IN OCCASIONE DEL CYBERSECURITY AWARENESS MONTH,
2N OFFRE UNA GUIDA AGGIORNATA PER PROTEGGERE GLI EDIFICI SMART
DAI CYBER-ATTACCHI

- *Secondo un recente sondaggio di Kaspersky è emerso che il numero di attacchi mirati a violare i dispositivi IoT è raddoppiato rispetto allo scorso anno (passando dal 16,17% al 32,72%). La maggior parte degli utenti (89%[1]), inoltre, è preoccupata per la sicurezza dei propri dispositivi.*
- *A un anno dalla prima guida di 2N sul tema cybersecurity, la società integra i consigli per le aziende sulla protezione del controllo degli accessi, alla luce del crescente livello di minaccia.*

Milano, 14 ottobre 2021 – In occasione del Cybersecurity Awareness Month 2021, che si celebra ogni anno ad ottobre, **2N** offre **utili consigli aggiornati per aiutare gli utenti e i proprietari di immobili a potenziare la sicurezza degli edifici smart**, alla luce del recente aumento degli attacchi informatici e della crescente vulnerabilità del controllo degli accessi domotici. Abbracciare l'innovazione e stare al passo con un futuro sempre più connesso e digitale in totale tranquillità, è possibile, adottando dei semplici ma efficaci accorgimenti.

Tomáš Vystavěl, Chief Product Officer di 2N, ha dichiarato: "In qualità di leader globale nei sistemi di controllo accessi IP, 2N ritiene necessario fornire ai clienti una guida sulla cybersecurity, da un lato per aiutare gli utenti ad affrontare l'incremento costante delle minacce e dall'altro, per aumentare la consapevolezza delle aziende nell'ambito del controllo degli accessi che, ad oggi, faticano ancora a stare al passo con questo tipo di eventi. Se il sistema di controllo accessi è compromesso, infatti, il funzionamento quotidiano dell'intero edificio e di conseguenza i suoi residenti e visitatori, trova rischio immediato. E se è vero che la consapevolezza generale è in aumento, è sempre più necessario accelerare il cambiamento".

Un recente report di **Kaspersky**, azienda leader nella cybersicurezza, ha infatti rivelato che durante i primi sei mesi del 2021 si sono verificati **oltre 1,5 miliardi di attacchi indirizzati a dispositivi IoT** (Internet of Things) come serrature, accessori smart per la casa e videocitofoni intelligenti. Per tracciare e prevenire questi attacchi, gli esperti di Kaspersky hanno creato degli

[1] Dati ottenuti tramite uno studio U&A effettuato nel primo semestre del 2020, su una base di utenti di smart home device in sette paesi.

honeypot, ovvero software speciali che imitano un dispositivo vulnerabile e una volta distribuiti pubblicamente su Internet vengono usati come "specchietti per le allodole" per attirare i criminali informatici. Secondo l'analisi, nel primo semestre 2021 **il numero totale di tentativi di infezione è raddoppiato rispetto al semestre precedente** (1.515.714.259 contro i 639.155.942 del secondo semestre 2020).

L'interesse da parte dei cyber-criminali per questo settore si è intensificato da quando è aumentato l'interesse da parte degli utenti per questi dispositivi. Secondo altri dati di Kaspersky, **l'89% degli individui è preoccupato per la sicurezza dei propri dispositivi**, è anche vero che gli utenti italiani credono di non essere abbastanza importanti per essere vittima di un hacker e proprio per questo rischiano di non proteggere adeguatamente i propri dispositivi connessi. Inoltre, secondo la *data privacy heatmap*[2] di Kaspersky, dopo la pandemia gli italiani sono molto più disposti a condividere i propri dati per ottenere maggiore libertà ed evitare nuove restrizioni.

Ecco allora i consigli aggiornati di 2N perché utenti e amministratori di edifici smart possano proteggersi da ogni minaccia, continuando a offrire e godere dei benefici dell'innovazione e della tecnologia:

1. **Perseguire la compliance adottando framework di controllo della sicurezza collaudati**. Due dei più rispettati sono ISO 27001 e SOC 2. Questi guidano le aziende nella creazione di sistemi e processi sicuri.
2. **Assicurarsi che il sistema di controllo accessi includa l'uso della crittografia e dell'autenticazione multi-fattore** per proteggere la comunicazione tra i dispositivi, gli amministratori e i device mobili e assicurarsi che non ci siano punti di accesso illeciti.
3. **Creare una rete indipendente dedicata esclusivamente ai dispositivi che gestiscono informazioni sensibili e assicurarsi che la comunicazione tra loro sia criptata.** È consigliabile mettere questi dispositivi in una LAN virtuale separata (VLAN) e assicurarsi che i produttori dei dispositivi o dei software installati utilizzino protocolli di implementazione come HTTPS, TLS, SIPS o SRTP di default.
4. **Creare diversi account con diversi privilegi**. Un utente potrà apportare solo le modifiche collegate ai suoi specifici compiti, mentre all'amministratore saranno forniti privilegi maggiori per la gestione dell'edificio e di tutti gli account collegati.
5. **Aggiornare il software regolarmente.** Installare l'ultima versione del firmware sui dispositivi in esecuzione è importante per mitigare i rischi di cybersecurity, poiché

[2] "*Stiamo perdendo il controllo sui nostri dati?",* giugno 2021
Consultabile a questo link: https://www.kaspersky.it/blog/europe-privacy-heat-map/24820/

ogni nuova release risolve i bug riscontrati sul software, implementando le patch di sicurezza più recenti.

6. **Formare i propri dipendenti per evitare le minacce di social engineering.** L'elemento umano è la parte più vulnerabile di qualsiasi sistema e gli hacker possono indurre le persone con l'inganno a commettere errori di sicurezza o a diffondere informazioni sensibili. È quindi necessario formare regolarmente i dipendenti sulle corrette procedure per la sicurezza.

Per scoprire ulteriori dettagli sull'approccio di 2N alla cybersecurity, è possibile visitare la seguente pagina: https://www.2n.cz/it_IT/informazioni-su-2n/cybersecurity

2N

2N è l'azienda leader a livello mondiale nei sistemi di controllo accessi IP.

Da sempre all'avanguardia nell'innovazione del settore, 2N ha sviluppato il primo citofono IP al mondo nel 2008 e il primo citofono LTE/4G dieci anni dopo. L'azienda offre un'intera gamma di soluzioni nel campo dei citofoni, delle unità di risposta e dei sistemi di controllo accessi. È specializzata nel settore residenziale e dispone di soluzioni per smartphone e tablet, basate sulla tecnologia Bluetooth.

2N prende sul serio sia l'innovazione che il design e vanta prestigiosi riconoscimenti come il Red Dot e l'iF Design Award.

Fondata nel 1991 in Repubblica Ceca con sede a Praga, 2N ha attualmente un team in altri otto paesi (USA, Regno Unito, Germania, Italia, Francia, Spagna, Emirati Arabi Uniti e Australia) e dispone di un'ampia rete di distributori in tutto il resto del mondo.

Per maggiori informazioni, visitare il sito http://2n.cz/it_IT/