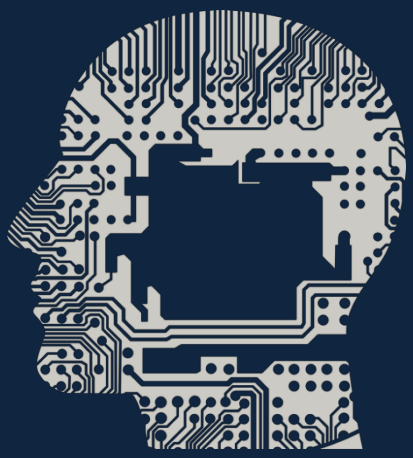
MARTA APSKATS:

- Pavasara IT drošības seminārs "Esi drošs"
- "Eiropas Digitālā nedēļa" Latvijā
- Kompromitēta ASUS atjauninājumu sistēma
- NATO kiberaizsardzības darba grupas sanāksme Latvijā
- Ieskats Huawei kiberdrošības izvērtēšanas centra pārraudzības valdes ikgadējā ziņojumā
- Marta kiberstāsti
- Statistika – biežāk konstatētās mobilo iekārtu ļaunatūras LV
- Pasākumu kalendārs



Attēli: Pixabay.com

PAVASARA IT DROŠĪBAS SEMINĀRS ,,ESI DROŠS''

28.martā, Digitālās nedēļas ietvaros, CERT.LV organizēja kārtējo IT drošības semināru „Esi drošs". Semināra mērķauditorija galvenokārt ir valsts un pašvaldību iestāžu atbildīgās personas par IT drošību, kā arī citi eksperti, kuri darbojas IT drošības jomā. Ikviens interesents pasākumu varēja vērot arī tiešraidē.

Pavasara seminārā apskatītās tēmas: apkopojums par CERT.LV piedāvātajiem risinājumiem; DoH! DNS over HTTPS; tīmekļa lietojumu drošība; mobilo iekārtu droša izmantošana valsts un pašvaldību iestādēs; e-adreses ieviešana un izaicinājumi, kā arī CERT.LV aktualitātes.

CERT.LV vadītāja Baiba Kaškina savā prezentācijā aicināja auditoriju iesaistīties arī nelielā aptaujā, brīvā formā atbildot uz pāris sagatavotiem interaktīviem jautājumiem platformā menti.com. Jautājumi palīdzēja labāk saprast, ko apmeklētāji īsti sagaida no CERT.LV, ko papildus vēlētos apgūt produktīvākam darbam, un ar kāda veida drošības problēmām ekspertiem ikdienā nākas saskarties visbiežāk. **TOP 3 atbildes uz pēdējo jautājumu: līderpozīcijā ir cīņa ar SPAM vēstulēm, otrajā vietā ierindojas biežās pikšķerēšanas kampaņas, savukārt trijnieku noslēdz – cilvēciskais faktors jeb interneta lietotāju nekompetence kibertelpā.**

SEMINĀRA „ESI DROŠS" PREZENTĀCIJAS UN VIDEO IERAKSTS PIEEJAMS ŠEIT: https://cert.lv/lv/2019/03/it-drosibas-seminars-esi-dross-marta

,,EIROPAS DIGITĀLĀ NEDĒĻA'' LATVIJĀ

No 25. līdz 29.martam Latvijā norisinājās "Eiropas Digitālā nedēļa", ko organizēja Latvijas Informācijas un komunikācijas tehnoloģijas asociācija (LIKTA) un Vides aizsardzības un reģionālās attīstības ministrija (VARAM). Šāda kampaņa Latvijā norit jau 10 reizi, un līdz šim bija pazīstama ar nosaukumu "E-prasmju nedēļa".

Kampaņas ietvaros gan Latvijas reģionos, gan lielākajās pilsētās noritēja dažādi tematiskie pasākumi, ar mērķi aicināt Latvijas iedzīvotājus un uzņēmējus pilnveidot savas digitālās prasmes, mācīties savā labā izmantot digitālās tehnoloģijas un pakalpojumus. (1) Arī CERT.LV jau vairākus gadus ir kampaņas aktīva atbalstītāja. Šogad kampaņas ietvaros 28.martā tika organizēts jau aprakstītais IT drošības seminārs "Esi drošs". Tāpat CERT.LV eksperti iesaistījās un dalījās ar savu pieredzi arī citos "Digitālā nedēļa 2019" pasākumos, piemēram, ekspertu diskusijā "Kibernakts 2019" un pasākumā "E-identitātes diena".

AVOTS (1): https://likta.lv/digitala-nedela/
EKSPERTU DISKUSIJA "KIBERNAKTS 2019": http://straume.lmt.lv/lv/konferences/konferences/kibernakts-2019/1039031
VAIRĀK PAR "DIGITĀLĀ NEDĒĻA 2019": http://eprasmes.lv/

KOMPROMITĒTA ASUS ATJAUNINĀJUMU SISTĒMA

Martā publiski kļuva zināms par vērienīgu uzbrukumu, kas faktiski tika pastrādās jau 2018. gadā, bet līdz šim bija palicis nepamanīts. **Noziedznieki, ieguvuši nesankcionētu pieeju ASUS atjauninājumu sistēmai, izmainīja "ASUS Live Update Utility" rīku, iekļaujot tajā "trojas zirga" ļaunatūru**, lai tā tiktu izplatīta un uzstādīta caur ASUS atjauninājumu oficiālajiem kanāliem".

Sešos mēnešos tika inficēti simtiem tūkstošu datoru. Kampaņas laikā neviens antivīruss atjauninājumiem pievienoto ļaundabīgo kodu nebija pamanījis. Uzbrukumu atklāja "Kaspersky Lab" 2018. gada novembrī, kad tā aktīvā fāze jau bija pagājusi.

Uzbrukums netika pamanīts savlaicīgi dēļ vairākiem faktoriem: **modificētie atjauninājumi saglabāja oriģinālo failu izmēru un bija korekti parakstīti ar "ASUSTeK Computer Inc." digitālajiem sertifikātiem**, turklāt ļaundabīgais kods izpildījās tikai uz aptuveni 600, uzbrucējiem iepriekš zināmiem, datoriem, kuri tika identificēti pēc tīkla karšu unikālajām MAC adresēm.

Ļaundabīgie atjauninājumi varēja nonākt jebkurā datorā, kurā laika posmā no 2018. gada jūnija līdz 2018. gada novembrim darbojās rīks "ASUS Live Update". Šī ir oficiāla programmatūra, caur kuru ASUS izplata aparātprogrammatūras (*firmware*) atjaunojumus, tādēļ, pērkot datoru ar ASUS komponentēm, tā bieži var izrādīties jau uzinstalēta.

Datoros, kuros ir uzinstalēts "ASUS Live Update" rīks, bet kuri nav bijuši iekļauti uzbrucēju mērķu sarakstā, ļaundabīgai programmatūrai ir jābūt izdzēstai automātiski ar 2019. gada 3. martā izlaisto ASUS atjauninājumu: https://www.asus.com/support/FAQ/1018727/

Ja ir aizdomas, ka kāda datorsistēma, kurā ir instalēts "ASUS Live Update", varētu būt nokļuvusi uzbrucēju sastādītajā mērķu sarakstā, lūdzam sazināties ar CERT.LV, rakstot uz cert@cert.lv.

NATO KIBERAIZSARDZĪBAS DARBA GRUPAS SANĀKSME LATVIJĀ

Šogad aprit 70 gadi kopš NATO (*North Atlanic Treaty Organization*) - Ziemeļatlantijas Līguma organizācijas izveides. Kā zināms, tās pamatmērķis ir "saglabāt un attīstīt savas aizsardzības spējas gan individuāli, gan kopējiem spēkiem, nodrošinot kopīgas aizsardzības plānošanas pamatu". NATO šo 70 gadu laikā ir izveidojusies par spēcīgāko aliansi vēsturē. Latvija NATO pievienojās pēc savas neatkarības atgūšanas - 2004.gadā.

Kiberaizsardzība ir izvirzīta kā viena no NATO pamat aizsardzības virzieniem - līdzīgi kā gaiss, zeme un ūdens. NATO kiberdrošības aizsardzības darba grupas (*NATO Cyber Defence Workhop*) tiek organizētas kopš 2000.gada, lai valstu nozares eksperti dalītos ar pieredzi, aktuālajiem notikumiem un problēmām. **Pateicoties ilggadīgai sadarbībai, šogad no 20.-22.martam Latvijai - Aizsardzības ministrijai un CERT.LV - bija tas gods Rīgā organizēt 20. sanāksmi.** CERT.LV pateicas NATO un Aizsardzības ministrijai par veiksmīgo sadarbību un iespēju piedalīties organizēšanas procesā.

Attēls: CERT.LV privātais arhīvs

APRĪĻA OUCH!

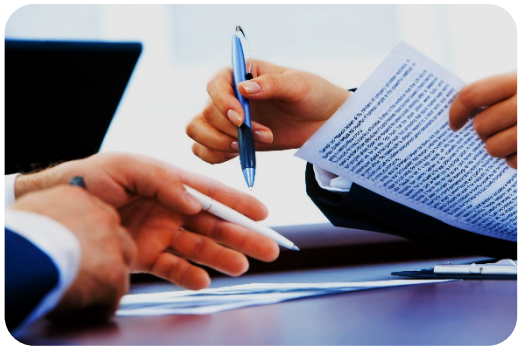
IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: Kā padarīt paroles vieglāk iegaumējamas

Jums bieži tiek teikts, ka jūsu izvēlētās paroles ir svarīgākais un primārais "vairogs" jūsu kontu aizsardzībai (kas tā arī ir!), bet reti jums tiek piedāvāts vienkāršs veids, kā droši izveidot un uzglabāt visas jūsu paroles. Aprīļa OUCH! numurā apskatīti trīs vienkārši soļi, kā vienkāršot paroles, pasargāt jūsu kontus un nosargāt jūsu nākotni.

Pilna raksta versija pieejama šeit: https://cert.lv/uploads/ieteikumi/201904-OUCH-April-Latvian.pdf

Ieskats Huawei kiberdrošības izvērtēšanas centra pārraudzības valdes ikgadējā ziņojumā



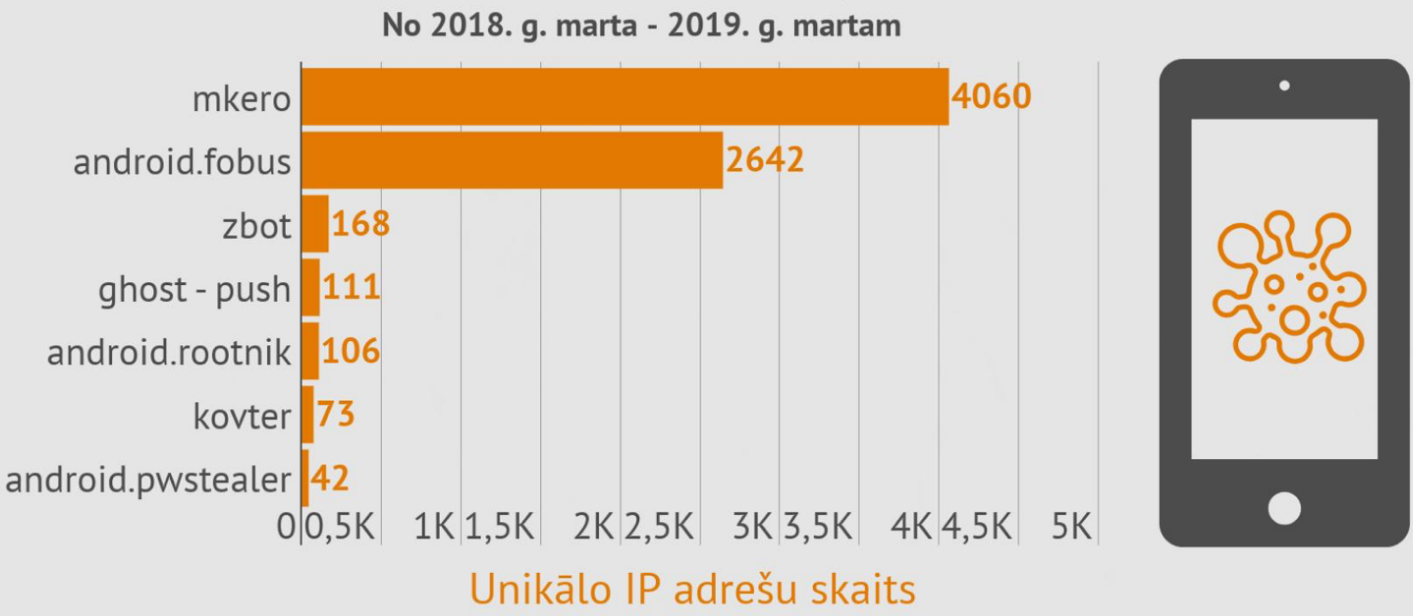
Lielbritānijā izvietotā Huawei kiberdrošības izvērtēšanas centra (*Huawei Cyber Security Evaluation Centre – HCSEC*) pārraudzības valdes **ikgadējais ziņojums atklāj būtiskus trūkumus Huawei realizētajā programmatūras izstrādes un kiberdrošības kompetencē**, norādot, ka šo produktu drošības risku pārvaldība kļūs arvien sarežģītāka. **Ziņojums identificē neskaitāmas nepilnības Huawei programmatūras izstrādes procesā**, tādus kā, integritātes un konfigurācijas vadības trūkumu, vāju programmatisko komponenšu dzīves cikla pārvaldību, novecojušus un vairāk neatbalstītus izstrādes rīkus, un elementāru drošības higiēnas neievērošanu programmatūras izstrādes vidēs.

Nepilnīgie programmatūras inženierijas un kiberdrošības procesi tieši ietekmē izstrādāto produktu drošību un kvalitāti, radot būtiskas bažas saistībā ar atklāto drošības ievainojamību lielo skaitu. Uzbrucējs, kurš pārzina šīs ievainojamības un ir ar pietiekošu piekļuvi to izmantošanai, var ietekmēt visu telekomunikāciju tīklu, atsevišķos gadījumos izraisot tā pienācīgas darbības atteici. Kā dažas no būtiskajām problēmām tiek minētas - plaša drošas programmatūras izstrādes prakses neievērošana, apjomīgs kritisku kļūdu daudzums dēļ tīšas, nedrošas programmēšanas un nekorektas operējošās sistēmas atmiņas pārvaldības realizācijas.

Huawei produktos tiek lietota novecojusi un vairs neatbalstīta reālā laika operējošā sistēma, kas rada risku, ka vienas drošības ievainojamības izmantošana ir pietiekoša, lai novestu pie pilnīgi visas sistēmas kompromitēšanas un vadības pārņemšanas. Lielbritānijas nacionālais kiberdrošības centrs (UK National Cyber Security Centre – NCSC), veicot meklēšanu Huawei programmatūras izstrādes datubāzē, atklāja neskaitāmas novecojušas un Huawei modificētas OpenSSL programmatūras bibliotēkas versijas, kurām ir publiski zināmas ievainojamības. OpenSSL bibliotēka tiek lietota droša komunikāciju kanāla izveidei un tā šifrēšanai.

Ziņojuma pilnā versija pieejama šeit:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

Statistika – biežāk konstatētās mobilo iekārtu ļaunatūras Latvijā



mkero: maksas servisi
android.fobus: paroļu zaglis
zbot: banku trojānis
ghost-push: maksas servisi
android.rootnik: paroļu zaglis
kovert: klikšķi uz reklāmām
android.pwstealer: paroļu zaglis

Kiberstāsti

CERT.LV 7. martā pienāca vairāki ziņojumi par traucējumiem Swedbank pakalpojumu darbībā. Traucējumi bija novērojumi gan saistībā ar internetbanku, mobilo lietotni, karšu norēķiniem, gan bankomātiem. CERT.LV apstiprina, ka efektīvas sadarbības rezultātā iegūtā informācija liecina par tehniskas dabas kļūmi sistēmā, kuru Swedbank ekspertiem izdevās operatīvi novērst. CERT.LV nekonstatēja ļaunprātīgu ārējo ietekmi. Vēlreiz pateicamies Swedbank par operatīvo komunikāciju un sadarbību.

• • •

Tika saņemts ziņojums par kādas vietnes meklētāja pakalpojuma atteices uzbrukumu, kas panāca pakalpojuma pārslodzi vairāk kā 6h garumā. Tika secināts, ka pieprasījumi vietnes meklētājam tiek veikti ne no Latvijas IP adresēm, un tie ir izkliedēti. CERT.LV rekomendēja papildu pārbaužu ieviešanu botu nošķiršanai no leģitīmiem apmeklētājiem, piemēram, izmantojot CAPCHA.

• • •

Martā CERT.LV turpināja saņemt ziņojumus no iedzīvotājiem par krāpnieciskām SMS krievu valodā. SMS tiek sūtītas no interneta, un to saturam pastāv dažādas variācijas. Kopīgā iezīme - SMS satur arī linku, kuru saņēmējs tiek aicināts atvērt, lai "saņemtu kompensāciju", "piedalītos izlozē" u.c. Tālāk links pārvirza saņēmēju uz vietnēm, kurās iespējams nodarboties ar finanšu ieguldījumiem vai arī veikt "komisijas maksu", lai saņemtu SMS solīto kompensāciju. CERT.LV aicina saņemtās SMS dzēst, nekādā gadījumā nevērt vaļā linkus un ziņot par notikušo savam operatoram. Ja gadījumā upuris savus norēķinu kartes datus ievadījis kādā no atvērtajām vietnēm, aicinām nekavējoties sazināties ar savu banku, un informēt par notikušo.

Kiberlaikapstākļi

				
Pakalpojuma pieejamība	**Lietu internets**	**Datu noplūde**	**Ļaunatūra un ievainojamības**	**Krāpšana**
Tehniski Swedbank darbības traucējumi	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Kompromitēta ASUS atjauninājumu sistēma	SMS krievu valodā

Tuvāko plānoto pasākumu kalendārs

02. **Oktobris - 3. oktobris -** Kiberdrošības konference „Kiberšahs 2019"

Adrese: Raiņa bulvāris 29, Rīga, LV-1459, Latvija;
Telefons: +371 67085888;
E-pasts: ziņot par incidentu: CERT@CERT.LV / sabiedriskās attiecības: prese@cert.lv
Vietne: www.cert.lv