COMUNICATO STAMPA

REGALI DI NATALE A PROVA DI CYBER SICUREZZA

Boom di shopping online e regali "smart" aprono le porte a possibili attacchi informatici. Obiettivi: furto dati personali ed estorsione digitale.
Ecco, dagli esperti del Gruppo IMQ, i consigli su come proteggersi.

Milano, 18 novembre 2020 – I regali hi tech sono tra i più desiderati e gettonati sotto l'albero di Natale. Spesso, però, gli apparecchi connessi, sia ad uso personale sia ad uso domestico, sono quelli che più espongono a rischi di sicurezza sul fronte digitale, aprendo potenzialmente la porta ai cyber criminali.
Il mondo della domotica/IoT si presenta, infatti, molto vulnerabile in generale e questo è stato dimostrato da molti studi: solo **nel primo semestre del 2020 gli attacchi rivolti ai dispositivi IoT sono aumentati del 35%** rispetto alla seconda metà del 2019[1], e questo perché ad oggi, dietro al cyber crime ci sono veri e propri **gruppi di criminali ben organizzati, con un fatturato che si aggira mediamente sui 1.500 miliardi di dollari all'anno**[2]. Gli scopi alla base dei loro intenti sono diversi, primo fra tutti quello remunerativo.

Smart TV, **assistenti vocali, proiettori fotografici**, **diffusori audio**, **dispositivi ad uso personale**, **smart watch**, **fitness tracker**, **console per videogiochi, lampadine e prese intelligenti, sensori di movimento connessi a sistemi di riscaldamento smart**: tutti regali che potrebbero esporre direttamente chi li riceve ad attacchi alla "persona" (phishing), con furto di dati personali (preferenze e abitudini quotidiane, navigazione, ma anche dati riguardanti la salute, come il battito cardiaco o l'ossigenazione del sangue) o redirezione della navigazione verso contenuti malevoli. Se interconnessi poi, creano un ecosistema integrato di dispositivi informatizzati: più questo ecosistema è vasto maggiori sono le possibilità di violazione.

Anche i **device "smart" per la domotica** - elettrodomestici come il frigorifero, allarmi casalinghi, termostati e cancelli, oggetti domestici singolarmente governabili tramite una connessione Internet - espongono l'utente a rischi, ma indirettamente perché potrebbero essere il veicolo per attacchi volti a causare un disservizio, come il blocco delle funzionalità che offrono, l'inattivazione di un allarme o lo spegnimento di un frigorifero. Spesso questi dispositivi consentono a qualcuno o qualcosa di entrare nella nostra vita, nella nostra abitazione o anche usare i nostri dispositivi per arrecare un danno a terzi.

"*Quando pensiamo ai rischi cyber connessi al mondo IoT, in particolare legato ai dispositivi domestici, ci sono due ambiti di preoccupazione*" segnalano gli esperti del Gruppo IMQ. "*La privacy - ossia quali informazioni i dispositivi raccolgono, come vengono trattate e usate - e la sicurezza in senso stretto. Ovvero: questi dispositivi consentono a qualcuno o qualcosa di entrare nella mia vita, nella mia abitazione o usare i miei dispositivi per arrecare un danno a terzi*?"

[1] Fonte: "*Microsoft Digital Defense Report*" https://www.microsoft.com/en-us/security/business/security-intelligence-report
[2] Fonte: "*Into the Web of Profit*", https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Un attaccante potrebbe anche abusare della potenza di calcolo o della connessione a Internet dei dispositivi: esempi sono il mining di bitcoin (la creazione di cryptomonete), la partecipazione a botnet (reti di dispositivi compromessi) usate per altri scopi, mettendo così la vittima in condizione di diventare intermediaria inconsapevole nell'esecuzione di attacchi informatici o movimentazioni di dati non autorizzati.

"*I device IoT attuali non sempre offrono livelli di sicurezza adeguati rispetto alla sicurezza nativa di un dispositivo desktop o di un dispositivo mobile come un cellulare o un tablet e questo fa lievitare i rischi*" aggiungono gli esperti del Gruppo IMQ. Spesso, poi, i dispositivi sono coperti da una garanzia di prodotto di tipo tradizionale, che non si estende alle falle di sicurezza nel software dell'apparecchio. "*Ciò si traduce all'atto pratico in una minor frequenza di rilascio di aggiornamenti software che possano sanare bug noti o vulnerabilità del software scoperte nel corso della vita di un device IoT*".

Ci sono poi alcuni comportamenti culturali e inconsapevoli che possono creare la situazione giusta per un attacco informatico. Per esempio, sottovalutare il device "smart" senza considerare che si sta parlando di piccoli computer, connessi ad Internet e di conseguenza possibile obiettivo di un attacco informatico.

Sempre legato al fattore culturale è anche la filiera dei device IoT. "L'informatizzazione degli oggetti è qualcosa di molto recente ed ha contaminato in maniera rapidissima un mondo che non era culturalmente vicino alla sicurezza informatica" spiegano gli esperto IMQ. *"Il venditore di elettrodomestici non sempre è preparato per aiutare il suo cliente nella configurazione in sicurezza informatica del forno o del frigorifero. L'elettricista che ha sempre realizzato impianti tradizionali, d'improvviso si è trovato tra le mani dispositivi connessi, senza che questo cambiamento, in alcuni casi, sia stato preceduto da adeguata preparazione sui pericoli ad esso associati*".

I consigli per avviare in sicurezza un nuovo regalo "smart"

Ma andiamo allora nel concreto e vediamo i consigli dei tecnici esperti in sicurezza informatica del Gruppo IMQ per tutti coloro che, scartando i regali di Natale, troveranno oggetti connessi, come uno **smart watch per il fitness**, uno **smart assistant a comando vocale** o una **smart TV**:

- Non lasciare le impostazioni o le password di default, preimpostate dall'installatore/ produttore;
- Utilizzare una nuova password e cambiarla periodicamente;
- Impostare password difficili da compromettere, non necessariamente complesse: è meglio una password lunga ma facile da ricordare che una password troppo complessa: MiPiaceAndareAlMareInInverno è molto meglio di P5:/R32@,1
- Se presente, attivare sempre l'autenticazione a due fattori per proteggere le credenziali di accesso;

- Aggiornare sempre il software dell'apparecchio quando il produttore ne rilascia uno nuovo e usare sempre e solo l'app ufficiale del produttore per configurare e gestire il dispositivo;
- Adottare gli standard WPA2 per le reti wireless;
- Se possibile utilizzare un account dedicato al (o ai) device smart, in modo tale che in caso di compromissione, ciò non comporti un furto di identità esteso ad altri aspetti della sfera personale della vittima.

Per quanto riguarda in generale la nostra rete Wi-Fi, i consigli invece sono:

- Nella casa connessa, se possibile creare nella rete domestica un network Wi-Fi secondario, dedicato esclusivamente agli smart device connessi, in modo da proteggere i dispositivi connessi all'altra Rete (ad esempio il pc di lavoro);
- Se possibile fare in modo che l'SSID di casa (*Service Set Identifier* - in pratica il nome della nostra rete Wi-Fi) non sia visibile: in questo modo si riduce ulteriormente il rischio di vedere intrusi nella nostra Rete.

"*L'utilizzo massiccio di dispositivi intelligenti e connessi è paragonabile a raccontare la nostra vita, nei più fini dettagli, ad uno sconosciuto. Il grave problema è che spesso non ne siamo consapevoli*" sintetizzano gli esperti del Gruppo IMQ. Per questo, la soluzione sta nel riconoscere alle persone la vera centralità nella sfida per la sicurezza informatica.

Shopping natalizio online: attenzione ai prezzi troppo bassi!

Dagli esperti arriva anche un segnale di attenzione sugli **acquisti natalizi, che – quest'anno più che mai – si prevede che avverranno in forma digitale**. "*Visto che quest'anno si stima un incremento considerevole dello shopping online, gli attaccanti stanno creando siti di e-commerce che mostrano una grande quantità di merce disponibile ma che in realtà non esiste, invogliando l'utente ad effettuare l'acquisto, senza poi ricevere la merce. **I prezzi fuori mercato presenti su un online shop, pop-up durante la navigazione o e-mail con offerte di Natale fin troppo convenienti devono essere un primo campanello di allarme***" osservano gli esperti del Gruppo IMQ.

Per questo è importante che, prima di fare un acquisto venga fatta una verifica sul venditore. Come? Controllando i feedback attraverso un motore di ricerca, cercando il nome del sito unito alla parola "feedback" oppure "è sicuro?" in modo da leggere i risultati da cui emerge un'idea del negozio online. Questo, al fine di verificare che il vendor sia noto, abbia delle recensioni molto positive sui portali di e-commerce, abbia una storia informatica non limitata all'ultimo anno, sia affidabile e solido dal punto di vista della propria durata. Qualche altro consiglio in vista dello shopping online:

- Non utilizzare un Wi-Fi pubblico per fare acquisti o operazioni finanziarie;

- Effettuare acquisti in siti con certificati di sicurezza https://;
- Attivare l'autenticazione a due fattori per accedere al proprio account: quasi tutte le piattaforme di e-commerce prevendono questa possibilità (ma pochi la utilizzano);
- Se un'offerta appare "troppo bella per essere vera", probabilmente è finta.

******

Nota per la redazione

I contenuti del presente documento sono frutto dell'esperienza degli esperti in cyber e software security appartenenti a **IMQ Intuity** e **IMQ Minded Security**, le due società di riferimento internazionale nel campo della sicurezza informatica, entrate di recente a far parte del **Gruppo IMQ**.

******

Il Gruppo IMQ

Il Gruppo IMQ rappresenta una delle più importanti realtà italiane nel settore della valutazione della conformità (certificazione, prove, verifiche, ispezioni). Forte della sinergia tra le società che lo compongono, dell'autorevolezza acquisita in quasi 70 anni di esperienza, della completezza dei servizi offerti, il Gruppo IMQ si pone come punto di riferimento e partner delle aziende che hanno come obiettivo la sicurezza, la qualità e la crescita sostenibile.
Il Gruppo IMQ è attualmente composto da IMQ Group S.r.l. (holding), IMQ S.p.A., CSI S.p.A., IMQ Intuity S.r.l, IMQ Minded Secuity S.r.l., IMQ CSI Deutschland GmbH (Germania), IMQ Iberica S.L. (Spagna), IMQ Tecnocrea S.L. (Spagna), IMQ Polska Sp. z o.o. (Polonia), IMQ Certification (Shanghai) Co. Ltd. (Cina), IMQ Turkey (Turchia), IMQ Gulf FZCo (Emirati Arabi Uniti). **www.imqgroup.eu**

Ufficio Stampa IMQ Claudia Sartori | +39 334 3936863 | c.sartori@sartoricomunicazione.it

Denise Dreon | +39 333 9049223 | d.dreon@sartoricomunicazione.it

Comunicazione IMQ Roberta Gramatica | +39 02 5073369 | roberta.gramatica@imq.it