LE MONITEUR
DES TRAVAUX PUBLICS ET DU BÂTIMENT

PAYS : France
PAGE(S) :12-14
SURFACE :257 %
PERIODICITE : Hebdomadaire

DIFFUSION :40642
JOURNALISTE : Fabrice Debiock

► **23 octobre 2020 - N°6108**

Cybersécurité

Le bâtiment connecté, talon d'Achille de la ville intelligente

La faible protection des smart buildings contre les cyberattaques fait redouter les pires scénarios. Une crainte renforcée par une législation ad hoc inexistante.

En janvier 2017, un rançongiciel a neutralisé le système de sécurité du Romantik Seehotel Jägerwirt, un établissement quatre étoiles situé dans les Alpes autrichiennes. Cette attaque a désactivé le dispositif de clés électroniques, empêchant les vacanciers de pénétrer dans leur chambre. En échange d'une rançon de 1500 euros payée en bitcoins, l'hôtel a pu reprendre la main sur ses serrures mais aussi sur sa caisse et son système de réservation.

Le scénario de touristes mis à la porte de leur chambre peut prêter à sourire. Mais appliqué à une tour de 50 étages par exemple, il devient beaucoup plus inquiétant. « Ce que nous craignons le plus, c'est une prise en mains à distance de la gestion technique du bâtiment, avance Pascal Zératès, directeur général de Kardham Digital, filiale du groupe Kardham spécialisée dans les technologies digitales appliquées à l'immobilier d'entreprise. Un scénario catastrophe consisterait à déclencher le système d'alarme de la tour tout en bloquant les issues de secours, avec un chauffage poussé à 50 °C et toutes les lumières éteintes. Cela pourrait entraîner des situations de panique et donc des drames humains. »

Si l'on étend le raisonnement aux villes intelligentes, les réactions en chaîne deviendraient rapidement apocalyptiques. On peut ainsi imaginer qu'un black-out énergétique survienne ou que des pirates prennent la main sur les panneaux d'affichage électronique, diffusant des messages erronés qui perturberaient la gestion d'une crise.

Auteurs de science-fiction. Lors de l'édition 2019 de la conférence Le Hack, à Paris, deux ingénieurs en sécurité informatique ont raconté qu'au cours d'un audit réalisé dans plusieurs villes européennes, ils avaient réussi à utiliser une armoire servant à la gestion des feux de signalisation pour se connecter à un réseau de caméras de surveillance et ce, sans être inquiétés et ni avoir à entrer le moindre mot de passe. Preuve que ces scénarios sont pris au sérieux, l'armée française a lancé, l'année dernière, le recrutement d'auteurs de science-fiction pour l'accompagner dans ses missions de prospective et d'anticipation des menaces à l'horizon 2030-2060. Parmi les sujets sur lesquels ces écrivains travaillent, la cybersécurité figure en bonne place.

Une étude de l'éditeur de logiciels de sécurité Kaspersky, publiée début 2019, a scruté 40 000 bâtiments connectés dans

INGEROP

« La maquette numérique doit être protégée dès sa création »

« Les processus d'ingénierie numérique (BIM, CIM et PLM) agrègent un grand nombre de données autour d'une composante commune : la maquette numérique. En raison de son caractère stratégique, celle-ci doit être protégée dès sa création afin d'éviter qu'un pirate ne s'en saisisse pour préparer une cyberattaque. Pour cela, nous avons conçu ScredIN, une solution grâce à laquelle la connaissance et la compréhension de toutes les informations structurant un projet sont protégées. A tout moment, tout ou partie de la maquette numérique peut être anonymisé en fonction des intervenants. L'humain demeure en effet un risque majeur dans ce domaine. Chaque personne (collaborateur, intérimaire, stagiaire, prestataire…) ne doit avoir accès qu'aux informations dont elle a véritablement besoin. Nous garantissons aussi que les données ne sont pas stockées à l'étranger. »

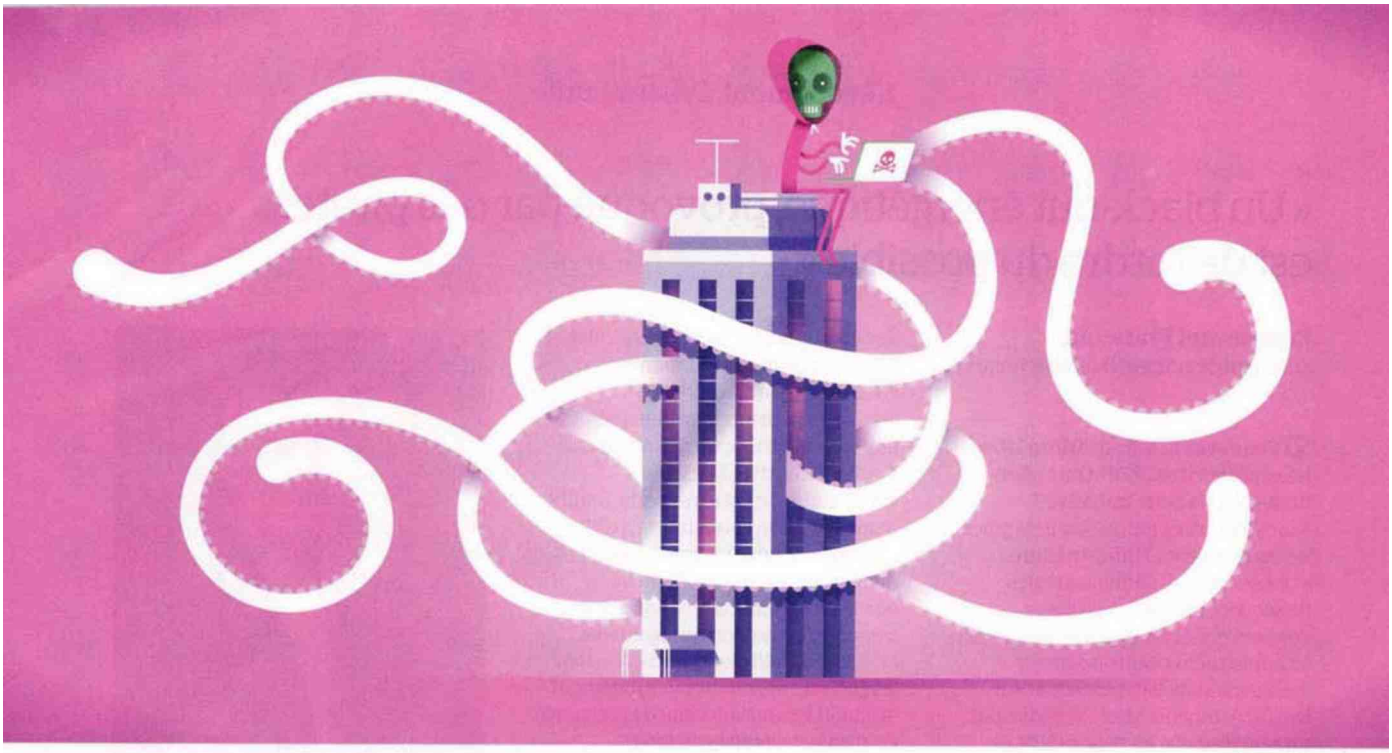
Rémi Brulurut, chef de service BIM et développement numérique chez Ingérop.

LE MONITEUR
DES TRAVAUX PUBLICS ET DU BÂTIMENT

PAYS : France
PAGE(S) :12-14
SURFACE :257 %
PERIODICITE : Hebdomadaire

DIFFUSION :40642
JOURNALISTE : Fabrice Debiock

► **23 octobre 2020 - N°6108**



PHILIPPE DEBRIEN

le monde. Résultat : 37,8 % d'entre eux avaient été confrontés à des cyberattaques. Dans la plupart des cas, une seule machine contrôle l'intégralité des systèmes : accès au bâtiment, ventilation, éclairage, fourniture d'eau, ascenseurs... Cet ordinateur, connecté à Internet, est donc aussi vulnérable qu'un PC familial. Les logiciels espions (spywares), l'hameçonnage (phishing) et autres rançongiciels (ransomwares) trouvent donc dans le smart building un extraordinaire terrain de jeu. Autre donnée révélée par cette étude : plus de deux tiers des bâtiments attaqués l'ont été depuis le web, tandis que les lecteurs amovibles (clés USB, disques durs externes...) ont ciblé un quart de ces smart buildings, tout comme les logiciels de messagerie (via des pièces jointes ou des liens insérés dans les e-mails).

Ségrégation des réseaux. Des mesures préventives doivent donc être prises dès la conception d'un bâtiment connecté. « Avant toute chose, il est impératif de cloisonner les deux principaux réseaux d'un bâtiment : le réseau IT, qui permet de gérer l'activité des entreprises ou des personnes présentes dans l'immeuble, et le réseau OT, qui regroupe toutes les technologies dites opérationnelles : réseaux d'énergie, capteurs, objets connectés... Cela permet d'éviter de corrompre le réseau opérationnel quand le réseau informatique est touché et, inversement, d'empêcher un pirate de progresser vers le réseau IT quand une faille est exploitée sur un objet connecté du bâtiment », expose William Culbert, directeur EMEA Sud de l'éditeur de logiciels BeyondTrust, spécialisé dans la gestion des accès privilégiés. Cette approche dite de « ségrégation » des réseaux est aujourd'hui la règle dans de nombreux secteurs d'activité, notamment dans l'industrie. La stratégie de défense et de sécurisation diffère en effet selon les réseaux : l'IT doit protéger la confidentialité des données, l'OT doit assurer la continuité de processus comme la climatisation, le chauffage, la fourniture d'électricité ou le contrôle des accès.

Mais la multiplication des objets connectés conduit à une certaine convergence entre l'IT et l'OT, ce qui rend de plus en plus poreuse la frontière entre les deux univers. « La ségrégation IT/OT reste un principe de base, un principe fort. Mais si toutes les technologies convergent vers un protocole de communication commun, les deux réseaux pourront à terme être interconnectés, voire fusionner », note Samy Tadjine, expert en cybersécurité industrielle chez Kaspersky.

« Arrêter de produire des objets à la va-vite ». Pour limiter les risques de cette convergence, encore faut-il que tous les objets connectés, à l'interface des deux mondes, soient suffisamment sécurisés. Selon une étude publiée début 2020 par Palo Alto Networks, autre société spécialisée en cybersécurité, 57 % des objets connectés utilisés par les entreprises sont vulnérables à des attaques de gravité moyenne à élevée. « Le plus souvent, ces produits sont conçus sans intégrer la moindre couche de sécurité, sans respecter la moindre bonne pratique sécuritaire, déplore Bertrand Trastour, directeur des ventes BtoB chez Kaspersky. Les fabricants pourraient utiliser un système d'exploitation sécurisé ou permettre de recevoir des mises à jour régulières. Il faut arrêter de produire de tels objets à la va-vite. Une serrure connectée, par exemple, si elle n'est pas sécurisée "by design" [dès sa conception, NDLR], c'est la catastrophe assurée. »

105,8 Mds €
Marché des smart buildings en 2024.
(Source : MarketsandMarkets)

2500 Mds €
Marché des villes intelligentes en 2025.
(Source : PwC)

Cartographier le réseau d'un bâtiment connecté ou d'une smart city doit permettre d'identifier l'ensemble des éléments qui les constituent et, par là même, les menaces potentielles. « Sans cette étape préalable, il n'est pas possible d'adopter une stratégie différenciée en fonction des risques, estime Bertrand Trastour. Si vous avez des objets connectés non sécurisés ou de vieux systèmes d'information faisant tourner des applications critiques →

LE MONITEUR
DES TRAVAUX PUBLICS ET DU BÂTIMENT

PAYS :France
PAGE(S) :12-14
SURFACE :257 %
PERIODICITE :Hebdomadaire

DIFFUSION :40642
JOURNALISTE :Fabrice Debiock

► 23 octobre 2020 - N°6108

« Un black-out énergétique, provoqué par des pirates, est de l'ordre du possible »

Emmanuel François,
président de la Smart Buildings Alliance.

Vous avez lancé en 2018 le label Ready2Services (R2S). Quel bilan tirez-vous de cette initiative ?
Ready2Services repose sur trois piliers : les équipements, l'infrastructure et les services. Il définit les règles de sécurité relatives aux objets connectés mais aussi à leur installation, à l'infrastructure sous-jacente et à la maintenance/exploitation. Sur les 100 bâtiments testés à ce jour, pas un seul n'est allé au-delà de 55 % de conformité à ce cadre. Nous sommes donc encore très loin de l'objectif. C'est la raison pour laquelle nous travaillons à une version 2 qui devrait voir le jour d'ici à la fin de l'année. Nous souhaitons également sortir une version S+ (Sécurité+) dédiée aux bâtiments et territoires stratégiques, comme les sites Seveso, les établissements recevant du public... La task force que nous avons créée est, d'emblée, internationale, car la solution ne peut pas être uniquement française ; elle doit être, a minima, européenne.

Y a-t-il urgence en la matière ?
Nous assistons actuellement à une multiplication des attaques informatiques, via des rançongiciels qui touchent des collectivités, des hôpitaux... Le jour où les pirates s'intéresseront aux bâtiments intelligents et à la smart city, les dégâts pourront être bien plus importants qu'une simple rançon. Prenez le cas d'un black-out énergétique. Selon les experts, il suffit d'une variation soudaine de 3 GW pour provoquer un effondrement du réseau électrique à l'échelle européenne. Cela correspond à environ un million de logements ou à 10 000 bâtiments tertiaires pour lesquels on augmenterait subitement le chauffage ou l'intensité de l'éclairage. Ce risque s'accroît également avec l'arrivée de nouvelles bornes de recharge : le déploiement de 100 000 d'entre elles est prévu d'ici à 2022.

Où en est la législation sur ces thématiques ?
Aujourd'hui, quand on s'intéresse au cadre juridique qui accompagne la numérisation des bâtiments, nous sommes face à un vide sidéral, au même titre que pour la cybersécurité d'ailleurs. Les réglementations existantes sont encore conçues en silos alors que le numérique repose sur une approche transversale qui lie tous les acteurs de la chaîne de valeur. Nous devons tout repenser. Cette refondation touche notamment la garantie décennale d'un bâtiment

GUILLAUME ATGER / LE MONITEUR

connecté. J'appelle d'ailleurs tous les assureurs à s'intéresser à ces questions. La transition numérique leur offre une formidable opportunité de maîtriser les risques et donc de contribuer au déploiement de la valeur. Au-delà, les bureaux d'études doivent eux aussi s'impliquer dans le risque cyber. Ils se limitent encore trop souvent aux règles et standards existants. ● **Propos recueillis par F. D.**

pour votre bâtiment, il faut les traiter à part. En revanche, les produits fonctionnant sous des systèmes d'exploitation récents, sécurisés, doivent être intégrés à la stratégie de sécurité globale du bâtiment. Cette dernière peut comporter, selon les cas, un outil de gestion de l'information des événements de sécurité (security information and event management, SIEM) ou un centre opérationnel de sécurité (security operations center, SOC). »

Ainsi, Kardham Digital a noué un partenariat avec l'éditeur français de logiciels de cybersécurité Wallix, pour construire une offre dédiée au marché du smart building. « Nous adressons les trois piliers de la chaîne de valeur : simplification du parcours de l'utilisateur, pilotage énergétique et pilotage cybersécuritaire du bâtiment. Sur ce dernier volet, Wallix nous accompagne sur le design, l'exploitation et la maintenance d'un SOC », déclare Pascal Zératès.

Vide juridique. Quant à la législation, elle est quasiment inexistante comme le déplore Emmanuel François, président de la Smart Buildings Alliance *(lire ci-dessus)*. A l'étranger, certains législateurs commencent à prendre le problème à bras-le-corps. C'est le cas de la Californie qui, en 2018, a adopté une loi relative aux objets connectés. Cette dernière impose aux fabricants d'équiper leurs produits avec des mesures de sécurité « raisonnables ». Cela signifie notamment que le mot de passe préprogrammé doit être unique pour chaque appareil vendu. Les mots de passe par défaut, tous identiques, sont donc interdits. Un espoir, bien maigre, face à une menace toujours plus inquiétante... ● **Fabrice Deblock**