OUCH! 2021. gada

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Mana iekārta ir uzlauzta. Ko tagad darīt?

Vai mana iekārta ir uzlauzta?

Lai arī cik droši jūs būtu, agrāk vai vēlāk var notikt negadījums, un jūs varat ciest kiberuzbrukumā. Zemāk uzskaitītas pazīmes, kas norāda, ka jūsu iekārta varētu būt uzlauzta, un ieteikumi, ko šādā situācijā darīt.

Jūsu tiešsaistes konti

- Jūsu draugi un ģimenes locekļi saņem no jums dīvainus ziņojumus vai uzaicinājumus, kurus jūs neesat sūtījuši.
- Ievadot paroli, jums paziņo, ka parole nav derīga, kaut arī jūs ļoti labi zināt, ka paroli esat ievadījuši pareizi.
- Jūs saņemat paziņojumus no vietnēm par pierakstīšanos tajās (log-in), kaut arī paši to neesat veikuši. Nespiediet uz saitēm šādos paziņojumos, lai pārbaudītu savus kontus. Tā vietā ierakstiet lapas adresi savā interneta pārlūkā pats, izmantojiet iepriekš saglabātu grāmatzīmi vai pārbaudiet kontu no mobilās lietotnes.

Jūsu dators un viedtālrunis

- Jūsu antivīruss ģenerē paziņojumus, ka jūsu iekārta ir inficēta. Pārliecinieties, ka tie tiešām ir jūsu antivīrusa paziņojumi, nevis uznirstoši logi kādā tīmekļa vietnē, kas cenšas jūs iebiedēt un panākt, ka piezvanāt uz paziņojumā norādīto telefona numuru vai lejupielādējat kaut ko. Neesat droši? Atveriet savu antivīrusa programmatūru un pārbaudiet, vai jūsu dators tiešām ir inficēts.
- Jums parādās uznirstošais logs, kurā tiek paziņots, ka jūsu dators ir sašifrēts un jums jāmaksā izpirkuma maksa, lai atgūtu savus failus.
- Lietotnes un programmas ik pa brīdim pārstāj darboties vai nepieciešams ļoti ilgs laiks, lai tās uzsāktu darbību.
- Pārlūkojot internetu, jūs bieži tiekat pārmesti uz vietnēm, kuras nemaz nevēlējāties apmeklēt, vai bez jūsu ziņas tiek atvērtas jaunas tīmekļa vietnes.

Finanses

- No jūsu maksājumu kartes vai bankas konta ir veikti savādi maksājumi, par kuriem droši zināt, ka tos neesat veikuši.

Ko tagad darīt? - Kā atgūt kontroli

Ja jums ir aizdomas, ka jūsu iekārta ir uzlauzta, saglabājiet mieru; jums izdosies to atrisināt. Ja uzbrukums ir saistīts ar jūsu darbu, necentieties situāciju atrisināt pašrocīgi, nekavējoties ziņojiet par notikušo. Ja uzlauzts jūsu personīgais konts vai iekārta, ir sekojošas lietas, ko varat darīt:

- **Tiešsaistes kontu atgūšana:** Ja jums joprojām ir piekļuve savam tiešsaistes kontam, pierakstieties tajā (log-in) no iekārtas, par kuru esat droši, ka tā nav inficēta, un nomainiet konta paroli. Kad esat pierakstījušies, uzstādiet unikālu un garu paroli, jo garāku, jo labāk. Atcerieties, katram jūsu kontam vajadzīga atšķirīga parole. Ja nevarat tās visas atcerēties, iesakām izmantot paroļu pārvaldnieku. Ja vien iespējams, pieslēdziet arī vairāku faktoru autentifikāciju (MFA) jūsu kontiem, lai nodrošinātu, ka uzbrucēji nevarēs tiem piekļūt atkārtoti. Ja vairs nevarat piekļūt savam kontam, sazinieties ar tīmekļa vietnes uzturētāju un informējiet viņu par to, ka jūsu konts ir pārtverts.
- **Personīgā datora vai iekārtas atgūšana:** Ja jūsu antivīruss netiek galā ar infekciju, vai arī jūs vēlaties būt pilnīgi pārliecināti, ka jūsu sistēma ir drošībā, apsveriet iespēju pārinstalēt operētājsistēmu, tādā veidā nodrošinot, ka sistēma tiks veidota pilnīgi no jauna. Tas ietver esošā cietā diska satura dzēšanu vai pilnīgu diska nomaiņu, kam seko operētājsistēmas atkārtota instalēšana un atjaunināšana. Neinstalējiet operētājsistēmu no rezerves kopijām (backups). Izmantojiet rezerves kopijas tikai personīgo failu atjaunošanai. Ja nejūtaties pārliecināti, ka tiksiet galā pašu spēkiem, apsveriet iespēju izmantot profesionāla servisa palīdzību. Vai arī, ja jūsu dators vai iekārta ir novecojusi, varbūt pienācis laiks iegādāties jaunu.
- **Ar finansēm saistītu kontu atgūšana:** Par problēmām ar savām maksājumu kartēm vai bankas kontiem nekavējoties sazinieties ar savu banku vai maksājumu karšu izsniedzēju. Piezvaniet viņiem, izmantojot uzticamu telefona numuru, piemēram, to, kas norādīts uz jūsu maksājumu kartes, kas redzams uz jūsu konta pārskata izrakstiem, vai norādīts viņu mājas lapā. Regulāri pārbaudiet savu kontu izrakstus un maksājumu vēsturi. Kā papildu drošības pasākumu apsveriet iespēju izmantot kredīta iesaldēšanu (pieejama ASV).

Ja esat cietuši finansiālus zaudējumus, vai arī jūtaties apdraudēti, ziņojiet par incidentu tiesībsargājošajām iestādēm.

Viesredaktors

Maxim Deweerdt (Twitter @alfasec) ir sertificēts pasniedzējs SANS institūtā, kas pasniedz galvenokārt kiberaizsardzības kursus. Viņš ir arī vadošais konsultants "NVISO", kur savu uzmanību koncentrē uz projektiem, kas saistīti ar apdraudējumu atpazīšanu, incidentu apstrādi un SOC briedumu.

Resursi

Kāpēc svarīgi veikt atjauninājumus:: https://www.sans.org/security-awareness-training/resources/power-updating
Rezerves kopijas:https://www.sans.org/security-awareness-training/resources/got-backups
Kā padarīt paroles vieglāk iegaumējamas: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Izspiedējvīrusi:https://www.sans.org/security-awareness-training/resources/got-backups
Ziņojiet par identitātes zādzību: https://www.vp.gov.lv/lv/iestades-kontakti
Kredīta iesaldēšana: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Tulkojums: CERT.LV