Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- Šta je enkripcija?
- Enkripcija u mirovanju
- Enkripcija u tranzitu

Enkripcija (Šifrovanje)

Šta je enkripcija?

Možda ste već do sada čuli za termin „enkripcija" i kao je treba koristiti u cilju zaštite poslovnih ili privatnih informacija. Međutim, koncepcija enkripcije može da vam se učini konfuznom. Pored toga, enkripcija ne može da vas zaštite od svega, postoje izvesna ograničenja. U ovom izdanju pokušaćemo da jednostavnom terminologijom objasnimo šta je enkripcija, zašto je treba koristiti i kako je ispravno implementirati.

Gost urednik

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**), konsultant iz Vašingtona, je vodeći instruktor za „Mobile Device Security and Ethical Hacking (SEC575) kurs i autor „Incident Response Team Management (MGT535)" kursa SANS instituta.

Verovatno na svojim uređajima imate ogromnu količinu osetljivih podataka, kao što su finansijski dokumenti, slike, el. pošta ili čak medicinski podaci. Ako se desi da jedan od svojih uređaja izgubite ili vam je ukraden, svi ti osetljivi podaci mogu biti dostupni osobi kod koje je uređaj. Pored toga, moguće ja da svoje finansijske transakcije, kao što su el. bankarstvo ili kupovina, obavljate preko Interneta. Ako su sajber-kriminalci u mogućnosti da nadgledaju vaše aktivnosti, postoji mogućnost da ukradu neke vaše podatke, na primer bankovne račune ili brojeve kreditnih kartica. U takvim situacijama enkripcija može da vas zaštiti tako što onemogućava ne autorizovanim osobama da pristupe ili modifikuju vaše informacije.

Kada informacije nisu enkriptovane, nazivaju se „običan-tekst" („plain-text"), i jednostavno im se može pristupiti ili ih modifikovati. Enkripcija konvertuje informacije u nečitljiv format nazvan „šifriran-tekst" („cipher-text"). Funkcioniše tako što se koriste kompleksne matematičke operacije i jedinstveni ključ da bi se informacija konvertovala u format šifriranog teksta. Svrha ključa je kao i kod običnih vrata, služi da zaključa ili otključa informaciju. Samim tim, da bi enkriptovana informacija bila zaštićena, potrebno je i da ključ bude na sigurnom. U principu enkripcija se koristi na dva načina, moguće je enkriptovati podatke u mirovanju (na primer podaci uskladišteni na vašem računaru) i podatke u kretanju (na primer kada se prenose preko računarske mreže, Interneta).

Enkripcija informacija u mirovanju

Primarni cilj enkripcije informacija u mirovanju je zaštita informacija u slučaju da je uređaj (računar ili mobilni uređaj) izgubljen ili ukraden. Pre petnaest godina ovo nije bila toliko bitna tema, obzirom da su većina računara u upotrebi

Enkripcija (Šifrovanje)

bila nezgrapni stoni uređaji koje je bilo teško pomerati unaokolo. Današnji laptopovi teže jedva neki kilogram, dok mobilni uređaji nešto više od stotinu grama. Pored toga što su veoma moćni i mogu da skladište ogromnu količinu podataka, treba imati na umu da ih je veoma lako izgubiti. Takođe, i drugi prenosivi medijumi mogu da skladište osetljive informacije, kao što su USB fleš drajvovi ili DVD ROM-ovi. Uobičajena tehnika enkripcije za ovakvu vrstu uređaja ili medijuma naziva se „Potpuna Enkripcija Diska“ („Full Disk Encryption“, FDE). To znači da je sve što se nalazi na uređaju automatski enkriptovano, nije potrebno da sam korisnik odlučuje da li će nešto bili ili ne enkriptovano. Većina današnjih operativnih sistema ima ovu funkciju fabrički ugrađenu, samo je potrebno uključiti je. Na primer, Mac OS X za tu namenu poseduje FileVault dok neke verzije Windows-a imaju Bitlocker. Ako vaši uređaji poseduju funkciju „Full Disk Encryption”-a, preporučujemo vam da je uključite. Pored toga, većina mobilnih telefona podržava „Full Disk Encryption” svog internog skladišta. Na primer, iOS, operativni sistem za iPhone-e i iPad-e, automatski uključuje ovu funkciju kada se postavi lozinka. U vezi korišćenja ove funkcije na vašem poslovnom računaru, raspitajte se kod odgovornih osoba. U vezi mogućnosti korišćenja ove funkcije na vašem privatnom računaru, kontaktirajte proizvođača ili proverite u raspoloživoj dokumentaciji.

Enkripcija je pouzdan način da se obezbede informacije, ali samo onoliko koliko je pouzdan i sam ključ enkripcije.

Enkripcija informacija u tranzitu

Informacije su takođe ranjive i dok su u tranzitu. Ako nisu enkriptovane, lako se preko mreže mogu nadgledati i čitati. Usled toga verovatno želite da osigurate da vaša osetljiva komunikacija preko računarskih mreže, na primer, el. bankarstvo, slanje el. pošte ili čak pristup društvenim mrežama bude enkriptovana. Najčešći način mrežne enkripcije je svakako HTTPS, i on obezbeđuje da je saobraćaj između vašeg pretraživala i vebsajta kome pristupate, enkriptovan. Potražite https:// u ULR-u polju vašeg pretraživaca, možda vidite katanac ili URL polje postane zeleno. Ovo su znaci da je komunikacija enkriptovana. U zavisnosti od pretraživača i vebsajta, moguće je videti i sva tri odjednom. Pored toga, kada se konektujete na javne bežične mreže (WiFi), budite sigurni da uvek kada je to moguće koristite enkripciju. Konačno, kada šaljete ili primate el. poštu, budite sigurni da je vaš softver za el. poštu podešen da to čini preko enkriptovanog kanala. Većina softvera za el. poštu omogućava enkripciju, a pored toga moguće je i da vaš internet provajder može da vam pomogne u vezi toga.

Enkripcija (Šifrovanje)

Pravilno implementiranje enkripcije

Bez obzira koji način enkripcije koristite ili kako ga koristite, za skoro sve forme enkripcije važe zajedničke smernice za ispravno korišćenje.

- Enkripcija je jaka onoliko koliko je sam ključ jak. Ukoliko neko zna ili kompromituje vaš ključ, imaće pristup vašim podacima. Preduslov uspešne enkripcije je bezbedan ključ.
- Ako koristite lozinku za svoj ključ, budite sigurni da je dovoljno dugačka i sigurna, i vodite računa da je ne izgubite i ne zaboravite. Ako je zaboravite, vaši podaci će biti zauvek zaključani.
- Enkripcije je jaka onoliko koliko je bezbedan vaš računar. Ako je vaš računar kompromitovan ili inficiran onda je moguće da sajber-kriminalci zaobiđu vašu enkripciju. Vodite računa da svoje uređaje držite na sigurnom.
- Ako imate mogućnost da birate između više opcija enkripcije, uvek izaberite najjači metod.

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 http://www.securingthehuman.org/

Dodatne informacije

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
iOS enkripcija:	http://support.apple.com/kb/ht4175
Android enkripcija:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows enkripcija:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Bezbednost tvog računara:	http://www.securingthehuman.org/ouch/2012#december2012
Menadžeri lozinke:	http://www.securingthehuman.org/ouch/2013#october2013

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