Elementi di sicurezza negli impianti domotici – parte terza

Dopo aver parlato di fattore umano e sicurezza degli impianti in una casa domotica, questo terzo articolo prova a descrivere le implicazioni di sicurezza legate alla connessione di questi impianti a servizi Internet esterni.

Uno dei fattori di successo della diffusione della domotica è la possibilità di accedere all'impianto tramite *smartphone* quando si è fuori casa per monitorare, intervenire o verificarne lo stato. Inoltre l'impianto stesso può recuperare informazioni importanti usando servizi terzi prima di decidere come comportarsi. Un esempio classico è il caso in cui, prima di avviare l'impianto di irrigazione, il sistema verifichi le condizioni meteo in zona così da avere maggiori informazioni per decidere quando e quanto innaffiare.

Infine, faremo il punto del nostro excursus fatto con i tre articoli scritti proponendo alcuni temi di discussione che saranno da affrontare per portare il giusto livello di consapevolezza all'interno di questo settore.

Connessione dall'esterno agli impianti domotici

Probabilmente i primi sistemi residenziali che hanno dato la possibilità di un controllo remoto sono stati gli impianti di antifurto e videocontrollo: la possibilità di controllare cosa stava succedendo dentro casa dall'esterno era – e lo è tutt'oggi – una funzionalità ritenuta importante. Inizialmente lo si faceva usando la linea telefonica, quindi quella GSM, veicolando le informazioni e l'interazione prima tramite suono e quindi tramite SMS. La successiva e naturale evoluzione è

stata quella dell'utilizzo di linee dati veloci (3G/4G, ADSL/Fibra) che ha consentito l'utilizzo crescente dello scambio di dati video e del progressivo passaggio all'interazione in tempo reale. Oggi è del tutto usuale collegarsi alle telecamere presenti nell'abitazione per verificare da remoto lo stato dell'alloggio, rispondere a un videocitofono dall'ufficio o spegnere le luci in tempo reale da qualunque parte del mondo ove sia disponibile una connessione Internet.

Ovviamente possiamo affermare – ed è obiettivamente banale – che ogni casa ed edificio connesso ad una linea dati tramite un operatore telefonico è niente più che un nodo di una rete. Ogni impianto domotico, quindi, è esposto ad ogni forma di attacco pensabile per un nodo di rete qualsiasi ed andrebbe protetto nello stesso modo. Purtroppo, però, questa consapevolezza non è così diffusa: pensare ad un'abitazione come se fosse un semplice terminale connesso è un passaggio culturale che al momento non è del tutto avvenuto nel settore (soprattutto per il residenziale).

Difatti la procedura più comune per permettere una connessione tramite app cellulare dall'esterno agli apparati interni di un impianto domotico è quella di "aprire le porte" ovvero impostare regole di NAT sul modem dell'operatore. Tipicamente le porte aperte sono le porte standard indicate dal produttore e sono reindirizzate direttamente sull'IP dell'apparato senza alcun meccanismo di identificazione intermedia (es. restringendo gli accessi a specifici MAC Address). Se sommiamo questa situazione con la poca abitudine a modificare le credenziali di accesso standard degli apparati (si faccia riferimento ai precedenti articoli) è chiaro quanto possa essere facile accedere allo *stream* di una telecamera interna usando uno scanner di rete – gli intervalli di indirizzi assegnati ad ogni operatore sono addirittura facilmente riscontrabili online [1] perfino segmentati per città [2] – ed un browser. Come evidenziato negli articoli precedenti, parte

della colpa di questa “insicurezza diffusa” va cercata anche nell’inadeguatezza dei prodotti disponibili che spesso non implementano protocolli sufficientemente recenti o mancano del tutto di meccanismi di autenticazione/crittografia o della possibilità di personalizzare i parametri di configurazione delle connessioni.

Non ci stancheremo mai di ricordare come buona parte della sicurezza possa essere raggiunta con una corretta architettura e progettazione, in particolare ricordiamo:

1. **separare nettamente la rete che ospita i *device* domotici dalla rete utente**. L’abbiamo sottolineato più volte precedentemente, la separazione delle reti tramite *router* e *firewall* accuratamente configurati è la condizione di minima sicurezza che bisogna iniziare a garantire. Inoltre, questa azione, non ha il minimo impatto sulle modalità di utilizzo dell’impianto da parte dell’utente che non dovrà barattare la sicurezza con un aumento di complessità;
2. **usare connessioni protette** per accedere all’interno degli impianti. Sostituire l’accesso remoto tramite NAT con VPN e SSH Tunneling in modo da garantire connessioni cifrate, autenticate e autorizzate. Questa opzione, purtroppo, in molti casi necessita un aumento di complessità delle procedure di connessione che l’utente finale deve effettuare per accedere.

L’aumento di complessità per l’utente finale non è da sottovalutare. Nell’ambito della domotica residenziale c’è una ipersensibilità alla complessità da parte degli utenti che percepiscono un netto calo del livello di comfort a fronte anche di un minimo aumento di complessità delle procedure. Questo può essere un grosso ostacolo alla messa in sicurezza di un impianto: l’utente solitamente preferisce barattare la sicurezza con la semplificazione. Al riguardo, fortunatamente, si può evidenziare un trend da parte dei produttori – in particolare dei prodotti legati alla sicurezza e

all’integrazione di sistemi [3] – che dimostrano un’attenzione maggiore al tema. Cresce da parte di questa classe di produttori l’offerta di app e *device* che si connettono con modalità sicure di accesso basate su VPN del tutto trasparenti all’utente[4].

Connessione degli impianti domotici a servizi esterni

Oltre alla necessità di accesso degli utenti ai propri impianti c’è oggi sempre maggiore necessità da parte degli impianti stessi di collegarsi verso servizi terzi di *storage*, elaborazione dati e servizi altri.

Ad esempio, il controllo vocale è al momento attuale uno dei trend tecnologici emergenti [5] e tutti i *device* che permettono questo tipo di controllo si appoggiano a server esterni di elaborazione, acquisizione dati e ricerca. In questo scenario, quindi, se avessimo un sistema domotico controllato da Alexa o Google Home, dovremmo consentire a questi *device* di comunicare con servizi esterni.

In tali scenari le criticità principali possono derivare da:

1. protocolli di comunicazione verso servizi terzi non sicuri;
2. condivisione di dati sensibili con soggetti terzi;
3. interruzione di connettività.

Fortunatamente casi di **protocolli di comunicazione non sicuri** stanno progressivamente riducendosi poiché il livello di sicurezza di servizi nati per sopravvivere online è mediamente alto, monitorato e mantenuto. Ovviamente diventa cruciale la scelta del fornitore: sarà necessario selezionare il fornitore di servizi che tenga in conto gli aspetti di sicurezza, che possa vantare una comprovata fiducia del mercato e che non sia stato scelto semplicemente per via del prezzo del *device*. Una valutazione di qualità del prodotto deve oggi essere fatta

sempre considerando la qualità e la sicurezza dei servizi offerti e non solo dell'oggetto in sé.

Il tema **della condivisione dei dati sensibili** come le credenziali di login, le API KEY e altri dati necessari alla connessione è altro tema da non sottovalutare in ambito domotico. Spesso questi dati sono forniti e condivisi con i servizi terzi con gran facilità senza soppesare bene se effettivamente il servizio attivato porti un beneficio concreto in termini di comfort e qualità della vita quotidiana o ne aumenti inutilmente la complessità. In caso di *data breach* dei siti dei fornitori di servizi, tutto il nostro impianto viene di conseguenza, esposto ad accessi non autorizzati. Se si usufruisce di servizi online, l'installatore o il manutentore dovrebbe predisporre per le connessioni *machine-to-machine* una politica per l'utilizzo di password sicure, differenziate e per il loro rinnovo periodico. Sicuramente la nuova normativa europea sul trattamento dei dati personali (GDPR) [6] – con l'obbligo di informare tempestivamente gli utenti in caso di violazione dei dati – dà l'opportunità di ripristinare rapidamente la sicurezza di un impianto domotico sempre che, ovviamente, si sia provveduto a definire una politica di manutenzione continuata e che i manutentori si siano organizzati per ricevere e gestire tali comunicazioni.

L'ultimo punto della nostra lista, **ossia la garanzia che il sistema funzioni in assenza di connettività**, può sembrare bizzarro. Per un impianto domotico, troppo spesso, la progettazione viene fatta partendo dai *device* e non dalle esigenze o subisce l'invasione dei prodotti *consumer* che non sempre hanno certe "malizie". Un esempio classico è quello delle *smart plug* che possono essere comandate solo da cellulare. Queste prese appoggiano tutta la loro intelligenza sulla condivisione di dati e statistiche verso server esterni che elaborano e presentano valori di consumo e altre statistiche sul cellulare dell'utente. Inoltre, sempre

passando attraverso il server, è possibile verificare lo stato della presa, alimentarla e disalimentarla. Tutta questa comunicazione che avviene attraverso il server del servizio, in caso di mancanza di connettività non consente ovviamente né di acquisire dati né di mandare comandi ai *device*. Un impianto domotico deve essere sempre autonomo dalla connettività per evitare che, mettendo fuori uso la linea dati, si resti "intrappolati" in casa.

La sicurezza nella domotica: una sfida ancora da vincere

Come abbiamo visto in questo trittico di articoli, la questione della sicurezza nella domotica residenziale è complessa e coinvolge tanti livelli diversi ovvero non solo quello tecnico, ma anche quello culturale e comportamentale dei tanti soggetti coinvolti.

Agli **utenti, i proprietari delle case**, deve essere oggi molto chiaro che il comfort di una casa in grado di capire e adeguarsi al proprio stile di vita e al proprio modo di interagire con l'ambiente ha un prezzo in termini di rischi di sicurezza. Sicurezza in senso non solo di esposizione ad attacchi malevoli che possono creare disagi o danni diretti, ma anche di esposizione verso soggetti privati terzi dei dati molto privati legati alle abitudini e ai comportamenti che si hanno in casa. Il tema della privacy dei dati raccolti da una casa è poco dibattuto e soprattutto poco percepito: sarà necessario accendere al più presto i riflettori sulla questione.

I **progettisti e gli installatori** hanno, in termini diretti, responsabilità verso il cliente e anche verso la comunità tutta sul tema della sicurezza. In particolare a loro va, oltre il dovere di dare maggiore priorità al tema nella realizzazione quotidiana del loro lavoro, l'onere di aumentare la consapevolezza sul tema dei loro clienti. Altra missione

importante è quella di accrescere la cultura della manutenzione continuativa degli impianti che da troppi operatori del settore è vissuta incredibilmente come un male ineluttabile piuttosto che come un'opportunità. Come abbiamo visto la logica del "tanto chi vuoi che si interessi alla casa del mio cliente" non regge più, anzi è un atteggiamento mentale che facilita i comportamenti criminali online. Anche se "il mio cliente" non subirà un danno diretto questo non affranca il tecnico dalla responsabilità di costruire una società più sicura. La prolificazione di impianti non protetti dagli accessi esterni non è solo un problema per i proprietari dell'impianto, ma diventa un problema di sicurezza più generale se si pensa che ogni impianto domotico può diventare un tramite per effettuare, ad esempio, un attacco. Al riguardo ricordiamo come nel 2016 ci fu un massiccio attacco DDoS che coinvolse alcuni dei maggiori siti web tra cui Amazon e Twitter. L'attacco partì da quasi 100.000 device tra IP Camera e altri dispositivi che erano stati penetrati dal virus *Mirai* grazie alla debolezza delle password usate [7]. Questo da un lato sottolinea che una cultura della sicurezza dell'abitazione non risponde alla sicurezza solo della vita di un singolo ma anche a quella di milioni di altre persone.

Infine **i produttori**, sono i soggetti più influenti su questo tema perché possono agire sia sui clienti finali che sui tecnici in modo diretto semplicemente aumentando la sicurezza dei propri prodotti. L'evoluzione e le richieste che vengono dal mercato della *smart home* e della domotica mettono evidentemente sotto pressione gli imprenditori che si vedono progressivamente costretti a rivoluzionare – anche profondamente – non solo i prodotti che offrono ma spesso la struttura con cui progettano e producono i prodotti stessi. Se volessimo inquadrare questa tendenza in una visione più ampia, legata al mercato della domotica, potremmo sottolineare come anche qui (forse con più resistenza rispetto ad altri mercati) stia progressivamente emergendo la trasformazione dei modelli di business da quelli tradizionali di vendita di semplici

prodotti alla vendita di servizi: non ti vendo più il device per rendere la casa domotica ma ti vendo un servizio (che in futuro includerà l'hardware stesso) che renderà la tua casa intelligente e accessibile. Questo cambio di paradigma implica un'assunzione di responsabilità diretta sulla sicurezza degli impianti/servizi offerti. Tuttavia questa sorta di innovazione predestinata non è una condanna destinata ai soli operanti nella domotica ma è un *trend* generale imposto dai nuovi paradigmi raccolti sotto il termine IoT (Internet of Things) [8] che, come ogni evento epocale, andrà abbracciato e non più combattuto.

Riferimenti

- Lista indirizzi ip degli operatori per stato – http://www.nirsoft.net/countryip/index.html
- Lista indirizzi ip degli operatori per città – https://en.ipshu.com/country_region_city_list
- I sistemi di integrazione dei sistemi sono centraline che elaborano i dati provenienti da differenti tipologie di impianti per valutare la migliore riposta "intelligente" da dare ai cambiamenti di stato della casa. A titolo esemplificativo: https://www.control4.com/solutions/products/controllers
- A titolo esemplificativo: http://www.insideci.co.uk/media/39387/using_myhome_away_from_the_home.pdf
- "Voice assistant integration is the top smart-home trend at CES" – https://www.businessinsider.com/voice-assistant-integration-top-smart-home-trend-ces-2018-1?IR=T
- "GDPR, cosa cambia per gli sviluppatori?" – https://blog.kiwifarm.it/gdpr-cosa-cambia-per-gli-sviluppatori/
- "How to Protect IP Camera System from Cyber Attack" – https://kintronics.com/protect-ip-camera-system-cyber-attack/

- “7 Ways the IoT Can Change the Business World” – https://www.iotevolutionworld.com/smart-home/articles/437712-7-ways-iot-change-business-world.htm

A cura di: **Matteo De Simone, Michelangelo De Bonis**

L’articolo Elementi di sicurezza negli impianti domotici – parte terza proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/elementi-di-sicurezza-negli-impianti-domotici-parte-terza/