OUCH! | August 2018

SANS SECURITY AWARENESS

OUCH!

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Dispozitivele inteligente domestice

Ce sunt dispozitivele inteligente de uz casnic?

În mod tradițional, doar câteva dintre echipamentele de uz casnic se pot conecta la Internet, cum ar fi calculatorul portabil, telefonul mobil sau consola pentru jocuri. Astăzi însă, din ce în ce mai multe dispozitive se conectează online, de la becuri sau incinte acustice până la televizoare, încuietorile ușilor sau autoturismul personal. În curând aproape orice dispozitiv din casă ar putea fi conectat la Internet. Aceste dispozitive conectate sunt deseori denumite colectiv Internet of Things[1] (IoT) sau dispozitivele casei inteligente (Smart Home Devices). Deși aceste obiecte interconectate aduc o mulțime de beneficii, ele creează și o serie de riscuri unice.

Care e problema?

Cu cât mai multe dispozitive sunt conectate în rețeaua domestică, cu-atât mai multe șanse sunt ca ceva să fie în neregulă. Răufăcătorii pot programa dispozitivele pe care le aveți pentru a lansa atacuri asupra altora, producătorii acestora pot colecta informații amănunțite despre activitatea dumneavoastră sau echipamentele în sine pot fi afectate, blocându-vă, spre exemplu, accesul. Multe companii furnizoare de astfel de dispozitive nu au experiența securității cibernetice, și o percep ca un cost suplimentar. Drept consecință, multe dispozitive pe care le cumpărați au elemente puține de securitate sau chiar deloc. De exemplu, unele au parole implicite care sunt bine cunoscute sau pe care nu le puteți actualiza sau configura.

Cum vă puteți proteja

Așadar, ce puteți face? Vrem, cu siguranță, să beneficiați de pe urma echipamentelor interconectate într-o manieră sigură, securizată. Acestea pot furniza funcții extraordinare care vă fac viața mai ușoară. În plus, pe măsură ce tehnologia evoluează, s-ar putea să nu aveți încotro, trebuind să le folosiți. Iată mai jos câteva măsuri pe care le puteți lua pentru a vă proteja.

Conectați numai ce este nevoie: Cea mai simplă metodă de securizare a dispozitivelor este să nu le conectați la Internet. Dacă nu aveți nevoie ca acestea să fie online, nu le conectați la rețeaua Wi-Fi. Chiar aveți nevoie ca prăjitorul de pâine să vă trimită mesaje de notificare pe telefonul mobil?

Aflați ce ați conectat online: Ce dispozitive aveți conectate în rețeaua domestică? Nu sunteți siguri că vă amintiți? Opriți conexiunea Wi-Fi și observați ce anume nu mai funcționează. Poate că nu veți identifica tot, dar s-ar putea să fiți surprinși de numărul dispozitivelor de care ați uitat.

Mențineți-le actualizate: Ca și calculatorul personal sau telefonul mobil, este crucial să mențineți actualizate toate echipamentele deținute. Dacă un dispozitiv are opțiunea actualizării automate, activați-o.

1 Rețeaua obiectelor interconectate, într-o traducere aproximativă

Parolele: Schimbați parolele de pe dispozitive cu o parolă unică, o propoziție-parolă puternică pe care doar dumneavoastră o știți. Cel mai probabil nu va trebui s-o scrieți decât o dată. Nu vă reamintiți toate propozițiile-parolă? Nici noi, nu vă faceți griji. Aveți în vedere folosirea unui program de gestiune a parolelor, pentru a le păstra în siguranță.

Opțiune de protecție a datelor personale: Dacă dispozitivul permite configurarea opțiunilor de protecție a datelor cu caracter personal, limitați volumul de informații pe care acesta le colectează și le partajează. O variantă ar fi pur și simplu să dezactivați orice funcție de partajare a informațiilor.

Producătorul: Cumpărați-vă dispozitivele de la companii pe care le cunoașteți și în care aveți încredere. Căutați produse care oferă securitate, cum ar fi disponibilitatea funcțiilor de actualizare automată, modificarea parolei implicite și a opțiunilor de protecție a datelor personale.

Înregistrarea audio permanentă: Dacă un dispozitiv poate prelua comenzi vocale, acesta înregistrează în permanență sunetul. De exemplu, echipamente ca Alexa sau Google Home pot înregistra conversații private. Aveți în vedere acest lucru atunci când alegeți locul din casă unde veți plasa aceste dispozitive și verificați opțiunile de confidențialitate.

Rețeaua pentru oaspeți: Luați în calcul plasarea acestor dispozitive inteligente într-o rețea Wi-Fi separată, pentru oaspeți, în locul celei principale, unde sunt conectate calculatoarele și telefoanele mobile inteligente. În acest fel, dacă unul dintre aceste dispozitive este infectat, calculatoarele personale și telefoanele mobile din rețeaua principală vor rămâne în siguranță.

Nu există niciun motiv pentru a vă teme de noile tehnologii, însă înțelegeți riscurile pe care acestea le comportă. Parcurgând acești pași simpli puteți ajuta la cearea unei Case Inteligente mult mai sigure.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Robert M. Lee *(@RobertMLee) este instructor certificat SANS, autorul cursurilor FOR578 - Cyber Threat Intelligence și ICS515 - ICS Active Defense and Incident Response. Robert este de asemenea CEO și fondator al companiei de securitate cibernetică axată pe domeniul industrial Dragos.*

Resurse online

Propoziții-parolă:	https://www.sans.org/u/GEB
Programele de gestiune a parolelor:	https://www.sans.org/u/GEG
Securizarea rețelei domestice:	https://www.sans.org/u/GEL