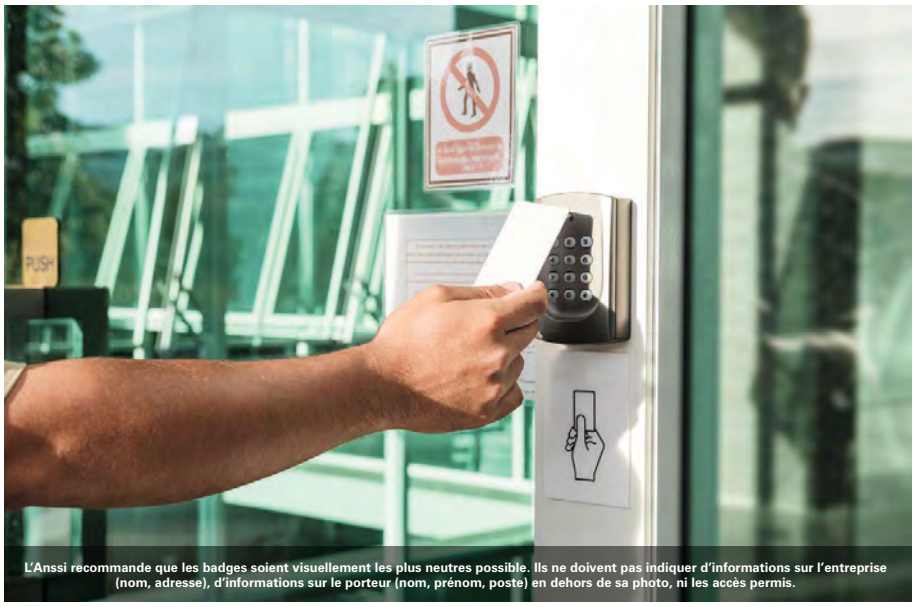
STid
Electronic Identification

JANVIER - 2018

Article - Contrôle d'accès - Les badges, le maillon faible du contrôle d'accès ?

PSM - Nº 245 - Janvier Février 2018

contrôle d'accès



L'Anssi recommande que les badges soient visuellement les plus neutres possible. Ils ne doivent pas indiquer d'informations sur l'entreprise (nom, adresse), d'informations sur le porteur (nom, prénom, poste) en dehors de sa photo, ni les accès permis.

Les badges, le maillon faible du contrôle d'accès ?

Depuis plusieurs décennies déjà, les badges ont pris le pas sur les clés et les codes pour accéder et circuler dans l'entreprise et, parfois, se connecter au réseau ou accéder à des services connexes. Des niveaux de sécurité très inégaux pour ces cartes qui peuvent mettre en jeu la sûreté de l'entreprise.

Les badges sont aujourd'hui les systèmes les plus répandus pour accéder aux bâtiments d'entreprise. Leur rôle est d'abord d'identifier le porteur – c'est-à-dire de communiquer une identité, inscrite sur le badge, censée correspondre à l'identité du porteur. Les badges peuvent également authentifier, c'est-à-dire prouver que l'identité du porteur est valide. Dans le cas d'une carte sans contact, l'authentification se fait par un échange cryptographique entre le badge et le lecteur. Pour assurer un niveau de sûreté optimal, les clés de cryptographie doivent être suffisamment élaborées pour que le badge ne puisse pas être cloné. Le badge authentifié ne certifie pas pour autant que le porteur est bien celui qu'il prétend être, car il peut avoir été emprunté ou volé. Le contrôle peut lui demander de le prouver par la saisie d'un code, par exemple, ou par de la biométrie. Les très médiatisées affaires de hacking ont sensibilisé les entreprises au fait que leur système de contrôle d'accès peut présenter des faiblesses, notamment au niveau des badges. Une préoccupation qui les amène à réviser leur système et à se poser la question du choix de la carte d'accès.

Article - Contrôle d'accès - Les badges, le maillon faible du contrôle d'accès ?

PSM - Nº 245 - Janvier Février 2018

Priorité au zonage

Pour Laurent Bourguignon, consultant chez Synetis, expert en cybersécurité, avant même de se lancer dans une migration de système et de changer les cartes, il faut se poser les bonnes questions à savoir, s'assurer d'un zonage pertinent : *« C'est une évidence, mais, en pratique, on constate bien souvent des écarts. La première des choses est de voir chez le client qui a accès à quel espace et si c'est vraiment nécessaire. Pour les zones sensibles, il est important de rajouter une couche logicielle de sécurité sur le badge dont seul le client a la maîtrise. Et surtout, il ne faut pas oublier de faire vivre les droits avec des recertifications périodiques et non automatiques. Cela évite que les badges de personnes ayant quitté l'entreprise – ou ceux de prestataires – se retrouvent entre des mains malveillantes. »*

Une sécurité « end to end »

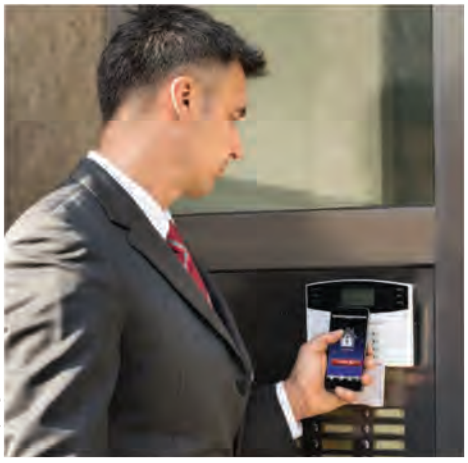
En tant que développeur de technologies d'identification sans contact et premier fabricant à obtenir la CSPN, la sécurité des badges est au cœur de l'activité de STid. « Lorsque nous intervenons, la sécurité des badges et sa technologie font souvent partie de la première question, remarque Pierre-Antoine Larrera de Morel, directeur commercial et associé chez STid. *Le badge est effectivement très important car c'est le premier maillon de tout un écosystème qui comprend également le lecteur, la transmission elle-même, le contrôleur et le logiciel. Notre rôle est d'orienter nos clients vers de bonnes pratiques pour garantir une sécurité des données de manière cohérente tout au long de la chaîne d'information, et de préférence avec des mécanismes certifiés. Il faut bien sûr que les badges ne soient pas clonables, et que les protocoles sécurisés ne puissent être ni interceptés, ni rejoués et qu'on ne puisse rien injecter. Les technologies ouvertes en ce sens sont préférables, car la sécurité est prouvée. Et une des clés de la sécurité est que l'entreprise garde la maîtrise de sa programmation du système de contrôle d'accès, de façon à ne pas être tributaire d'un fournisseur ou d'un fabricant. C'est d'ailleurs à nous concepteur de solutions haute sécurité, de fournir des outils simples et conviviaux pour rendre accessibles la maîtrise des paramètres. »*

La question de la migration

Dans l'ensemble, le niveau de sécurité du contrôle d'accès augmente, car la prise de conscience des risques est de plus en plus forte estime Pierre-Antoine Larrera de Morel *« Le badge d'accès est comparable à la clé d'une porte : pas la peine d'avoir un système sophistiqué si la clé n'est pas à la hauteur. Si les systèmes Prox disparaissent, il reste encore beaucoup de cartes Mifare Classic qui présentent des failles bien connues. La migration vers des systèmes Desfire EV2 est aujourd'hui une solution pour améliorer la sécurité. »* Une migration qui doit se planifier. Une première étape va consister au changement des lecteurs, en favorisant des lecteurs susceptibles de prendre en charge plusieurs technologies, celles existantes dans l'entreprise, mais aussi celles qui pourront être utilisées dans l'avenir, comme le NFC ou le Bluetooth. Cela permet, notamment, de pouvoir faire coexister plusieurs systèmes et d'anticiper les évolutions.

SIO, un secret bien gardé et transportable

Si la migration vers un système plus sûr semble une nécessité pour nombre d'entreprises, la question légitime est de savoir si ce nouveau système va être pérenne et ne pas nécessiter une nouvelle mise à niveau, voire un changement de l'ensemble lecteur, logiciel, badges dans un proche avenir.



POUR ALLER PLUS LOIN

Deux guides complémentaires à consulter impérativement avant une installation ou un changement sur son système de contrôle d'accès :

- Le Référentiel APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation.
  www.cnpp.com
- Guide sur la sécurité des technologies sans-contact pour le contrôle des accès physiques. Édité par l'Anssi.
  www.ssi.gouv.fr/

Article - Contrôle d'accès - Les badges, le maillon faible du contrôle d'accès ?

PSM - N° 245 - Janvier Février 2018

contrôle d'accès

PAROLE D'EXPERT

RENAUD LIFCHITZ
Consultant cybersécurité, Digital Security

© DR

« UNE SUITE D'ACCÈS REFUSÉS POUR UN BADGE PEUT ÊTRE LE SIGNE D'UNE TENTATIVE D'INTRUSION. »

« Digital Security est régulièrement consulté pour évaluer la sécurité des systèmes de contrôle d'accès. J'estime, qu'actuellement, même si cela s'améliore, deux tiers du parc est relativement faible sur le plan de la sécurité, avec des systèmes de badges RFID basse fréquence ou haute fréquence de type Mifare Classic. Ce sont des systèmes bon marché, mais il est relativement facile de copier les identifiants, de créer une carte clone et d'ouvrir les accès. Les cartes DESfire apportent une bien meilleure sécurité (avec quelques failles résiduelles sur les versions EV0 et EV1). Les versions EV2, pour lesquelles on ne connaît pour l'instant pas d'attaques ayant abouti sont à privilégier. Le chiffrement suit les recommandations de l'Anssi et se montre efficace. Quel que soit le système de badges choisi, pour bien sécuriser son contrôle d'accès, il est important de penser à changer la clé de chiffrement – ne pas laisser la clé du constructeur par défaut – d'accorder ou de retirer les droits en fonction des changements dans l'entreprise (arrivée, départ, perte de badges…) et d'avoir un système de détection des mauvais usages. Une suite d'accès refusés peut être le signe d'une tentative d'intrusion. Si le journal d'appel est relié à la vidéosurveillance, cela pourra permettre de s'assurer de la nature des échecs successifs sur un accès. »

© Getty images

Le badge se dématérialise

Facilité, économie, ergonomie, tendance… le téléphone mobile séduit de plus en plus les entreprises pour en faire leur badge d'accès. Une bonne idée ? *« Oui,* affirme Pierre-Antoine Larrera de Morel, directeur commercial chez STid, *à condition de ne pas négliger la sécurité. Un téléphone est perçu comme étant plus exposé aux attaques qu'un badge. L'essentiel est alors d'avoir un système qui empêche l'utilisation frauduleuse des données de l'application. D'où l'intérêt de la solution que nous proposons : une authentification mutuelle forte avec le lecteur et des mécanismes de chiffrement et de signature des données rendant l'échange unique, non interprétable, non rejouable. Même si elle est interceptée, elle ne pourra pas être réutilisée, car elle n'est valable qu'une fois. Pour la partie serveur, l'hébergement et les communications associées intègrent quant à elles des sécurités de niveau bancaire. Cela va tout à fait dans le sens des recommandations de l'Anssi et de la RGPD. » L'autre avantage est la gestion décentralisée des badges virtuels qui facilite l'administration. « Sur notre plate-forme, explique le représentant de STid, l'attribution des droits ou leur révocation se fait en un clic, sans que le détenteur du badge ait à se déplacer. »*

Badges mobiles, NFC ou Bluetooth ?

La question du protocole de transmission tend à favoriser le Bluetooth, comme le confirme Laurent Bourguignon, de Synedis. *« Le NFC présente une contrainte majeure : il n'est pas pour l'instant compatible avec Apple, ce qui exclut son usage d'une partie du parc téléphonique, mais aussi d'autres dispositifs comme les tablettes ou les montres. »* Le NFC présente cependant un certain nombre d'avantages : il est plus rapide et la distance requise entre l'émetteur et le lecteur de quelques centimètres – contre plusieurs mètres pour le Bluetooth – empêche, en principe, la captation non désirée des données de transmission. L'avenir dira si l'un des deux protocoles l'emporte dans le domaine du contrôle d'accès. Prudents, les fabricants proposent désormais des lecteurs compatibles avec les deux systèmes. ■

3 QUESTIONS À

LAURENT BOURGUIGNON
Consultant en cybersécurité, Synetis

© DR

Le téléphone est-il le badge de demain ?
C'est, en tout cas, ce qu'annoncent les prévisionnistes. Le cabinet d'analyse Gartner, spécialisé dans ce domaine, estime qu'en 2020, 20 % des entreprises utiliseront les smartphones à la place des badges d'accès physiques alors qu'elles n'étaient que 5 % en 2016. Le Bluetooth présent sur la totalité des smartphones va sans doute devenir le protocole de référence.

Est-ce à dire que le Bluetooth est une technologie sûre ?
En soi, le Bluetooth n'est pas sûr. C'est un système très complexe, et la complexité est l'ennemie de la sûreté. BlueBorne, un ensemble de huit vulnérabilités mises à jour en septembre dernier sur des milliards de machines l'a récemment montré. Plusieurs de ces vulnérabilités permettaient, simplement en passant à portée de connexion de l'appareil, de déclencher des attaques ou de récupérer des données transmises. En revanche, c'est un système ouvert qui peut bénéficier des avancées de tous. Quelques semaines après la révélation des failles Blueborne des patches de corrections ont été mises en place. Il faut davantage considérer le Bluetooth comme un canal de communication, et fortement sécuriser les données transférées du badge virtuel sur le téléphone vers le lecteur.

Comment expliquez-vous cet engouement ?
Le Bluetooth n'est pas parfait, et les technologies d'accès physique l'utilisant sont émergentes mais vont se développer et s'améliorer. Il y a une forte adhérence de la part des utilisateurs et des entreprises, pour qui le « badgeage » par téléphone véhicule une image de modernité. De plus, les utilisateurs font bien plus attention à leur téléphone qu'à leur badge : une perte, un vol, sont immédiatement signalés et un oubli très rare. Dans certaines banques, le taux de renouvellement des badges d'accès monte jusqu'à 50 % par an, ce qui s'avère coûteux et pose un sérieux problème de sûreté. Avec les téléphones, on est certain de ne pas atteindre ces taux de perte et que les anomalies remonteront très vite.