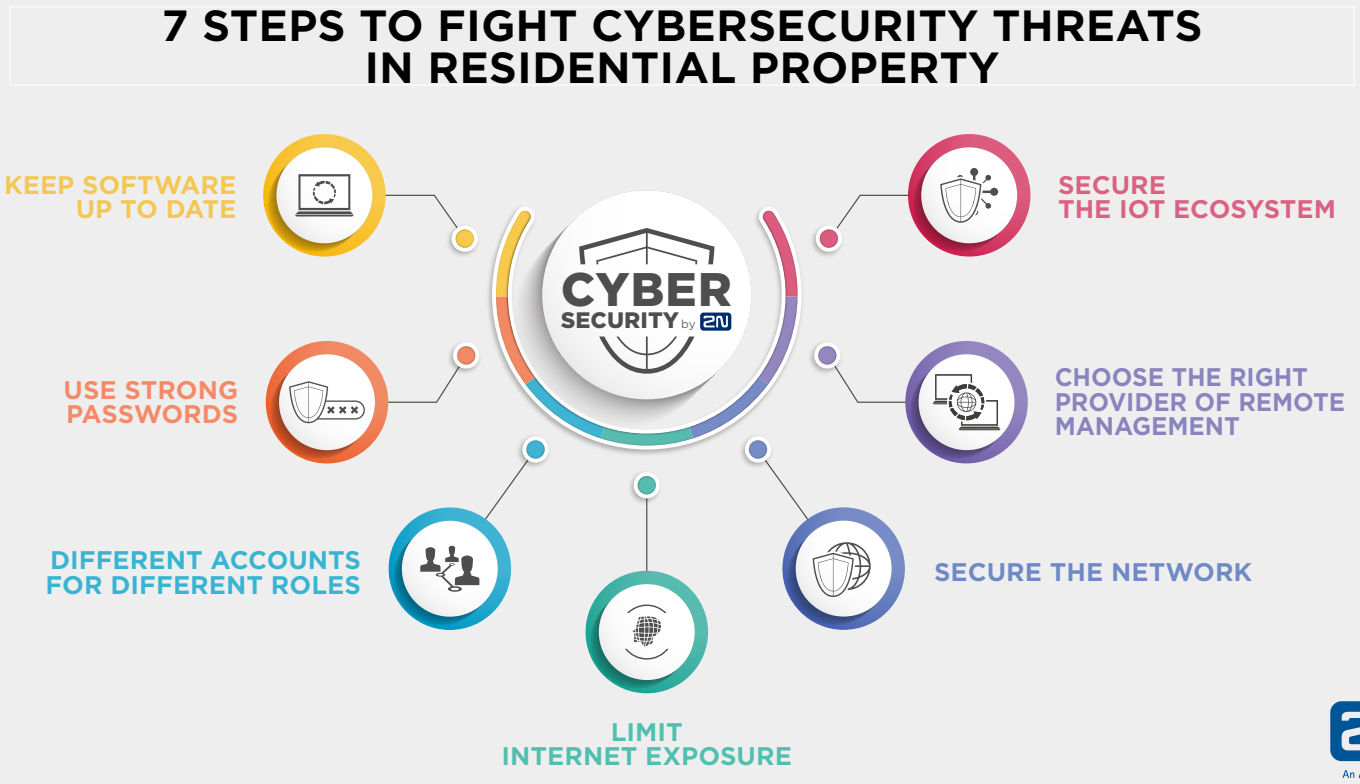

Maximale beveiliging is essentieel voor de bescherming van slimme gebouwen tegen cyberaanvallen

Dat het uiterst belangrijk is om te zorgen voor veiligheid en om hoge beveiligingsstandaarden te hanteren, zodat slimme gebouwen en essentiële data tegen verlammende aanvallen kunnen worden beschermd, zal niemand ontkennen, zo verklaart 2N, de wereldwijde leider in IP-access control systems. Om aandacht te schenken aan de maand voor cyberveiligheid heeft 2N in samenwerking met het Kaspersky, de wereldleider op het gebied van cyberveiligheid, essentieel advies gepubliceerd om de consument, maar ook beheerders van bedrijfsgebouwen, in staat te stellen zich tegen cyberaanvallen te wapenen.

Deze actie komt voort uit onderzoek van Kaspersky. Dit bedrijf kwam erachter dat België op de zesde plaats stond voor wat betreft cyberaanvallen op beheerssystemen voor slimme gebouwen overal in Europa. In België moest bijna 40% van de slimme gebouwen een cyberaanval op de systemen afslaan. Dit zijn aanvallen inclusief allerlei varianten van spyware – malware, waarmee geprobeerd wordt om inloggegevens tot bankrekeningen en andere waardevolle info te stelen.

De toepassing van slimme technologieën in gebouwen is in het dagelijks leven doorgedrongen en daarmee zijn de gebruikers verzekerd van comfort en flexibiliteit. Van liften, verwarming tot alarmsystemen en toegangsbeheersystemen: het aandeel aan netwerken gekoppelde kritische systemen die met elkaar, met slimme telefoons en met IoT communiceren, groeit.

Het is nu belangrijker dan ooit dat gebruikers op de hoogte zijn van eventuele kwetsbare plekken in hun systemen, waarbij het raadzaam is om adequate maatregelen te nemen. Bij intelligent beheer en de toepassing van hoge veiligheidsstandaarden, zijn slimme gebouwen uiterst effectief. Ze ondersteunen energie-efficiency-maatregelen en helpen daarmee op bedrijfskosten te besparen.

Als er in deze systemen ingebroken wordt, lopen niet alleen de dagelijkse routines in het gebouw een risico, maar ook de bewoners. Zo kunnen fysieke en virtuele inbrekers gebruik maken van intercoms en apparatuur voor toegangscontrole om achter wachtwoorden te komen, om onversleutelde conversaties "af te luisteren" en volledig toegang te verkrijgen tot data, applicaties en persoonlijke eigendommen. Dan wordt ransomware losgelaten, worden er man-

in-the-middle aanvallen uitgevoerd en kan men zelfs het gebouw binnensluipen.

2N's Chief Product Officer Tomáš Vystavěl verklaarde: "Slimme intercoms ontwikkelen zich snel en worden overal in Europa onmisbaar in woningen en kantoren. Toch kunnen sommige apparaten de consument blootstellen aan het risico van hack-operaties, waarmee ze kwetsbaar worden en waarbij de cyberveiligheid in het geding kan komen. Door een apparaat te kiezen dat aan bepaalde veiligheidsstandaarden voldoet, wordt de eerste stap gezet om de bewoners onkreukbare veiligheid van hun woning te kunnen bieden."

De adviezen van 2N en Kaspersky met betrekking tot de manieren om slimme gebouwen, essentiële data en beveiliging tegen hackers te beschermen zijn:

- Kies voor een betrouwbare, op maat gemaakte beveiligingsoplossing die specifiek voor ICS-omgevingen is ontworpen en waarmee uw netwerk altijd beschermd wordt.
- Zet een onafhankelijk netwerk op – exclusief gericht op apparatuur die gevoelige informatie verwerkt; maak gebruik van virtual LAN (VLAN) en zorg ervoor dat de fabrikanten van de geïnstalleerde apparatuur of software standaard implementatieprotocollen zoals HTTPS, TLS, SIPS of SRTP gebruiken.
- Bescherm uw IoT-ecosysteem: zet een afzonderlijk netwerk van IoT-apparatuur op, waarbij u voor uw router een sterk wachtwoord kiest. Installeer nooit nieuwe elektronische apparatuur zonder dat u de fabrikant en zijn beveiligingsstandaarden checkt.
- Maak verschillende accounts aan met verschillende rechten: gebruikers zullen alleen veranderingen kunnen doorvoeren met betrekking tot hun specifieke taken, terwijl de administrator grotere rechten heeft, zodat hij het gebouw en alle daaraan gekoppelde accounts kan beheren.
- Werk uw software regelmatig bij: door de laatste firmware-versie op uw apparatuur te installeren, minimaliseert u de risico's die met cyberveiligheid verbonden zijn. Elke update herstelt fouten in de software door de nieuwste veiligheidspatches toe te passen.
- Gebruik complexe, sterke wachtwoorden of ten minste wachtwoorden met 6 karakters in een combinatie van cijfers, letters en symbolen.
- Houd regelmatig veiligheidscontroles van de IT-structuur om eventuele kwetsbaarheden vast te kunnen stellen en te elimineren.
- Train het beveiligingsteam dat verantwoordelijk is voor de bescherming van de IT-infrastructuur om de meest gangbare bedreigingen te kunnen herkennen en aan te pakken.

www.2N.cz
www.kaspersky.com