Article - TECHNOLOGIES SANS CONTACT LE CONTRÔLE D'ACCÈS SE PROTÈGE DES CYBERATTAQUES

PSM - Hors-série - Juillet 2018

Le contrôle d'accès se protège des cyberattaques

Ouverture d'accès par carte ou téléphone, le contrôle d'accès physique se virtualise de plus en plus et devient par conséquent une cible de choix pour les hackers. De nouvelles menaces auxquelles les directeurs de sûreté doivent désormais se préparer.

La sécurité du sans contact commence dès les transmissions cryptées entre le badge et le lecteur.

© Getty

La cybersécurité du système de contrôle d'accès est désormais un chapitre incontournable de tous les appels d'offre. Certaines attaques récentes très médiatisées ont alerté les directeurs de sûreté. *«On a affaire à une demande paradoxale,* explique Dominique Auvray, directeur marketing de Gunnebo Electronic Security. *D'un côté, les entreprises veulent des systèmes légers et confortables, accessibles du Web, et d'autre part, une sécurité optimale. En devenant partie intégrante du système d'information des entreprises, les systèmes de contrôle d'accès sont susceptibles d'être victimes de cyberattaques. La sécurisation de la chaîne de bout en bout ne doit plus être une vue de l'esprit, mais devenir une réalité.»* L'impératif de cybersécurité, comme le précise l'Anssi (Agence nationale de la sécurité des systèmes d'information) concerne le parc informatique dans son ensemble, depuis le développement de la bureautique jusqu'à la conception du système industriel intégré à la chaîne production. Et la sûreté physique qui repose désormais sur des infrastructures et des applications informatiques est concernée au premier chef. L'Anssi s'est intéressée aux systèmes de sûreté et a déterminé des recommandations qui sont aujourd'hui une base pour construire un système de protection physique limitant les risques de cyberattaques. *«Depuis la promulgation de la loi de programmation militaire en 2013,* rappelle Laurent Rouyer, expert européen en cybersécurité chez Til Technologies, *les 249 OIV (opérateurs d'importance vitale) ont l'obligation de sécuriser leur site – et le contrôle d'accès, selon les guides de l'Anssi. Une obligation qui s'est étendue aux 12 SAIV (secteur d'activité d'importance vitale), ce qui concerne des milliers d'entreprises. Les guides de l'Anssi demandent que les systèmes soient sécurisés intrinsèquement contre les actes de malveillance et d'intrusion et ont édité une série de recommandations. Cette évolution fait que, désormais, les appels d'offres demandent aux fournisseurs de répondre dans leurs propositions aux guides de l'Anssi. Toutefois, il ne suffit pas que le constructeur respecte ces guides. L'intégrateur-installateur doit mettre en œuvre les produits dans les règles de l'art, et le client doit activer les fonctionnalités – comme le cryptage – dans sa propre informatique, et surtout faire systématiquement les mises à jour.»* La sécurité de bout en bout commence par les hommes qui la mettent en place.

Protéger le badge, qu'il soit physique ou dématérialisé

Pour Martial Gonzalez, d'HID Global, un badge insuffisamment sécurisé reste la principale faille dans le contrôle d'accès. *«Avant de mettre en place un système de contrôle d'accès, nous auditons la sécurité en place, du badge au serveur. Les badges Mifare Classic, encore très présents, peuvent être clonés en quelques secondes. Une des premières mises à niveau est le passage à des cartes à microprocesseur bien plus sécurisées avec une gestion des clés d'authentification repensée.»* Il en va de même pour les badges dématérialisés. *«Lorsque nous avons lancé notre badge dématérialisé, Stid Mobile,* indique Vincent Dupart, *nous nous sommes fixés comme objectif une sécurité de type Desfire, avec un Secure Element, afin que les identifiants puissent circuler sur les réseaux Wweb, Bluetooth, sans pouvoir être décryptés. Toutefois, dans certains établissements, les directeurs de sûreté souhaitent des solutions offline, complètement cloisonnées. C'est un choix que nous respectons, et nous offrons des solutions de contrôle* ●●●

Pour aller plus loin

- «Guide de sécurité des technologies sans contact pour le contrôle des accès physiques», téléchargeable sur le site de l'Anssi.
- «Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques» téléchargeable sur www.ssi.gouv.fr
- Document technique pour la conception et l'installation contrôle d'accès (APSAD D 83), téléchargeable sur le site du CNPP.

STid
Electronic Identification

JUILLET - 2018

Article - TECHNOLOGIES SANS CONTACT LE CONTRÔLE D'ACCÈS SE PROTÈGE DES CYBERATTAQUES

PSM - Hors-série - Juillet 2018

Technologies sans contact

●●● *d'accès offline tout aussi sécurisées.»* La certification de la puce EAL4+ reste un critère de référence sur lequel s'appuyer.

Les lecteurs jouent la transparence

Afin d'éviter que les données soient capturées directement sur le lecteur, l'Anssi recommande une architecture dite de type 1 utilisant un lecteur transparent, c'est-à-dire qui ne contient aucune clé de lecture de badge. À défaut, un lecteur de type 2, c'est-à-dire dont les données s'effacent en cas d'arrachement, est jugé acceptable. De même, les informations contenues dans les unités de traitement local, nécessaires à l'authentification, doivent être protégées physiquement – avec une accessibilité restreinte – et logiquement par des clés de chiffrement. Pour Laurent Brière, directeur d'Addixi, qui développe Addlock, une solution complète de contrôle d'accès physique et d'accès logique, *«le chiffrement et l'authentification sont la clé de la sécurité. Il faut impérativement que les données soient cryptées, en lecture et en écriture, même si cela reste très souvent sur le réseau interne de l'entreprise. Dans notre cas, nous appuyons sur des normes reconnues, telles que l'Iso 14443 A et B (normes de sécurisation des cartes RFID des technologies Desfire V1 et V2) qui sont, à ce jour, les plus sûres.»*

Serveur et logiciel de gestion du système

Alors qu'il contrôle les accès physiques, le serveur est soumis aux mêmes règles de protection que les systèmes informatiques : pare-feu, antivirus, application des correctifs de sécurité, gestion des mots de passe et authentification. L'Anssi a publié un guide «d'hygiène informatique». Celui-ci reprend une quarantaine de règles essentielles pour assurer la sécurité des systèmes d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui. La règle du cloisonnement est souvent rappelée par les constructeurs et développeurs. *«Nous incitons nos clients à bien séparer ce qui relève du contrôle d'accès physique des autres applications de l'entreprise,* insiste Laurent Brière, d'Addixi, *de façon à ce que le contrôle d'accès ne soit pas exposé en cas d'attaques sur d'autres fonctionnalités.»* Le logiciel de gestion du système est considéré par l'Anssi comme le point névralgique des systèmes de gestion d'accès physiques par technologie sans contact. Le logiciel installé sur le serveur de gestion a pour rôle de communiquer d'un point de vue logique avec les unités de traitements local. La sécurité passe par une authentification pour contrôler l'accès au logiciel et la gestion des droits associés.

Technologies ouvertes ou fermées ?

Le débat fait rage. *«Au vu de mon expérience,* indique Guillaume Gamelin, de F-Secure, société spécialisée dans la cybersécurité, *j'estime que plus le logiciel est spécifique et développé "maison", moins il a de risques de se faire pirater. Pour une entreprise désireuse de protéger ses accès, nous préconisons d'éviter les solutions standards, largement diffusées, qui, tôt ou tard, révèleront des failles.»* Au contraire, pour Martial Gonzalez d'HID Global : *«Le risque des technologies propriétaires, que ce soit une encryption, un protocole de communication ou un hardware, est d'être lié à un constructeur ou un développeur, sans avoir la certitude que ces technologies vont suivre l'évolution des menaces. L'utilisateur aura tout intérêt à embrasser le standard ouvert du marché qui lui garantira son investissement et une parfaite interopérabilité et indépendance.»*


© DR

VINCENT DUPART, PRÉSIDENT DE STID

«Valider la fiabilité des solutions nécessite une actualisation permanente. Nous travaillons avec des sociétés extérieures de Pentester (hackers éthiques) qui réalisent en permanence des "attaques" sur nos solutions afin d'en évaluer la sûreté, et de pouvoir réaliser des patchs que nous fournissons à nos clients. C'est désormais indispensable pour assurer à nos clients une sécurité optimale.»

Maîtriser les données, la clé de la sécurité

Alors qu'il y a quelques années, la maîtrise des données étaient l'apanage des constructeurs ou des installateurs, on assiste aujourd'hui à un renversement de tendance, accentué par la mise en place du RGPD : *«Il est anormal,* soutient Vincent Dupart de Stid, *que certains constructeurs proposent encore de gérer les clés. Nous offrons plusieurs options à nos clients, hébergement des données chez nous, dans leur propre serveur ou sur le cloud – de préférence en Europe – mais c'est à l'utilisateur final d'établir ses clés de cryptage à l'aide d'outils cryptographiques reconnus. Nous encourageons les utilisateurs à utiliser des systèmes identiques à ceux qu'utilisent les banques, qu'ils choisissent un contrôle d'accès offline ou online. L'utilisateur doit être le seul à connaître ses clés, c'est à mon avis le b.a.-ba de la sécurité.»*
En résumé, conclut Laurent Rouyer de Til Technologies : *«Il faut que le produit retenu respecte le guide de l'Anssi, idéalement avec une architecture 1 de lecteur transparent, ou éventuellement 2, des outils cryptographiques qui respectent le RGS (AES 128 Bits minimum). Toutes les communications doivent être cryptées de bout en bout de la carte au serveur et l'utilisateur doit maîtriser les clés. Le réseau IP doit être certifié TLS. Enfin, le maintien en condition de sécurité est indispensable : cela se traduit par l'implémentation de patchs dès qu'une vulnérabilité est découverte.»*

«Le chiffrement et l'authentification sont les clés de la sécurité.»
LAURENT BRIÈRE, ADDIXIS