ITIESĪBAS

Komercdarbība 07:00, 9. Jūl. 2019


# Kā rīkoties, ja "uzlauzta" parole?

Viktorija Jarkina, ZAB "SORAINEN", zvērināta advokāte, Dr.iur.

https://www.itiesibas.lv/raksti/atbild-eksperts/komercdarbiba/ka-rikoties-ja-uzlauzta-parole/15207

**Saņēmu e-pasta vēstuli, kuras "Subject" ailītē ierakstīta mana datora parole, bet tekstā aicinājums sūtītājam pārskaitīt 1400 Amerikas Savienoto Valstu dolāru, jo viņš it kā esot lejupielādējis informāciju no mana datora. Tā kā datorā glabājas manam uzņēmumam būtiska informācija, satraucos, vai ir pietiekami tikai nomainīt paroli, lai sevi pasargātu? Kādas ir manas tiesības sūdzēties par šāda veida uzbrukumu (vai tā mēģinājumu)? Vai vienkārši jāsamierinās, ka digitālajā vidē nevaru justies pilnībā drošs? Kā man rīkoties?**

Datoram un informācijai tajā iespējams piekļūt dažādos veidos. Viens no izplatītākajiem veidiem ir, izveidojot savienojumu ar datoru jeb inficējot to, ko var izdarīt ar speciālu programmu palīdzību. Šādu programmu iespējams aktivizēt, slēpti nosūtot e-pastā pielikumus, kas tiek atvērti, vai arī atverot internetsaites, kā rezultātā kibernoziedznieks ir ieguvis savienojumu ar datoru. Šādā gadījumā personai ir iespēja lejupielādēt failus, lasīt e-pastus un veikt citas darbības kā datora lietotājam. Paroles iegūšanai šādām programmām mēdz būt funkcija *keylogger* jeb taustiņu pierakstītājs, ar kuras palīdzību tiek pierakstīts ikviens uz datora klaviatūras nospiestais taustiņš, tostarp ievadītās paroles.

Ar paroles nomainīšanu nebūtu pietiekami, lai sevi pasargātu. Ieteicams pārbaudīt, vai datorā ir instalētas un atjaunotas antivīrusu programmas. Papildus nav ieteicams izmantot vienu un to pašu paroli vairākās tīmekļa vietnēs, tostarp arī datora ielogošanās paroli. Mēdz notikt dažādu interneta portālu lietotāju e-pasta adrešu un paroļu noplūšana un nelegāla vākšana, pēc kā iegūtie dati tiek publiskoti vai ļaunprātīgi izmantoti. Ja datora paroli esat izmantojis arī citās ielogošanās vietās, tad pastāv iespēja, ka šādā veidā parole ir noplūdusi. Pārbaudīt, vai konta drošība tikusi apdraudēta datu aizsardzības pārkāpumā, iespējams tīmekļa vietnē Haveibeenpwned.com, ievadot e-pasta adresi.

Paroles aizsardzībai ieteicams izmantot arī divkāršo autentifikācijas metodi jeb divu faktoru autentifikāciju, ko izmantot piedāvā dažādās tīmekļa vietnēs, sociālajos tīklos, internetbankās un e-pastos. Šāda metode darbojas, atnākot īsziņai ar unikālu kodu, kas jāievada papildus lietotājvārdam un parolei. Pastāv arī speciālas autentifikācijas aplikācijas, piemēram, "Microsoft Authenticator" (ja tiek izmantots "Microsoft Windows"), kas, katru reizi pieslēdzoties profilam, ģenerē jaunu kodu un pieprasa apstiprinājumu telefonā. Līdz ar to bez telefona profilam nav iespējams piekļūt. Lai gan pirmšķietami šāda pieeja šķiet sarežģīta, tā tomēr sniedz lielāku drošību un aizsardzību datiem. Tādējādi ieteicams to izmantot svarīgākajiem e-pastiem, internetbankai un sociālajiem tīkliem.

Lai turpmāk mazinātu kibernoziegumu risku un pasargātu sevi:

- ieteicams lietot un regulāri atjaunot antivīrusa programmas;
- jāatturas no aizdomīgu interneta vietņu apmeklēšanas, aizdomīgu e-pastu pielikumu un internetsaišu atvēršanas, lai neaktivizētu inficētus failus;
- jāpārliecinās par e-pasta sūtītāja patieso eksistenci;
- nav ieteicams atbildēt uz aizdomīgiem e-pastiem;
- jāizmanto atšķirīgas un pietiekami garas paroles, kuras būtu ieteicams regulāri mainīt.

Turpretim, raugoties no juridiskā viedokļa, jāsecina, ka persona šajā gadījumā, visticamāk, jau izdarījusi nodarījumu pret informācijas sistēmas drošību, jo ieguvusi datora paroli, kā norādīts e-pasta nosaukumā. Tas varētu būt noticis, patvaļīgi piekļūstot, pārtverot, izmantojot kaitīgās ierīces vai citādā veidā. Šāds noziedzīgs nodarījums, kas ir mazāk smags noziegums, kvalificējams saskaņā ar Krimināllikuma 241.panta 1.daļu, proti, patvaļīga piekļūšana automatizētas datu apstrādes sistēmas resursiem, ja tas saistīts ar sistēmas aizsardzības līdzekļu pārvarēšanu vai ja tas izdarīts bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības un ja ar to radīts būtisks kaitējums. Taču, ja paroles iegūšana, piekļūstot automatizētas datu apstrādes sistēmas resursiem, veikta ar mērķi iegūt mantisku labumu, tad šāds noziedzīgs nodarījums kvalificējams pēc minētā panta 2.daļas kā smags noziegums, proti, izdarīts mantkārīgā nolūkā. Šāds tīšs noziedzīgs nodarījums apdraud automatizētās datu apstrādes sistēmas lietotāju informācijas pieejamības intereses.

Tā kā būtisks kaitējums šajā nodarījumā ir obligāts kriminālatbildības nosacījums, tad ir nepieciešams izvērtēt, vai tāds ir konstatējams, proti, vai ir radušies zaudējumi vai izdevumi. Ja konstatējams būtisks kaitējums, proti, ir noticis likuma 241.panta 1. vai 2.daļā regulētais noziedzīgais nodarījums vai ir pamats uzskatīt, ka kāds mēģina to izdarīt, tad iespējams ziņot par likumpārkāpumu, vēršoties Valsts policijas Ekonomisko noziegumu apkarošanas pārvaldes Kibernoziegumu apkarošanas nodaļā ar iesniegumu.

Kibernoziedznieku pielietotie maldināšanas veidi un datorkrāpnieciskās shēmas kļūst arvien pārdomātākas. Veids, kā apturēt šo attīstību, ir ziņot par noziedzīgiem nodarījumiem u.c. pretlikumīgām un aizdomīgām darbībām. Ziņojot tiesībaizsardzības iestādēm, pastāv iespēja, ka arī citas personas tiks pasargātas no kļūšanas par upuri kibernoziegumā. Tādējādi nedrīkst samierināties ar radušos situāciju un ir nepieciešams ziņot, lai pasargātu sevi u.c. no kibernoziegumu radītajām sekām.