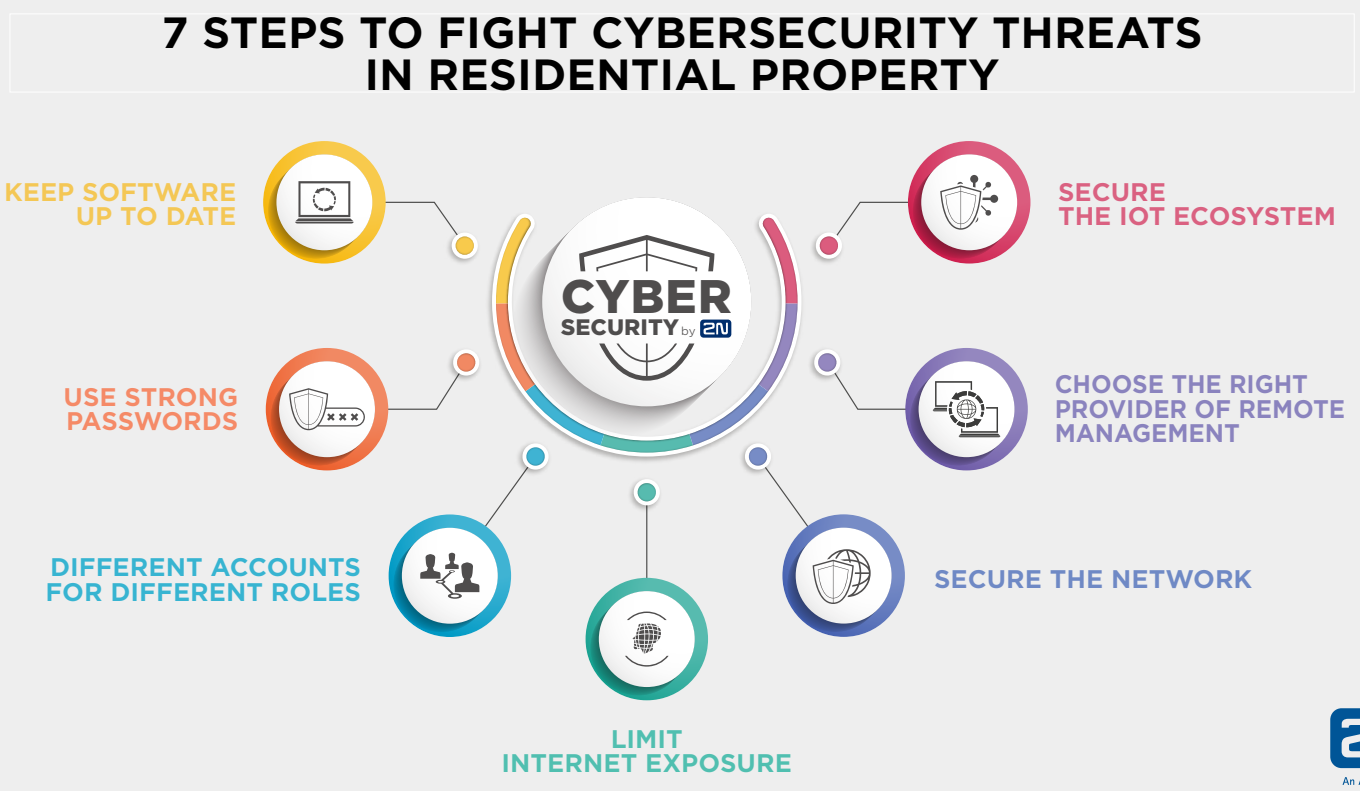

Une sécurité maximale est essentielle à la protection des bâtiments intelligents contre les cyberattaques

Personne ne niera l'importance cruciale de veiller à la sécurité et aux normes de sécurité élevées pour protéger les bâtiments intelligents et les données essentielles contre des attaques paralysantes, déclare 2N, leader mondial en systèmes de contrôle d'accès IP. Pour attirer l'attention en ce mois de la cybersécurité, 2N et Kaspersky, leader mondial dans le domaine de la cybersécurité, ont publié des conseils pertinents pour armer le consommateur mais aussi les gestionnaires de bâtiments d'exploitation contre les cyberattaques.

Cette action est le résultat d'une étude de Kaspersky. L'entreprise a constaté que la Belgique se positionnait en sixième place en matière de cyberattaques de systèmes de gestion des bâtiments en Europe. En Belgique, près de 40% des bâtiments intelligents ont dû parer à une cyberattaque de leurs systèmes. Les attaques sont des variantes de spyware – malware qui tentent de voler les données de connexion de comptes bancaires et autres informations précieuses.

L'intégration de technologies intelligentes dans les bâtiments imprègne la vie quotidienne des utilisateurs qui bénéficient d'un confort et d'une flexibilité. Des ascenseurs au chauffage jusqu'aux systèmes d'alarme et systèmes de gestion d'accès : la part des systèmes critiques couplés aux réseaux qui communiquent entre eux, via les téléphones intelligents et l'IoT, est en augmentation.

Il est crucial de conscientiser les utilisateurs à d'éventuelles vulnérabilités dans leurs systèmes, et de les conseiller à prendre des mesures adéquates. Une gestion intelligente et l'application de normes de sécurité élevées rendent les bâtiments intelligents extrêmement effectifs. Ils supportent les mesures d'efficience énergétique et contribuent à réduire les coûts d'exploitation. Si ces systèmes sont piratés, les routines quotidiennes dans le bâtiment – mais aussi les résidents – courent un risque. Des intrus physiques et virtuels peuvent utiliser les systèmes d'interphonie et les équipements de contrôle d'accès pour obtenir des mots de passe, pour 'écouter' des conversations non verrouillées et avoir un accès complet aux données, aux applications et aux biens personnels. Le ransomware est déployé, une attaque de 'l'homme du milieu' est mise en place qui permet même de s'infiltrer dans le bâtiment.

Tomáš Vystavěl, 2N's Chief Product Officer: « Les systèmes d'interphonie intelligents se développent rapidement et deviennent indispensables dans les habitations et les bureaux en Europe. Pourtant, certains appareils peuvent exposer le consommateur à un risque de piratage qui le rend vulnérable et compromet la cybersécurité. Opter pour un dispositif conforme aux normes de sécurité spécifiques est un premier pas vers une sécurité incraquable des logements de résidents. »

2N et Kaspersky proposent des conseils pour protéger les bâtiments intelligents, les données essentielles et la sécurité contre les pirates:

- Choisissez une solution de sécurité fiable sur mesure, développée spécifiquement pour les environnements ICS et qui protègera toujours votre réseau.
- Prévoyez un réseau indépendant – exclusivement dédié aux dispositifs traitant les informations sensibles -, utilisez un LAN virtuel (VLAN) et assurez-vous que les fabricants des équipements ou logiciels installés utilisent les protocoles d'implémentation standard comme HTTPS, TLS, SIPS ou SRTP.
- Protégez votre écosystème IoT: prévoyez un réseau distinct avec l'équipement IoT et choisissez un mot de passe fort pour votre routeur. N'installez jamais un nouvel équipement électronique sans avoir vérifié les normes de sécurité du fabricant.
- Créez différents comptes avec différents droits: les utilisateurs peuvent uniquement apporter des modifications à leurs tâches spécifiques, tandis que l'administrateur a des privilèges plus importants qui lui permettent de gérer le bâtiment et les comptes associés.
- Mettez votre logiciel régulièrement à jour: en installant la dernière version du firmware, vous minimisez les risques liés à la cybersécurité. Toute mise à jour répare les failles du logiciel en appliquant les derniers correctifs de sécurité.
- Utilisez des mots de passe forts et complexes ou du moins des mots de passe avec 6 caractères dans une combinaison de chiffres, de lettres et de symboles.
- Effectuez régulièrement des contrôles de sécurité de l'infrastructure IT pour identifier d'éventuelles vulnérabilités et les neutraliser.
- Formez l'équipe de sécurité responsable de la protection de l'infrastructure IT pour pouvoir reconnaitre et traiter les menaces les plus courantes.

www.2N.cz
www.kaspersky.com