Mēneša ziņu izlaidums Nr. 01/2019

WWW.CERT.LV

Janvāra apskats:

- Jauns regulējums pamatpakalpojumu un digitālo pakalpojumu sniedzējiem
- Prakstiskās kiberdrošības mācības „Crossed Swords 2019”
- Loterija ar nepatīkamu pārsteigumu bankas kontā
- Kā pazaudēt 50 000 „Instagram” sekotāju
- Kiberlaikapstākļi
- Kiberstāsti
- Statistika: CERTu kopienas runātāju sadalījums sanāksmēs

Attēli: Pixabay.com

Jauns regulējums digitālo un pamatpakalpojumu sniedzējiem

Jaunie Ministru kabineta noteikumu grozījumi papildina 2018.gada 11.oktobra grozījumus *Informācijas tehnoloģiju drošības likumā* (ITDL), ar kuriem Latvijā tika ieviesta 2016.gada 6.jūlija direktīva 2016/1148 - NIS (*Nework and Information Security*) direktīva, kuras mērķis ir visās ES dalībvalstīs noteikt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību. Jaunais regulējums ir saistošs **pamatpakalpojumu** un **digitālo pakalpojumu** sniedzējiem.

Tīkliem un informācijas sistēmām ir būtiska nozīme, veicinot preču un pakalpojumu brīvu apriti un personu brīvu pārvietošanos Eiropas Savienībā. Šo sistēmu būtiski traucējumi neatkarīgi no tā, vai tie ir tīši vai netīši un kur tie notiek, var ietekmēt dalībvalstis atsevišķi un ES kopumā. Tāpēc tīklu un informācijas sistēmu drošībai ir būtiska nozīme iekšējā tirgus netraucētas darbības nodrošināšanā. Līdz šim katrā dalībvalstī bija atšķirīgs tiesību subjektu loks, uz kuriem attiecās nacionālā līmenī noteiktās IT drošības prasības un incidentu ziņošanas kārtība.

Ieviešot direktīvu nacionālā līmenī, atbildīgājām ministrijām līdz 2019.gada 31.janvārim bija jāpieņem lēmums par **pamatpakalpojuma sniedzēja** un **pamatpakalpojuma statusa** piešķiršanu (pēc kritērijiem, kas noteikti 2019. gada 15. janvāra MK noteikumos Nr. 43).

Vairāk par jauno regulējumu lasi šeit: https://cert.lv/lv/2019/02/jauns-regulejums-pamatpakalpojumu-un-digitalo-pakalpojumu-sniedzejiem

Prakstiskās kiberdrošības mācības „Crossed Swords 2019”

Ikgadējās tehniskās kiberdrošības mācības „Crossed Swords 2019” tika organizētas janvāra beigās Tallinā, Igaunijā, sadarbojoties NATO apvienotajam kiberaizsardzības izcilības centram (CCDCoE) un CERT.LV. **Mācībās piedalījās tehniskie eksperti, kā arī nacionālo Kiberpavēlniecību un speciālo vienību pārstāvji.** Mācību galvenā uzmanība tika vērsta uz sarkanā karoga komandu ofensīvo prasmju attīstību kiberoperāciju plānošanā, izpildē un reaģēšanā uz apdraudējumu. Tā kā arvien vairāk valstīs tiek izveidotas Kiberpavēlniecības, tad mācībās pirmo reizi tika iekļauta pavēlniecības komponente, kuru pārraudzīja Igaunijas Aizsardzības spēku Kiberpavēlniecība.

Vairāk par mācībām: https://cert.lv/lv/2019/02/macibas-crossed-swords-2019-integre-kiberkomponenti-liela-meroga-operacijas

Loterija ar nepatīkamu pārsteigumu bankas kontā

CERT.LV arī janvārī turpināja saņemt ziņojumus no interneta lietotājiem par aizdomīgu loteriju, kurā it kā iespējams laimēt jaunākos *Samsung* un *Apple* viedtālruņus. Loterijas mērķis ir panākt, ka lietotājs abonē piekļuvi vietnes *iqbraintrainer.com* resursiem, par ko katru mēnesi no lietotāja bankas konta tiek atvilkti 29 EUR. Loterija tika izplatīta Lattelecom, LMT un, iespējams, citu Latvijā izmantotu interneta pakalpojuma sniedzēju vārdā.

Vairāk par krāpniecisko loteriju: https://cert.lv/lv/2019/01/loterija-ar-nepatikamu-parsteigumu-bankas-konta

KĀ PAZAUDĒT 50 000 SEKOTĀJU LIETOTNĒ „INSTAGRAM''

Attēls: no I. Busuļa „Instagram" arhīva

Latvijā labi pazīstamā mūziķa Intara Busuļa sociālā tīkla „Instagram" sekotāji janvārī iespējams pamanīja, ka mūziķa aktivitātes šajā platformā negaidīti pieklusušas. Tā vietā daļa attapās sekojam mistiskam kontam ar nosaukumu @fr1endgokturkx2. Izrādās, **mūziķis bija kļuvis par upuri pikšķerēšanas uzbrukumam**, **kas veiksmīgi ticis maskēts kā „Instagram" piedāvājums verificēt Intara Busuļa kontu – piešķirot tam oficiālu „zilo ķeksīti"** (Verified Badge). „Zilais ķeksītis" tiešām eksistē un tas parasti tiek piešķirts slavenību, atpazīstamu blogeru un uzņēmumu kontiem, kas atbilst noteiktiem kritērijiem. Prestižais „zilais ķeksītis" liecina par to, ka konts ir īsts un tas nav pakaļdarinājums. Šāda verifikācijas zīme šobrīd piešķirta, piemēram, grupas „Prāta vētra", Swedbank Latvija un Kristapa Porziņģa kontiem. **Diemžēl, šādu verifikācijas zīmi nav tik vienkārši iegūt, un par tās piešķiršanu lemj pats „Instagram".**

Ņemot vērā „Instagram" popularitāti, **šis sociālais tīkls šķiet interesants arī kibernoziedzniekiem.** Viņi attiecīgi meklē dažādus ceļus, kā piekļūt kontiem ar lielu sekotāju skaitu. I. Busuļa gadījumā tika saņemts e-pasts it kā no „Instagram" atbalsta centra (*info@Instagram-help.gq)* par to, ka viņa lietotāja konts ticis izvērtēts un apstiprināts „zilā ķeksīša" saņemšanai. Protams**, tālāk e-pastā tiek lūgts apliecināt konta īpašumtiesības, nospiežot uz piedāvātā linka**. Saite tālāk aizved uz viltotu „Instagram" lapu, kurā tiek lūgts ielogoties. Ielogojoties, **konta piekļuves dati līdz ar visiem 51 200 sekotājiem automātiski nonāk ļaundaru rokās**, kas operatīvi pārdēvē kontu citā vārdā, lai to būtu maksimāli grūti atgūt. Mūziķis tālāk centās komunicēt ar pašu „Instagram", atkārtoti mēģinot pierādīt savu identitāti. **Diemžēl kontu atgūt neizdevās, tas tika dzēsts.** Šobrīd konts ir izveidots no jauna un pieejams zem oriģinālā lietotājvārda: @intarsbusulis.

Protams, tā gadīties var katram, tādēļ **CERT.LV aicina ikvienu pievērst pastiprinātu uzmanību gan saņemto e-pastu adresēm** (salīdzināt tās ar oficiālajā mājas lapā norādītajām), gan **arī vietņu nosaukumiem – vai tajos neparādās lieki burti, dīvaini atvasinājumi un pielikumi** – pirms vietnē vadām savu lietotājvārdu un paroli. **Iesakām izmantot arī divu faktoru autentifikāciju**, lai pieslēgtos „Instagram" un citiem sociālajiem tīkliem.

VAIRĀK PAR PIKŠĶERĒŠANAS UZBRUKUMIEM LASI ŠEIT: https://www.cert.lv/lv/2018/04/ouch-aprila-numura-ka-atpazit-pikskeresanu

KIBERLAIKAPSTĀKĻI

				
PAKALPOJUMA PIEEJAMĪBA	**LIETU INTERNETS**	**DATU NOPLŪDE**	**ĻAUNATŪRA UN IEVAINOJAMĪBAS**	**KRĀPŠANA**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Datu noplūde (770 milj. lietotāji) „Collection #1", kur apkopotas vairākas vēsturiskas noplūdes	Būtiski incidenti netika reģistrēti	Krāpnieciska loterija LMT un Lattelecom vārdā

FEBRUĀRA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: Personalizēta krāpšana

Kibernoziedznieki turpina rast arvien jaunus veidus, kā cilvēkus apmuļķot. Arvien populārāks kļūst jaunais krāpšanas veids – personalizētā krāpšana. Kibernoziedznieki ievāc vai nopērk informāciju par miljoniem cilvēku, un tad izmanto šo informāciju, lai personalizētu uzbrukumus. Februāra OUCH! lasiet, kā šie uzbrukumi darbojas. Jo vairāk jūs zināsiet par šādiem uzbrukumiem, jo vieglāk būs tos atpazīt un apturēt.

Pilna raksta versija pieejama šeit: https://cert.lv/uploads/ieteikumi/201902-OUCH-February-Latvian.pdf

KIBERSTĀSTI

No kādas privātpersonas tika saņemts e-pasts par nošifrētu iekārtas saturu, kuru ļaundari piedāvā atgūt, veicot apmaksu Bitcoin. Lietotājam izdevās vīrusu neitralizēt, izmantojot antivīrusa programmatūru, taču faili palika šifrēti. CERT.LV aicināja lietotāju apmeklēt vietni *www.nomoreransom.org* un pārliecināties, vai dati nav atgūstami bez maksas. Vietnes sadaļā "Kripto Šerifs" iespējams augšupielādēt sašifrētā faila paraugu vai arī norādīt informāciju, kas pieejama saņemtajā izpirkuma pieprasījumā no ļaundariem. Tas var palīdzēt identificēt „saķerto" vīrusu un noskaidrot, vai *www.nomoreransom.org* var piedāvāt piemērotu atšifrēšanas atslēgu. Atslēgu saraksts periodiski tiek papildināts. Vietne pieejama arī latviešu valodā.

• • •

Kāds Latvijas uzņēmums informēja CERT.LV par konstatētu iejaukšanos biznesa sarakstē. Pēc tam, kad uzņēmuma pārstāvis nosūtīja ieskenētu rēķinu klientam Turcijā, tika saņemts zvans no šī klienta, kurš centās noskaidrot, vai sūtītais rēķins tiešām nācis no uzņēmuma Latvijā. Tika atklāts, ka aptuveni 1,5h pēc oriģinālā e-pasta izsūtīšanas, klients Turcijā ir saņēmis vēl vienu e-pastu it kā no Latvijas uzņēmuma, - no domēna, kas izskatījās līdzīgs oriģinālajam. Īstais domēns no viltojuma atšķīries tikai vienā burtā, izmaiņas veiktas arī sūtītā rēķina bankas konta numurā. Tā kā klientam bijusi līdzīga situācija arī iepriekš, krāpniecība tika laikus pamanīta un neviens necieta. CERT.LV nosūtīja viltotā rēķina rekvizītus policijai, kā arī sniedza uzņēmumam instrukcijas, kā rīkoties tālāk, lai izvairītos no līdzīgām situācijām nākotnē.

• • •

CERT.LV konstatēja kādu Latvijā reģistrētu vietni, kurā ievietots kaitīgs Javaskript kods, kas no vietnes "minijs.xyz/mage.js" apmeklētāju interneta pārlūkos iekļauj kredītkaršu datu pārtveršanas kodu. Apmeklētāji, kas ievadījuši savus datus šajā vietnē pēc šī kaitīgā koda pievienošanas, tos ir neapzināti nodevuši uzbrucēju rīcībā. CERT.LV sazinājās ar vietnes īpašniekiem un lūdza noskaidrot, kas un kad ir veicis minēto vietnes modifikāciju, kā arī ieteica atjaunot vietnes CMS un spraudņu versijas. Tāpat tika lūgts identificēt pircējus, kuri ievadījuši kredītkaršu datus pēc lapas kompromitēšanas, un informēt tos par notikušo.

CERTU KOPIENAS (TF-CSIRT) RUNĀTĀJU SADALĪJUMS NO 2016.-2018.G.

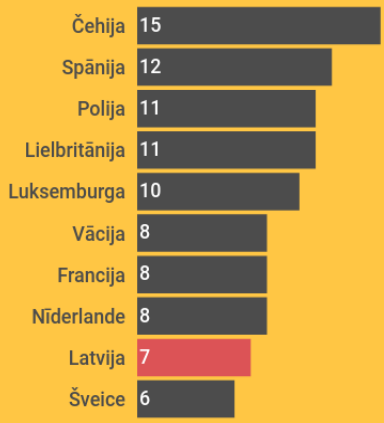
Prezentācijas	Pārstāvētās organizācijas	Starptautiskās organizācijas	Pārstāvēto valstu kopējais skaits
170	89	15	28

Pārstāvēto organizāciju TOP 10
(pēc runātāju skaita)

1. CIRCL (Luksemburga)
2. CERT.LV (Latvija)
3. BT (Lielbritānija)
4. ENISA (Starptautiska org.)
5. RIPE (Starptautiska org.)
6. CERT Polska (Polija)
7. CSIRT.CZ (Čehija)
8. CZ.NIC (Čehija)
9. GÉANT (Starptautiska org.)
10. NCSC-NL (Nīderlande)

Visas pārstāvētās valstis

Pārstāvēto valstu TOP 10
(pēc runātāju skaita)



PASĀKUMU KALENDĀRS

- **25. - 31. marts:** Eiropas Digitālā nedēļa Latvijā
- **28. marts:** IT drošības seminārs „Esi drošs"
- **15. - 16. aprīlis:** Baltic Domain Days 2019 in Tallinn
- **2-3. 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