Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Internet stvari (IoT)**
- **Rizici vezani za IoT**
- **Kako da zaštite svoje IoT uređaje**

Internet stvari (IoT)

Šta je „Internet stvari“ (IoT)

U prošlosti je tehnologija bila relativno jednostavna, samo je računar bio povezan na Internet i korišćen za dnevne aktivnosti. Onda je tehnologija napredovala i mobilni uređaji su postali sastavni deo naših života, pametni telefoni i tableti. Danas ti uređaji obezbeđuju snagu klasičnih računara iz naših džepova. Obzirom na njihovu mobilnost takvi uređaji su sa sobom doneli sebi specifične bezbednosne izazove. Najnoviji veliki tehnološki napredak predstavljaju Internet stvari (Internet of Things). Internet stvari, ili skraćeno IoT, predstavljaju sve svakodnevne uređaje koji se povezuju na Internet, od uređaje kao što su zvona na vratima, sijalice, dečije lutke i termostati, pa do kompleksnih kućnih aparata. Tako povezani uređaji čine život mnogo udobnijim i jednostavnijim, na primer da se svetlo automatski aktivira kada vaš pametni telefon prepozna da ste blizu kuće. IoT tržište napreduje neverovatnom brzinom tako da se novi uređaji pojavljuju na nedeljnom nivou. Međutim, kao i mobilni uređaji, IoT uređaji takođe donose svoje specifične bezbednosne rizike. U ovom izdanju pomoći ćemo vam da razumete rizike koje sa sobom donese i šta možete da uradite da obezbedite svoje IoT uređaji, svoju kuću i svoju porodicu.

Gost urednik

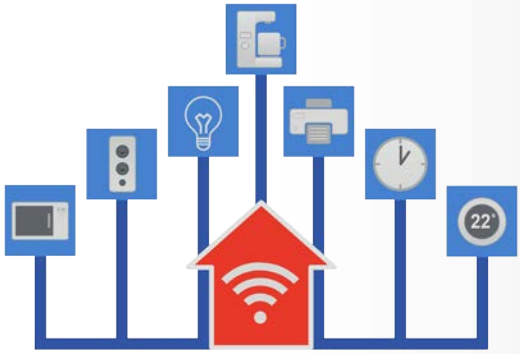
James Lyne (**@jameslyne**) je globalni rukovodilac istraživanja vezanih za bezbednost u kompaniji Sophos. Sertifikovani je instruktor pri SANS institutu i često glavni voditelj na industrijskim konferencijama.

Rizici vezani za IoT

Snaga IoT uređaja, bar većine njih, je u njihovoj jednostavnosti. Na primer, uključite aparat za kafu i on odmah traži da se poveže na vašu Wi-Fi mrežu. Međutim, ta jednostavnost ima svoju cenu. Najveći problem sa IoT uređajima je da većina kompanija koje ih proizvode nema nikakvog iskustva na polju bezbednosti, već u proizvodnji kućnih aparata, ili se radi o „start-up“ kompanijama sa Kickstarter-a koje pokušavaju da naprave svoje proizvode na najefikasniji način, što je brže moguće. Takve kompanije su uglavnom usresređene na profit a ne na sajber bezbednost. Kao rezultat, većina IoT uređaja su danas u ponudi imaju ili malo ili uopšte nemaju ugrađenu sajber zaštitu. Na primer, neki imaju fabričke lozinke koje su dobro poznate, verovatno već objavljene na Internetu, a koje ne mogu da se promene. Osim toga, mnogi od ovih uređaja

Internet stvari (IoT)

nemaju opcije ili mogućnost da ih konfigurišete, tako da ste ograničeni na ono što vam je isporučeno. Da bi stvari bile još gore, mnoge od ovih uređaja je veoma teško ažurirati, ili čak i nemaju tu opciju. Kao rezultat mnogi od IoT uređaja koji se danas korite će veoma brzo zastareti sa poznatim bezbednosnim propustima koje je nemoguće otkloniti, i na taj način ostati zauvek ranjivi na sajber pretnje.



Znajte koji IoT uređaji su vam povezani na mrežu, izolujte ih kada je to moguće, ažurirajte ih redovno i zaštitite ih jakim propusnim frazama.

Kako da zaštite svoje IoT uređaje

Šta možete da uradite? Ono što želimo je da mogućnosti IoT uređaja koristite bezbedno i efikasno. IoT uređaji poseduju sjajne funkcionalnosti koje život čine jednostavnijim, štede novac, i mogu da povećaju nivo fizičke bezbednosti vašeg doma. Pored toga, kako se tehnologija razvija možda uskoro i nećete imati izbora nego da koristite IoT uređaje. Usled toga veoma je važno da se što pre upoznate se sa koracima koji mogu da pomognu da zaštitite svoje IoT uređaje, a sami tim i sebe, svoj dom i svoju porodicu.

- **Povežite samo ono što je neophodno**: Najjednostavniji način da obezbedite IoT uređaje je da i ne povezujete na Internet. Ako vam nije neophodno da budu on-line, nemojte ih povezivati na vašu Wi-Fi mrežu.
- **Odvojite Wi-Fi mrežu**: Ako vam nije neophodno da IoT uređaji budu on-line, uzmite u obzir da kreirate posebnu, odvojenu Wi-Fi mrežu samo za njih. Mnogi Wi-Fi pristupni uređaji imaju mogućnost kreiranja dodatnih mreža, na primer mreže za goste. Druga opcija je nabavka dodatnog Wi-Fi pristupnog uređaja samo za IoT uređaje. Na takav način izolovaćete IoT uređaje u posebnu mrežu, tako da se oni neće moći da naude vašim računarima ili mobilnim uređajima koji su povezani na vašu primarnu, kućnu Wi-Fi mrežu (koji su još uvek glavna meta sajber kriminalaca).
- **Ažurirajte kada je to moguće**: Kao i kod računara i mobilnih uređaja, ako je to moguće, redovno ažurirajte IoT uređaje. Ako postoji opcija automatskog ažuriranja, obavezno je koristite.
- **Jaka lozinka**: Postavite lozinke na svojim IoT uređajima na jedinstvene i jake propusne fraze, koje su samo vama poznate. Ne možete da zapamtite sve svoje propusne fraze? Ne brinite, ne možemo ni mi, uzmite u obzir korišćenje menadžera lozinki za bezbedno generisanje i čuvanje.

Internet stvari (IoT)

- **Opcije privatnosti**: Ako vaš IoT uređaj dozvoljava da konfigurišete opcije privatnosti, limitirajte informacije koje delite. Jedna od opcija je i da onemogućite bilo kakvo deljenje informacija.
- **Razmislite o zameni**: U nekom trenutku možda ćete želeti da zamenite svoj IoT uređaj, na primer kada bude imao previše poznatih bezbednosnih propusta koji ne mogu biti popravljeni ili ako na tržištu bude dostupan noviji uređaj sa boljim ugrađenim bezbednosnim funkcionalnostima.

Jedno rešenje koje odgovara svim uređajima ne postoji, tako da je preporučljivo proveriti šta je najbolja praksa za svaki IoT uređaj ponaosob. Na nesreću većina IoT uređaja je napravljena bez uzima sajber bezbednosti u obzir, tako da proizvođači ne obezbeđuju mnogo bezbednosnih informacija. Ali kako svest o važnosti sajber bezbednosti raste, nadamo se da će sve više i više proizvođača IoT uređaja obraćati više pažnje na bezbednosne funkcionalnosti svojih uređaja i informacije kako da ih obezbedite i ažurirate.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org.

Dodatne informacije

Propusne fraze:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_se.pdf
Menadžeri lozinki:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_se.pdf
Bezbednost vašeg novog tableta:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_se.pdf
Bezbednost vaše kućne mreže:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_se.pdf

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Preveo: Nenad Varinac