

Casa intelligente, Sifis Home: il progetto contro gli attacchi informatici

Maria Cattini | 26/10/2021 | Sicurezza digitale

Il progetto è promosso dal Cnr e finanziato con fondi europei, ha l'obiettivo di creare standard di sicurezza per i dispositivi della casa intelligente

"Alexa, svegliami domani alle 7.00 con la nona sinfonia di Beethoven". "Ehi Google, chiama mia madre". Gli **home assistant** sono i dispositivi più intimi tra quelli che abbiamo in casa. Ed è probabile che ci conoscano meglio di chiunque altro, perché sono in grado di **incrociare una montagna di dati** ma poi, con estrema naturalezza, anche di **consigliarci sulle scelte migliori**, compresi gli acquisti. Comodità, efficienza, accoglienza e coccola. La **smart home** è così.

Bello, vero? Se non fosse che è un castello sì, ma di carte, a rischio attacco informatico.

Qualche tempo fa, la rivista *Which?* dell'Associazione inglese dei consumatori ha realizzato un test con una finta smart home piena di dispositivi connessi e ha aspettato per vedere cosa sarebbe accaduto. In una settimana la smart home è stata vittima di 12mila attacchi informatici.

Mi direte: è la tecnologia, bellezza! Invece: dipende dal tipo di tecnologia. Perché le alternative ci sono sempre. In occasione dell'**Internet Festival**, che si è tenuto alcuni giorni fa a Pisa, l'**Istituto di informatica e telematica** del **Consiglio nazionale delle ricerche** (Cnr) ha illustrato il progetto **Sifis-Home**, che ha l'obiettivo di offrire un framework di sicurezza per ambienti **smart home**. Sifis-Home consente lo sviluppo di applicazioni capaci di rilevare e reagire dinamicamente agli attacchi informatici e rispettose della privacy, aumentando così il controllo e la fiducia degli utenti finali di smart home.

I rischi per la smart home

Il sistema smart home è un paradigma applicativo emergente che sta guadagnando sempre più popolarità. Secondo i dati del Politecnico di Milano, il valore di mercato nel 2021 degli **smart home devices** è di 505 milioni di euro (seppur in flessione del 4% rispetto all'anno precedente).

*"In questo mercato sono ancora **presenti notevoli barriere e preoccupazioni**, principalmente legate alla sicurezza informatica di ogni dispositivo e alla sicurezza all'interno dei sistemi smart home, nonché alla **privacy e all'integrità dei dati prodotti e consumati**, la maggior parte dei quali sono personali e sensibili",* riferisce Andrea Saracino, ricercatore del Cnr e coordinatore del progetto Sifis Home: *"Molti dispositivi smart home utilizzano soluzioni di sicurezza personalizzate e proprietarie che non tengono conto delle interazioni con altri dispositivi. Inoltre, gli sviluppatori devono sviluppare applicazioni adattabili a diversi sistemi e architetture, e gli **aspetti di sicurezza sono spesso trascurati o mal affrontati**".*

Sifis Home è dunque un *framework full stack* di sicurezza per ambienti smart home, un servizio con invio di dati al cloud solo se anonimizzati. Finanziato con fondi di **Horizon 2020**, in partnership con Intel, Ericson, Politecnico di Torino, si compone di quattro linee di sviluppo: progettazione di software privacy e cybersecurity by design; creazione di meccanismi di certificazione; promozione di **marketplace** premianti per smart device compliant; progettazione di un **sistema operativo**

domestico proattivo.

*“È un progetto che mira a creare un **sistema alternativo a quello predominante delle big tech**, con forte enfasi sulla sicurezza, oltre che alla funzionalità. Qualsiasi azienda produttrice di smart device che vorrà attenersi a questi standard, potrà essere certificata e premiata sul marketplace”,* prevede Saracino. Il resto, lo dovrà fare il mercato. Cioè noi stessi.

Fonte: Claudia Morelli, Wired

Il progetto è promosso dal Cnr e finanziato con fondi europei, ha l'obiettivo di creare standard di sicurezza per i dispositivi della casa intelligente

“Alexa, svegliami domani alle 7.00 con la nona sinfonia di Beethoven”. “Ehi Google, chiama mia madre”. Gli **home assistant** sono i dispositivi più intimi tra quelli che abbiamo in casa. Ed è probabile che ci conoscano meglio di chiunque altro, perché sono in grado di **incrociare una montagna di dati** ma poi, con estrema naturalezza, anche di **consigliarci sulle scelte migliori**, compresi gli acquisti. Comodità, efficienza, accoglienza e coccola. La **smart home** è così.

Bello, vero? Se non fosse che è un castello sì, ma di carte, a rischio attacco informatico.

Qualche tempo fa, la rivista *Which?* dell'Associazione inglese dei consumatori ha realizzato un test con una finta smart home piena di dispositivi connessi e ha aspettato per vedere cosa sarebbe accaduto. In una settimana la smart home è stata vittima di 12mila attacchi informatici.

Mi direte: è la tecnologia, bellezza! Invece: dipende dal tipo di tecnologia. Perché le alternative ci sono sempre. In occasione dell'**Internet Festival**, che si è tenuto alcuni giorni fa a Pisa, l'**Istituto di informatica e telematica** del **Consiglio nazionale delle ricerche** (Cnr) ha illustrato il progetto **Sifis-Home**, che ha l'obiettivo di offrire un framework di sicurezza per ambienti **smart home**. Sifis-Home consente lo sviluppo di applicazioni capaci di rilevare e reagire dinamicamente agli attacchi informatici e rispettose della privacy, aumentando così il controllo e la fiducia degli utenti finali di smart home.

I rischi per la smart home

Il sistema smart home è un paradigma applicativo emergente che sta guadagnando sempre più popolarità. Secondo i dati del Politecnico di Milano, il valore di mercato nel 2021 degli **smart home devices** è di 505 milioni di euro (seppur in flessione del 4% rispetto all'anno precedente).

*“In questo mercato sono ancora **presenti notevoli barriere e preoccupazioni**, principalmente legate alla sicurezza informatica di ogni dispositivo e alla sicurezza all'interno dei sistemi smart home, nonché alla **privacy e all'integrità dei dati prodotti e consumati**, la maggior parte dei quali sono personali e sensibili”,* riferisce Andrea Saracino, ricercatore del Cnr e coordinatore del progetto Sifis Home: *“Molti dispositivi smart home utilizzano soluzioni di sicurezza personalizzate e proprietarie che non tengono conto delle interazioni con altri dispositivi. Inoltre, gli sviluppatori devono sviluppare applicazioni adattabili a diversi sistemi e architetture, e gli **aspetti di sicurezza sono spesso trascurati o mal affrontati**”.*

Sifis Home è dunque un *framework full stack* di sicurezza per ambienti smart home, un servizio con invio di dati al cloud solo se anonimizzati. Finanziato con fondi di **Horizon 2020**, in partnership con Intel, Ericson, Politecnico di Torino, si compone di quattro linee di sviluppo: progettazione di software privacy e cybersecurity by design; creazione di meccanismi di certificazione; promozione di **marketplace** premianti per smart device compliant; progettazione di un **sistema operativo domestico** proattivo.

*“È un progetto che mira a creare un **sistema alternativo a quello predominante delle big tech**, con forte enfasi sulla sicurezza, oltre che alla funzionalità. Qualsiasi azienda produttrice di smart device che vorrà attenersi a questi standard, potrà essere certificata e premiata sul marketplace”, prevede Saracino. Il resto, lo dovrà fare il mercato. Cioè noi stessi.*

Fonte: Claudia Morelli, Wired