OUCH! | 2016.gada jūnijs

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Šifrēšana

Kas ir šifrēšana?

Varbūt esat dzirdējuši cilvēkus pieminam šifrēšanu un ka Jums tā jāizmanto Jūsu un Jūsu informācijas aizsardzībai. Tomēr šifrēšana var būt neskaidra un Jums jāsaprot tās robežas. Šajā izdevumā mēs paskaidrojam, kas ir šifrēšana, kā tā Jūs pasargā un kā to ieviest un izmantot pareizi.

Viesredaktors
Francesca Bosco (**@francibosco**) ir pētniece un projektu vadītāja, kas darbojas ar projektiem, kas saistīti ar kibernoziegumiem, kiberdrošību un tehnoloģiju nelikumīgu lietošanu. Viņa strādā Apvienoto Nāciju Pār reģionu Noziedzības un Tieslietu Izpētes institūtā un ir Tehnoloģiju un likumu centra līdzdibinātāja.

Jūsu ierīcēs ir daudz sensitīvas informācijas, piemēram, personīgie dokumenti, foto un e-pasti. Ja kāda no Jūsu ierīcēm pazūd vai tiek nozagta, informācijai var piekļūt tas, kas iegūst ierīci. Tāpat Jūs tiešsaistē arī veicat sensitīvas darbības, piemēram, iepirkšanos vai bankas transakcijas. Ja kāds novērotu šīs aktivitātes, tie varētu nozagt Jūsu informāciju, piemēram, finanšu kontu vai kredītkartes informāciju. Šifrēšana Jūs pasargā šādās situācijās, nodrošinot to, ka neautorizēti cilvēki nespēj piekļūt vai modificēt šo informāciju.

Šifrēšanai ir vairāku tūkstošu gadu ilga vēsture. Šodien šifrēšana ir daudz sarežģītāka, taču mērķis ir tas pats - nodot slepenu ziņu no viena punkta uz otru, nodrošinot, ka tai var piekļūt tikai tie, kam uz to ir tiesības. Kad informācija nav šifrēta to sauc par vienkāršu tekstu. Tas nozīmē, ka Jebkurš var vienkārši tai piekļūt vai izlasīt. Šifrēšana pārvērš šo informāciju nesalasāmā formā ko sauc par šifrētu tekstu. Šodienas šifrēšana izmanto sarežģītas matemātiskas darbības un unikālu atslēgu, lai pārvēstu Jūsu informāciju šifrētā tekstā. Atslēga ir tas kas “aizslēdz” un “atslēdz” Jūsu informāciju. Vairumā gadījumu atslēga ir Jūsu parole.

Ko Jūs varat šifrēt?

Vispārīgi ir divu tipu dati ko šifrēt: dati miera stāvoklī (piemēram, dati, kas tiek saglabāti Jūsu mobilajā ierīcē) un dati kas tiek pārvietoti (piemēram, saņemot e-pastu vai nosūtot ziņu draugam).

Šifrēšana

Datu šifrēšana miera stāvoklī ir būtiska, lai aizsargātu informāciju gadījumā, ja Jūsu mobilā iekārta vai dators tiek pazaudēts vai nozagts. Šodienas ierīces ir ļoti jaudīgas un spēj saglabāt ārkārtīgi lielu informācijas daudzumu, vienlaikus tās ir ļoti vienkārši pazaudēt. Papildus sensitīva informācija var būt arī citos pārnēsājamās datu ierīcēs, kā USB diski vai ārējie cietie diski. Pilna diska šifrēšana (FDE) ir plaši pielietota šifrēšanas tehnika, kas nošifrē visu disku Jūsu sistēmā. Tas nozīmē, ka viss sistēmā ir automātiski nošifrēts un Jums pat nav jāizlemj ko šifrēt un ko nē. Mūsdienās vairums datoru piedāvā FDE, bet Jums tā parasti ir jāieslēdz. Mac datoriem tas tiek saukts par FileVault, Windows datoros atkarībā no versijas var izmantot Bitlocker vai Device Encryption. Vairums mobilo iekārtu arī piedāvā FDE. iOS automātiski iespējo FDE tikko tiek uzstādīta parole. Sākot no Android 6.0 (Marshmallow) arī Google prasa, lai FDE būtu iespējota pēc noklusējuma ar nosacījumu, ka iekārta atbilst noteiktiem minimāliem standartiem.

Šifrēšana ir spēcīgs līdzeklis Jūsu informācijas aizsardzībai, bet tā ir tikai tik spēcīga kā Jūsu atslēga.

Informācija ir jāaizsargā, arī to pārraidot. Ja dati nav šifrēti, tie var tikt monitorēti, izmainīti vai pārtverti tiešsaistē. Tādēļ Jums nepieciešams nodrošināt, ka jebkādas sensitīvas tiešsaistes darbības tiek šifrētas. Izplatītākais tiešsaistes šifrēšanas tips ir HTTPS. Tas nozīmē, ka visa datu pārraide starp Jūsu Internet pārlūku un mājas lapu tiek šifrēts. Meklējiet https:// adreses laukā, slēdzenes ikonu Jūsu pārlūkā, vai pārliecinieties, ka Jūsu adreses lauks kļūst zaļš. Cits piemērs ir e-pasta nosūtīšana. Vairums e-pasta klientu piedāvā šifrēšanas iespējas taču tās bieži Jums jāaktivizē. Trešais piemērs ir šifrēt datus gadījumos, kad lietotāji sarunājas viens ar otru, piemēram, iMessage, Wickr, Signal, WhatsApp vai Telegram. Šāda veida aplikācijas izmantot šifrēšanu, kas neļauj trešajai pusei piekļūt datiem, kamēr tie tiek pārraidīti no vienas sistēmas vai iekārtas uz otru. Tas nozīmē, ka izlasīt informāciju varat tikai Jūs un persona, kurai tā tiek nosūtīta.

Dariet to pareizi

Lai aizsargātos izmantojot šifrēšanu, svarīgi ir to izmantot pareizi.

Šifrēšana

- Jūsu šifrēšana ir tikai tik spēcīga kā Jūsu atslēga. Ja kāds spēj uzminēt vai iegūt atslēgu, tas varēs arī piekļūt datiem. Aizsargājiet atslēgu. Ja izmantojat paroli, izvēlieties spēcīgu un unikālu paroli. Jo parole garāka jo grūtāk to uzbrucējam uzminēt. Neaizmirstat savu paroli, jo bez atslēgas Jūs nespēsiet atšifrēt informāciju. Ja Jūs nevarat atcerēties visas paroles, izmantojiet paroļu pārvaldnieku.
- Jūsu šifrēšana ir tikai tik spēcīga kā Jūsu iekārtu drošība. Ja iekārta ir kompromitēta vai inficēta ar ļaundabīgu programmatūru, uzbrucējs var apiet šifrēšanu. Tādēļ ir svarīgi aizsargāt savu ierīci izmantojot antivīrusu, drošas paroles un regulāri to atjaunojot.
- Daudzas mobilās aplikācijas un datorprogrammas piedāvā spēcīgu šifrēšanu, lai aizsargātu Jūsu datus un sakarus. Ja aplikācija, ko Jūs apsverat izmantot nepiedāvā šifrēšanu, pamēģiniet alternatīvas.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Šifrēšanas apraksts:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Paroles:	https://securingthehuman.sans.org/ouch/2015#april2015
Paroļu pārvaldnieki:	https://securingthehuman.sans.org/ouch/2015#october2015
Kas ir ļaundatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Jūsu planšetes aizsardzība:	https://securingthehuman.sans.org/ouch/2016#january2016

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Tulkojums: Edgars Tauriņš