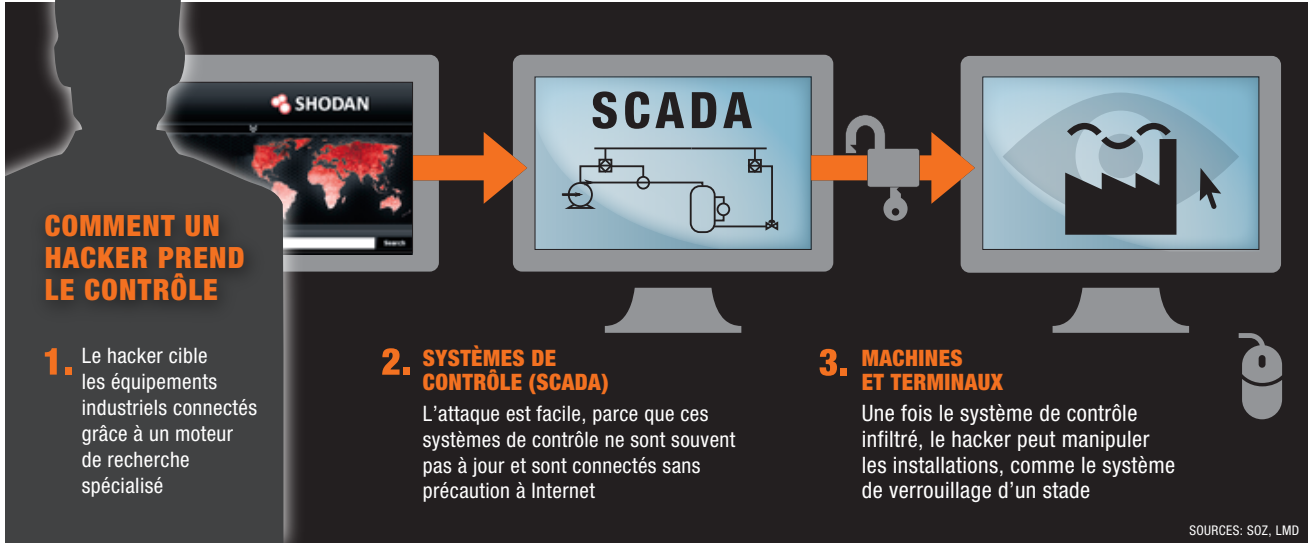


ENQUÊTE DES WEBCAMS DE PRIVÉS AU PARC SAINT-JACQUES DE BÂLE, DE NOMBREUSES IN STALLATIONS SUISSES CONNECTÉES À INTERNET SONT VULNÉRABLES

Ouvrir les portes d'un stade ou lire votre déclaration d'impôt? «Même mon cousin peut le faire»



INTERNET Le Parc Saint-Jacques à Bâle, des archives du canton de Vaud ou une station d'épuration à Zurich: une étude inédite montre que plus de 2700 équipements industriels connectés en Suisse ne sont pas suffisamment protégés. Les privés ne sont pas en reste: une webcam placée dans la chambre de bébé ou les photos de vacances d'inconnus sont accessibles sans mot de passe.

Alexander Haederli
Florian Imbach

Durant une année, le système de verrouillage des portes du plus grand stade de Suisse, le Parc Saint-Jacques à Bâle, a été accessible au monde entier depuis un simple navigateur Internet. Pire: une faille de sécurité permettait de récupérer le mot de passe et de pénétrer au cœur du système. Le complexe rhénan peut accueillir 38 500 spectateurs, mais aussi plusieurs milliers de visiteurs dans les allées du centre commercial qui comprend quarante magasins dont Manor, C&A ou Kookaï.

Un cambrioleur ou un vandale aurait pu ouvrir l'entrée du personnel durant la nuit puis pénétrer dans le complexe. Il avait aussi la possibilité de désactiver les alarmes ou de choisir à quel moment les portes du stade s'ouvrent chaque jour et quand elles se ferment.

Premier test au niveau suisse
Le problème de sécurité du Parc Saint-Jacques est un exemple parmi les milliers d'autres. C'est ce que révèle le premier test systématique des infrastructures connectées en Suisse. L'entreprise italienne IS Group a passé notre pays à la loupe pour recenser les systèmes de contrôle, appelés SCADA ou ICS dans le jargon. Résultat: au moins 2742 installations sont en danger*. Parmi elles, de petites centrales électriques, des stations d'épuration des eaux, des usines. Elles sont en danger parce que les exploitants les ont connectées directement à Internet, généralement pour les gérer à distance. «C'est grave parce qu'elles sont mises en ligne sans véritable réflexion en matière de sécurité», déplore Francesco Ongaro, l'un des experts d'IS Group. Souvent, ces systèmes ne sont pas à jour et facilement

attaquables. Le hacker peut alors prendre le contrôle à distance de l'installation.

Dans le canton de Vaud, le Dépôt et Abri des biens culturels (DABC), installé dans l'ancienne centrale nucléaire de Lucens, était aussi accessible par Internet. Le système de déshumidification, installé il y a quatre ans, souffre de la même faille que les portes du stade bâlois. Le mot de passe, facilement interceptable, permet de modifier la température et le taux d'humidité. «Des livres et des périodiques sont entreposés dans les endroits concernés», précise Philippe Pont, chef du Service immeubles, patrimoine et logistique. Un arrêt du système pourrait conduire à la dégradation de ces objets. «Nous n'étions pas au courant de cette faille de sécurité. Nous avons déconnecté le système d'Internet en attendant de sécuriser l'accès.»

« En connectant leurs systèmes à Internet, ces gens facilitent grandement le travail aux personnes malintentionnées »

FRANCESCO ONGARO
Expert en sécurité informatique

A Zurich, il était possible de se connecter sans mot de passe au panneau de contrôle d'une station de pompage des eaux usées. «Une manipulation à distance n'était pas possible», assure l'exploitant qui a néanmoins modifié la configuration de l'appareil. Bâle, Lucens, Zurich: l'expert italien Francesco Ongaro hoche la tête en signe de désapprobation. «En connectant leurs systèmes à Internet, ces gens facilitent grandement le travail aux personnes malintentionnées.» Selon lui, pas besoin d'être un hacker pour causer des dommages à ces installations. «Mon cousin pourrait attaquer la plupart d'entre elles.» Par exemple en inondant le système de requêtes jusqu'à ce qu'il lâche. Il serait ainsi possible de stopper la production d'une entreprise concurrente. Certains appareils présentent des failles de sécurité largement connues. C'est le cas au Parc Saint-Jacques et aux Archives vaudoises. Tous deux

sont basés sur un système fabriqué par l'entreprise Saia-Burgess Controls à Morat, rachetée l'année dernière par le géant mondial Honeywell. Problème: le système d'authentification est si mal conçu qu'il est possible, sans grand effort, d'intercepter le mot de passe non crypté au moment où le navigateur se connecte à l'installation. Cette faille a été révélée publiquement au mois de mai dernier dans un magazine spécialisé en Allemagne. Le fabricant a alors expliqué que ces produits n'étaient pas conçus pour être connectés à Internet sans mesure de protection, comme un pare-feu. «Nous avons prévenu les clients concernés et proposé un patch afin de crypter le mot de passe», explique André Gross, responsable des ventes pour la Suisse.

Pourtant, des dizaines de systèmes obsolètes sont toujours en ligne. Une inertie qui s'explique en partie par une dilution de la responsabilité. Au Parc Saint-Jacques, l'installateur rejette la faute sur ses clients. L'administrateur du site, la société Basel United, renvoie vers ISS, l'exploitant. Qui à son tour renvoie à Wincasa, le propriétaire. Dans un premier temps, l'exploitant nous a confirmé qu'il s'agissait du système de verrouillage et qu'il était possible d'ouvrir les portes d'accès au stade et au centre commercial. Une explication qui correspond à nos observations. Deux jours plus tard, Wincasa nous livrait une autre version: selon eux, seule une porte d'accès au centre commercial, aurait été concernée. Même si cette affirmation est correcte, cette brèche était suffisante pour pénétrer dans le complexe. Myriam Dunn Cavelti, chercheuse spécialisée dans la cybersécurité à l'Ecole polytechnique de Zurich, estime que le cas bâlois pose un sérieux problème de sécurité. Elle n'est guère étonnée que les responsabilités ne soient pas claires. «Ce genre de cas est typique dans ce domaine, analyse-t-elle. Chacun se renvoie la balle et personne ne veut assumer.»

Le confort avant la sécurité
Et puis, pour certaines entreprises, la sécurité passe au second plan, constate à Berne Max Klaus, vice-directeur de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information Melani. Le problème touche notamment de nombreuses PME qui acceptent d'investir pour s'offrir le confort de pouvoir gérer leurs installations à distance, mais pas suf-



Le système de verrouillage des portes du Parc Saint-Jacques à Bâle était accessible au monde entier depuis n'importe quel navigateur Internet.

Richard Martin/Presse Sports/freshfocus



► **Système de contrôle**
Voici l'un des panneaux de contrôle auxquels pouvait avoir accès un hacker, sans trop d'efforts. Il lui aurait ensuite été possible de désactiver des alarmes et même de déverrouiller certaines portes d'accès.

LA VIE PRIVÉE DES SUISSES ACCESSIBLE EN UN CLIC

► **CONNECTÉS** Au téléphone, Pascale Zanni n'en revient pas. «N'importe qui peut avoir accès à mes photos et à mes fichiers? Sans mot de passe? C'est effrayant!» Cette infirmière vaudoise de 40 ans stockait de nombreux fichiers sur un disque dur externe connecté à Internet. Sans qu'elle s'en doute, les photos de ses enfants, la correspondance avec sa banque ainsi que ses e-mails privés étaient accessibles à n'importe quel internaute via un simple navigateur Internet. A l'instar des équipements industriels comme celui du Parc Saint-Jacques de Bâle, les appareils des particuliers sont aussi toujours plus nombreux à être connectés. Avec le risque de graves atteintes à la sphère privée. Suite à notre appel, Pascaline a immédiatement débranché son disque dur du réseau. Mais combien de personnes évaluent ainsi involontairement leur vie? Un moteur de recherche spécialisé, qui recense les objets connectés à Internet, indique que plus de 3300 systèmes de stockage en réseau de la marque Iomega, l'un des leaders du marché, sont connectés en Suisse. Suite à des pointages que nous avons effectués, on peut estimer que 1500 d'entre eux sont accessibles sans mot de passe. A cela s'ajoutent les webcams, les ordinateurs, les imprimantes: au total, plus de 884 000 appareils seraient connectés à Internet en Suisse, selon une étude inédite réalisée par l'entreprise italienne de sécurité informatique IS Group.

► **WEBCAMS** L'exemple des webcams est édifiant: des dizaines de caméras sont connectées à Internet sans protection – ou, presque aussi grave, en laissant le mot de passe «admin» ou «12345» proposé par le fabricant. Le monde entier peut alors pénétrer dans un salon à Neuchâtel, une cuisine à Zurich et même une chambre de bébé en Argovie et observer en direct et en toute discrétion ce qui s'y passe. Le danger est bien réel. Aux Etats-Unis, un pirate âgé de 19 ans est récemment parvenu à se connecter à la webcam de «Miss Teen USA». Il a tenté de faire chanter sa victime, en menaçant de mettre en ligne des photos d'elle nue. Encore plus glauque: à Houston, au Texas, des parents ont surpris un inconnu en train de parler à

leur petite fille de 2 ans pendant qu'elle dormait via le visiophone placé dans sa chambre et relié à Internet. Lorsqu'ils sont entrés dans la pièce, la voix sortie de l'appareil qui, jusque-là, insultait l'enfant s'en est prise aux deux adultes, traitant le père de «débile» et la mère de «pute».

► **NAS** En termes de quantité de données personnelles, les Network Attached Storage ou NAS battent tous les records. Ces disques durs externes se connectent à l'ordinateur, mais également à Internet, généralement via un câble branché directement au routeur. Ils permettent aux utilisateurs d'accéder à leur fichier, notamment des films ou de la musique, depuis n'importe quel appareil. Ils sont également utilisés pour stocker les sauvegardes d'un ordinateur. Autrement dit: on y trouve souvent l'entier des dossiers et des fichiers d'un ménage. Y compris des fichiers de type «Password.doc» contenant l'entier des mots de passe de l'utilisateur. Les déclarations d'impôt, elles aussi, sont à portée de clic. Celle de Charles-Etienne Bill, un retraité bernois, était librement accessible. «Je stocke aussi toute ma comptabilité personnelle, précise-t-il au téléphone tout en débranchant son NAS. Evidemment cela peut avoir des conséquences très ennuyeuses.»

«Au-delà du voyeurisme, c'est pro-

blématique parce que l'on y trouve des informations qui peuvent servir à se faire passer pour autrui», observe David-Olivier Jaquet - Chiffelle, professeur spécialisé en cybercriminalité et en identités numériques à l'Université de Lausanne. Exemple avec le NAS de ce haut cadre d'une fédération sportive installée sur l'arc alémanique: des copies numériques de ses papiers d'identité et de son permis de conduire côtoient son relevé de carte Visa et de son compte bancaire. «On a alors sa signature, le numéro de compte, le nom de son conseiller et on connaît le solde ainsi que les dernières transactions, analyse le professeur. Avec ces informations, une personne malintentionnée a de bonnes chances de parvenir à effectuer un virement.» Sans oublier la possibilité de supprimer des données ou, plus pernicieux, d'en ajouter. «On peut imaginer que des pirates utilisent cet espace gratuit pour stocker du matériel pédopornographique», ajoute le criminologue. Enfin, le NAS peut aussi être sciemment infecté par un malware pour contaminer les ordinateurs qui s'y connectent.

► **FAILLE** Pourquoi les utilisateurs ne protègent-ils pas mieux leurs données? Parce que ce n'est pas toujours simple. Reprenons l'exemple de la marque Iomega: de nombreux utilisateurs, dont un cadre zurichois d'un géant mondial de l'informatique, nous ont assuré utiliser un mot de passe. Leurs données étaient pourtant accessibles en tapant simplement l'adresse IP de leur NAS dans un navigateur. Un problème connu du fabricant: sur certains modèles, le mot de passe ne protège que l'accès à la console d'administration de l'appareil. Le contenu, lui, est librement accessible par défaut. «Des améliorations ont été effectuées il y a une année et, désormais, le périphérique NAS et le partage de contenu sont tous deux protégés par défaut», assure Catherine Ladousse, directrice de la communication de l'entreprise. Cette faiblesse de certains NAS Iomega est connue des pirates. Au moins une dizaine de disques durs en Suisse avaient déjà été visités avant notre passage. Un plaisantin a même laissé une trace de son intrusion: il a ajouté un fichier dans le répertoire principal pour suggérer aux propriétaires de revoir leur configuration. •



Une caméra placée dans cet appartement et connectée à Internet permet d'observer ses occupants en train de cuisiner.



Cette webcam, installée dans une chambre de bébé, était également accessible sans mot de passe.