Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Šta je enkripcija?**
- **Šta se može enkriptovati?**
- **Pravilno korišćenje**

Enkripcija

Šta je enkripcija (šifrovanje)?

Do sada ste već puno puta čuli za termin „enkripcija“ i kako je potrebno koristi je da bi ste zaštitili sebe i svoje informacije. Međutim, enkripcija može biti zbunjujuća i potrebno je shvatiti njena ograničenja. U ovom izdanju objasnićemo na jednostavan način šta je enkripcija, kako može da vas zaštiti i kako da je pravilno implementirate.

Gost urednik

Francesca Bosco (**@francibosco**) je istraživač i saradnik na projektima vezanim za sajber kriminal, bezbednost i zloupotrebe tehnologija. Radi u inter-regionalnom institutu za istraživanje kriminala i pravosuđe pri Ujedinjenim Nacijama i ko-osnivač je centra za tehnologiju i pravo.

Na svojim uređajima skladištite ogromnu količinu osetljivih informacija, na primer lična dokumenta, fotografije i el. poštu. Ako je jedan od vaših uređaja izgubljen ili ukraden, svi vaši osetljivi podaci mogu biti dostupni onom ko je u posedu uređaja. Osim toga, možda preko svojih uređaja obavljate osetljive finansijske transakcije, kao što su bankarske transakcije ili el. kupovina. Ako neko može da nadgleda vaše on-line aktivnosti verovatno bi mogao da ukrade vaše osetljive informacije, kao što su bankarski računi ili brojevi kreditnih kartica. U takvim situacijama enkripcija može da vas zaštiti tako što će onemogućiti neautorizovane osobe da pristupe ili modifikuju vaše informacije.

Enkripcija je u upotrebi već hiljadama godina. Danas, ekripcija je daleko sofisticiranija, ali služi istoj svrsi – da tajnu poruku prenese sa jednog na drugo mesto obezbeđujući da samo ovlašćene osobe mogu da je pročitaju ili joj pristupe. Kada informacija nije enkriptovana, naziva se običan tekst (plain-text), što znači da svako može jednostavno da joj pristupi i da je pročita. Enkripicija takvu informaciju konvertuje u nečitljiv format pod nazivom šifriran tekst (chiper-text). Danas se enkripcija zasniva na korišćenju kompleksnih matematičkih operacija i jedinstvenog ključa za konvertovanje informacija u šifriran tekst. Ključ služi za zaključavanje i otključavanje informacija. U većini slučajeva, vaš ključ je lozinka ili propusni kod.

Šta možete da enkriptujete?

Uopšteno postoje dva tipa enkripcije, „podaci u mirovanju“ (odnosi se na podatke koji su uskladišteni na uređajima) i „podaci u pokretu“ (odnosi se na podatke koji su u procesu tranzita).

Enkripcija

Ekripcija podataka u mirovanju je od vitalnog značaja ukoliko je vaš uređaj izgubljen ili ukraden. Današnji uređaji su izuzetno moćni i sadrže ogromnu količinu informacija, ali se mogu i veoma lako izgubiti. Osim toga, i drugi tipovi prenosivih medijuma takođe mogu sadržati osetljive informacije, na primer USB fleš diskovi ili eksterni tvrdi diskovi. Potpuna enkripcija diska, „Full Disk Encryption“ (FDE) je široko korišćena tehnika enkripcije celokupnog diska vašeg uređaja. Podrazumeva da se sve što je na sistemu automatski enkriptuje, nije potrebna nikakva vaša akcija ili odluka šta enkriptovati, a šta ne. Danas, većina uređaja poseduje FDE opciju, ali je potrebno da je sami aktivirate. Na Mac računarima se zove „FileVault“ dok na Windows računarima, zavisno od verzije, možete koristiti „Bitlocker“ ili „Device Encryption“. Većina mobilnih uređaja takođe podržava FDE. iOS na iPhone i iPad uređajima automatski pokreće FDE kada se postavi propusni kod. Od Android 6.0 (Marshmallow) sistema, Google podrazumeva aktivaciju FDE kao osnovnu postavku sistema, ako hardver to omogućava.

Enkripcija je moćan način zaštite vaših informacija, ali je jaka onoliko koliko je jak vaš ključ.

Informacije mogu biti ugrožene takođe kada su i u tranzitu. Ako nisu enkriptovane, mogu biti nadgledane, modifikovane ili presretnute. Usled toga veoma je preporučljivo da je svaka osetljiva on-line transakcija i komunikacija enkriptovana. Uobičajeni tip on-line enkripcije je HTTPS, koji podrazumeva da je saobraćaj između vašeg pretraživača i Internet stranice enkriptovan. Vidite https:// u adresi Internet stranice, ikonicu zaključanog katanca, ili polje adrese Internet stranice zelene boje. Drugi primer predstavlja slanje i primanje el. pošte. Većina klijenata el. pošte obezbeđuju opciju enkripcije koju je uglavnom potrebno da sami aktivirate. Treći primer enkripcije podataka u tranzitu je između dva korisnika koji komuniciraju pomoću „iMessage“, „Wickr“, „Signal“, „WhatsApp“ ili „Telegram“ aplikacija. Takve aplikacije koriste enkripciju od jednog do drugog kraja (end-to-end) koja sprečava treće strane da pristupe podacima dok se prenose sa jednog na drugi sistem ili sa jednog na drugi uređaj. To znači da samo vi i osoba sa kojom komunicirate možete da pročitate poslatu poruku.

Pravilno korišćenje

Da bi ste bili sigurni da ste zaštićeni enkripcijom, veoma je važno da je pravilno koristite.

Enkripcija

- Enkripcija je jaka koliko je jak ključ enkripcije. Ako neko pogodi ili dođe do vašeg ključa, imaće pristup vašim podacima. Zaštitite svoj ključ. Ako koristite lozinku ili propusni kod za svoj ključ, budite sigurni da su jaki i jedinstveni. Što je lozinka duža to je teže da se pogodi ili otkrije. Nemojte zaboravljati lozinku, pošto bez ključa ne možete dekriptovati svoje informacije. Ako ne možete da zapamtite sve svoje lozinke koristite Menadžere lozinki.
- Enkripcija je jako koliko su sigurni vaši uređaji. Ako je vaš uređaj kompromitovan ili inficiran malicioznim softverom, sajber kriminalci mogu da zaobiđu enkripciju. Zbog toga je veoma važno da preduzmete i druge korake u cilju zaštite svojih uređaja, uključujući korišćenje antivirusa, jake lozinke i ažuriranje sistema i aplikacija.
- Danas u cilju zaštite podataka i komunikacije, većina aplikacija za mobine uređaja i računarskih aplikacija omogućavaju jaku enkripciju. Ako neka od njih koju planirate da koristite to ne omogućava, razmislite o alternativi.

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 securingthehuman.sans.org/ouch/archives.

Dodatne informacije

Objašnjenje enkripcije:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
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
Šta je malver:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_se.pdf
Bezbednost vašeg novog tableta:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_se.pdf

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