WWW.CERT.LV

FEBRUĀRA APSKATS:

- CERT.LV aprit 8 gadi kibertelpā
- Uz Smart-ID lietotājiem orientēta pikšķerēšanas kampaņa
- Krāpnieciskās loterijas turpinās
- Aizsardzības ministra vārdā no Krievijas serveriem izsūtīti viltus e-pasti
- Aizsardzība pret e-pasta nosūtītāja adreses viltošanu
- Februāra kiberstāsti
- Statistika – dalībnieku skaits CERT.LV pasākumos un prezentācijās 2018. gadā

CERT.LV APRIT 8 GADI KIBERTELPĀ

2019.gada 1.februārī CERT.LV komanda atzīmēja 8 gadus Latvijas kibertelpā! Ar gandarījumu atskatījāmies uz paveikto un kopā priecājāmies par pozitīvajām pārmaiņām Latvijas informatīvajā telpā! Arvien biežāk lietotāji ir spējīgi pamanīt un atpazīt krāpnieku centienus, arvien nopietnāka attieksme pret kiberdrošības jautājumiem novērojama gan valsts un pašvaldību iestādēs, gan kritiskās infrastruktūras uzņēmumos! Protams, jauni izaicinājumi kiberdrošības jomā rodas katru dienu, līdz ar to CERT.LV komandai jābūt modrai un zinošai, lai varētu profesionāli reaģēt uz jebkuru apdraudējumu. Novēlu visiem veiksmīgu un kiberdrošu gadu! – **Baiba Kaškina, CERT.LV vadītāja.**

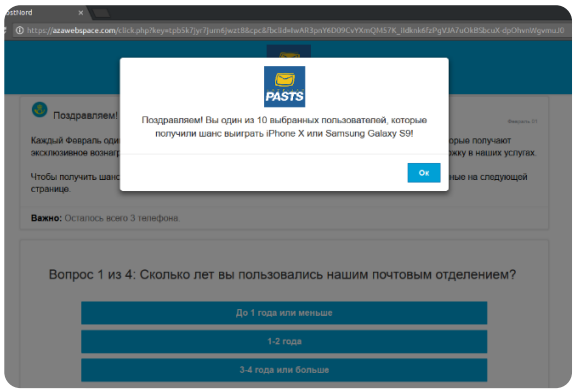
UZ SMART-ID LIETOTĀJIEM ORIENTĒTA PIKŠĶERĒŠANAS KAMPAŅA

Februāra pēdējā nedēļas nogalē Igaunijā SEB un Swedbank klienti piedzīvoja masveida pikšķerēšanas kampaņu ar mērķi izkrāpt sensitīvu bankas klientu informāciju un veikt nesankcionētus naudas pārskaitījumus. Nedēļu vēlāk šādu pašu kampaņu piedzīvoja arī Latvijas SEB bankas klienti.

VAIRĀK PAR KRĀPNIECĪBU LASI ŠEIT: https://cert.lv/lv/2019/03/uz-smart-id-lietotajiem-orienteta-pikskeresanas-kampana

Foto: Pixabay.com

KRĀPNIECISKĀS LOTERIJAS TURPINĀS



CERT.LV arī februārī turpināja saņemt ziņojumus par krāpnieciskām loterijām, **šoreiz it kā "Latvijas Pasts" vārdā.** Lietotāji savu mobilo iekārtu vai datoru interneta pārlūkos saņēma paziņojumus par iespēju iegūt *iPhone XS* vai *Samsung Galaxy S9* viedtālruni, ja **ātri atbildēs uz četriem vienkāršiem jautājumiem** par pasta pakalpojumu izmantošanu. Pēc jautājumu atbildēšanas, lai garantētu drošu viedtālruņa piegādi, loterijas dalībniekiem tika lūgts **veikt maksājumu 3 EUR apmērā** par pasta pakalpojuma izmantošanu.

Ja lietotājs ievadīja savas maksājumu kartes datus, viņš, atbilstoši vietnes lietošanas nosacījumiem (*Terms & Conditions*), **veica parakstīšanos uz pakalpojumu, kura izmantošana izmaksā 49.99 EUR mēnesī** (pirmās piecas dienas ir bez maksas).

VAIRĀK PAR KRĀPNIECISKO LOTERIJU LASI ŠEIT: https://cert.lv/lv/2019/02/krapnieciskas-loterijas-turpinas

Aizsardzības ministra vārdā no Krievijas serveriem izsūtīti viltus e-pasti

Foto: Pixabay.com

19. februārī, izmantojot viltus e-pasta adresi, **aizsardzības ministra Arta Pabrika vārdā vairākiem adresātiem valsts iestādēs tika izsūtīta ziņa ar nepatiesu un kompromitējošu saturu.**

Viltus e-pasti ar aizsardzības ministra A. Pabrika parakstu izsūtīti no Krievijā bāzētiem serveriem. Saturs veidots aizsardzības ministra vārdā, kurā viņš it kā skaidro, ka 16. februārī apmeklējis kādu bāru Vecrīgā, kurā piedalījies divdomīgās brīvā laikā aktivitātēs.

Aizsardzības ministrija skaidro, ka šis e-pasts ir uzskatāms par klasisku identitātes viltošanas operāciju ar spiegošanas elementiem, lai noskaidrotu, no kādām IP adresēm e-pasts ir apskatīts.

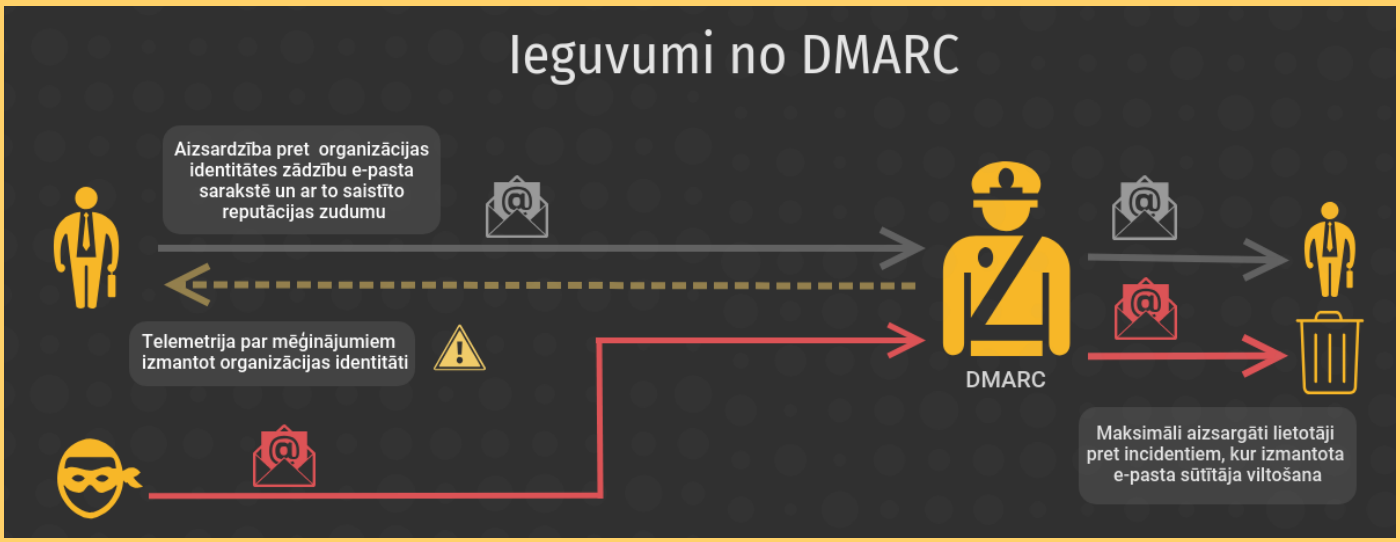
Turklāt šis ir veids, kā iespējami plašā mērogā diskreditēt aizsardzības ministru un aizsardzības nozari kopumā ar mērķi veicināt sabiedrības neuzticību. **Aizsardzības ministrija aicina sabiedrību neuzticēties viltus e-pasta sūtījumiem un kritiski izvērtēt saņemto informāciju.**

Avots: https://www.mod.gov.lv/lv/zinas/aizsardzibas-ministra-varda-no-krievijas-serveriem-izsutiti-viltus-e-pasti

Aizsardzība pret e-pasta nosūtītāja adreses viltošanu

Protokolu saime, kas nodrošina e-pastu apmaiņu, ir fundamentāli nedroša un elementāri izmantojama ļaunprātīgos nolūkos. Lai pasargātu sevi un citus no sūtītāja lauka (From) viltošanas**, CERT.LV eksperti iesaka izmantot DMARC (Domain-based Message Authentication Reporting and Conformance) protokolu.**

DMARC ir protokols**, kas nodrošina e-pastu autentiskuma pārbaudi atbilstoši noteiktām e-pasta politikām**, un domēna lietotājam var sniegt atskaiti par šādu politiku pārkāpumiem. Ar DMARC saistītie drošības protokoli ir radīti ar mērķi, lai e-pasta saņēmējs varētu pārliecināties, ka adresē norādītais sūtītājs ir patiesais domēna un e-pasta lietotājs, kā arī lai identificētu nesankcionētas izmantošanas jeb e-pasta adreses viltošanas gadījumus. Šādi incidenti, kad e-pasta saņēmējam tiek norādīta tam zināma un populāra e-pasta adrese, ir novērojami tā saucamajos "*CEO fraud*" un pikšķerēšanas kampaņās.



Plašāka informācija par DMARC un mūsdienīgu e-pasta standartu ieviešanas nosacījumiem pieejama šeit: https://cert.lv/lv/2019/03/aizsardziba-pret-e-pasta-nosutitaja-adreses-viltosanu

Marta OUCH!

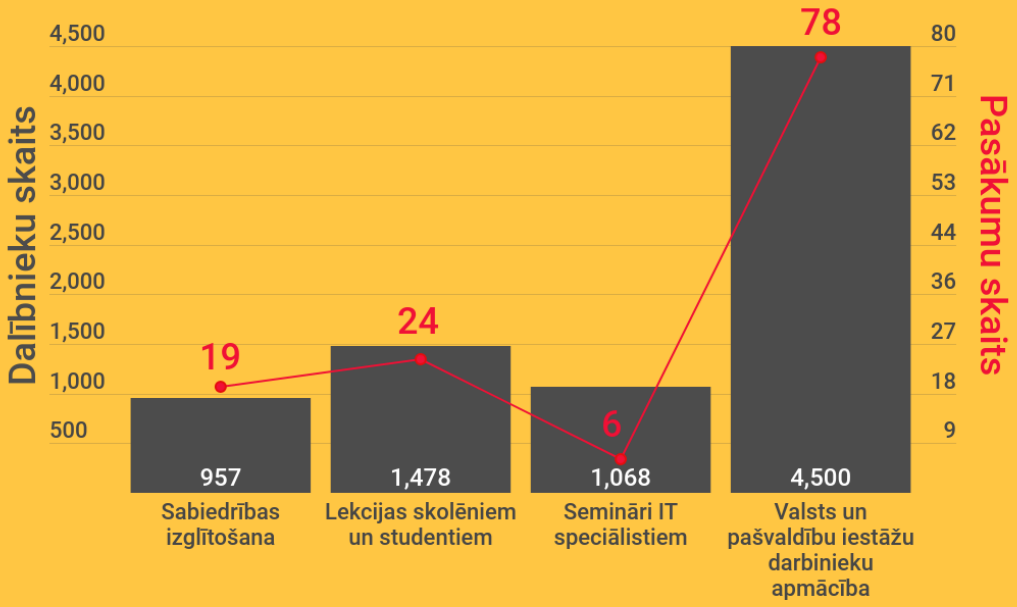
Ikmēneša informācijas drošības biļetens ikvienam

Biļetena tēma: Kā atbrīvoties no mobilās iekārtas

Mobilās iekārtas turpina attīstīties un pilnveidoties pārsteidzošā ātrumā. Tā rezultātā, daļa cilvēku katru gadu tās regulāri maina. Diemžēl, iekārtu īpašnieki bieži neiedomājas, cik daudz viņu personīgās informācijas patiesībā glabājas šajās ierīcēs. OUCH! marta numurā mēs apskatīsim, kā ierīces droši iztīrīt, pirms no tām atbrīvoties.

Pilna raksta versija pieejama šeit: https://cert.lv/uploads/201903-OUCH-March-Latvian.pdf

Dalībnieku skaits CERT.LV pasākumos un prezentācijās 2018. gadā



Kopējais dalībnieku skaits

8003

Kopējais pasākumu skaits

127

Kiberstāsti

• • •

Mēneša ietvaros no vairākiem Latvijas uzņēmumiem tika saņemti ziņojumi par uzlauztiem un sašifrētiem datu serveriem un dzēstām failu kopijām. Vairumā gadījumu tika konstatēts, ka pie vainas ir Dharma saimes izspiedējvīruss, kura jaunākās versijas nav nevienam izdevies atšifrēt vairākus gadus. Šāda servera uzlaušana parasti notiek, izmantojot RDP (attālināto pieeju) no publiskā interneta. Lai šādas situācijas neatkārtotos, CERT.LV iesaka paaugstināt RDP drošību, kā arī rezerves kopijas uzglabāt tā, lai kopijas ir neatkarīgas no kopējamās sistēmas. Ja iespējams, CERT.LV rekomendē nemaksāt hakeriem, bet izveidot šifrēto failu kopiju, jo pastāv iespēja, ka šos failus varēs atšifrēt kaut kad nākotnē. Kā arī, ja uzbrukums uzņēmumam radījis būtiskus zaudējumus, CERT.LV aicina vērsties Valsts policijā ar iesniegumu.

• • •

Februāra vidū CERT.LV saņēma ziņojumu no kādas privātpersonas par neslavas celšanu un nepatiesas informācijas atainošanu personai agrāk piederošajā vietnē, kuru šobrīd apsaimnieko ar azartspēlēm saistīts uzņēmums. No privātpersonas sniegtās informācijas saprotams, ka problēmas sākušās, kad persona nolēmusi mainīt vietnes domēna vārdu un veco lūgusi tā brīža lapas uzturētājam likvidēt. CERT.LV vēlas atgādināt, ka domēna vārds nav īpašums, uz kuru tā pirmajam izmantotājam ir neierobežotas tiesības. Tiesības izmantot domēna vārdu tiek piešķirtas tikai uz laiku, kamēr tas ir apmaksāts kādā no konkrētās zonas reģistratūrām. Ja ir pārtraukta domēna vārda uzturēšanu, tad citai personai ir tiesības reģistrēt tādu pašu domēna vārdu, un ievietot tajā sev vēlamo saturu. Strīdi par domēna vārdu izmantošanas tiesībām tiek risināti civiltiesiskā ceļā. Ja esošais īpašnieks piekrīt, ir iespējams atgūt kontroli pār šo domēnu bez tiesas iesaistes.

• • •

No vairākiem interneta lietotājiem februāra otrajā pusē tikai saņemti satraukti ziņojumi par SPAM e-pastu pieplūdumu no kādas Latvijas pašvaldības. SPAM e-pastā sliktā latviešu valodā tā saņēmēji tika aicināti apstiprināt savu e-pasta adresi un piedalīties 1milj. EUR izlozē. CERT.LV sazinājās ar minēto pašvaldību un noskaidroja, ka 2 tās darbinieki kļuvuši par upuriem dažādos pikšķerēšanas uzbrukumos, un, pašiem nezinot, ļaundariem darījuši zināmu piekļuvi saviem e-pastu kontiem, no kuriem vēlāk ticis izsūtīts SPAMs. Pašvaldība reaģēja operatīvi, un situācija tika veiksmīgi atrisināta, kā arī tika veiktas pārrunas ar cietušajiem darbiniekiem, lai izvairītos no līdzīgām situācijām nākotnē.

KIBERLAIKAPSTĀKĻI

				
PAKALPOJUMA PIEEJAMĪBA	**LIETU INTERNETS**	**DATU NOPLŪDE**	**ĻAUNATŪRA UN IEVAINOJAMĪBAS**	**KRĀPŠANA**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Vairāki Latvijas uzņēmumi cieta no šifrējošiem izspiedējvīrusiem	Krāpnieciska loterija „Latvijas Pasts" vārdā; SEB vārdā pikšķerēšana

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

25. **MARTS - 31. MARTS -** Eiropas Digitālā nedēļa Latvijā

28. **MARTS** - e-Identitātes diena no plkst. 11:00 – 13:00

28. **MARTS** - IT drošības seminārs „Esi drošs" no plkst. 13:00 – 17:00

28. **MARTS** – LVRTC organizēta ekspertu diskusija "Kibernakts 2019" no plkst. 20.00 – 21.30

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