Ikmēneša Informācijas drošības izdevums Tev

Vai esmu „uzlauzts”?

Pārskats

Lai cik droši jūs šķietami arī justos, tieši tāpat kā vadot automašīnu, agrāk vai vēlāk var notikt negadījums. Zemāk ir ieteikumi, kā noteikt, vai jūs kāds ir uzlauzis, un ja tas tā ir noticis, ko darīt tādā gadījumā? Jo ātrāk jūs atklāsiet, ka ir noticis kas nelāgs, jo lielāka iespēja ir atrisināt problēmu.

Pazīmes, ka jūs esat uzlauzts:

- **Jūsu antivīrusa programma ziņo par sistēmas infekciju. Pārliecinieties, ka tā ir tiešām jūsu programma, kas ģenerē paziņojumus, nevis kādas mājas lapas uzlecošais logs, kas mēģina jūs apmānīt, lai jūs instalētu programmu vai pazvanītu uz krāpniecības telefona numuru. Neziniet kā pārliecināties? Atveriet savu antivīrusa programmu.**
- **Uzlecošais logs jums paziņo, ka datora faili ir šifrēti un pieprasa izpirkuma maksu, lai tos atgūtu.**
- **Jūsu interneta pārlūks atver mājas lapas, ko neesat gribējis atvērt.**
- **Jūsu datora lietotnes nepārtraukti pārstāj darboties vai “uzkaras”, parādās jaunas programmu ikonas vai atveras dīvaini programmu logi.**
- **Jūsu parole nedarbojas, lai arī jūs esat pārliecināts, ka ievadījāt to pareizi.**
- **Draugi vaicā, kādēļ jūs viņiem sūtat e-pastus, bet jūs droši zināt, ka neesat šādus e-pastus sūtījis.**
- **Bankas izdrukā parādās izdevumi, ko jūs neesat veicis.**

Kā rīkoties

Ja jums ir aizdomas par to, ka esat kļuvis par hakeru upuri, - nevilcinieties, bet tā vietā rīkojieties!. Ja problēma ir saistīta ar darbu, nemēģiniet to atrisināt paša spēkiem, bet ziņojiet atbildīgajām personām. Ja tas ir privātais konts vai sistēma, zemāk ir daži ieteikumi, ko jūs varat darīt, lai ierobežotu nodarīto ļaunumu.

Nomainiet paroles: ne tikai paroles datorā vai mobilajā ierīcē, bet paroles visiem saviem tiešsaistes kontiem. Neizmantojiet paroļu maiņai inficētu datoru, izmantojiet tādu, par kura drošību esat pārliecināts. Sāciet ar svarīgākajiem kontiem. Ja nevarat atcerēties paroles, izmantojiet paroļu pārvaldnieku.

Finanses: Ja problēmas saistītas ar norēķinu karti vai bankas kontu, sazinieties ar jūsu banku vai citu finanšu pakalpojumu sniedzēju. Izmantojiet drošu un uzticamu telefona numuru, piemēram, to, kas norādīts uz jūsu norēķinu kartes vai jūsu konta pārskatā, vai apmeklējiet bankas mājas lapu no uzticama datora. Papildus apsveriet domu nobloķēt bankas kartes.

Antivīruss: Ja antivīrusa programma jūs informē par inficētu failu, sekojiet tās norādēm. Vairums šādu programmu dod lietotājiem ieteikumus, kā rīkoties inficēta faila gadījumā.

Pārinstalēšana: Ja nav iespējams salabot inficēto datoru, vai jūs vēlaties būt pārliecināts, ka sistēma ir droša, pārinstalējat operētājsistēmu. Rezerves kopijas izmantojiet tikai personīgo failu atgūšanai, nevis sistēmas instalēšanai. Ja neesat pārliecināts, kā veikt sistēmas pārinstalēšanu, izvēlieties profesionālu palīdzību. Vai arī, ja dators ir vecs, izvērtējat iespējas iegādāties jaunu. Visbeidzot, kad esat atjaunojis sistēmu, pārliecinieties, vai tajā ir uzstādīti jaunākie programmatūras atjauninājumi un vai ir ieslēgta automātiskā atjaunināšana, ja šāda opcija tiek piedāvāta.

Rezerves kopijas: viens no svarīgākajiem aizsardzības pasākumiem ir iepriekšēja sagatavošanās ar regulāru rezerves kopiju veidošanu. Ir risinājumi, kas veido rezerves kopijas katru dienu vai pat katru stundu. Neatkarīgi no tā, kādu risinājumu izvēlaties, regulāri pārbaudiet, vai tiešām spējat atjaunot failus no rezerves kopijām. Bieži vien rezerves kopijas ir vienīgā iespēja atjaunot failus pēc hakeru uzbrukuma.

Tiesībsargājošās iestādes: Ja jūtaties jebkādā veidā apdraudēts, paziņojiet par incidentu tiesībaizsardzības iestādēm. Valsts policijai, piemēram, ir izveidota mājas lapa www.manadrosiba.lv

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.

Viesredaktors

Dr. Johannes Ullrich *(@johullrich) ir SANS Tehnoloģiju institūta Pētniecības Dekāns, SANS „Internet Storm Center" direktors un SANS partneris. Viņš ir izveidojis DShield - sensoru sadarbības tīklu, un vada ikdienas "Internet Storm Center" drošības ziņu podkāstu.*

Resursi

Rezerves kopijas:	https://www.sans.org/u/JGP
Paroļu frāzes:	https://www.sans.org/u/JGU
Paroļu pārvaldnieki:	https://www.sans.org/u/JGZ
Kas ir ļaunatūra:	https://www.sans.org/u/JH4
Digitālās drošības alianse:	http://www.e-drosiba.lv/

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš