



Domotica

Di Michele Braga



Smart home sicure

I sistemi smart per la casa e connessi alla Rete sono pronti per resistere agli attacchi informatici?

La crescente diffusione nel mercato consumer delle tecnologie smart per la casa, sta portando a un incremento rapido del numero delle funzioni di sicurezza, di sorveglianza e di controllo delle abitazioni esposte sulla Rete attraverso i sistemi di controllo e gestione che offrono gateway per l'accesso remoto agli utenti.

Un aspetto che andrebbe valutato in anticipo, prima di dover correre ai ripari è quello relativo alla sicurezza di tali sistemi contro gli attacchi informatici.

Quando in campo domotico si parla di sicurezza contro le effrazioni ci si riferisce a una serie di sistemi hardware e servizi che consentono di rilevare un tentativo di intrusione, di attivare reazioni automatizzate a livello locale e di notificare l'informazione in remoto al proprietario e eventualmente alle forze dell'ordine.

A differenza degli impianti classici utilizzati in passato, ma molto diffusi ancora oggi, i sistemi di sicurezza domotici combinano le funzioni di sicurezza standard (allarmi di protezione perimetrale esterna, protezione perimetrale interna

e protezione volumetrica) con altri dispositivi legati al controllo degli accessi (serrature elettroniche, tapparelle e lucernari motorizzati), alla videosorveglianza interna e con i servizi telefonici e informativi per assicurare non solo una gestione locale, ma anche remota.

Gli impianti in commercio possono essere divisi in due grandi categorie: quelli di tipo integrato e quelli meno strutturati che prevedono l'utilizzo di uno sciame di sensori e dispositivi collegati prevalentemente per mezzo di una

rete wireless e tipicamente connessi a un servizio di gestione cloud esterno. Al di là delle diversità specifiche in termini di caratteristiche e costi d'installazione, i quesiti da porsi quando si decide di implementare funzioni di sicurezza sono relativi alle differenze in termini di resistenza contro gli attacchi esterni e a come proteggere in modo corretto i punti più vulnerabili delle proprie difese.

Le prime sono quelle generalmente offerte dai grandi brand che si occupano di home e building automation. Gli impianti di tipo integrato utilizzano generalmente collegamenti di tipo cablato. In questo modo si riducono al minimo le possibilità di attacco informatico diretto ai singoli sensori o punti di controllo;



L'hub proposto da SmartThings è una soluzione consumer molto diffusa e di facile installazione



Controllo interfaccia KNX/IP di Gewiss da utilizzare in un sistema domotico integrato connesso attraverso la rete Ethernet. Supporta fino a cinque connessioni simultanee e può essere utilizzato con l'App HAPPY HOME per smartphone e tablet (disponibile per i sistemi Android e iOS) per la gestione dell'impianto domotico KNX via rete cablata o Wi-Fi da remoto.

i malintenzionati dovrebbero quindi avere accesso fisico a uno dei dispositivi per poter accedere alla rete di controllo del sistema domotico. In questo caso il punto critico è il nodo di connessione della centrale domotica con i servizi Internet esterni.

L'hub di connessione è, infatti, il punto più esposto e al tempo stesso è quello da cui dipende la gestione dell'intero impianto. Per questo motivo dovrebbe essere corredato di protezioni invalicabili, ma non sempre è così.

Un impianto domotico ben realizzato dovrebbe in primo luogo far uso di cablaggi fisici dove possibile in modo da ridurre al minimo i punti di accesso attraverso comunicazioni radio, disporre di protezioni adeguate sui dispositivi wireless presenti e mettere in sicurezza punto più critico, ovvero la centralina di connessione alla Rete.

Sebbene sia molto conveniente dal punto di vista economico e di installazione, l'utilizzo della connettività wireless fornisce un possibile vettore di attacco senza la necessità di avere accesso fisico ai dispositivi o alla rete. Non sorprende che la rapidità con la quale il mercato si sta evolvendo abbia portato a rilasciare prodotti che presentano vulnerabilità ormai accertate. Lo scorso mese di agosto, secondo un'analisi eseguita da

Tripwire, è risultato che alcuni device molto popolari – SmartThing Hub, WinkHub e MiOS Vera – mostrano vulnerabilità ad attacchi esterni. Tali vulnerabilità potrebbero permettere ai malintenzionati di prendere il controllo del sistema smart e di sfruttarlo a proprio vantaggio, trasformando il sistema di sicurezza in un bacino di informazioni preziosissime per chi volesse introdursi nell'abitazione. Grazie al controllo dei sensori posizionati sugli accessi, quelli di presenza e delle videocamere è possibile scoprire se e



quando avete lasciato la vostra abitazione, quali varchi sono stati lasciati aperti (magari avete volutamente lasciato socchiusa una finestra per far circolare l'aria) e in quali stanze sono presenti persone. Ancora, l'accesso alla rete smart permetterebbe di cambiare le impostazioni dell'impianto di allarme, di aprire le serrature elettroniche e di accedere all'eventuale rete domestica e ai dispositivi ad essa connessi per sottrarre informazioni personali.

Per ottenere un ambiente domestico non solo smart, automatizzato, sicuro, ma anche protetto è necessario implementare quelle difese che dovrebbero generalmente essere adottate anche per proteggere una rete domestica che non controlla una smart home. Tali difese prevedono l'utilizzo di un firewall e di connessioni Vpn (Virtual Private Network) sulle quali tutte le informazioni viaggiano in modo cifrato. Va comunque prestata inoltre particolare attenzione a quali altri dispositivi sono presenti nella rete domestica, a come sono collegati e configurati. Basta infatti inserire nel punto sbagliato della rete un dispositivo visibile dall'esterno e facilmente attaccabile per lasciare una porta di accesso aperta che può essere utilizzata per sottrarre informazioni utili o addirittura prendere il controllo dell'intero impianto.

Poiché la maggior parte degli utenti non è esperta di sicurezza informatica, la responsabilità ricade al momento sui produttori dei dispositivi come singoli elementi o come parti di soluzioni più complesse e, ovviamente, degli installatori.

“

La rete informatica di casa avrà bisogno di solide protezioni via via che le abitazioni diventeranno più smart.