faibles
Réseaux/trames GTB-ILP séparés physiquement
Réseaux/trames protégés par firewalls
Connexions VPN pour les stations/îlots déportés
Switch équipés de fonctions de sécurité
Accès WLAN avec WPA2 (Enterprise)
Protection contre les logiciels malveillants et mises à jour pour PC
Concept de sauvegarde avec instructions de restauration
Protection de l'installation physique/de l'armoire de commande
Possibilités de fonctionnement d'urgence (sans GTB)
Niveau de la mise en service
Ajustement (limitation) des autorisations accordées
Critères/durée de validité de mot de passe, déconnexion automatique
Renforcement des appareils/PC/composants (services/accès etc. inutilisés désactivés)
Journaux utilisateurs (avec signature) pour le traçage
Étapes à suivre/règles de comportement
Information/formation de l'utilisateur
Niveau de la maintenance
Mises à jour/mises à niveau de la sécurité
Adaptations système relatives à la sécurité
Tests réguliers de sécurité/sauvegarde
Niveau de l'utilisateur
Bonnes pratiques concernant le nom d'utilisateur/ mot de passe
Utilisation/contrôle de la sauvegarde
Sensibilisation aux dangers/vigilance
Menace (attaque)
Intention d'attaque
Lecture de données/espionnage
Données d'accès/mots de passe
Données du bâtiment
Plaisanteries, mauvaises blagues, expériences
Manipulation/sabotage
Comportement erroné (manipulations involontaires)
Actes de vengeance/volonté de nuire
Fraude (compteur, données de facturation)
Vol (support : éclairage/portes coupe-feu)
Terrorisme (support : éclairage/ portes coupe-feu)
Plaisanteries, mauvaises blagues, expériences
Attaque interne/externe (LAN/WAN)
Moyen d'attaque
Par accès web
Par IP/Bacnet/Telnet, etc
Sur (solutions) Cloud/Hosted Data
Malware (cheval de Troie, virus etc.)
Usurpation d'identité (spoofing, fishing)
Par clé USB
Point d'attaque
ASn
LE-PC
Armoire de commande
(conséquences/dommages)
Perte de la sécurité
Arrêt de la production
Vol
Coûts

Conclusion

L'**éventail d'actions de sécurité informatique possibles au sein d'une installation d'automatisation de bâtiments** est considérable. Entre passivité et mise en place de toutes les mesures à disposition, un monde de possibilités s'ouvre. Entre « une installation dans laquelle n'importe quel informaticien moyen peut pénétrer » et « un déploiement d'efforts gigantesque/une installation presque impossible à pénétrer pour un expert en piratage aux intentions hostiles », tous les degrés de sécurisation sont possibles. Chacun sous-entend bien sûr des **efforts** et des **coûts** différents.

L'**évaluation du risque** individuel est au cœur de chaque projet. L'**étendue des cas de figure** est également immense. Pour beaucoup de bâtiments, le danger se limite aux conséquences d'un penchant pour les **jeux, les expérimentations techniques ou les blagues**. Les bâtiments abritant des objets susceptibles d'être convoités ou pouvant servir de cible à des ennemis reconnus ou encore les édifices publics importants à sensibilité élevée sont en revanche exposés à des **risques très sérieux**.

Il est vivement recommandé de mettre en place dans tous les bâtiments des **mesures de sécurité fondamentales correspondant aux derniers développements technologiques dans le domaine**. Elles aident à se défendre contre la plupart des attaques et à se protéger contre les conséquences de **jeux/expérimentations** évoquées plus haut. Elles contribuent également à empêcher les **erreurs de manipulation** qui, combinées à des **erreurs logicielles** jamais totalement exclues, restent la cause majeure de pannes.

Le **facteur humain** reste souvent une source essentielle de risque : les accès utilisateur avec un utilisateur qui reste connecté en permanence, des mots de passe cachés sous le clavier, des mots de passe prêtés, des accès administrateur par défaut qui n'ont pas été modifiés. En bref, un **manque de précaution, de conscience du danger et de vigilance** ! Des formations spécifiques et une information régulière des collaborateurs peut aider à y pallier.

L'auteur

Franklin Linder, ingénieur en électronique FH est rédacteur technique au SAUTER Head Office à Bâle. Il dispose de 20 ans d'expérience dans le développement, l'application et la commercialisation de systèmes d'automatisation de bâtiments.

Portrait de l'entreprise

En tant que prestataire mondial de solutions pour la technologie d'automatisation des « Green Buildings » de premier plan, SAUTER assure le bien-être et un climat ambiant optimal dans les environnements durables. Spécialiste en la matière, SAUTER développe, produit et commercialise des systèmes de GTB qui augmentent l'efficacité énergétique des bâtiments et assure l'optimisation énergétique de l'exploitation des installations techniques grâce à des prestations de services globales. De la planification à l'exploitation, en passant par la mise en œuvre, ces produits, solutions et prestations permettent d'assurer, durant tout le cycle de vie du bâtiment, une haute efficacité énergétique dans des bureaux, des immeubles administratifs, des centres de recherche et de formation, des hôpitaux, des bâtiments industriels, des laboratoires, des aéroports, des centres de loisirs, des hôtels ou des centres de gestion des données. Avec plus de 100 ans d'expérience et des compétences

technologiques éprouvées, SAUTER est un intégrateur de systèmes confirmé, garantissant une innovation permanente et une qualité suisse. Distingué pour le meilleur système d'automatisation, la meilleure prestation/service énergétique ainsi que la certification pour les produits eu.bac et BTL, SAUTER fournit aux utilisateurs comme aux exploitants une vue d'ensemble de la consommation et des flux énergétiques, et de ce fait de l'évolution des coûts.