Casa 24 PLUS Il Sole 24 ORE
Settimanale
Data 05-03-2015
Pagina 24
Foglio 1 / 2

INTERNET OF THINGS

Se la domotica non è così sicura

Spesso i sistemi online presentano falle su accesso e privacy: ecco quali e come limitarle

di **Dario Aquaro**

Internet delle cose, e delle case. In scia all'affermazione del fenomeno Internet of things (Iot), si diffondono tra le soluzioni domotiche i sistemi di monitoraggio (videocamere, sensori di movimento, dispositivi d'allarme) connessi in rete. L'automazione delle case non riguarda solo frigoriferi che avvisano su scadenze o scarsità degli alimenti, impianti elettrici o climatizzatori regolabili a distanza, ma anche la rilevazione di presenze e accessi, continua e in remoto.

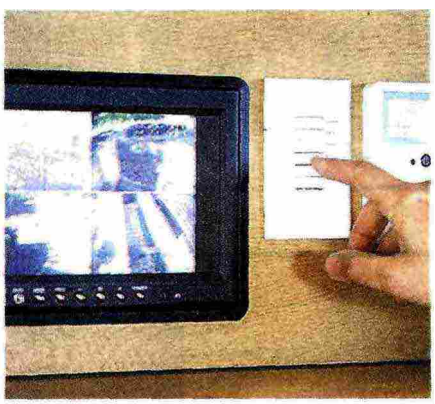
Governare dal proprio device quel che avviene in casa è senz'altro uno dei vantaggi della smarthome. La connessione in rete degli apparecchi intelligenti e la loro gestione deve però fare i conti con una basilare questione di affidabilità, sui versanti della sicurezza e della privacy. Guardando alle implicazioni e ai rischi dell'Iot, una ricerca Hp – concentrata su 10 sistemi di sicurezza per la casa con connessione internet, compresi i relativi componenti applicativi mobili e cloud – ha rilevato che tutti i sistemi presentano alte vulnerabilità: problemi di protezione con password, crittografia e autenticazione (si veda l'articolo sotto).

Per carità, non certo da queste "nuove criticità" dipende l'attuale record di furti in abitazione registrato dal Censis: più che raddoppiati negli ultimi dieci anni (689 al giorno). Ma è un fatto che con l'incedere dell'Iot (nel 2015 secondo Gartner verranno utilizzati 4,9 miliardi di dispositivi connessi, +30% rispetto al 2014, che arriveranno a 25 miliardi entro il 2020) l'attenzione di imprese, utenti e vigilanza debba spostarsi sugli aspetti "invisibili" della sicurezza. Quanto è vulnerabile il sistema di monitoraggio? E l'accesso alle nostre informazioni?

Con il parere 8/14, a settembre i garanti della privacy europei (gruppo di lavoro ex articolo 29 direttiva 95/46/Ce) hanno individuato nell'asimmetria informativa e nella mancanza di controllo sui propri dati la principale criticità dei dispositivi Iot (da qui l'importanza del trattamento e di un'informativa chiara e dettagliata). E hanno messo in luce come, con le attuali tecnologie, la portabilità venga spesso esaltata a scapito della sicurezza e i dispositivi siano esposti agli attacchi esterni. La cura deve quindi avvenire nella fase di progettazione.

«La semplicità d'uso degli oggetti rende l'utente finale indipendente. Ma a che prezzo? È ovvio che più voglio servizi, più cedo privacy – spiega Andrea Natale, coordinatore del Gruppo Tvcc Anie Sicurezza –. Nella Iot non si deve considerare solo il prodotto, ma anche chi lo installa, chi lo vende, lo gestisce, chi trasmette i dati eccetera. Il fai da te è rischioso. E c'è davvero bisogno di una collaborazione più stretta tra i produttori».

Fino a quando i sistemi di protezione della sicurezza e della privacy non saranno contemplati già nella progettazione originale dei dispositivi (e non aggiunti in seguito), l'Iot continuerà a rappresentare un rischio più che un beneficio. La pensa così Marianna Vintiadis, managing director di Kroll, società leader in intelligence, anche in campo di cyber risk. Qualche piccolo suggerimento: «Se il dispositivo non è dotato di un sistema di crittografia interno, non comprarlo. Subito dopo l'acquisto, cambiare la password predefinita, ricondurla a qualcosa di personale e non facilmente intuibile, e modificare anche il nome utente, in molti casi "admin". Abilitare il dispositivo a rilevare, segnalare e registrare tutte le connessioni attive, le azioni di log in e log off, con notifica sul proprio account email. Controllare periodicamente gli accessi al sistema e – conclude Vintiadis – se si notano azioni insolite come accessi a orari inconsueti, cambiare la password e considerare la possibilità di disattivarlo».



Hi-tech. Il fai da te spesso causa vulnerabilità

LA PAROLA CHIAVE

IoT

Internet of Things o "Internet delle cose" è un neologismo riferito all'estensione a oggetti fisici delle potenzialità del web. Grazie al collegamento alla rete possono infatti comunicare dati gli uni con gli altri e acquisire quindi informazioni aggregate, per poter poi agire conseguentemente in una determinata maniera.

LA RICERCA

Password e «cloud» i punti deboli

Autorizzazione insufficiente, interfacce non sicure, problemi di privacy, mancanza di crittografia delle trasmissioni. Sono i 4 punti nevralgici dei sistemi di sicurezza per la casa connessi a internet. Lo evidenzia un'analisi Hp, realizzata con il proprio servizio di test "Fortify on Demand" sui 10 sistemi più diffusi e relativi componenti applicativi mobili e cloud.

L'80% dei dispositivi analizzati richiede una password di complessità e lunghezza insufficienti, spesso consentendo chiavi come "1234" o "123456". Nessun sistema è in grado di bloccare gli account dopo un certo numero di tentativi non riusciti. Sei apparecchi su dieci presentano problemi legati alle interfacce web, facilmente aggredibili con tecniche di "harvesting" (processo che consente di identificare gli account utente esistenti), e sfruttando le carenze applicative. E anche se tutti i sistemi analizzati implementano la tecnologia di criptazione del traffico, molte connessioni verso la cloud (60%) restano vulnerabili agli attacchi (tra cui quelli di tipo Poodle). Tutti i sistemi, d'altra parte, raccolgono informazioni personali dell'utente (nome, indirizzo, data di nascita, numero di telefono e persino di carta di credito): un'esposizione che è preoccupante, con-

Anie

Casa 24 PLUS Il Sole 24 ORE
Settimanale
Data 05-03-2015
Pagina 24
Foglio 2 / 2

siderata la scarsa affidabilità dei sistemi.

«Non è però il momento di fare allarmismo sul problema della sicurezza – commenta Angela Tumino, responsabile dell'Osservatorio internet of things del Politecnico di Milano –. Certo un po' tutti dovremmo imparare a usare password complesse. A mano a mano che gli oggetti intelligenti si diffonderanno nelle case italiane, le aziende aumenteranno gli investimenti per ridurne la vulnerabilità. Così è stato per tanti prodotti tecnologici, si pensi alla facilità di clonare i primi cellulari». L'ultimo report disponibile dell'Osservatorio parla di sei milioni di oggetti interconnessi in Italia. Solo l'1% delle abitazioni è però dotato di dispositivi per il telecontrollo del riscaldamento e/o l'antintrusione: «Con l'affermarsi delle tecnologie wireless all'interno dell'abitazione e con la crescente disponibilità di dispositivi Ble (Bluetooth low energy) – spiega il report – si arriverà a oltre 3 milioni di oggetti domestici connessi nel 2016». – **D. Aq.**


Mercato
Se la domotica non è così sicura
Password e schede i punti deboli
MILANO - BICOCCA
SEDE PRESTIGIOSA
AFFITTASI
BUILDING
A BETTER
WORLD
mipim