SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Maggio 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

- Cos'è l'Internet delle cose
- Nuove problematiche
- Proteggere i dispositivi

L'Internet delle cose

Cos'è l'Internet delle cose

Nel passato, la tecnologia era piuttosto semplice: collegavi il tuo computer a Internet e lo utilizzavi per le tue attività quotidiane. Le innovazioni tecnologiche hanno poi introdotto smartphone e tablet, i dispositivi mobili, nelle nostre vite: è come avere un computer in tasca, ma con nuovo e peculiari problematiche di sicurezza. Il nuovo grande progresso tecnico è costituito dall'Internet delle cose, in inglese Internet of Things, da cui la sigla IoT. L'Internet delle cose è la possibilità di connettere in rete tutti quei dispositivi di cui facciamo uso nella nostra vita quotidiana, dispositivi come il campanello di casa, le lampadine, i termostati, i frigoriferi. Questi strumenti connessi possono rendere la nostra vita più semplice, facendo in modo, ad esempio, di accendere le luci dell'ingresso quando il nostro telefono capisce che ci stiamo avvicinando a casa. Il mercato dell'IoT si muove a un ritmo straordinario: ogni settimana vengono creati nuovi dispositivi intelligenti in grado di connettersi in rete. Come però con i dispositivi mobili, anche il mondo dell'IoT è caratterizzato da problematiche di sicurezza particolari. In questa newsletter vi aiuteremo a capire quali sono questi rischi e cosa potete fare per rendere sicuri i dispositivi IoT, la vostra casa e, in ultimo, la vostra famiglia.

L'autore di questo numero

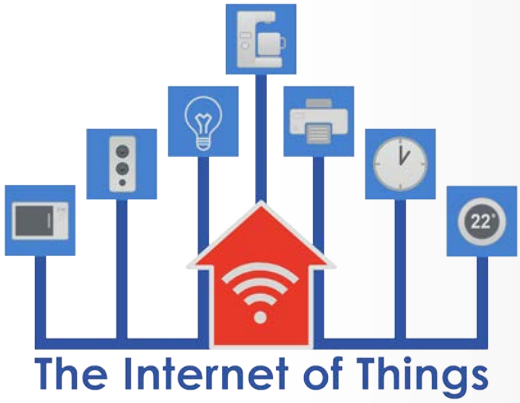
James Lyne (**@jameslyne**) è Global Head of Security Research di Sophos. James, che si definisce "un vero geek", ha una vastissima esperienza tecnica, le cui conoscenze coprono tutti gli ambiti della sicurezza IT. È un istruttore certificato SANS e spesso è relatore presso le più importanti conferenze di settore.

Nuove problematiche

Il problema con l'Internet delle cose è che le nuove apparecchiature sono semplici da usare: connettete la macchinetta del caffè ed essa vi chiede di potersi collegare alla rete di casa. Tutta questa semplicità però ha un costo. Il più grande problema è che molte aziende produttrici non hanno esperienza con i problemi di sicurezza, poiché il loro expertise è costruire elettrodomestici. O ancora si tratta di startup create con lo scopo di sviluppare un prodotto nel modo più veloce ed efficiente, ad esempio su una piattaforma di crowdfunding. Questa aziende sono focalizzate sui profitti, non sulla cybersicurezza e come risultato molti dispositivi IoT disponibili sul mercato non hanno alcuna possibilità di essere protetti: alcuni hanno password di default conosciute, spesso anche pubblicate su Internet che non possono essere cambiate. Molti altri non

L'Internet delle cose

permettono la possibilità di poter essere configurati. Per peggiorare ulteriormente le cose, anche l'aggiornamento può essere molto difficoltoso, qualora questa possibilità esista. Come risultato, molti dispositivi che usate potrebbero rapidamente diventare obsoleti se affetti da vulnerabilità che non possono essere eliminate, lasciandovi indifeso in modo permanente.



Scoprite quali dispositivi IoT sono collegati alla vostra rete, isolatevi laddove possibile, manteneteli aggiornati e proteggeteli con password forti.

Proteggere i dispositivi

E ora, cosa possiamo fare? Vogliamo sfruttare le potenzialità dei dispositivi IoT in modo sicuro ed efficace, perché essi possono rendere la nostra vita più semplice, farci risparmiare e forse aumentare la sicurezza fisica di casa. È possibile, inoltre, che il progresso tecnologico non ci lasci scelta per cui saremo comunque costretti a comprare dei dispositivi IoT. Di seguito potete trovare alcuni suggerimenti che vi aiuteranno a proteggere la vostra casa e voi stessi.

- **Connettete solo ciò che vi serve**. Il modo più semplice per rendere sicuro un dispositivo è di non connetterlo a Internet. Se non vi serve online, non collegatelo alla rete Wi-Fi.
- **Separate le reti Wi-Fi**. Se i dispositivi IoT devono essere per forza collegati, create una rete Wi-Fi dedicata. Molti access point permettono di creare reti aggiuntive, come la rete per gli ospiti (Guest network). Un'altra possibilità è di comprare un secondo access point Wi-Fi da dedicare ai dispositivi IoT, in modo che possano essere ospitati su una rete isolata e non utilizzati per attaccare computer e dispositivi mobili connessi alla rete principale di casa, che costituisce l'obiettivo primario per i criminali informatici.
- **Aggiornate quando possibile**. Così come il Vostro PC, mantenete aggiornati anche I dispositivi IoT. Se esiste l'opzione di aggiornamento automatico, abilitatela.
- **Password forti**. Cambiate ogni password con una passphrase unica e forte, che solo voi conoscete. Non riuscite a ricordare tutte le password? Usate un password manager, un'applicazione che vi consentirà di conservarle e gestirle in sicurezza.
- **Opzioni di privacy**. Se I dispositive IoT vi permettono di configurare le opzioni di privacy, limitate la quantità di informazioni che condividono. L'opzione più semplice è di disabilitare ogni condivisione.

L'Internet delle cose

- **Considerate la sostituzione**. Ad un certo punto sarà necessario sostituire il dispositivo IoT caratterizzato da troppe vulnerabilità conosciute a cui non è possibile porre rimedio o qualora siano disponibili device molto più sicuri.

Non esiste un unico rimedio per tutti i dispositivi, per cui è opportuno verificare le best practice e le pubblicazioni che spiegano come renderli sicuri. Sfortunatamente, molti dispositivi non vengono sviluppati considerando la loro sicurezza come fattore prioritario, per cui i produttori non forniscono informazione alcuna sull'argomento. Con l'aumento della sensibilità sui temi della sicurezza, ci aspettiamo che sempre più aziende lavorino per migliorare la protezione di questi dispositivi e offrano una maggiore quantità di informazioni su come renderli sicuri.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito

http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf
Proteggere la rete di casa:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley