CYBERSÉCURITÉ

COMBATTRE DE NOUVEAUX RISQUES ÉMERGENTS

Photo © AdobeStock

TEXTE : **FRANÇOIS PLOYE**
PHOTOS : **ADOBESTOCK, ALDES, CEDEO, JPM, UNITECNIC**

Avec le développement des objets connectés et du smart building, avec l'accélération de la transition numérique en général, la cybersécurité doit être prise en compte par tous les métiers du secteur du bâtiment.

Tous les équipements communicants, les logiciels ou systèmes connectés, les stockages distants de données, sont concernés par le risque d'attaque informatique. Le développement des réseaux IP (Internet protocol) branchés en continu sur Internet, la dissémination des objets connectés, mais aussi les échanges croissants de données numériques ont entraîné le développement des risques « cyber ». Une spécificité du secteur du bâtiment réside en outre dans l'utilisation de la maquette numérique BIM dont la confidentialité et l'intégrité des données doivent être assurées, ainsi que la traçabilité des échanges, que ce soit pour le travail collaboratif au bureau, sur chantier via la réalité virtuelle et augmentée ou en phase d'exploitation. « *L'attaque n'est pas forcément ciblée et motivée par l'intérêt du bâtiment, il peut s'agir de cybercriminalité opportuniste. Un virus par exemple ne cible pas en fonction de l'intérêt. Le monde des objets connectés à Internet demeure le plus exposé mais la sécurité s'améliore* », assure Yves Duchesne, expert en cybersécurité et CEO (Chief executive officer) de la société d'expertise Acceis. Chaque métier du bâtiment est mobilisé dans le cadre d'une politique globale de sécurité informatique, soit dans sa gestion et ses échanges quotidiens de données numériques, soit dans la mise en œuvre ou la maintenance d'équipements et de systèmes connectés. Cette politique doit être réfléchie dès le départ d'un projet et mise en œuvre soigneusement sur le terrain avec des mises à jour régulières et des audits fréquents. La défaillance peut venir d'une négligence humaine basique comme laisser le mot de passe par défaut ou en mettre un trop facile à craquer.

Des précédents inquiétants

Si tous les jours, les systèmes informatiques subissent de multiples attaques, la quasi-totalité sont heureusement stoppées par les sécurités et protections type pare-feu et rendues inopérantes par la cryptographie des données. Néanmoins, les menaces sont si diverses qu'un acronyme leur a été donné, celui de Stride pour Spoofing (falsification), Tampering (altération), Repudiation (répudiation), Information disclosure (divulgation de l'information), Denial of service (déni de service) et Elevation of privilege (élévation de privilèges). Ces attaques peuvent déboucher sur de l'espionnage, de la destruction, du chantage, du sabotage, du vol ou de la destruction de notoriété.

Rares sont les attaques réussies qui sont rendues publiques. Début 2017, les responsables de l'hôtel de luxe autrichien Seehotel Jägerwirt ont choisi eux de communiquer sur une mésaventure assez courante dans la profession. Lors du week-end d'ouverture de la saison d'hiver, les 21 et 22 janvier, avec un hôtel complet, tout le parc informatique (réservations, système de clés électroniques pour entrer dans les chambres, paiement) a été paralysé par des hackers qui ont demandé une rançon en bitcoins de 1 500 dollars payables sur le darkweb. Si les portes des chambres pouvaient s'ouvrir manuellement, le fonctionnement de l'hôtel était paralysé et la direction a préféré payer la rançon. Ces attaques de type « ramsonware » peuvent aussi ▷▷▷

toucher les particuliers. Par exemple, un thermostat connecté qui est mis à jour via un serveur peut être piraté. « *Une rançon en "bitcoin" est alors exigée. La défaillance peut venir du constructeur de thermostat via des failles dans le produit ou de l'installateur qui doit vérifier l'équipement, authentifier la connexion, changer les paramètres de base...* », détaille Mathieu Gallissot, expert au Laboratoire d'électronique et de technologie de l'information (Leti) du CEA.

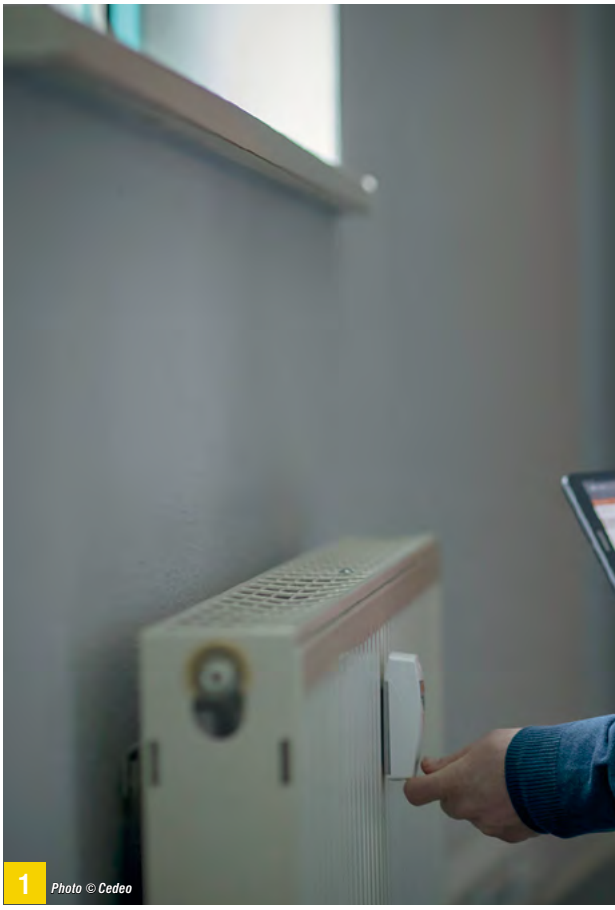
Un danger sans frontières

En étant connectés, les équipements (chaudières, thermostats, serrures, vidéosurveillance, systèmes de ventilation, etc.) deviennent des cibles et peuvent à leur tour contaminer les autres réseaux du bâtiment. Les objets connectés mal sécurisés peuvent être contrôlés et mobilisés par les pirates pour lancer des cyber-attaques massives sur une cible, par une attaque de type DDOS dite « déni de service distribué ». Un cas connu est celui du logiciel malveillant *Mirai* qui a mené plusieurs attaques à grande échelle en 2016 dont une sur l'hébergeur français OVH, en contrôlant à distance des dispositifs grand public tels que des caméras pilotables à distance ou encore des routeurs domestiques. « *Les modems de chaufferies peuvent être piratés pour envoyer des SMS en masse qui dépassent le forfait défini avec le fournisseur télécom. Un de nos clients a ainsi eu une soixantaine de chaufferies piratées et a dû payer 50 000 euros de SMS sur six mois après avoir négocié avec son fournisseur télécom. Un pirate à l'autre bout du monde peut aussi couper le chauffage, ce qui peut être dommageable pour une crèche ou une maison de retraite* », met en garde Cédric Castella, chef de marché chez Lacroix-Sofrel. Il faut aussi prévoir que la propre défaillance d'une entreprise peut entraîner un dommage chez un de ses clients. « *Par exemple avec un hacking via le système de domotique et de surveillance, via des objets connectés ou un coffre-fort électronique, l'entreprise peut se faire attaquer et contaminer une autre entreprise de son écosystème. Le chauffagiste peut être piraté et hacké et chez un de ses clients, comme une résidence collective, la température des logements peut être augmentée, entraînant un surcoût de facture* », confie Nathalie Acas, souscripteur-concepteur au département des Branches spécialisées de la mutuelle SMABTP.

Risque sur le réseau électrique

Les risques peuvent potentiellement être de plus grande ampleur comme l'ont montré plusieurs chercheurs. En août 2018, Saleh Soltan de l'Université de Princeton a communiqué les résultats d'une étude montrant qu'en piratant seulement 42 000 chauffe-eau électriques connectés, les pirates informatiques pouvaient effondrer 86 % du réseau électrique polonais. Via une cyberattaque, les hackers peuvent se constituer un réseau de machines zombies (« botnet ») de type systèmes d'air conditionné, chauffages ou encore chauffe-eau afin de provoquer une hausse subite et artificielle de la consommation énergétique d'un réseau électrique donné. Ils pourraient ainsi sur une zone géographique déterminée provoquer une panne de courant généralisé. Déjà, en 2016, des chercheurs israéliens et canadiens avaient démontré qu'il suffirait à un pirate de propager un virus sur un peu plus de 15 000 ampoules connectées, via le protocole de communication sans fil *Zigbee* lors d'une mise à jour, pour en prendre le contrôle. En les allumant simultanément, le réseau électrique d'une ville d'une dimension de Paris pourrait s'effondrer.

"En étant connectés, les équipements (chaudières, thermostats, serrures, vidéosurveillance, systèmes de ventilation, etc.) deviennent des cibles et peuvent à leur tour contaminer les autres réseaux du bâtiment"



1 Photo © Cedeo

▲

1 Cedeo propose aux installateurs *Temperly*, une solution de répartition de frais de consommation de chauffage ou d'eau d'une résidence collective, fonctionnant avec des compteurs *Qundis*. Les données télérelevées via une passerelle toutes les deux minutes sont anonymisées et ne peuvent pas servir aux hackers.

▶

2 *T.One AquaAIR* d'Aldes, une pompe à chaleur multifonction pour le chauffage par l'air, le rafraîchissement et la production d'eau chaude, pilotable depuis le smartphone.

Analyser les risques des objets connectés

La prolifération des objets connectés a entraîné des risques cyber supplémentaires. Les chercheurs ont déjà démontré que tous les objets, depuis le pacemaker jusqu'à la voiture autonome, peuvent être piratés. Les objets connectés du bâtiment (chaudière, thermostats, ascenseurs, automates pour la ventilation, système de sécurité incendie, caméras de vidéosurveillance, etc.) ne sont pas davantage à l'abri. Leurs défaillances peuvent avoir de multiples causes d'autant que chaque objet diffère en protocoles (capteurs, systèmes d'exploitation, etc.), et l'évaluation de l'efficacité de sa protection demande des tests spécifiques. Sur les objets autonomes électriquement, la priorité est à l'économie d'énergie pour garantir cette autonomie, ce qui fait que la puissance de calcul embarquée peut se révéler insuffisante pour assurer un chiffrement (cryptage) efficace. De plus, la faible bande passante disponible ne facilite pas les mises à jour à distance. Par ailleurs, de très nombreux acteurs – dont des start-up – veulent se positionner sur un marché ▷▷▷

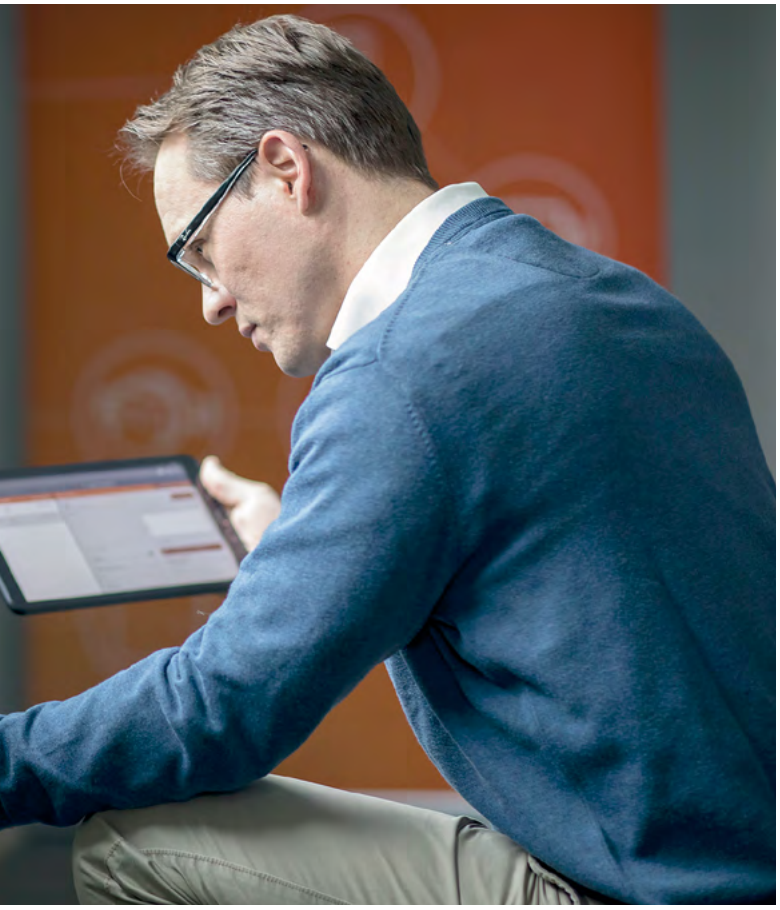


Photo © Aldes 2

NORMES PRODUITS ET CERTIFICATIONS

La spécificité des systèmes et des équipements dans le bâtiment est d'avoir une durée de vie assez longue, or dès qu'ils sont connectés, il existe un risque cyber. L'ennemi est le taux de renouvellement assez lent des équipements par rapport à l'évolution des technologies.

« *Un groupe de travail est en place dans le cadre du Cyber Act via la Communauté européenne pour certifier les objets connectés avec des avis de sécurité. De plus, les installateurs peuvent se référer au label R2S (Ready2Services) pour les prestataires, défini par la SBA (Smart buildings alliance) et Certivéa. Pour le résidentiel, la reconnaissance "prestataire Smart Home de confiance" co-défini par la FFD (Fédération française de domotique) et l'Afnor intègre déjà des notions de confiance numérique. L'installateur doit envoyer de la documentation à l'Afnor pour montrer qu'il a une démarche structurée avec un certain nombre de points mis en place qui sont définis dans le référentiel* », complète Mathieu Gallissot du CEA-Leti. Le label R2S en particulier apporte des réponses concernant les procédures de sécurité, la mise en place des mécanismes de surveillance des trafics et des logiciels malveillants, la sécurisation des accès aux systèmes et le chiffrement (cryptage) des communications.

Afin d'améliorer la qualité d'objets ou de systèmes connectés, les fabricants peuvent s'appuyer dans le développement de leurs produits sur des normes liées à la sécurité des systèmes d'information en général tels que l'ISO 27001 et l'ISO 27002 au niveau international, ou les recommandations de l'Anssi (Agence nationale de la sécurité des systèmes d'information) au niveau national. Ainsi il y a deux ans, le fabricant Lacroix-Sofrel a sorti une nouvelle plateforme technique (un superviseur) pour l'eau puis fin 2018 pour l'énergie. C'est le résultat d'un travail mené avec l'Anssi qui a défini deux niveaux de protection, un premier niveau de certification si le système est conforme aux cahiers des charges et un second niveau dit de qualification où sont réalisés des tests de hacking. Le processus long et coûteux est généralement réservé aux installations critiques ou opérateurs d'importance vitale (OIV) comme le traitement de l'eau.

« *Notre plateforme technique est en cours de qualification pour les chaufferies. Seuls étaient qualifiés au sens Anssi pour l'instant des produits trop puissants pour être utilisés en chaufferie. Notre produit sera le premier à être qualifié pour chaufferie* », met en avant Cédric Castella, chef de marché chez Lacroix-Sofrel. ■

jugé prometteur avec un résultat variable. La sécurité n'est pas toujours leur priorité lorsque l'accent est mis sur le développement accéléré d'un produit attractif en design, en fonctionnalités et en autonomie. « *Au CEA-Leti nous travaillons suivant deux axes. Le premier est celui de la protection des personnes car le connecté entraîne de nouveaux risques et de nouvelles surfaces d'attaque, qui nécessitent de développer des contre-mesures face à la cyber-malveillance* », confie Mathieu Gallissot. Les équipes du Leti comme d'autres équipes de chercheurs travaillent à l'échelle de l'objet connecté pour assurer sa protection, par un mécanisme d'authentification et un algorithme robuste de chiffrement de la communication par cryptographie. La mise à jour doit aussi être prévue car le chiffrement peut être facilement craqué sur les objets qui ont 10 à 15 ans d'existence et qui sont protégés par un ancien protocole.

« *Deuxièmement, le souhait des utilisateurs est que la cybersécurité apporte de la stabilité, de la confiance dans les données et, dans le cas du résidentiel, que la vie privée soit protégée. Plus que de sécurité, on parle davantage de confiance numérique* », continue Mathieu Gallissot. La mise en application du Règlement général sur la protection des données (RGPD) au 25 mai 2018 en France et en Europe a eu pour but de créer ce cadre de confiance numérique sur la protection des données personnelles avec une transparence et une traçabilité. L'enjeu est de mettre un niveau de protection suffisant en regard des risques encourus.

« *Cela a un coût, il faut établir des priorités via une analyse de risques. Par exemple est-ce que le niveau de sécurité d'un protocole est suffisant pour un bureau, un magasin, un hôpital ? Déterminer le risque le plus important permet de prendre les bonnes contre-mesures. En résidentiel, l'enjeu est la protection des données, dans l'industrie, la protection des process et pour les hôpitaux qui sont fréquemment visés, il faut qu'ils demeurent en état de fonctionnement* », poursuit Mathieu Gallissot. Il est bénéfique de bien analyser le risque et les impacts pour cibler et chiffrer le coût des protections à mettre en place. Les mécanismes de protection, la robustesse des mécanismes de cryptographie et d'authentification est une course technologique permanente. C'est le cas par exemple pour les objets communicants à faible débit. Des travaux de recherche portent sur les algorithmes de cryptographie allégée. Pour ceux disposant d'une très faible capacité de traitement, un agrégateur (ou « passerelle ») va les relier et assurer une partie des calculs et leur fournir des services. Parmi les pistes explorées figurent aussi l'algorithme de la blockchain utilisé pour sécuriser les transactions du bitcoin. Cette technologie pourrait être exploitée pour sécuriser les données issues des objets connectés. Plusieurs initiatives ont été lancées dans cette voie, dont une initiée par la start-up SmartHab dont l'idée est d'héberger et de sécuriser sur leur plate-forme avec une blockchain toutes les données relatives aux objets connectés au cloud et gérés à l'échelle d'un bâtiment ou sur un ensemble de bâtiments. Contrairement aux algorithmes du bitcoin, la blockchain implémentée ici est peu gourmande en énergie avec un protocole de type Ethereum.

3 Photo © Unitecnic

Photo ©JPM 4

Vigilance pour le contrôle d'accès

« *Le principal talon d'Achille de la politique cybersécuritaire est le contrôle d'accès qui est la technologie clairement la plus attaquée par les pirates. Les systèmes sont généralement installés par les électriciens qui ne maîtrisent pas forcément la sécurité. En fonction de la technologie de contrôle d'accès, il est possible de copier un badge ou de le pirater pour ouvrir la porte* », assure Yves Duchesne (Acceis). L'évolution du marché mondial d'ici 2025 est dessinée dans une nouvelle étude intitulée *Le contrôle d'accès en 2018*, réalisée par Ifsec Global et IHS Markit et sponsorisée par le fabricant Assa Abloy (1). L'étude se focalise sur les technologies sans fil, une technologie mise en avant par Assa Abloy au travers de ses solutions. 22 % des systèmes de contrôle d'accès installés dans les entreprises sont désormais mixtes filaires et sans fil et la part des systèmes 100 % câblés ne fait que chuter. Plus coûteux, les dispositifs sans fil sont plus simples à installer et ne nécessitent ni alimentation ni câblage système, les rendant particulièrement appréciés dans l'existant. Néanmoins, si les installateurs sont favorables au sans-fil qui simplifie leur pose, leurs clients sont davantage réticents. L'usage de smartphones comme identifiant d'accès en remplacement des badges plastiques est encore balbutiant. En effet, les responsables de la sécurité informatique dans les entreprises ont des inquiétudes concernant la sécurité d'utilisation du Bluetooth, ainsi que la grande diversité de systèmes d'exploitation et de protections informatiques installées sur les téléphones des utilisateurs. Une réponse est de restreindre l'usage en contrôle d'accès à des équipements mobiles (téléphones et tablettes) définis et gérés par l'entreprise. En résidentiel, un exemple datant de 2016 mais instructif est celui des chercheurs américains Anthony Rose et Ben Ramsey, qui ont présenté au salon Def Con 24 de Las Vegas le résultat de tests d'effraction réalisés sur seize serrures connectées qui s'ouvraient en communiquant via le protocole *Bluetooth Low Energy* avec le smartphone de l'utilisateur (celui-ci ayant préalablement téléchargé une application et entré un mot de passe). Ils ont pu ouvrir 12 de ces 16 serrures, par une attaque informatique assez simple en communiquant suivant le protocole *Bluetooth* utilisé par les serrures. Une des failles les plus grossières chez quatre de ces douze serrures était l'envoi du mot de passe en clair sur le smartphone, et il était même possible sur deux de ces serrures de changer le mot de passe initial et ainsi bloquer l'accès à l'utilisateur légitime. À noter en parallèle qu'une des quatre serrures ayant résisté pouvait être ouverte assez simplement avec un tournevis... Pour les chercheurs, une explication réside dans le fait que certains fabricants privilégient la robustesse mécanique de leurs serrures connectées au détriment de leur inviolabilité informatique. « *Nous intervenons comme assistance à maîtrise d'ouvrage sur les projets pour fournir des briques de cybersécurité. Il nous est aussi possible de rechercher les vulnérabilités d'une installation avant livraison. La prestation dite "red team" sert à tester en grandeur nature la robustesse de la protection avec une vraie attaque informatique et une tentative physique d'intrusion dans les locaux...* », complète Yves Duchesne (Acceis).

3 L'application de contrôle d'accès *DOM ENiQ* d'Unitecnic a obtenu, avec son niveau de cryptage extrêmement élevé, la certification VdS 2 étoiles de l'organisme de certification allemand.

4 Le système de contrôle d'accès sans fil *SMARTair* de JPM (Groupe Assa Abloy) s'installe sur toutes portes existantes pour le résidentiel ou le tertiaire, et peut s'utiliser avec un smartphone. Il utilise pour la communication des données plusieurs niveaux de cryptage (SSL, AES128).

(1) L'étude est téléchargeable sur www.assabloy.fr.

Protéger les automates

Les automates connectés qui contrôlent les équipements du bâtiment constituent un point de vigilance de la sécurité informatique. Typiquement, la télégestion et le contrôle à distance se font avec un boîtier connecté dans la chaufferie et un automatisme précis, un système qui permet le suivi d'exploitation et le pilotage des circuits de distribution. Auparavant, la connexion se faisait par intermittence avec une carte de communications RTC par téléphone. « *La fin des réseaux analogiques et l'arrivée du tout IP est un grand changement. Maintenant la connexion se fait par carte Ethernet (via box ADSL), ou en moins coûteux par modem GSM et carte SIM (2G ou 3G). Nous avons ainsi des clients qui peuvent avoir de très grands SCADA (supervisory control and data acquisition) (2) ou de l'hypervision (3), des équipements qui sont connectés en permanence sur IP et peuvent subir une attaque soit orientée, soit aléatoire* », explique Cédric Castella (Lacroix-Sofrel). Filiale du groupe industriel Lacroix, Lacroix-Sofrel est un spécialiste de la télégestion et fabrique, conçoit et commercialise des automates pour les réseaux d'eau potable et d'assainissement ainsi que pour les réseaux de chaleur et les chaufferies diffuses.

Construire une architecture solide

La cybersécurité passe par des mesures de niveaux de complexité croissante, conseille Cédric Castella. À la base, de bonnes pratiques sont nécessaires. Chaque technicien doit se connecter avec son compte individuel. Il ne faut pas de compte générique et il faut un système régulier de révocation des mots de passe. À un deuxième niveau, l'adresse IP de l'équipement connecté doit être caché en utilisant un VPN (Virtual private network), un tunnel crypté qui sécurise la communication. Au niveau au-dessus, des certificats d'authentification et des clefs de protection individuelle forment une sorte de bulle protégeant les communications entre tous les produits du même client. C'est une infrastructure de gestion des clefs ou PKI (Public key infrastructure). Par exemple, un produit de l'exploitant A ne peut être vu que par les autres produits de l'exploitant A. Enfin, au dernier niveau, les équipements de terrain peuvent émettre des logs (4) sur des serveurs. Ces traces de l'exécution d'un programme permettent de suivre les essais de connexions, de détecter un fonctionnement anormal et donc de faire un suivi de la cybersécurité. Le chiffrement se fait via le tunnel VPN et les clefs d'authentification, complété dans le cas de Lacroix-Sofrel par l'utilisation d'un protocole propriétaire Lacbus-RTU qui optimise la communication vers les Scada, fait de la remontée d'alarmes en optimisant la bande passante. En revanche, les automates connectés qui ont 30 à 40 ans d'existence ne peuvent plus être programmés par perte de compétence et/ou des outils de développement. Il faut les changer ou les encapsuler pour les protéger derrière des pare-feu. « *Dans le cas d'un parc ancien, d'une installation existante, c'est plus compliqué et il est préférable de faire migrer le parc. S'il est possible de mettre un VPN, en revanche le processus de certification entre produits n'est pas possible ni la gestion d'un compte individuel* », avertit Cédric Castella.

“Il appartient à la maîtrise d'ouvrage de protéger l'intégralité des données échangées autour d'un chantier par la mise en place d'un contrat spécifique TRC Cyber, complémentaire à la garantie Tous risques chantier (TRC) et bénéficiant à l'ensemble des intervenants à l'acte de construire pendant toute la phase de réalisation de l'ouvrage”

Une approche globale

La politique de sécurité informatique doit être confiée à des experts et plusieurs précautions doivent être prises, comme la protection physique des équipements critiques pour éviter de se brancher directement dessus, le masquage des adresses IP des équipements connectés qui ne doivent pas être accessibles sur Internet et le cloisonnement en différents réseaux privés et segmentés. « *Il est vraiment important pour la sécurité de cloisonner les différents flux et différents réseaux. La clef contre la malveillance réside dans un bon cloisonnement, sans quoi le hacker peut rebondir sur un équipement comme la gaine de ventilation ou une lumière connectée* », assure Yves Duchesne (Acceis). Des précautions sont à prendre dès la conception de l'architecture informatique. Cédric Castella confirme : « *Les responsabilités doivent être bien définies. Les produits ne doivent pas échanger en local mais en haut de Scada vers Scada ou d'une interface logicielle vers une autre. Il est préférable aussi d'avoir un seul système qui descend des ordres et des commandes vers les équipements. Plusieurs systèmes peuvent lire les données mais un seul doit être autorisé à les modifier, afin de bien définir qui est responsable du budget et de la sécurité. Enfin, le superviseur soit avoir confirmation que l'ordre a bien été pris en compte localement par réception d'un message d'acquittement de l'ordre en local* ».

Concernant la cybersécurité du secteur du BTP, les assureurs peuvent délivrer des garanties aux entreprises après analyse de risques, en mettant en exergue les points les plus cruciaux. « *Le numérique fait dorénavant partie de l'activité. Par ailleurs, il appartient également à la maîtrise d'ouvrage de protéger l'intégralité des données échangées autour d'un chantier par la mise en place d'un contrat spécifique TRC Cyber, complémentaire à la garantie “Tous risques chantier” (TRC) et bénéficiant à l'ensemble des intervenants à l'acte de construire pendant toute la phase de réalisation de l'ouvrage* », explique Clotilde Zucchi, directrice du département des Branches spécialisées de SMABTP. Il revient à chaque entreprise de souscrire une assurance cyber-risque garantissant à la fois les dommages qu'elle pourrait subir du fait d'une attaque de ses systèmes d'information et la mise en cause de sa responsabilité pour avoir transmis un virus à un tiers ou subi une compromission des données détenues. « *Le système de climatisation connecté peut en effet transmettre un virus et de là contaminer le réseau informatique d'un tiers. Un lien permanent de connexion expose au risque cyber. L'idée est de pouvoir, après un sinistre, redémarrer l'activité le plus vite possible* », assure Nathalie Acas, souscripteur-concepteur au département des Branches spécialisées de SMABTP. Les entreprises du BTP doivent désormais acquérir et intégrer de nouvelles compétences autres que celles liées au BTP. La cybersécurité est un sujet collectif. ■

(2) En français, des systèmes de contrôle et d'acquisition de données, c'est-à-dire des systèmes de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.

(3) L'hypervision est la centralisation des outils de supervision.

(4) Il s'agit d'une sorte de journal de bord horodaté qui liste et stocke un historique d'évènements.