OUCH! | Februarie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Rețeaua WiFi personală**
- **Dispozitivele proprii**

Securizarea rețelei de acasă

Generalități

Cu ani în urmă rețelele de calculatoare domestice erau relativ simple, frecvent formate dintr-un punct de acces fără fir și un calculator sau două, folosite pentru accesul la Internet, cumpărături online sau jocuri. Între timp acestea au devenit din ce în ce mai complexe. Acum conectăm la aceste rețele mult mai multe dispozitive și le folosim pentru multe alte lucruri în afară de navigarea pe Web sau conținut multimedia. În acest buletin informativ discutăm modul în care puteți crea o rețea securizată acasă, pentru dumneavoastră și pentru restul familiei.

Editor Invitat

Cheryl Conley coordonează echipa de instruire și sensibilizare asupra securității informației din cadrul companiei Lockheed Martin, valorificând campania „The I Campaign™“, cu o audiență de peste 100,000 de angajați. Aceasta include asocieri și grupuri focus de susținere în întreaga companie, pe lângă un program de tip phishing la nivel mondial. Urmăriți-o pe Cheryl la **@conleychera**.

Rețeaua WiFi personală

Aproape orice rețea domestică de calculatoare începe cu o rețea fără fir, uneori cunoscută ca rețea WiFi. Aceasta facilitează conectarea fără fir a oricărui dispozitiv personal la Internet, de la calculatoare portabile și tablete până la console pentru jocuri sau televizoare. Multe rețele domestice fără fir sunt controlate de router-ul Internet, care este un dispozitiv instalat în casă de furnizorul de servicii de acces Internet. Însă, în unele cazuri, rețeaua este controlată de un sistem separat, denumit punct de acces fără fir, care este apoi conectat la router-ul de acces Internet. Indiferent ce variantă e folosită în rețeaua Dumneavoastră, ambele funcționează la fel, prin emiterea de semnale radio. Dispozitivele diferite din casă se conectează la acestea folosind astfel de semnale. Din acest punct, aceste dispozitive se pot conecta atât la Internet cât și la oricare alt dispozitiv prezent în rețeaua din casă. Aceasta înseamnă că securizarea rețelei WiFi este un element cheie în protecția casei. Vă recomandăm următorii pași pentru securizarea ei.

- Schimbați parola implicită a contului de administrator pe router-ul de acces Internet sau punctul de acces WiFi, în funcție de care dintre acestea controlează rețeaua. Contul de administrator este cel care permite modificarea parametrilor de configurație pentru rețeaua personală fără fir. Problema este că multe echipamente de acces fără fir la Internet sunt livrate cu parole inițiale pentru administrare ce sunt bine cunoscute, deseori fiind publicate pe Internet. În consecință, asigurați-vă că schimbați parola de administrator cu una puternică, unică, pe care doar Dumneavoastră o cunoașteți.
- Schimbați denumirea implicită a rețelei WiFi (uneori cunoscută ca SSID). Acest nume este ceea ce văd dispozitivele ce caută o conexiune locală fără fir. Dați rețelei un nume unic pe care să-l puteți identifica cu ușurință, dar asigurați-vă că nu

Securizarea rețelei de acasă

conține nicio informație personală. Nu e nici un avantaj în configurarea rețelei cu nume ascuns, deoarece multe instrumente de inventariere a rețelelor fără fir sau un răufăcător iscusit pot descoperi cu ușurință rețelele ascunse.

Pentru a vă proteja rețeaua personală de-acasă, securizați rețeaua fără fir și actualizați și protejați cu parole toate dispozitivele conectate în rețea.

- Asigurați-vă că numai persoanele de încredere se pot conecta și pot folosi rețeaua Dumneavoastră fără fir și că sunt criptate conexiunile. Faceți aceasta activând un nivel de securitate crescută. În acest moment, cea mai bună opțiune este folosirea mecanismului de securizare cunoscut ca WPA2. Activând această opțiune, persoanele care se conectează vor avea nevoie de o parolă și, odată conectați, activitatea lor online va fi criptată. Verificați să nu folosiți mecanisme de securitate învechite, cum ar fi WEP, sau să nu folosiți niciun mecanism de protecție, adică o rețea deschisă. Rețelele deschise permit oricui accesul la rețeaua Dumneavoastră fără nicio formă de autentificare.
- Asigurați-vă că parola folosită de cei care se conectează la rețeaua Dumneavoastră fără fir este una puternică și că e diferită de cea pentru administrator. Rețineți că cel mai probabil e nevoie să introduceți parola doar o dată pentru fiecare dispozitiv, deoarece acestea pot memora și păstra parola.
- Multe rețele fără fir oferă posibilitatea unei configurații de rețea de tip „oaspete“ (guest network). Aceasta permite unui vizitator accesul la Internet, dar vă protejează rețeaua domestică personală, pentru că vizitatorii nu se vor putea conecta la dispozitivele care o alcătuiesc. Dacă adăugați o rețea „oaspete“, asigurați-vă că activați WPA2 și o parolă unică pentru aceasta.
- Dezactivați „WiFi Protected Setup“ sau alte mecanisme ce permit ca un nou dispozitiv să se conecteze la rețea fără a cunoaște parola și opțiunile de configurare.
- Dacă aveți dificultăți în reamintirea acestor parole diferite, vă recomandăm călduros să folosiți un program de gestiune a parolelor, pentru păstrarea lor în siguranță.

Nu sunteți siguri pe modul cum se pun în practică aceste recomandări? Cereți sprijinul furnizorului de servicii de acces Internet, citiți documentația ce a însoțit router-ul sau dispozitivul de acces sau consultați site-urile web corespunzătoare lor.

Dispozitivele proprii

Următorul pas este cunoașterea dispozitivelor conectate la rețeaua Dumneavoastră și securizarea lor. Acest lucru era simplu pe vremea când erau doar câteva dispozitive conectate. Acum în schimb, în lumea actuală „permanent conectată“,

Securizarea rețelei de acasă

aproape orice dispozitiv se poate conecta la rețeaua domestică de calculatoare, incluzând aici televizoarele, consolele pentru jocuri, sistemele de monitorizare a copiilor, difuzoare, termostatul sau chiar și autoturismul personal. O modalitate ușoară de inventariere a echipamentelor conectate la rețeaua de-acasă este utilizarea unui program de scanare a rețelei, de exemplu Fing. Aceste aplicații, ce pot fi instalate pe calculatorul personal sau pe dispozitivul mobil, scanează rețeaua WiFi și raportează toate dispozitivele conectate la aceasta. Odată ce ați identificat toate dispozitivele conectate la rețea, trebuie să vă asigurați că fiecare dintre ele este securizat. Cea mai bună modalitate în care puteți face asta este să vă asigurați că ele funcționează permanent cu cea mai recentă versiune de sistem de operare sau software preinstalat. Acolo unde e posibil, activați funcția de actualizare automată pe fiecare dintre ele. Dacă oricare dintre dispozitive necesită o parolă, folosiți întotdeauna o parolă puternică, unică. În final, asigurați-vă că verificați site-ul furnizorului de servicii de acces Internet, pentru că s-ar putea să vă pună la dispoziție unelte gratuite pentru a vă ajuta în securizarea rețelei personale de acasă.

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
Cartarea rețelei de-acasă:	http://l.rud.is/home-network-mapping

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