GET
Azkoyen Time & Security Division

Il est temps de vraiment sécuriser votre entreprise

Ne délaissez pas votre contrôle d'accès

« Nous prenons soin de vous, pendant que vous vous occupez de vos affaires ! »

Il est temps de vraiment sécuriser votre entreprise

Ne délaissez pas votre contrôle d’accès

La cybersécurité, LE sujet dont les journalistes tech, les experts et presque tous ceux qui sont impliqués dans les TIC d'une manière ou d'une autre, ne semblent pas cesser de parler. Après quelques incidents malheureux, des fuites de données et d'autres événements très médiatisés au cours des dernières décennies, la sécurisation de l'infrastructure numérique est devenue une priorité absolue pour presque toutes les entreprises. Et parce que le monde de la cybersécurité est erratique et change fortement d'année en année, la plupart des (grandes) entreprises n'hésitent pas à investir chaque année des millions d'euros dans le nec plus ultra de la sécurité numérique. C'est une façon de penser compréhensible, qui se traduit trop souvent par un retard de la sécurité physique de l'entreprise, comme le contrôle d'accès. Car « les employés ont leur propre badge qu'ils utilisent pour entrer. Et cela se passe bien depuis des années, de la même manière. Pourquoi changer maintenant ? ». C'est une citation courante lorsque le sujet est abordé. Et il y a, malheureusement, une erreur dangereuse là-dedans. Une erreur qui peut entraîner des dommages irréparables et beaucoup de problèmes inutiles…

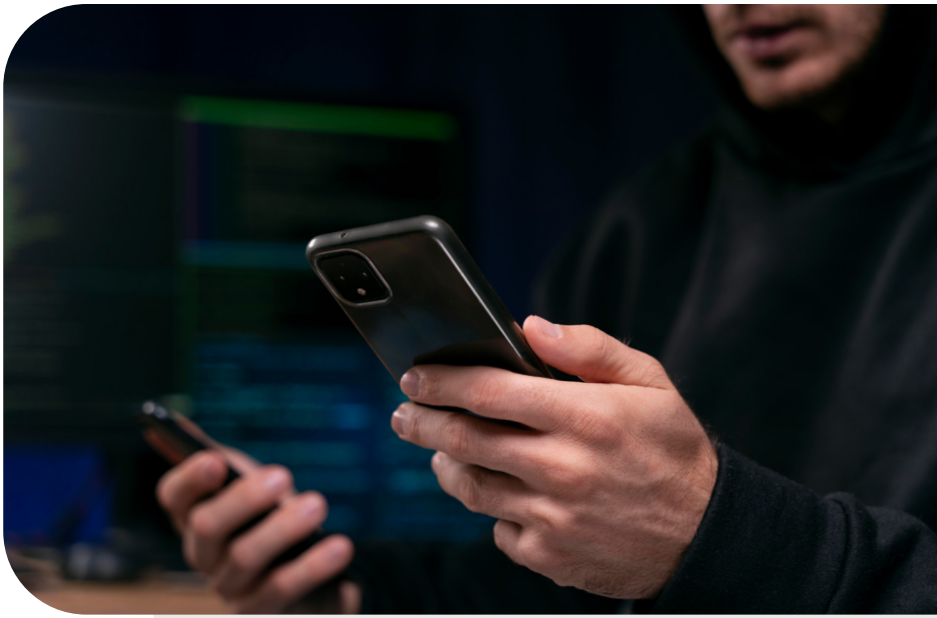
Les badges d'accès peuvent également être piratés

« Si ça marche, ça marche ». C'est l'approche avec laquelle de nombreuses entreprises abordent leur contrôle d'accès. Les employés reçoivent leur propre badge qui ouvre les portes, de sorte que les visiteurs indésirables sont écartés. Et ça marche en principe bien depuis dix, quinze voire vingt ans. Et donc, à première vue, il ne semble pas y avoir de raison de faire les choses différemment. Le monde de la cybersécurité évolue peut-être rapidement, mais les anciens badges et scanners usuels font tout 'simplement' leur travail. N'est-ce pas?

Nous constatons beaucoup cette façon de penser. Et cela est probablement lié au fait que de nombreuses entreprises (et même les experts en TIC sur place) ne savent peut-être pas que les badges d'accès peuvent également être piratés. Parce que non seulement la cybersécurité est en constante évolution, les criminels utilisent également de plus en plus des moyens numériques pour accéder à des emplacements physiques. Et cela peut désormais se faire "juste" avec le smartphone. Un exemple : en tant que cybercriminel, avec la bonne application, vous n'avez qu'à tenir votre téléphone portable contre la poche d'un employé qui ne se doute de rien pour récupérer toutes les données qui se trouvent sur le badge d'accès obsolète dans

cette poche. Ensuite, ce criminel peut copier tout le badge d'accès. Et tout cela, sans que le malheureux employé dont le badge vient d'être copié ne s'en aperçoive. Cela semble peu probable, mais ce n'est qu'un des risques que vous courez si votre système de contrôle d'accès a plus de quinze ans, voire dix ans.

Non seulement la cybersécurité est en constante évolution, mais les criminels utilisent également de plus en plus des moyens numériques pour accéder à des emplacements physiques.



Des millions investis en cybersécurité et pourtant une intrusion

Les anciens badges peuvent donc être copiés avec la plus grande facilité. Et cela a des conséquences désastreuses pour la sécurité de votre entreprise. Après tout, un ancien lecteur de badges ne reconnaîtra jamais qu'un badge a été copié. Et cela permet aux criminels de rentrer littéralement par la porte arrière, ou même par la porte d'entrée. Et toutes les portes de votre bâtiment s'ouvrent aussi tout simplement, comme elles le feraient pour l'employé dont le badge a été copié. Et une fois qu'un criminel est à l'intérieur, les choses peuvent aller vite. Hypothétiquement, une clé USB contenant un logiciel rançonneur ou crypto-verrouilleur suffit désormais pour arrêter l'ensemble de votre entreprise, ou pour voler des données précieuses ou même de l'argent. Une fois que le criminel est à l'intérieur et que les portes sont ouvertes, il lui suffit de trouver un PC connecté au réseau local. L'USB peut alors être inséré dans le port USB et le mal est fait. Même la meilleure cybersécurité ne peut rien contre une telle intrusion. ■

Fausses accusations et dégâts émotionnels

Le journal de données de votre système d'accès peut probablement suivre quelles portes sont ouvertes à quelle heure. Et une fois l'intrusion découverte, il est logique de se pencher sur le badge responsable. Et vous verrez : les traces indiquent toutes votre employé qui ne se méfie de rien, dont le badge a été copié. Ensuite, il est identifié à tort comme suspect et, en plus des dommages matériels, les dégâts émotionnels sont également incroyablement importants. Par exemple, si l'employé en question n'a pas d'alibi vérifiable, cela peut entraîner une enquête longue et interminable. Bref, en tant que directeur ou responsable du département TIC, vous voulez à tout prix éviter cette situation. Et c'est alors que l'amélioration de la sécurité de votre entreprise s'impose.

La nouvelle technologie est pratiquement impénétrable

Pour la sécurité de votre entreprise, il est impensable que vous investissiez des millions d'euros dans la cybersécurité, et que vous ignoriez ensuite le fait que votre contrôle d'accès est une vraie passoire. Cela peut et doit donc se faire différemment, pour vous, vos données et vos collaborateurs. C'est pourquoi il est grand temps que vos badges, lecteurs de badges et l'infrastructure sous-jacente soient remplacés par des techniques plus récentes et plus sûres telles que le MIFARE DESFire. Vos employés peuvent simplement ouvrir les portes avec leur propre badge ou carte d'accès, comme avant. Cependant, ces nouvelles techniques ne peuvent pas être piratées ou copiées, car elles sont cryptées avec des cryptages de pointe qui, tout comme votre ancien logiciel, dureront des années. Et grâce à l'innovation technologique, les nouveaux badges offrent également de nouveaux avantages, comme le téléchargement d'un solde pour le paiement à la cantine. Cela rend non seulement votre entreprise plus sûre, mais aussi plus conviviale pour vos employés. ■

Non seulement la cybersécurité est en constante évolution, mais les criminels utilisent également de plus en plus des moyens numériques pour se frayer un chemin.

Il est temps de vraiment sécuriser votre entreprise

Commençons par dire qu'il est bien sûr très important que votre cybersécurité soit en ordre. Cependant, une fois que le contrôle d'accès de votre entreprise est très obsolète, les nombreuses couches de cybersécurité ne peuvent malheureusement plus rien faire. Et puis votre entreprise court toujours un risque inutile de cambriolages, avec toutes les conséquences que cela comporte. Heureusement, il existe des techniques plus récentes et plus sûres qui assurent vraiment la sécurité de votre entreprise, sans modifier structurellement la façon dont vos employés ouvrent la porte le matin. Mais une chose est sûre : les criminels seront vraiment laissés pour compte cette fois-ci.

Êtes-vous prêt à vraiment sécuriser votre entreprise ? Nous nous ferons un plaisir de vous parler pour discuter des possibilités. Cela rendra votre entreprise impénétrable sur tous les fronts !

Vous voulez qu'on continue à en parler ensemble ?
Alors vous pouvez nous appeler au +32 (0)3 312 92 30.
Nous avons hâte de vous parler !

GET
Azkoyen Time & Security Division

GET nv
Antwerpsesteenweg 107
2390 Malle, Belgique
+32 3 312 92 30
info@get.be
www.get.be

GET Nederland bv
Albert Einsteinweg 4
8218 NH Lelystad, Pays-Bas
+31 320 25 37 90
info@get.nl
www.get.nl