SANS SECURITY AWARENESS
cegeka
OUCH! | Ianuarie 2018
Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Rețeaua personală wireless**
- **Dispozitivele personale**
- **Parolele**
- **Copiile de siguranță**

Realizarea domiciliului securizat cibernetic

Generalități

Cu ani în urmă crearea unei domiciliu securizat cibernetic era un lucru simplu, majoritatea nu erau altceva decât o rețea wireless cu câteva calculatoare conectate. Astăzi tehnologia a devenit mult mai complicată și este parte integrantă din toate laturile vieților noastre, de la dispozitivele mobile și consolele pentru jocuri la termostatele din gospodărie sau poate chiar și aparatele frigorifice. Prezentați aici sunt patru pași simpli pentru realizarea unei case securizată cibernetic.

Editor Invitat

Matt Bromiley e manager de incidente în activitatea cotidiană în care-și ajută clienții de toate mărimile să facă față breșelor de securitate. Este de asemenea instructor SANS și predă cursul FOR508, Analiza Criminalistică Digitală și Răspunsul la Incidente. Urmăriți-l pe Matt la **@mbromileyDFIR**.

Rețeaua personală wireless

Aproape orice rețea domestică wireless începe cu o rețea wireless (sau Wi-Fi). Aceasta este mijlocul care permite conectarea dispozitivelor la Internet. Majoritatea rețelelor domestice sunt controlate de către router-ul de acces Internet sau un dispozitiv de acces wireless separat de acesta. Ambele funcționează la fel, prin emiterea de semnale radio dispozitivele din casă se vor conecta la ele. Aceasta înseamnă că securitatea rețelei wireless este un element critic al asigurării protecției casei. Recomandăm următorii pași în vederea securizării acesteia:

- Modificați parola implicită a contului de administrator pentru router-ul sau dispozitivul de acces wireless, în funcție de care dintre ele controlează rețeaua personală wireless. Contul “admin” este cel ce vă permite configurarea parametrilor de funcționarea pentru rețeaua wireless.
- Asigurați-vă că doar persoane de încredere se pot conecta la rețeaua dumneavoastră. Faceți asta prin activarea unui mecanism puternic de securitate. În acest moment cea mai bună variantă disponibilă este protocolul WPA2. Activându-l este necesară o parolă pentru acces, ulterior traficul generat de activitatea online fiind criptat.
- Asigurați-vă că parola folosită pentru conectarea la router-ul wireless este una puternică și că e diferită de cea pentru contul de administrator. Rețineți că e necesar să introduceți parola doar o dată pentru fiecare dispozitiv care se conectează, deoarece acestea memorează și păstrează parola.
- Multe rețele wireless permit ceea ce se numește „Guest Network” („rețea pentru oaspeți”). Aceasta permite vizitatorilor conectarea la Internet, dar protejează rețeaua dumneavoastră domestică fiindcă ei nu se pot conecta la oricare dintre celelalte dispozitive din rețeaua dumneavoastră personală. Dacă adăugați o rețea „Guest” asigurați-vă că ați activat protocolul WPA2 cât și o parolă unică pentru această rețea.

Realizarea domiciliului securizat cibernetic

Nu sunteți siguri în privința parcurgerii acestor pași? Cereți asistența furnizorului de servicii de acces Internet sau consultați-le site-ul, studiați documentația care a însoțit router-ul Internet sau dispozitivul de acces wireless sau site-urile producătorilor acestora.

Urmați acești patru pași simpli pentru realizarea unui domiciliu securizat cibernetic; securizați rețeaua personală Wi-Fi, activați actualizarea automată, folosit propoziții-parolă unice și activați realizarea copiilor de siguranță.

Dispozitivele personale

Următorul pas este să știți ce dispozitive sunt conectate la rețeaua personală wireless, asigurând-vă că toate sunt securizate. Acest lucru obișnuia să fie simplu când aveați unul-două calculatoare. Acum în schimb mai toate dispozitivele se pot conecta la o rețea domestică, inclusiv telefoanele mobile, televizoarele, consolele de jocuri, dispozitivele de monitorizare a bebelușilor, difuzoarele sau probabil că și autoturismul personal. Odată ce ați identificat toate aceste dispozitive din rețeaua personală, asigurați-vă că fiecare dintre ele este securizat. Cel mai bun mod în care puteți face asta este să vă asigurați că actualizarea automată pe fiecare dintre ele este activă. Răufăcătorii caută în continuu noi vulnerabilități pe diferite echipamente și sisteme de operare. Activând funcția de actualizare automată calculatorul și dispozitivele personale vor avea permanent cea mai recentă versiune de software, ceea ce le face mult mai dificil de accesat de către infractori.

Parolele

Următorul pas este să folosiți parole puternice, unice, pentru fiecare dintre dispozitivele personale sau conturile online. Cuvintele cheie aici sunt *puternic* și *unic*. V-ați săturat de parole complicate ce sunt greu de ținut minte și dificil de scris? Și noi. Folosiți o propoziție-parolă în schimb. Aceasta este un tip de parolă care folosește serii de cuvinte care sunt ușor de memorat, cum ar fi „*Unde este cafeaua mea?*” sau „*soare-gogoși-fericit-pierdut*”. Cu cât e mai lungă propoziția-parolă, cu atât mai puternică. O parolă unică înseamnă folosirea unei parole diferite pentru fiecare dispozitiv sau cont online. În acest fel, dacă o parolă este compromisă, toate celelalte conturi sau echipamente sunt încă în siguranță. Nu puteți memora toate aceste parole puternice și unice? Nu vă îngrijorați, nici noi. Acesta este motivul pentru care recomandăm folosirea unui program de gestiune a parolelor, care este un program de securitate special ce stochează în siguranță toate parolele într-un seif virtual, criptat.

În final, activați verificarea în doi pași acolo unde este disponibilă, mai ales pentru conturile online. Verificarea în doi pași este și mai puternică. Aceasta folosește parole, dar și un al doilea pas, cum ar fi un cod trimis pe telefonul mobil sau o aplicație de pe acesta care generează codul pentru dumneavoastră. Verificarea în doi pași este, probabil, singura și cea mai importantă măsură de protecție personală online, și e mult mai ușor de folosit decât credeți.

Realizarea domiciliului securizat cibernetic

Copiile de siguranță

Uneori, oricât de precauți sunteți, puteți fi victima unui atac informatic. Dacă aceasta este situația, deseori singura modalitate în care puteți să vă recuperați informațiile personale este să le restaurați din copii de siguranță. Asigurați-vă că faceți periodic copii de siguranță ale oricăror informații importante și că verificați restaurarea lor. Multe dispozitive mobile permit realizarea copiilor de siguranță pe platformă Cloud. Pentru multe calculatoare s-ar putea să trebuiască să cumpărați un gen de software sau serviciu de realizare a copiilor de siguranță, ce sunt de regulă destul de ieftine și ușor de folosit.

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 securingthehuman.sans.org/ouch/archives

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.

Resurse

Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2017#april2017
Programe de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2017#september2017
Autentificarea în doi pași:	https://securingthehuman.sans.org/ouch/2017#december2017
Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2017#august2017

Echipa editorială: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducere: Cosmin Hănulescu

