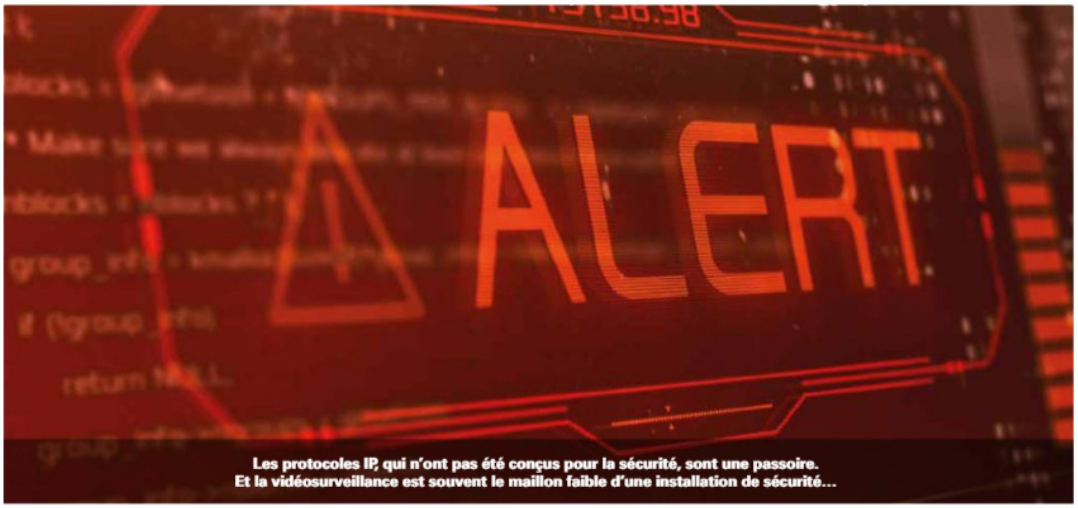
Dossier
IoT, réseaux ... tous vos systèmes de sécurité sont vulnérables !

PSM - N°266 - Juillet 2021

dossier



Les protocoles IP, qui n'ont pas été conçus pour la sécurité, sont une passoire. Et la vidéosurveillance est souvent le maillon faible d'une installation de sécurité…

IoT, réseaux… tous vos systèmes de sécurité sont vulnérables !

Dans la vaste nébuleuse qu'est devenu l'Internet des objets (Internet of Things ou IoT) et dans laquelle s'inscrivent évidemment les caméras de surveillance, les systèmes de contrôle d'accès, les détecteurs d'intrusion…, tous les « objets » connectés peuvent constituer une faille de sécurité.

LA PAROLE À

YOANN KASSIANIDES
Délégué général de l'ACN

© DR

« QUI SERA RESPONSABLE EN CAS D'INCIDENT ? »

« L'Alliance pour la confiance numérique rassemble les entreprises (leaders mondiaux, PME et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité et de l'identité numérique. Dans le contexte qui voit se développer de manière exponentielle les réseaux et l'IoT, il est primordial que toutes les entreprises concernées par les problématiques que cela implique collaborent. Cette approche doit impérativement être holistique et partagée et inclure, notamment, outre les entreprises de la filière de la confiance numérique, les utilisateurs finaux, et les institutionnels, afin de faire émerger une vision commune et généralisée de la sécurité et de la confiance numérique. Au-delà du défi de la sécurité de l'ensemble des développements numériques qui reste à relever, c'est bien de la souveraineté numérique et de l'autonomie stratégique de notre pays et de l'Europe dont il est question. Tous les acteurs économiques doivent comprendre qu'ils n'ont plus le luxe de l'inaction. L'offre française en matière de "confiance numérique" existe, est disponible et répond à ces enjeux. Il n'est pas normal que des pans entiers de l'IoT ne soient pas sécurisés comme ils pourraient l'être : les industriels doivent intégrer ces notions de sécurité et de confiance dès la conception de leurs produits et solutions afin d'éviter le problème insoluble de la sécurisation d'objets, tels les caméras par exemple, qui n'ont pas été pensés pour être sécurisés. »

MOÏSE MOYAL
Délégué à la sécurité numérique des régions Provence-Alpes-Côte d'Azur et Corse, Anssi

« IL Y A UN INTÉRÊT CONCURRENTIEL À ÊTRE CERTIFIÉ OU QUALIFIÉ ANSSI. »

« L'Anssi concentre ses messages sur l'intérêt de ses certifications et qualifications produits sous la bannière Visa de sécurité. En effet, à partir du moment où l'on intègre du numérique pour ensuite le mettre en réseau, il doit répondre à certaines exigences en matière de sécurité. C'est à cet effet que nous avons publié un guide de *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*. Par ailleurs, nous recommandons que pour les systèmes d'information d'importance vitale (ou SIIV) que les produits passent par la certification Anssi. C'est très important et doit permettre de faire comprendre aux acteurs de la sécurité électronique qu'il y a un intérêt financier à être certifié ou qualifié Anssi : pouvoir accéder à certains marchés. »

Dossier
IoT, réseaux ... tous vos systèmes de sécurité sont vulnérables !

PSM - N°266 - Juillet 2021

© Getty Images

© DR

« Nous collaborons avec l'Anssi, l'ACN, et avec les industriels pour pousser une démarche commune de sécurité cyber des systèmes de sécurité physique. »

ANNE-ISABELLE PARODI, SECRÉTAIRE GÉNÉRALE DE SPAC

● ● ● *confiance, c'est-à-dire des solutions fonctionnelles et résistantes aux cyberattaques. »*
Les membres de Spac travaillent également à la généralisation du standard SSCP. *« Ce protocole est très important car, d'une part, il est le seul sur le marché à être complètement ouvert et, d'autre part, il est le seul à être certifié CSPN (certification de sécurité de premier niveau) par l'Anssi, en faisant partie de la cible de sécurité »*, insiste Anne-Isabelle Parodi.

■ *Un sujet malheureusement de plus en plus sensible*

« Les attaques cyber se structurent et semblent même devenir de plus en plus simples à mener. Or, les protocoles IP, qui n'ont pas été conçus pour la sécurité, sont une passoire. Et la vidéosurveillance est souvent le maillon faible d'une installation de sécurité, déplore Dominique Legrand, président de l'AN2V. *Et beaucoup d'utilisateurs croient à tort que leur réseau est étanche. La question n'est pas de savoir si on sera hacké mais quand on le sera ? »* Il ajoute : *« Il faut donc prendre les mesures qui s'imposent. C'est-à-dire enta-* ● ● ● *mer une vraie étude d'impact pour se préparer à réagir et faire preuve de résilience et comment gérer une crise si tous les réseaux sont indisponibles : téléphones filaires, répertoires sur papier, etc. »*
La bataille est-elle perdue face aux pirates ? *« Non, si on prend tout de suite les bonnes mesures,* considère Virgile Augé. *Il faut d'abord faire preuve de sobriété. On déploie beaucoup de matériels dans l'IoT. Sont-ils tous nécessaires ? Il existe des mesures simples à prendre. On les connaît : elles ont été publiées par l'Anssi. »* Il conclut : *« La situation est similaire à celle de la Guerre froide. Le feu nucléaire a été remplacé par le feu cyber… L'attaque est là tapie et invisible. Elle n'attend que l'ordre de déclenchement. L'IoT n'est qu'un des multiples supports possibles de cette future attaque. Attaque par ailleurs peut être déjà initiée dans ses actes invasifs et préparatoires mais pas encore repérée parce que n'ayant pas encore provoqué de dégâts. »* ■