WWW.CERT.LV

DECEMBRA APSKATS:

- 2018. gada kiber-pēcgarša
- Krāpnieciski brīdinājumi par nokavētu nodokļu maksājumu
- Nacionālā enciklopēdija pieejama arī tiešsaistē
- Gods kalpot Latvijai
- Mazcenas risinājums drošai informācijas apstrādei
- IT drošības seminārs „Esi drošs”
- Kiberstāsti
- Kiberlaikapstākļi
- Statistika: unikālo IP adrešu skaits pa apdraudējuma veidiem 2018. un 2017. gadā

Attēli: Pixabay.com

2018. GADA KIBER- PĒCGARŠA

Gadu mijā ir svarīgi atcerēties un analītiski izvērtēt nu jau aizvadītos 12 mēnešus kiberdrošības šķērsgriezumā – spilgtākās tendences, lielākos izaicinājumus, nozīmīgākās uzvaras un zaudējumus. Tikpat svarīgi šķiet ieskicēt arī nākamā gada prognozes un būtiskākos iespējamos pagrieziena punktus.

Pasaulē 2018. gads paliks atmiņā kā gads, kad **tika ieviesta ES vispārīgā datu aizsardzības regula (GDPR) ar visām no tā izrietošajām sekām –** datu drošības politikas pārskatīšanu kā uzņēmumos, tā arī valsts un pašvaldību iestādēs. Ironiskā kārtā tieši pēdējā gada laikā **notikušas vienas no iespaidīgākajām pasaules mēroga datu noplūdēm pēdējā piecgadē**, piemēram, *Marriott International* viesnīcu ķēde ar 500 miljoniem nopludinātu klientu datu, kā arī plaši izskanējušās Facebook nedienas ar gandrīz 90 miljoniem lietotāju profilu. Un tā ir tikai aisberga redzamā daļa. **Masveidā GDPR aizsegā tika organizētas arī pikšķerēšanas kampaņas** ar mērķi izgūt sensitīvu lietotāju informāciju.

Savukārt **aizvadītais gads Latvijā pagāja Saeimas vēlēšanu zīmē**, kur pastiprināta uzmanība bija pievērsta nevien politiskajām debatēm un kandidātiem, bet arī paša vēlēšanu procesa pārskatāmībai un kiberdrošībai. CERT.LV vērtējumā kibertelpā **vēroto aktivitāti vēlēšanu laikā jāklasificē kā mērenu, valsts drošību un vēlēšanas neapdraudošu, bez būtiski satraucošiem pavērsieniem.** Ar dažādu intensitāti tika novēroti vairāki uzbrukumi e-pasta sistēmām, tīmekļa vietnēm un tīkla infrastruktūrai, arī mērķiem valsts sektorā. Taču tiem neizdevās radīt kaitējumu, vai iedzīvotājiem jūtamu efektu, jo tos izdevās veiksmīgi atvairīt. **Pamanāmākais incidents vēlēšanu laikā bija sociālā tīkla Draugiem.lv sākuma lapas izķēmošana.**

2018. GADA TOP ZIŅAS LV KIBERTELPĀ:

1. TIKA IEVIESTA GDPR REGULA;
2. KIBERUZBRUKUMS E-VESELĪBAI;
3. SAEIMAS VĒLĒŠANAS: DRAUGIEM.LV IZĶĒMOŠANA;
4. KIBERUZBRUKUMS SIA „BIĻEŠU PARADĪZE” VIETNEI;
5. ĻAUNATŪRA LR IEKŠLIETU MINISTRIJAS IT SISTĒMĀS;
6. INFICĒTI MIKROTIK MARŠRUTĒTĀJI UN KOMPROMITĒTAS IOT IERĪCES;

Nosacīti mierīgas vēlēšanas varbūt kādam raisa izlūziju, ka Latvija ir pietiekami maza un nenozīmīga, lai kāds censtos ietekmēt mūsu IKT infrastruktūru un drošību, diemžēl par pretējo liecina CERT.LV jau iepriekš **apzinātā ļaunatūra Latvijas Republikas Iekšlietu ministrijas IT sistēmās**. Ļaunatūras tehniskie parametri norāda uz **iespējamu Krievijas Federācijas drošības dienestu nesankcionētu iejaukšanos**. Nozīmīgs darbs pie seku analīzes un instrukciju atjaunošanas noritēja arī 2018. gadā.

Iejaukšanos no ārpuses šogad piedzīvoja arī citi svarīgi valsts pārvaldes un privātā sektora resursi. Gada sākumā pārslodzes uzbrukumā **(DDoS) cieta E-veselība**, savukārt 2 mēnešus vēlāk ziņu virsrakstus sasniedza DDoS **uzbrukums SIA „Biļešu paradīze” vietnei**, laikā, kad liela daļa Latvijas iedzīvotāju steidza iegādāties biļetes uz XXVI Vispārējo latviešu Dziesmu un XVI Deju svētkiem. Dažāda mēroga piekļuves lieguma uzbrukumi pret valsts pārvaldes interneta resursiem notiek ik dienu, visbiežāk resursu turētāji to ietekmi nemaz nejūt, ja resursam ir nodrošināta piemērota aizsardzība.

Pozitīva tendence, kas iezīmējās 2018. gada šķērsgriezumā, ir i**nterneta lietotāju pieaugošā modrība un atbildības sajūta,** par ko liecināja saņemtie informatīvie ziņojumi par dažādām krāpnieciskām kampaņām – lietotāji dalās ar

saviem novērojumiem. Populārākās pērnā gada sociālās inženierijas kampaņas saistītas ar krāpnieciskiem zvaniem krievu valodā, aicinot veikt noguldījumus kriptovalūtā; e-pastiem, kuros minēta lietotāja parole un kuros ļaundaris apgalvo, ka veicis videoierakstu, lietotājam „sērfojot" pieaugušo vietnēs. **Gada nogalē ievērojamu apjukumu radīja arī krāpnieciski e-pasti Finanšu ministrijas vārdā par nokavētu nodokļu apmaksu, kas sakrita arī ar finanšu gada noslēgumu.**

Tāpat pozitīvi vērtējama arī sabiedrības pieaugošā interese par dažādu programmatūru un ierīču izcelsmi un ar to saistītajiem riskiem, **kā tas pērn bija vērojams Yandex Taxi, Kaspersky un Huawei gadījumos**.

2018. gada kontekstā noteikti jāatzīmē arī novērotais kāpums ielaušanās mēģinājumu apjomā, kas skaidrojams ar **inficētiem MikroTik maršrutētājiem un kompromitētu lietu interneta (IoT) iekārtu skaita palielināšanos**, kas ir iekļautas robotu tīklos un veic automatizētus uzbrukumus, lai šos tīklus paplašinātu. Inficēto iekārtu apjoma mazināšanai CERT.LV veica iekārtu īpašnieku apziņošanu, taču inficēto iekārtu apjoms sarūk lēni, jo daļai lietotāju trūkst izpratnes vai zināšanu par infekcijas novēršanu.

CERT.LV prognozē, ka 2019. gadā iespējams pat krasi **pieaugs šo kompromitēto IoT ierīču skaits**. Daļa šo ierīču varētu nebūt pasargātas arī no kriptovīrusiem, tādēļ IoT iekārtu īpašniekiem būtu lietderīgi saprast, ka nošifrēt iespējams ne vien datorā glabātās bērnu bildes, bet arī, piemēram, viedo mājas apkures sistēmu. Attiecīgi var nākties maksāt papildu izpirkuma maksu, lai ziemā nenosaltu, - tāda, diemžēl, ir nākotnes skarbā realitāte, ja turpināsim ignorēt pastāvošos riskus.

2019. gads **varētu iezīmēt arī lēnu, bet nozīmīgu pāreju no ierastajām 8-9 simbolu parolēm uz citiem, daudz drošākiem risinājumiem, kā piemēram, divfaktoru autentifikācija.** Kā novērojams, arī bankas jau iepriekš uzsākto pāreju no kodu kartēm uz Smart-ID un kodu kalkulatoriem 2019. gadā pakāpeniski ievirzīs finiša taisnē.

Protams, arī krāpnieciska rakstura e-pastu kampaņas 2019. gadā nevienu nesaudzēs, tās kļūs tikai viltīgākas, labāk pārdomātas un organizētas. Kā dažos gadījumos bija novērojams jau 2018. gadā – arī latviešu valoda, attīstoties tulkošanas programmatūrām, vairs nebūs tas redzamākais indikators pēc kā atpazīt krāpniekus. Te joprojām palīdzēt var tikai veselais saprāts un piesardzība.

Krāpnieciski brīdinājumi par nokavētu nodokļu maksājumu

Pērnā gada decembrī CERT.LV saņēma virkni ziņojumu par krāpnieciskiem e-pastiem it kā Finanšu ministrijas vārdā ar norādīto sūtītāja adresi finance@fm.gov.lv. **Krāpnieciskā e-pasta temats: "nokavētu nodokļu maksājumu: Nauda, kas paredzēta valsts budžetam, ir arī jūsu nauda!"** E-pasta pielikumā atrodams par PDF dokumentu maskēts .ZIP arhīva fails. Atverot šo failu, dators tiek inficēts ar vīrusu, kas ievāc datorā uzglabātās paroles un, iespējams, sašifrē iekārtā esošos failus, lai pieprasītu izpirkuma maksu par failu atgūšanu.

Vairāk: https://cert.lv/lv/2018/12/krapnieciski-bridinajumi-par-nokavetu-nodoklu-maksajumu

Gods kalpot Latvijai!

- 2018.gada nogalē **CERT.LV vadītāja B.Kaškina un viņas vietnieks V.Teivāns saņēma Latvijas Republikas Aizsardzības ministrijas goda rakstu** par veiksmīgu sadarbību un atbalstu, tā sniedzot savu ieguldījumu Latvijas valsts aizsardzībā un drošībā.
- Latvijas Republikas Valsts policija 2018.gada 5.decembrī atzīmēja savu 100.gadi, kuras ietvaros tika **pasniegtas jubilejas goda zīmes "Latvijas Valsts policijai 100".** Esam lepni, jo arī CERT.LV vadītājas vietnieks V.Teivāns par sniegto atbalstu Valsts policijai saņēma šādu apbalvojumu.

Mazcenas risinājums drošai informācijas apstrādei

Eksistē jomas, kurās ar mazu budžetu un bez specifiskām zināšanām ir jānodrošina augstas drošības informācijas apstrāde – piemēram, **pētnieciskie žurnālisti, NVO, u.c.** Drošības risinājuma izvēle vislielākajā mērā ir atkarīga no apdraudējuma raksturojuma. **Sagatavotajā rakstā apskatīts potenciālais apdraudējums pret Latvijas pētniecisko žurnālistu, kura rīcībā esošā informācija atsevišķus indivīdus interesē tādā mērā, ka tie ir gatavi nolīgt kibernoziedzniekus.** Rakstā aplūkots CERT.LV drošības ekspertu vērtējumā viens no labākajiem risinājumiem, kurā sabalansēta drošība, funkcionalitāte un lietošanas ērtums - izmantojot Google pakalpojumus.

Pilnā raksta versija pieejama šeit: https://cert.lv/lv/2019/01/mazcenas-risinajums-drosai-informacijas-apstradei

IT drošības seminārs „Esi drošs"

6.decembrī CERT.LV rīkotajā IT drošības seminārā "Esi drošs" tika pārrunātas **svarīgākās atziņas par E-adreses ieviešanu, izmaiņas IT drošības likumā un NIS direktīvā.** Klātesošo interesi piesaistīja pētījuma rezultāti, **kas var notikt, ja netiek pagarinātas domēna vārda lietošanas tiesības**, un padomi drošākai attālināto darbu veikšanai. Taču lielāko uzmanību piesaistīja un aktīvākās diskusijas raisīja K.Podiņa stāstījums **par mūsdienīgu e-pasta standartu ieviešanas nosacījumiem valsts un pašvaldību iestādēs.**

Seminars klātienē pulcēja 144 dalībniekus, taču tiešsaistē šoreiz rekordliels skaits – 605.

Semināra prezentācijas un video ieraksti ir pieejami CERT.LV mājas lapā: https://cert.lv/lv/2018/11/it-drosibas-seminars-esi-dross

Janvāra OUCH!

Ikmēneša informācijas drošības biļetens ikvienam

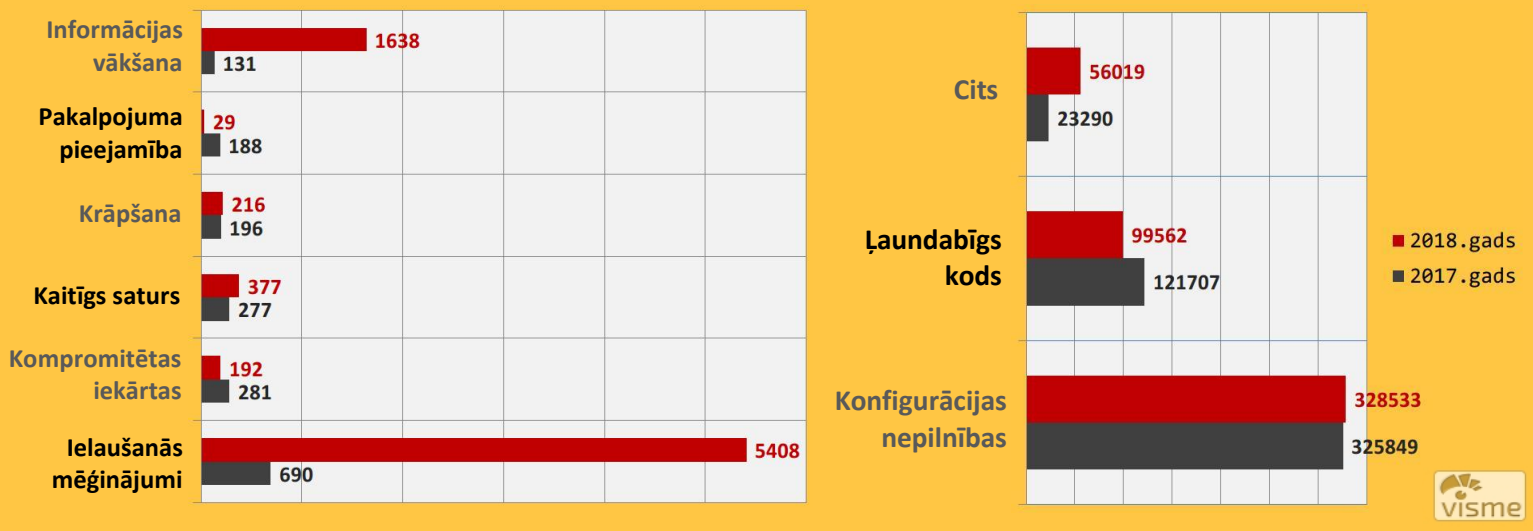
Biļetena tēma: informāciju par sevi tiešsaistē

Jānvāra OUCH! Izdevumā lasiet, kā veikt izpēti par sevi un noskaidrot, kāda informācija par jums ir publiski pieejama. Gudrā vārdā šo procesu sauc par OSINT (Open Source Intelligence). Paturiet prātā, ka kiberuzbrucēji izmanto tādus pat rīkus un metodes. Jo vairāk uzbrucēji var uzzināt par jums, jo labāk viņi var pielāgot uzbrukumu.

Pilna raksta versija pieejama šeit: https://cert.lv/uploads/ieteikumi/201901-OUCH-January-Latvian.pdf

Statistika: Unikālo IP adrešu skaits pa apdraudējuma veidiem

Piezīme: Grafikā redzamajās sadaļās - „Informācijas vākšana" un „Ielaušanās mēģinājumi" – pieaugums 2018. gadā, salīdzinot ar 2017.gadu, daļēji saistīts gan ar jauniem pievienotiem datu avotiem konkrētajiem apdraudējuma veidiem, gan ar inficētiem MikroTik maršrutētājiem un IoT iekārtu skaita palielināšanos.



KIBERSTĀSTI

• • •

Kā pozitīvs piemērs jāmin kāds Latvijas uzņēmums, kurš decembra sākumā CERT.LV izpētei pārsūtīja krāpniecisku biznesa e-pastu ar aizdomīgu pielikumu, tā vietā, lai pašrocīgi veiktu pārbaudi. Pievienotais fails saturēja *keyloggeri* - klaviatūras rakstzīmju ievades pārtveršanas programmu. CERT.LV par minēto krāpniecību informēja gan pašu uzņēmumu, gan iesaistīto IP adrešu īpašniekus.

• • •

No kāda Latvijas uzņēmuma decembra pirmajā pusē tika saņemts ziņojums par 2 viltus vietnēm, kurās bez atļaujas izmantots minētā uzņēmuma logo un pārkopēts oficiālās vietnes saturs. Šādas vietnes parasti tiek izveidotas, lai, slēpjoties aiz oriģinālajām vietnēm, varētu izpildīt savu skriptus, piemēram, statistikai vai domēna vārda popularizēšanai. CERT.LV informēja vietņu hostinga kompāniju par autortiesību pārkāpumu, kā arī ieteica to darīt pašam uzņēmumam, ar mērķi panākt operatīvāku hostinga kompānijas reakciju. Vietnes tika slēgtas.

• • •

No kādas pašvaldības institūcijas tika saņemts ziņojums par to, ka kāda visiem brīvi pieejama vietne satur teksta formāta VOIP telefonu konfigurācijas failus (ar lietotājvārdiem un parolēm), un VPN savienojuma izveides sertifikātus. Ar šiem datiem varēja veikt nesankcionētu pieslēgumu VOIP centrālei, kā arī visticamāk veikt un saņemt konkrētā lietotāja zvanus. CERT.LV informēja visas iesaistītās un atbildīgās institūcijas par konstatētajām nepilnībām, kā arī sniedza ieteikumus problēmas risināšanai. Situācija dienas laikā tika veiksmīgi atrisināta un konfigurācijas faili izņemti no vietnes.

KIBERLAIKAPSTĀKĻI

				
PAKALPOJUMA PIEEJAMĪBA	**LIETU INTERNETS**	**DATU NOPLŪDE**	**ĻAUNATŪRA UN IEVAINOJAMĪBAS**	**KRĀPŠANA**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Saņemts ziņojums par ļaunatūru komand- un kontroles centriem LV IP adresēs	Krāpnieciskie e-pasti par nenomaksātiem nodokļiem; Krāpnieciski e-veikali pirmsvētku periodā

NACIONĀLĀ ENCIKLOPĒDIJA PIEEJAMA ARĪ TIEŠSAISTĒ

Nacionālā enciklopēdija ir universāla populārzinātniska enciklopēdija latviešu valodā. Latvijas valsts simtgadei ir sagatavots īpašs drukātais sējums par Latviju, taču enciklopēdiju pamatā veido elektroniskā versija ar ilgtermiņa vīziju - ar iespēju to pastāvīgi papildināt un pilveidot ar jaunām zināšanām. No 18.12.2018 ikvienam pieejama enciklopēdijas elektroniskā versija: enciklopedija.lv.

ESAM LEPNI, JO SAVU PIENESUMU SATURAM DEVIS ARĪ **CERT.LV:** https://enciklopedija.lv/skirklis/4467

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