OUCH! | Agosto 2018

OUCH!

SANS SECURITY AWARENESS

La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

Dispositivi Smart Home

Cos'è un dispositivo Smart Home?

Nel passato solo alcuni dei dispositivi di casa potevano connettersi a Internet, come ad esempio laptop, smartphone o console di videogiochi. Tuttavia oggi, un numero sempre grande di dispositivi si connette a Internet, dalle lampadine e gli altoparlanti alle serrature delle porte e persino le sarrature della tua auto. Presto, quasi tutti i dispositivi di casa potrebbero essere collegati a Internet. Questi dispositivi collegati spesso si chiamano Internet of Things (IoT) o dispositivi Smart Home. Nonostante questi dispositivi connessi offrano una grande quantità di comodità, potrebbero nascondere dei pericoli unici.

Qual è il problema?

Più dispositivi sono collegati alla rete della tua casa, più è elevata la probabilità che si verifichi qualche violazione. Gli hacker possono programmare i tuoi dispositivi per attaccarne altri, i venditori possono raccogliere informazioni complete sulle tue attività o i tuoi dispositivi potrebbero essere infettati e bloccarti. Molte aziende che producono questi dispositivi non hanno esperienza con la cyber security e considerano la sicurezza solo un costo. Di conseguenza, molti dei dispositivi acquistati hanno poca o nessuna sicurezza integrata. Un esempio su tutti, alcuni dispositivi hanno password predefinite ben note o non è possibile aggiornarle o configurarle.

Come posso proteggermi

Che cosa si può fare? Sicuramente vogliamo fare in modo che tu possa usare i dispositivi connessi, in modo sicuro e protetto. Questi dispositivi possono fornire funzionalità meravigliose che semplificano la tua vita. Inoltre, man mano che la tecnologia cresce, potresti non avere altra scelta che usare i dispositivi intelligenti. Ecco i passaggi chiave da seguire per proteggersi.

Collega solo i dispositivi di cui hai bisogno: Il modo più semplice per proteggere un dispositivo è non collegarlo a Internet. Se non è necessario che il dispositivo sia online, non collegarlo alla rete Wi-Fi. Hai davvero bisogno che il tuo tostapane ti invii notifiche al telefono?

Sii sempre informato su cosa hai collegato: Quali dispositivi hai collegato alla tua rete domestica? Non sei sicuro o non ricordi? Spegni la tua rete wireless e vedi cosa non funziona più. Rimarrai sorpreso di quanti dispositivi hai dimenticato.

Attenzione agli aggiornamenti: Proprio come il tuo computer e i tuoi dispositivi mobili, è fondamentale tenere aggiornati tutti i tuoi dispositivi. Se il tuo dispositivo ha la possibilità di aggiornarsi automaticamente, abilita questa funzionalità.

Password: Cambia le password dei tuoi dispositivi con una passphrase unica e potente che solo tu sai. Molto probabilmente dovrai inserirla una sola volta. Non riesci a ricordare tutte le tue passphrase? Non preoccuparti, neanche noi. Prendi in considerazione l'utilizzo di un gestore di password per archiviarle in modo sicuro.

Opzioni di Privacy: Se il tuo dispositivo ti consente di configurare le opzioni di privacy, limita la quantità di informazioni che raccoglie o condivide. Una delle possibili opzioni è semplicemente disabilitare qualsiasi capacità di condivisione delle informazioni.

Venditori: Acquista i tuoi dispositivi da un'azienda che conosci e di cui ti fidi. Cerca prodotti che supportino la sicurezza, come consentire di abilitare l'aggiornamento automatico, modificare la password predefinita e modificare le impostazioni sulla privacy.

Sempre in ascolto: Se un dispositivo può accettare i comandi vocali, è costantemente in ascolto. Ad esempio, i tuoi dispositivi Alexa e Google Home possono registrare conversazioni sensibili. Considera questa evenienza quando decidi dove posizionare i dispositivi all'interno della tua casa e rivedi le opzioni sulla privacy.

Rete Guest: Considera la possibilità di mettere i tuoi dispositivi Smart Home su una rete WiFi "Guest" separata anziché sulla rete WiFi primaria che utilizzi per i tuoi computer e dispositivi mobili. In questo modo, se uno Smart Device è infetto, i tuoi computer o dispositivi mobili sulla tua rete principale saranno al sicuro.

Non c'è motivo di temere le nuove tecnologie, ma cerca sempre di capire il rischio che comportano. Con questi pochi semplici passaggi puoi contribuire a creare una Smart Home molto più sicura.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

L'autore di questo articolo

Robert M. Lee (@RobertMLee) è un istruttore certificato SANS, autore di FOR578 - Cyber Threat Intelligence e ICS515 - ICS Active Defense and Incident Response. Robert è anche l'amministratore delegato e fondatore della società di sicurezza informatica industriale Dragos.

Risorse

Passphrases:	https://www.sans.org/u/GEB
Password Managers:	https://www.sans.org/u/GEG
Securing Your Home Network:	https://www.sans.org/u/GEL