SAUTER
Für Lebensräume mit Zukunft.

La sécurité informatique dans la gestion technique de bâtiments

Numéro de document : D100236547
Révision : 04
Version : 01

Im Surinam 55
4058 Bâle
Suisse

Tél. : +41 61 – 695 55 55
Fax : +41 61 – 695 55 10
www.sauter-controls.com
info@sauter-controls.com

Numéro de document : D100236547
Révision : 04
Version : 01

Sommaire

Table des révisions

Date	Édition, rév./ver.	Modification	Chapitre	Page
03/2021	04/01	Révision générale		

Table des illustrations

Liste des symboles

Information

Informations relatives à la manipulation du produit.

Invitation à effectuer une action

Le lecteur est incité à passer à l'action.

Lien hypertexte

Renvois vers des liens ou des applications en ligne.

Avertissement

Avertissements à prendre en compte avant l'exécution d'une opération.

Structure

Nature et source du danger

Conséquences

- ▶ Mesures

1 Résumé

La question de la sécurité informatique dans la gestion technique de bâtiments (GTB) n’est plus un sujet mineur que l’on peut simplement ignorer. Le paysage informatique a radicalement changé ces dernières années. Outre l’accessibilité générale des solutions de GTB via Internet, deux autres changements considérables ont eu lieu ces dernières années. D’une part, la virtualisation des applications et l’externalisation vers le Cloud ont conduit à l'émergence de nouvelles solutions mais aussi de nouveaux prestataires. D’autre part, la croissance rapide de l’IdO (« Internet des objets ») a mené à l’apparition d’une quantité incroyable de nouveaux appareils et données, augmentant de manière exponentielle le besoin de communications Internet et d’accès aux services Cloud.

Alors que récemment la GTB pouvait être considérée comme une solution isolée, une intégration complète avec de nombreux autres meiters et appareils est à présent nécessaire. Ceci entraîne également un changement dans le comportement et les attentes des utilisateurs. Globalement, cela conduit à une prolifération des possibilités d’attaque pour les cybercriminels.

Contrairement aux infrastructures informatiques en général, la menace concerne cependant plus que de « simples » données dans le cas de la gestion technique de bâtiments. Du fait des connexions physiques d’un système de GTB avec installations techniques du bâtiment (ventilation, éclairage, portes, systèmes d’accès), les attaques peuvent avoir des conséquences sur la sécurité du bâtiment lui-même.

Le risque effectif encouru par le bâtiment est spécifique à chaque projet et dépend fortement de la vulnérabilité du système de GTB et du degré de dépendance du bâtiment vis-à-vis de ce dernier.

En principe, trois types de mesures peuvent être prises pour protéger un système de GTB : la protection des différents appareils/PC/logiciels ; la protection de l’infrastructure informatique, c’est-à-dire des réseaux et des accès au réseau ; les mesures de protection au niveau des processus.

L’application de mesures de protection des appareils/PC/logiciels commence déjà chez le fabricant. La CEI 62443-3-3 fournit une liste d’exigences vis-à-vis desquelles les fabricants doivent fournir des solutions. Les mesures de protection de l’infrastructure informatique et leur mise en place pour les appareils/PC/logiciels sont du ressort du fabricant de l’installation, tandis que les donneurs d’ordres, maîtres d’ouvrage et bureaux d’étude en posent le cadre, en particulier budgétaire, à travers leurs appels d’offres et leurs cahiers des charges. Il existe à la fois des normes internationales (comme CEI 62443) et des recommandations d’associations nationales, en particulier pour les installations essentielles ou stratégiques.

Les travaux relatifs à la sécurité informatique d’une installation s’étendent tout au long du processus de développement 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 intitulé « La sécurité informatique dans le domaine de la gestion technique de bâtiments » donne un aperçu des mesures de protection possibles. Dans les graphiques, vous trouverez des informations supplémentaires concernant les différentes menaces potentielles. Pour une approche systématique, il est recommandé de consulter la norme CEI 62443. Les recommandations ou régulations locales doivent également être prises en compte. Il est recommandé de faire appel à des experts spécialisés.

Le présent livre blanc traite exclusivement des mesures de sécurité informatique à appliquer contre toute attaque ou intervention indésirable provenant de l’extérieur. Les aspects relatifs à la disponibilité des systèmes informatiques et à la sécurité technique des installations CVC ne sont abordés que sous l’angle de la minimisation des dommages en cas de panne de la commande.

2 Introduction/généralités

Ce livre blanc intitulé « La sécurité informatique dans le domaine de la gestion technique de bâtiments » traite exclusivement des mesures de sécurité informatique contre toute attaque ou intervention indésirable provenant de l'extérieur. La disponibilité des systèmes informatiques (« sûrs », dans le sens de « qui ne tombent jamais en panne », « ne plantent jamais », « redondants », etc.), qui est souvent perçue comme faisant partie intégrante de ce sujet, n'est pas abordée ici. La sécurité de l'installation CVC en tant que telle (alimentation de secours, systèmes de verrouillage matériel, exécution redondante de certaines fonctions, etc.) n'est ici abordée que sous l'angle d'une minimisation des dommages en cas de panne de la commande.

L'intérêt croissant pour la question de la sécurité informatique dans le domaine de la gestion technique de bâtiments (GTB) s'explique par le développement technologique de ces dernières années. Depuis un certain temps déjà, les technologies d'automatisation intègrent des niveaux d'intelligence de plus en plus élevés. Les AP et unités de gestion locale ont depuis longtemps évolué pour devenir des micro-ordinateurs spécifiques aux différents secteurs et dotés de systèmes d'exploitation intégrés. Par conséquent, les technologies informatiques générales déjà existantes ont été largement adoptées en matière de communication. En ce qui concerne les appareils de terrain, la tendance penche également vers toujours plus d'intelligence intégrée et des technologies de communication de plus en plus sophistiquées. Il en va de même pour la commande de locaux, où les appareils mobiles privés (PAP) ou de nouveaux concepts d'utilisation avec assistance vocale (par ex. Amazon Alexa!, Google Nest Hello, etc.) se sont imposés. Ces nouvelles solutions (Cloud, IA) nécessitent des interfaces et des protocoles supplémentaires (WiFi™[1], Bluetooth®[2], LoRaWAN®[3], Web-API, MQTT, OPC, etc.) qui engendrent à leur tour des possibilités d'attaque supplémentaires.

Le développement de la GTB au cours des 10 à 15 dernières années a été marqué par la normalisation 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 au niveau des réseaux, des protocoles et des objets, ce qui a permis une ouverture des systèmes.

L'utilisation de standards informatiques généraux pour communiquer a rendu possible l'intégration des systèmes de gestion technique de bâtiments dans les structures déjà en place de la branche Business IT. L'utilisation d'Internet

[1] Wi-Fi®, le logo Wi-Fi, le logo Wi-Fi CERTIFIED et les autres marques sont des marques déposées de Wi-Fi Alliance.

[2] © 2021 Bluetooth SIG, Inc

[3] LoRa, LoRaWAN®, Copyright © 2021 LoRa Alliance®

pour la communication à distance s'est imposée, ce qui a ouvert à la GTB des possibilités de communication quasi illimitées.

Toutes ces modernisations ont apporté aux clients et exploitants de la gestion technique 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 la GTB. Cette vulnérabilité est désormais sensiblement identique à celle des infrastructures informatiques générales.

Du fait de la connexion des systèmes de GTB 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 « simplement » les 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 donc être considérables.

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, ni la même sensibilité aux conséquences de l'attaque.

Les risques sont minimisés si « seuls » les équipements CVC (Chauffage-Ventilation-Climatisation) sont raccordés au système de gestion technique du bâtiment, et non 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 dont le niveau de sécurité requis est particulièrement élevé (aéroports, gares, etc.). Les menaces auxquelles de tels bâtiments sont exposés peuvent, dans les cas extrêmes, inclure des actes de violence ou des attaques terroristes par piratage informatique.

Les dispositifs de sécurité mis en place doivent donc 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. Dans ce cadre, une stratégie de défense en profondeur (« defense-in-depth »), c'est-à-dire l'utilisation de multiples mesures et technologies de protection, est généralement recommandée. Un renforcement de la sécurité passe cependant toujours par des mesures coûteuses et laborieuses. Une sécurité totale et infaillible dans le domaine de la gestion technique de bâtiments est, malgré les plus grands efforts, impossible à garantir complètement.

3 Éléments constitutifs de la sécurité informatique dans la GTB

Les mesures de protection permettant d'améliorer la sécurité d'une gestion technique de bâtiments (GTB) en réseau reposent sur deux niveaux principaux :

Tout comme les habitants d'une ville peuvent être protégés par la porte d'entrée de leur propre maison et/ou par les fortifications de la ville, les mesures de protection des systèmes de GTB peuvent être prises au niveau des appareils (unités de gestion locale, PC, etc.) et/ou au niveau des accès aux réseaux concernés. De même qu'il est certainement préférable de ne pas laisser entrer le danger dans la ville et pour cela de fortifier les portes de la ville, il est crucial, en GTB, de renforcer en premier lieu la protection des accès aux réseaux. Cependant, même les portes et les enceintes de la ville ne sont jamais étanches à 100 %. Par ailleurs, des individus dangereux peuvent également venir de l'intérieur de la ville. C'est pourquoi, parallèlement, la protection des différents appareils de GTB locaux est essentielle.

Un bon résultat ne peut être atteint qu'en combinant les mesures à ces deux niveaux.

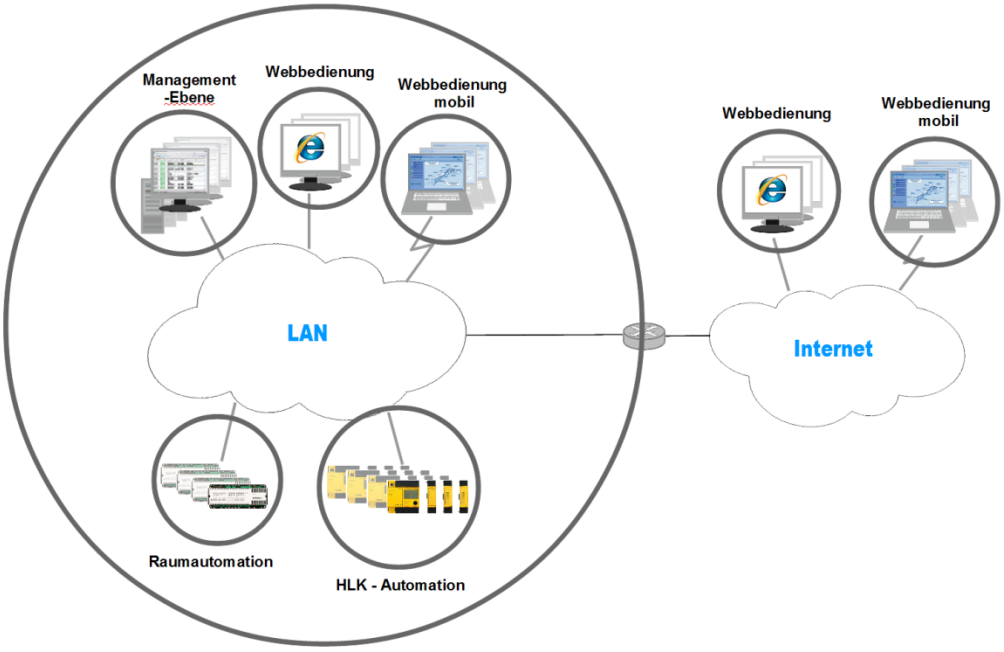

Fig. 1 : Domaines et réseaux du système de GTB

Au cours du cycle de vie d'une installation de GTB, les mesures à prendre au niveau des appareils/logiciels commencent déjà chez le fabricant des produits. Celui-ci intègre à ses produits d'usine les mesures de sécurité les plus complètes possibles. Cela peut inclure 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 de GTB a alors une influence faible ou du moins indirecte sur les actions mises en œuvre au niveau de l'infrastructure informatique, c'est-à-dire au niveau des réseaux/segments de réseaux et de leurs accès. Ceux-ci sont conçus en étude de projet et réalisés par le fabricant de l'installation de GTB (généralement en coopération avec le responsable informatique du client/de l'exploitant du bâtiment/du maître d'ouvrage). Il détermine si l'exploitation de l'installation de GTB ou au moins de la couche d'automatisation s'effectue sur un réseau isolé et réservé à la GTB, 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 éventuels réseaux WLAN peuvent être sécurisés. Les maîtres d'ouvrage et bureaux d'étude fixent, quant à eux, les exigences fonctionnelles et le cadre budgétaire.

Les mesures de sécurité informatique s'étendent tout au long du cycle de vie d'une installation. Comme expliqué ci-dessus, elles démarrent déjà chez le fabricant des appareils et des programmes utilisés et se poursuivent lors de l'étude de projet, la réalisation et la mise en service de l'installation. Cependant, même plus tard, dans 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.

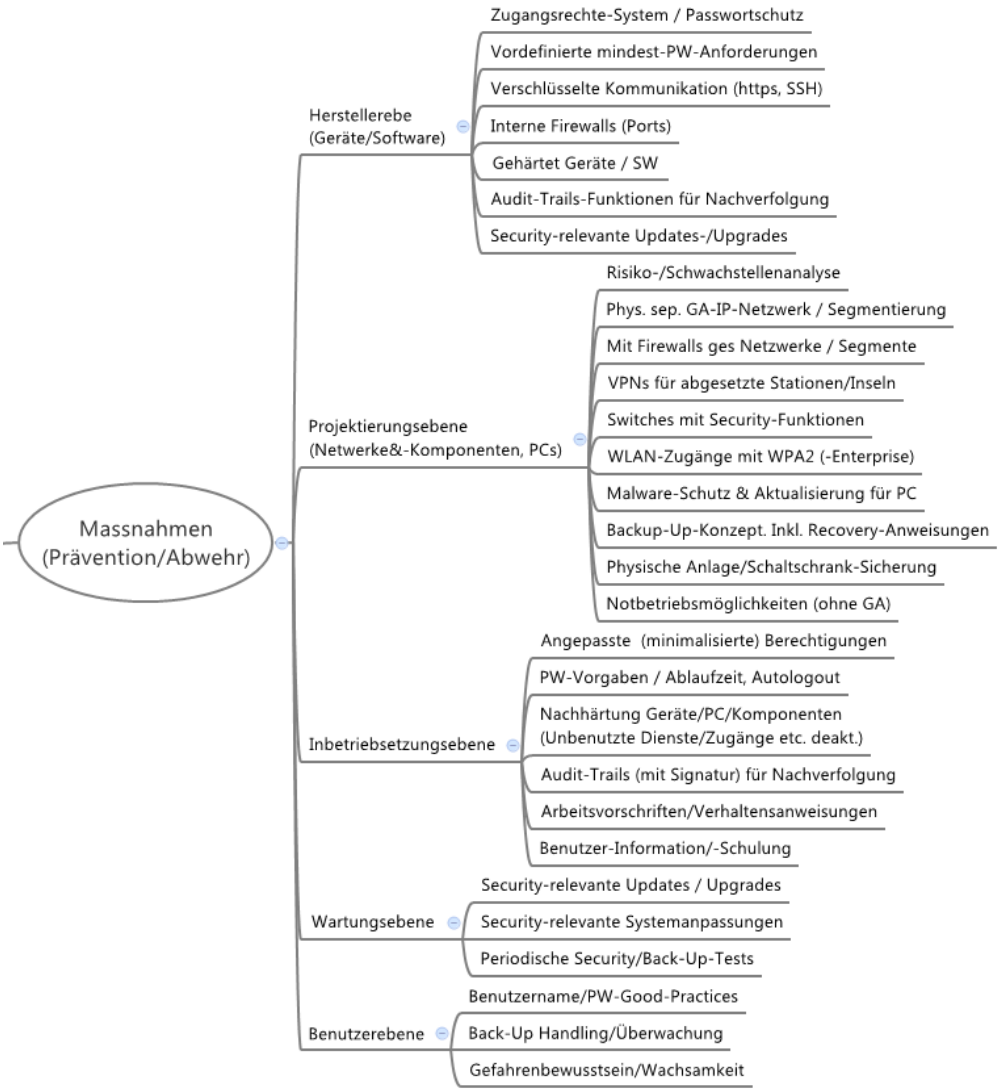

Fig. 2 : Mesures en fonction du niveau de responsabilité

3.1 Éléments au niveau du fabricant

Sont concernés les appareils dotés d'un système d'exploitation intégré (unités de gestion locale, appareils réseau, capteurs intelligents, Smart Actuators), ainsi que le logiciel du système de gestion (logiciel SCADA/BEMS, logiciel d'analyse et de gestion énergétiques).

En tant que fabricant, SAUTER a développé modulo 6 en fonction de la norme CEI 62443-3-3 afin d'intégrer des mesures et des solutions de cybersécurité. Le document [1] constitue un guide à cet égard. Les mesures comprennent notamment :

Identification / Authentification, droit d'accès

Tant sur modulo 6 que sur SAUTER Vision Center, les comptes d'utilisateur du serveur web peuvent être configurés avec différents niveaux d'accès et d'exigence en matière de mot de passe. Le mot de passe par défaut doit obligatoirement être changé sur les unités modulo 6.

Contrôle de l'utilisation

Grâce à la liste de contrôle des accès intégrée, l'accès au réseau par d'autres participants peut être explicitement autorisé (liste blanche) ou explicitement interdit (liste noire).

Journalisation

Le serveur web intégré dans les unités modulo 6 enregistre toutes les actions de l'utilisateur sous la forme d'un journal utilisateur. Cela permet de retracer toute intervention des utilisateurs. Ce système s'apparente à SAUTER Vision Center, où des exigences encore plus élevées (conformément à FDA Cfr 21 Part 11) sont prises en charge.

Contrôle d'intégrité

La Building Data Integrity Solution (modu615-BM) permet de vérifier périodiquement l'intégrité des données sur toutes les unités d'une installation. Toute violation de l'intégrité déclenche une alarme et, si nécessaire, la réinitialisation de la configuration de l'unité concernée. Cette solution mobilise un système de blockchain, de cryptage (TLS) et d'authentification à deux facteurs en tant que fonctions standard.

Réaction rapide aux événements

Toute violation de l'intégrité déclenche une alarme et, si nécessaire, la réinitialisation de la configuration de l'unité concernée.

Cryptage

L'utilisation du cryptage TLS est standard sur modulo 6. Tous les protocoles qui le prennent en charge offrent des options telles que le serveur web avec HTTPS. En outre, BACnet/SC est intégré de sorte que BACnet ne communique plus en texte clair, mais uniquement avec des unités préenregistrées qui prennent également en charge BACnet/SC. BACnet/SC utilise TLS et n'est disponible que sous forme cryptée.

Séparation des réseaux : 2 interfaces de réseau

La double interface permet, par exemple, de connecter l'unité de gestion locale au réseau informatique de l'entreprise et d'accéder au serveur web, ainsi qu'à des services Cloud tels que le serveur météo ou le serveur d'e-mail, tandis que le système de gestion technique de bâtiments avec BACnet/IP, physiquement séparé, fonctionne simultanément sur un réseau distinct. Le flux de données s'en trouve effectivement limité.

Backup/Restore

Cette fonctionnalité de base est prise en charge par l'intégralité des outils de configuration. Cette fonction permet de restaurer la configuration ainsi que le programme de contrôle. Grâce à la Building Data Integrity Solution, cette restauration peut même être effectuée automatiquement dès qu'une modification non autorisée est détectée.

Disponibilité

L'architecture interne des unités modulo 6 donne la priorité aux fonctions de régulation sur toutes les autres tâches, de sorte que si des interfaces sont surchargées (par ex. en cas d'une erreur de configuration du réseau BACnet ou d'une attaque DoS sur le serveur web), celles-ci sont bloquées et la régulation continue à fonctionner normalement.

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

Tous les appareils et produits logiciels disposant d'accès utilisateur (serveurs web, accès de configuration, etc.) doivent bien évidemment être équipés d'un système de droits d'accès configurable avec protection par 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 système d'authentification approprié. Cela concerne par exemple les sources des données des logiciels d'analyse et de gestion énergétiques.

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

Par ailleurs, lorsque les droits d'accès sont définis, l'accès doit être limité au strict minimum, c'est-à-dire n'afficher que ce qui est nécessaire (« need-to-know ») ou ne permettre que ce qui est nécessaire (« fonctionnalité minimale »).

Exigences minimales prédéfinies en matière de 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 fonctions élémentaires pour une bonne protection.

Le fabricant doit mettre de telles fonctionnalités à disposition dans ses produits afin qu'elles puissent, lors de la mise en service, être définies en fonction du niveau de sécurité exigé par l'installation. Si le fabricant programme les exigences minimales dans ses produits de manière définitive

et que celles-ci ne peuvent plus être adaptées ultérieurement au niveau de sécurité de l'installation, elles risquent souvent d'être trop élevées.

En revanche, il est judicieux d'intégrer d'usine une option ou, mieux, une obligation de modification de l'utilisateur Admin et de son mot de passe par défaut après la mise en service, c'est-à-dire après une certaine période de fonctionnement ou selon un critère prédéfini. Bon nombre des piratages informatiques relayés à grand bruit par les médias reposent précisément sur cette lacune. Bien souvent, le mot de passe par défaut n'a pas été modifié après la mise en service et a été facile à trouver parmi les listes des mots de passe de différents fabricants disponibles sur Internet.

Communication cryptée (HTTPS, SSH)

Pour une bonne sécurisation de la communication, les produits doivent être en mesure d'utiliser une communication sécurisée TLS (HTTPS, SSH) pour leur serveur web et leurs interfaces de configuration. Outre le cryptage de la communication, les participants à la communication sont ainsi également identifiés de manière fiable (par le biais de certificats, s'ils sont exploités via une Public Key Infrastructure, ou PKI).

Pare-feu internes (ports)

Tous les appareils compatibles réseau d'un système (en général un 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 et, 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. Il est également recommandé que, dans le cadre d'un balayage des ports, seuls les ports effectivement disponibles donnent une réponse positive, et que tous les autres n'en donnent aucune.

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 telles que Telnet (port 23) ou FTP (port 20) représentent pour les pirates des possibilités supplémentaires bien connues pour s'introduire dans les systèmes matériels de gestion technique de bâtiments. Les variantes cryptées sont ici aussi à privilégier (SSH, FTPS).

Fonctions de journal d'audit (avec signature)

Pour l'analyse ultérieure d'une attaque réelle ou même présumée (erreurs de manipulation, jeux), tous les systèmes devraient prendre en charge les fonctions de journal d'audit (enregistrement des activités de l'utilisateur).

Celles-ci permettent non seulement d'identifier l'intrus/le responsable, mais aussi de déterminer où sont localisés les dommages ou les conséquences devant être corrigés.

Pour une traçabilité fiable des attaques graves, ces enregistrements doivent pouvoir être sécurisés à l'aide d'une signature de sorte qu'ils ne puissent pas être modifiés intentionnellement par un intrus rusé ou involontairement par un intervenant négligent.

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 de GTB doit mettre à jour ou à niveau ses produits sur le plan de la sécurité et mettre à disposition les canaux de distribution correspondants.

Éléments au niveau de l'étude de projet

Au cours de l'étude d'un projet de gestion technique de bâtiment, l'infrastructure informatique et ses éléments de sécurité (entre autres) sont déterminés. Il s'agit notamment de définir la topologie (des réseaux et segments 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 du système de gestion.

En outre, des mesures devraient déjà être prévues à ce stade en cas de perturbations dues à une attaque.

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/points faibles

L'analyse des risques constitue la base de toute étude de projet portant sur les éléments de protection appropriés. Comme le risque n'est pas le même pour tous les bâtiments ni pour tous les systèmes de GTB, il est indispensable de procéder à une analyse des risques spécifique au projet. Celle-ci détermine l'étendue des mesures de sécurité à mettre en œuvre. Les facteurs à prendre en compte incluent le degré de vulnérabilité du bâtiment et l'étendue des fonctions de GTB : CVC, éclairage, portes (coupe-feu), systèmes d'accès, etc.

Séparation physique / segmentation des réseaux IP de GTB

Comme les systèmes de GTB modernes utilisent le standard IP (OSI, couche 3) comme base de presque toute leur communication, il est naturellement tentant, pour des raisons de coût, de partager l'infrastructure

réseau IP déjà existante d'un bâtiment. Cependant, notons que ceci ne constitue pas la meilleure option en termes de sécurité informatique pour le système de GTB. Indépendamment des éventuelles questions de performance et de disponibilité, la protection des réseaux ne peut pas s'adapter de manière optimale aux exigences de la GTB. En effet, les contraintes posées par d'autres applications doivent être prises en compte. De plus, cette utilisation partagée de l'infrastructure réseau permet à de nombreux utilisateurs de pénétrer directement dans le réseau de GTB par le biais d'éventuels accès supplémentaires (porteurs de risques correspondants).

Réseaux/segments 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 encore 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, ou 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 supplémentaires pour les programmes malveillants qui ne sont pas détectés par les machines concernées.

Une segmentation plus précise des réseaux concernés permet d'encore renforcer leur sécurité. Cette subdivision du réseau local permet à chacun des sous-réseaux d'être protégé à ses frontières par des pare-feu. Il est ainsi possible de mieux limiter l'impact négatif des machines touchées par un virus à l'intérieur du réseau local.

De nos jours, les pare-feu sont souvent intégrés au routeur dans le même appareil. Les fonctions des pare-feu sont en outre couvertes par des switch d'une intelligence croissante. Ces trois fonctionnalités sont de plus en plus souvent combinées dans des appareils toujours plus performants.

Connexions VPN pour les unités/îlots déportés

La connexion d'unités ou d'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 l'unité/îlot déporté(e) et le réseau/segment local interne à l'installation. Comme le nom l'indique, l'unité/îlot distant(e) est intégré(e) virtuellement à ce réseau/segment local. 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 (TLS), les personnes

non autorisées n'ont pratiquement aucune possibilité d'épier l'accès ou de le détourner à des fins malveillantes.

Sécuriser par VPN les unités déportées est non seulement intéressant pour les unités distantes (sur WAN/Internet) mais également pour les unités d'autres segments dans des réseaux plus importants.

Switch équipés de fonctions de sécurité

L'utilisation de switch avec fonctions de sécurité intégrées est particulièrement utile si, malgré les objections émises ci-dessus, une infrastructure réseau déjà existante doit être partagée entre le système de GTB et d'autres utilisateurs. Ces fonctions peuvent considérablement améliorer la sécurité des composants de GTB raccordés au réseau commun grâce au filtrage des 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 en outre en mesure de rassembler certains utilisateurs d'un même réseau (par ex. les utilisateurs du système de GTB) dans un VLAN. Ceux-ci communiquent ainsi au sein de leur propre réseau virtuel et ne sont alors visibles et accessibles pour les autres utilisateurs du réseau que si le routeur/pare-feu employé l'autorise explicitement.

Dans certains cas, ces switch peuvent être configurés manuellement à l'aide de White Lists/Black Lists. 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 permet d'empêcher 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 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 », dans lequel l'authentification a lieu via un seul mot de passe pour tous (Preshared Key), la variante « Enterprise » prend en charge des mots de passe différents, soit appartenant à des comptes utilisateur (LDAP/Active Directory, RADIUS), soit par le biais de 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 suffisamment longs et complexes sont utilisés et que le WPS est désactivé.

Protection contre les logiciels malveillants et actualisation pour PC

Outre la protection réseau, il faut également déterminer, lors de la phase d'étude de projet, quel type de protection contre les logiciels malveillants doit être installé sur l'ordinateur de gestion concerné. Pour que celui-ci reste durablement efficace, un concept d'actualisation applicable doit également être défini.

La protection contre les logiciels malveillants prévient l'action des virus informatiques, logiciels espion et chevaux de Troie connus, entre autres, et les élimine lorsque c'est possible. Étant donné que seuls les logiciels malveillants connus peuvent être détectés, il est important d'effectuer régulièrement les 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 faut s'attendre à ce que le 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 généralement être effectuée de toute urgence. L'existence dès le départ d'une procédure clairement définie et dotées de consignes de récupération pas à pas testées et mises en pratique au préalable (voir ci-dessous) constitue dans ce cas une aide précieuse.

Comme les fichiers de sauvegarde contiennent en général aussi des copies de données très sensibles, il est crucial de prévoir, dès l'étude de projet, un emplacement sûr où ils pourront être stockés. Il convient d'accorder une attention particulière notamment aux éléments contenant des informations de configuration système et des données de gestion des utilisateurs, qui peuvent présenter un grand intérêt pour un pirate avisé.

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

La sécurité physique du système, des armoires de commande et des équipements de communication ne sert pas seulement à prévenir les attaques malveillantes, mais aussi à bloquer tout accès négligent par des personnes non autorisées.

Dans le cadre de la cybersécurité, il convient surtout de mentionner la sécurisation des points d'accès physiques aux appareils, aux armoires de commande et aux dispositifs de communication. En aucun cas les ports (libres ou occupés) Ethernet, USB et de configuration destinés aux ordinateurs, aux UGL ou aux routeurs, par exemple, ne doivent être rendues accessibles.

Possibilités de fonctionnement d'urgence (sans GTB)

En cas d'attaque avec 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 se révéler hautement salvatrices.

Il en va de même pour les systèmes de verrouillage matériels intégrés aux installations techniques (par ex. 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 de l'étude de projet en matière de cybersécurité doivent être mises en œuvre et complétées. Tous les paramètres relevant de la sécurité (autorisations, exigences de mot de passe, ports, etc.) doivent être définis et les mesures de protection doivent, si possible, être testées afin de garantir leur bon fonctionnement. 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 sont adaptés (c'est-à-dire limités/minimisés) aux tâches des utilisateurs/groupes, plus le risque d'attaques ciblées est faible, ainsi que celui d'erreurs de fonctionnement involontaires. C'est le principe du « need-to-know » / « fonctionnalité minimale » qui s'applique ici par défaut. Il implique de n'autoriser l'accès qu'aux données et fonctions qui sont nécessaires à l'utilisateur en particulier, et à aucune autre.

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 permettent 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. La convivialité rivalise avec la sécurité, et il convient de rappeler que plus les exigences en matière de mot de passe sont grandes, plus la difficulté pour les utilisateurs augmente. Plus la graphie du mot de passe est longue et compliquée, plus l'utilisateur devra le changer souvent. Plus il aura de mots de passe différents à retenir, plus il ressentira la nécessité de les noter quelque part. Après tout, l'utilisateur emploie aussi des mots de passe dans sa vie privée ; 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. À un moment donné, il devient impossible de se souvenir de tous ses mots de

passe professionnels et privés, ce qui pousse souvent à tenir une liste de mots de passe sur son smartphone. On peut aussi noter ses mots de passe dans des gestionnaires de mots de passe gratuits plus ou moins sécurisés, les inscrire 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, un « (post-)durcissement » de tous les appareils (Linux) et 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 qui sont effectivement nécessaires au fonctionnement souhaité doivent rester sur les appareils. Plus le système sera léger, moins l'agresseur sera susceptible de trouver des outils utiles et plus sa tâche sera difficile.

Les PC sont particulièrement touchés. Les autres appareils (par ex. les UGL) 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 défaillance, des journaux de bord (journaux utilisateur), actifs et accessibles à tout moment, revêtent une importance capitale. Ils servent d'une part au suivi des connexions, et peuvent d'autre part simplifier considérablement la récupération du système ou des données en cas de panne.

Les journaux de bord doivent potentiellement être activés et configurés lors de la mise en service. 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 aussi être mis en place sur les systèmes d'exploitation des bases de données et les routeurs, ce qui permet d'optimiser la surveillance.

Comme il faut présumer qu'un agresseur particulièrement qualifié tentera d'effacer toute trace de son attaque dans les journaux utilisateur, il peut être opportun de sécuriser les journaux des installations sensibles par un mécanisme de signature numérique. La signature numérique protège les données enregistrées grâce à une clé de signature et empêche toute modification ultérieure.

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 conduite

Les étapes à suivre/règles de conduite définitives et testées (procédure opérationnelle permanente ou Standard Operating Procedure, POP)

concernant la cybersécurité doivent être présentes dès la mise en service de l'installation, et ce, sous deux aspects principaux. D'un côté, des étapes/règles doivent être prévues pour le fonctionnement normal, en vue de contribuer à ce que tous les mécanismes de sécurité soient opérationnels sur la longue durée et tenus à jour. De l'autre, des étapes/règles doivent s'appliquer en cas d'attaque/de panne, et contenir toutes les informations/étapes à suivre concernant la détection et la stratégie de réduction et de réparation des dommages.

Les étapes de travail/règles de conduite (POP) prévues pour le fonctionnement normal contiennent notamment des processus opérationnels, des check-lists et, idéalement, des fonctions de rappel de 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 surveillance a-t-il exercé son rôle ? Ces étapes de travail/règles de conduite constituent une des pierres angulaires de l'effort global de prévention ou de réduction des risques.

Si un événement venait à affecter le bon fonctionnement du système de GTB, il faut escompter 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 de toute urgence. Des règles de conduite claires et pratiques avec consignes pas à pas se révèlent dans ce cas être une aide précieuse. En plus d'apporter une aide à la récupération, elles peuvent également contenir des informations concernant les voies de signalisation, numéros d'appel, niveaux d'escalade, mesures d'urgence, etc.

Information à/formation de l'utilisateur

Dans l'exploitation quotidienne d'un 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 aussi les exploitants/utilisateurs du système, est ici d'une importance capitale.

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

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

Outre la formation technique des collaborateurs, 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.

Le fait de se pencher sur les thèmes relevant de la cybersécurité au sein d'une formation spécifique (indépendamment des autres thèmes) leur donne plus de poids. Il est également utile de rafraîchir régulièrement ces connaissances afin de maîtriser le sujet sur la durée et d'éviter les incidents. N'oublions pas non plus les séances d'information pour les nouveaux collaborateurs.

Les thèmes de la conduite et de la récupération après un incident méritent donc leur propre bloc de formation.

Éléments au niveau de la maintenance

Les techniques d'attaque d'installations informatiques sont en constante évolution. C'est également le cas des technologies de défense. Un système de GTB peut donc également continuer à se développer.

Il incombe aux techniciens de maintenance (en matière de 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. Ce n'est que de cette manière que les mécanismes de protection pourront faire face à l'évolution constante des techniques d'attaque.

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

Adaptations système relatives à 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.

Étant donné l'évolution des menaces qui planent sur les systèmes informatiques et mécanismes de sécurité de ces systèmes, il peut devenir nécessaire, en plus de maintenir les mesures de sécurité existantes, de procéder à des adaptations systèmes plus étendues et exhaustives.

Tests périodiques 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 aussi de périodiquement tester les procédures à effectuer 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 est également nécessaire de contrôler, à des intervalles réguliers et dans le cadre d'évaluations de la sécurité, que les exploitants/utilisateurs de l'installation respectent les codes de conduite informatique.

Éléments au niveau de l'utilisateur

Comme nous l'avons à présent maintes fois souligné, le niveau de sécurité informatique d'une installation de GTB ne peut être élevé et le demeurer 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. Ceux-ci sont les premiers à pouvoir signaler des événements anormaux.

Bonnes 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, le cas échéant, adapté au risque auquel l'installation est exposée.

En outre, les utilisateurs sont tenus de choisir des mots de passe aussi difficiles à pirater que possible. Cela implique d'exclure tout élément facile à deviner, comme le nom, le nom du partenaire/des enfants, la date de naissance, etc. Certains pirates (ou individus qui expérimentent ou cherchent à s'amuser) écrivent des algorithmes qui comparent les mots de passe avec des données personnelles, en vue de les pirater.

C'est avant tout la longueur, plus encore que la complexité, qui rend un mot de passe sûr. Par exemple, des phrases sont tout à fait adaptées, tant qu'il ne s'agit pas de citations célèbres par exemple. Elles présentent le grand avantage d'être plus faciles à retenir (par ex. « 1 x Sauter c'est toujours Sauter » ou « mon préféré est aussi le meilleur »).

Bien évidemment, les bonnes pratiques interdisent également 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 complètes des processus de sauvegarde automatisés. Il peut être nécessaire de 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 et 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 techniques tels que les topologies de systèmes, les concepts de sécurité, etc., y compris toutes leurs copies, constituent également des informations très attrayantes pour un individu mal intentionné, et doivent donc être conservés de manière adéquate.

Sensibilisation aux dangers/vigilance

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

Comme bien souvent, le facteur humain constitue le risque principal. 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 au niveau d'autorisation le plus élevé possible.

Processus et audits

Diverses organisations sont actives dans ce domaine. La norme CEI 62443 constitue par exemple une bonne référence, très étroitement liée à la série ISO 27000. Ces références portent sur divers aspects de la sécurité, depuis le développement des produits jusqu'à l'arrêt de leur production, en passant par leur cycle de vie complet. Elles prennent en compte les processus, le développement du produit, les utilisateurs du produit tels que les intégrateurs de systèmes, et enfin les utilisateurs finaux. La cybersécurité concerne tous ceux qui entrent en contact avec les produits et les systèmes. Il est important de définir un objectif clair et de mobiliser tous les moyens nécessaires pour l'atteindre. La sécurité informatique est un processus en constante évolution et doit pouvoir s'adapter aux menaces récurrentes et changeantes.

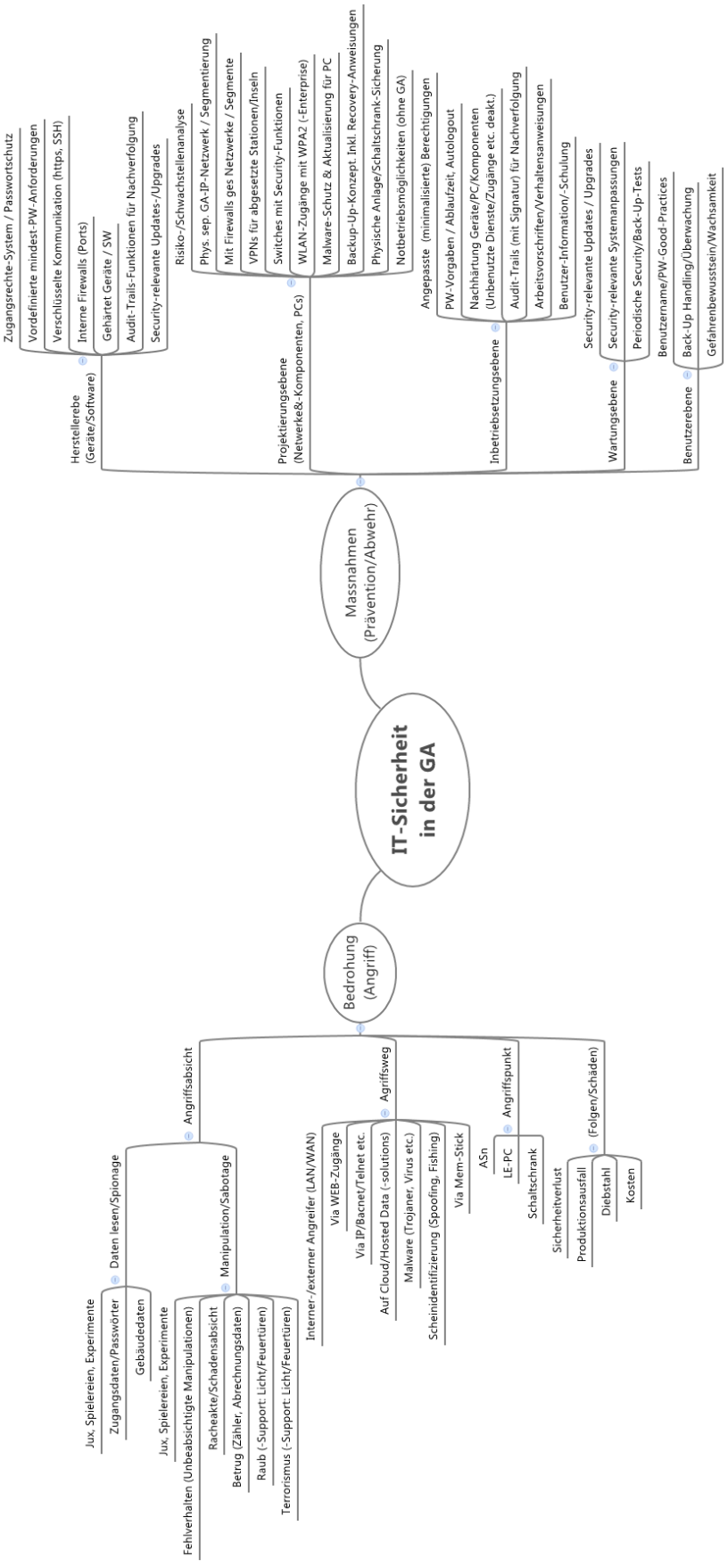

Fig. 3 : Menaces et contre-mesures de la sécurité informatique en GTB

4 Conclusion

L’éventail des actions possibles en matière de sécurité informatique d’une installation de GTB est énorme. Entre inaction et mise en œuvre de toutes les mesures envisageables, il existe une infinité de nuances. Entre « une installation dans laquelle n’importe quel informaticien ordinaire peut pénétrer » et « un système très complexe / presque impossible à déjouer, même pour un pirate expert aux intentions hostiles », tous les degrés de sécurisation sont possibles, avec les divers degrés d’effort et de coût qui en découlent.

L’évaluation du risque spécifique à chaque projet est un aspect central. À cet égard aussi, l’étendue des cas de figure est immense. Pour beaucoup de bâtiments, le danger se limite aux conséquences d’un penchant pour le ludique, les expérimentations techniques, les plaisanteries ou les essais hasardeux. Les bâtiments abritant des objets susceptibles d’être convoités ou pouvant servir de cible à des ennemis reconnus, ou encore les édifices publics importants et particulièrement vulnérables, sont en revanche exposés à des risques très sérieux.

Quel que soit le bâtiment, il est vivement recommandé de mettre en place des mesures de sécurité fondamentales et basées sur les derniers développements technologiques du secteur concerné. Elles permettent de contrer la plupart des attaques et de se protéger contre les conséquences des actes irresponsables évoqués plus haut. Elles contribuent également à prévenir les erreurs de manipulation qui, combinées à des erreurs logicielles que l’on ne peut jamais totalement exclure, restent la cause majeure des pannes.

Le facteur humain est, comme souvent, une source essentielle de risque. Accès opérateur avec un utilisateur qui reste connecté en permanence, mots de passe cachés sous le clavier, prêts ou échanges de mots de passe, accès administrateur par défaut qui n’ont pas été changés ; bref, manque de soin, de perception et de vigilance ! Des formations spécifiques et la communication régulière d’informations aux collaborateurs peut aider à le pallier.

L’auteur

Franklin Linder, ingénieur en électronique, 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 de gestion technique de bâtiments.

Portrait de l’entreprise

En tant que premier prestataire mondial de solutions pour la technologie d’automatisation des « Green Buildings », SAUTER assure le bien-être et le 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 une

exploitation optimisée en énergie 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 proposer le meilleur système d'automatisation, la meilleure prestation de service énergétique et certifié 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.

5 Références

[1]	VDMA, V. D.-u. (02/2021). VDMA 24774:2021-21. IT-Sicherheit in der Gebäudeautomation (Cybersécurité dans l'automatisation de bâtiments). VDMA, Verband Deutscher Maschinen- und Anlagenbau (Fédération allemande des ingénieurs).
[2]	CEI – Commission électrotechnique internationale (08/2013). Industrial communication networks – Network and system security – Partie 3-3 : System security requirements and security levels (éd. 1.0). Genève, Suisse : CEI, Genève, Suisse.
[3]	VDMA, Verband Deutscher Maschinen- und Anlagenbau (Fédération allemande des ingénieurs). (2016). Security in Automation – Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau (Profil des normes de sécurité informatique pour la construction de machines et d'installations). Produkt- und Know-how-Schutz (Protection des produits et du savoir-faire). Berlin : HiSolutions AG. Extrait de https://industrialsecurity.vdma.org/documents/16227999/16499033/1492086887896_INS_NAM_2016_Industrial_Security_CEI62443.pdf/c2e80bdb-c820-42cb-b3cc-fedd68571e1e
[4]	ZVEI, Zentralverband Elektrotechnik- und Elektronikindustrie (Association centrale de l'industrie électrotechnique et électronique) (2017). Orientierungsleitfaden für Hersteller (Guide de référence pour les fabricants) CEI 62443, Francfort-sur-le-Main : ZVEI. Extrait de ZVEI, Zentralverband Elektrotechnik- und Elektronikindustrie : https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_CEI_62443/Orientierungsleitfaden_fuer_Hersteller_CEI_62443.pdf
[5]	Cybersecurity for modulo 6. An Overview. Implementing CEI 62443 for Building Automation. 11/2019, 5^{e} révision, Fr. SAUTER AG. https://extranet2.ch.sauter-bc.com/wp-content/uploads/sites/13/2020/01/1071060-26.pdf

6 Répertoire des abréviations

Abréviation	Terme
par ex.	par exemple

7 Index

L

M

O

P

R

S

T

U

V

W