OUCH! | Mai 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce este „Internet of Things“ (IoT)**
- **Problemele IoT**
- **Protecția dispozitivelor conectate IoT**

Despre „Internet of Things“ (IoT)

Ce este Internet Of Things (IoT)

În trecut tehnologia era relative simplă, pur și simplu conectai calculatorul la Internet și-l foloseai pentru activitățile cotidiene. Apoi tehnologia a avansat, dispozitivele mobile intrând în viețile noastre, cum ar fi telefoanele inteligente sau tabletele. Aceste dispozitive vă pun acum performanța unui calculator de birou în propriile buzunare. Deși mult mai mobile, aceste dispozitive au adus, de asemenea, propriile provocări unice de securitate. Acum, următorul avans tehnic semnificativ este rețeaua electronicelor inteligente de consum, interconectate prin Internet, cunoscută sun denumirea consacrată „Internet of Things“ (IoT). Internet of Things, deseori prescurtat IoT, e tot ce ține de conectarea obiectelor de uz cotidian la rețeaua Internet, de la soneriile de la ușă și becurile de iluminat, la păpușile de jucărie sau termostate. Aceste dispozitive conectate ne pot face viețile mai ușoare, bunăoară având luminile aprinse automat atunci când telefonul vă este recunoscut la apropierea de casă. Piața dispozitivelor IoT evoluează într-un ritm amețitor, noi echipament apărând în fiecare săptămână. Cu toate astea, la fel ca dispozitivele mobile, dispozitivele IoT vin de asemenea cu problemele lor specifice de securitate. În acest buletin informativ vă ajutăm să înțelegeți care sunt aceste riscuri și ce puteți face pentru securizarea propriilor dispozitive IoT, a casei și nu în ultimul rând a familiei proprii.

Editor Invitat

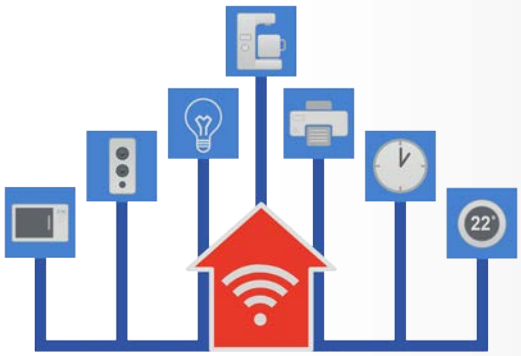
James Lyne (**@jameslyne**) este șeful departamentului global de cercetare în securitate al companiei Sophos. Un „tocilar de anvergură“, cum se autocaracterizează, expertiza lui acoperă variate domenii ale securității informației. Este instructor certificat al institutului SANS și apare deseori ca principal prezentator în conferințele de specialitate.

Problemele IoT

Puterea IoT stă în aceea că majoritatea dispozitivelor sunt simple. De exemplu, vă alimentați automatul de cafea și acesta vă solicită conectarea la rețeaua WiFi din casă. Toată această simplitate, în schimb, are un cost. Cea mai mare problemă a dispozitivelor IoT este că multe companii ce le manufacturează nu au experiență în domeniul securității, expertiza lor fiind în producția de aparate de uz casnic. Sau poate sunt companii în pragul lansării pe piață — startup, ce încearcă să dezvolte un produs în cel mai eficient și rapid mod cu putință, de exemplu pe platforma Kickstarter. Aceste companii se concentrează pe obținerea de profit, nu pe securitatea cibernetică. Drept consecință, multe dispozitive IoT cumpărate astăzi au mecanisme de securitate minime înglobate, sau nu au deloc. De exemplu, unele au parole implicite ce sunt bine-cunoscute, probabil accesibile pe Internet, parole ce nu pot fi schimbate. În plus, multe dintre aceste dispozitive nu au opțiuni sau capacitatea de a fi

Despre „Internet of Things“ (IoT)

configurate, sunteți limitați la ceea ce s-a livrat. Pentru a face lucrurile și mai proaste, multe dintre ele pot fi actualizate cu dificultate sau s-ar putea nici să nu aibă această capacitate. Rezultatul este că multe dispozitive IoT pe care le folosiți se uzează moral foarte repede, rămân cu vulnerabilități cunoscute ce nu pot fi reparate, lăsându-vă astfel permanent expuși riscurilor.



Cunoașteți ce dispozitive IoT se conectează la rețeaua personală, izolați-le atunci când se poate, mențineți-le actualizate și protejați-le cu propoziții-parolă puternice.

Protecția dispozitivelor conectate IoT

Așadar, ce-i de făcut? În mod cert vrem să profitați efectiv de puterea dispozitivelor IoT într-o manieră securizată. Aceste echipamente pot oferi funcționalități extraordinare care vă fac viața mai ușoară, vă ajută să economisiți bani și, probabil, să vă îmbunătățiți securitatea fizică a casei. În plus, pe măsură ce tehnologia evoluează, nu veți avea alte opțiuni decât să cumpărați sau să folosiți dispozitive IoT. Iată câțiva pași pe care-i puteți urma pentru a vă proteja dispozitivele IoT și pe dumneavoastră înșivă.

- **Conectați numai ce aveți nevoie**: Cea mai ușoară metodă de securizare a unui dispozitiv IoT este să nu-l conectați la Internet. Dacă nu aveți nevoie ca acesta să fie online, nu-l conectați la rețeaua personală WiFi.
- **Separați rețelele WiFi**: Dacă aveți nevoie să conectați online dispozitivele IoT, luați în considerare configurarea unei rețele WiFi separate, doar pentru acestea. Multe echipamente de acces WiFi au capacitatea configurării de rețele suplimentare, cum ar fi o rețea pentru oaspeți — guest network. O altă opțiune este achiziția unui echipament de acces WiFi doar pentru dispozitivele IoT. Acesta va menține dispozitivele IoT într-o rețea separată, acestea neputând fi folosite pentru a cauza probleme sau pentru a lansa atacuri asupra calculatoarelor sau mobilelor conectate la rețeaua domestică primară (care rămâne principalul punct de atracție pentru răufăcători).
- **Actualizați atunci când e posibil**: La fel ca PC-ul sau mobilele, mențineți-vă dispozitivele IoT actualizate. Dacă acestea au opțiunea de actualizare automată, activați-o.
- **Parole puternice**: Schimbați orice parolă de pe dispozitivele personale IoT cu o propoziție-parolă unică, pe care nu o cunoaște nimeni altcineva. Nu puteți să vă reamintiți toate parole? Nu vă îngrijorați, nici noi nu reușim. Luați în calcul folosirea unui program de gestiune a parolelor pentru a le păstra securizate.
- **Opțiuni de confidențialitate**: Dacă dispozitivul IoT vă permite configurarea opțiunilor de confidențialitate, limitați volumul de informații pe care le partajează. O opțiune este să dezactivați pur și simplu orice partajare de informații de care este capabil.

Despre „Internet of Things“ (IoT)

- **Aveți în vedere înlocuirea**: La un moment dat veți dori să înlocuiți un dispozitiv IoT atunci când cel deținut are prea multe vulnerabilități cunoscute ce nu pot fi reparate sau există dispozitive mai noi care au mai multe funcții de securitate încorporate.

Nu există o soluție unică pentru toate dispozitivele, așa că merită să verificați cele mai bune practici și orice publicații despre securizarea lor. Din nefericire multe dispozitive IoT nu au fost dezvoltate având securitatea cibernetică drept obiectiv, așa că mulți fabricanți nu oferă prea multe informații de securitate. Dar, pe măsură ce gradul de conștientizare a securității cibernetice crește, sperăm să vedem din ce în ce mai mulți furnizori de produse IoT care integrează elemente de securitate în produsele lor și oferă mai multă informație despre cum să le protejăm și să le actualizăm.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS http://www.securingthehuman.org

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Programe de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2015#october2015
Securizarea tabletei:	https://securingthehuman.sans.org/ouch/2016#january2016
Securizarea rețelei de acasă:	https://securingthehuman.sans.org/ouch/2016#february2016

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducere: Cosmin Hănulescu