CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

FEBRUĀRĪ AKTUĀLI:

- FEBRUĀRIS – CERT.LV JUBILEJAS MĒNESIS
- CISCO VPN IEVAINOJAMĪBA
- POLITISKAJĀ KIBERTELPĀ IZSKAN ZIŅAS PAR KRIEVIJAS SAISTĪBU AR ,,NOTPETYA''
- VILTUS LOTERIJAS
- DATI UN DROŠĪBA, ,,STRAVA'' PIEMĒRS
- KIBERSTĀSTI
- ,,NOMORERANSOM'' PROJEKTS
- CERT.LV LEPOJAS
- SKAITĻI UN FAKTI

Attēli: Pixbay.com

FEBRUĀRIS – CERT.LV JUBILEJAS MĒNESIS

"Katru gadu CERT.LV komandai 1. februāris ir īpašs – CERT.LV dzimšanas diena! Šogad aprit jau 7 gadi Latvijas kibertelpā! Paveikts ir daudz šajos 7 – sabiedrība mums uzticas, mūsos ieklausās un kļūst arvien modrāka. Komanda ir izaugusi no pāris darbiniekiem līdz pienācīgam teju 30 cilvēku kolektīvam. Kaut arī daudz ir paveikts, tomēr tikpat un vēl vairāk ir jāpaveic! Lai izdodas!" B.Kaškina, CERT.LV vadītāja.

CISCO VPN IEVAINOJAMĪBA

Februāris sākās ar kibertelpas entuziastu un ekspertu bažām par jauno ievainojamību, ar kuru janvāra beigās nāca klajā starptautiskais interneta tehnoloģiju milzis - Cisco. Ievainojamība konstatēta Cisco ASA (*Adaptive Security Appliance*) programmatūrā, kas integrēta vairākās Cisco ražotajās tīkla drošības iekārtās. Ar apdraudēto produktu klāstu varat iepazīties Cisco oficiālajā vietnē: www.cisco.com, pie drošības padomiem (*Security Advisories*), ievadot meklētājā ievainojamības **CVE identifikācijas numuru: CVE-2018-0101**.

Kāpēc ievainojamība ir bīstama? Tā potenciālajiem ļaundariem dod iespēju attālināti pārņemt kontroli pār iekārtu, iepriekš uz to nosūtot izpildāmo kodu. Otrkārt, ievainojamība sniedz ļaundariem iespēju traucēt iekārtas darbu, to attālināti restartējot. Tāpat ievainojamības ļaunprātīgas izmantošanas rezultātā var tikt atteikts ienākošais VPN (*Virtual Private Network*) savienojuma pieprasījums.

Tādēļ aicinām interneta lietotājus, kuru īpašumā ir kāds no Cisco produktiem, pārliecināties, vai tas nav iekļauts apdraudēto produktu sarakstā. Ja produkts tomēr atrodas riska grupā, **tad aicinām izmantot Cisco piedāvātos ielāpus un atjauninājumus**, kas paredzēti konkrētās ievainojamības neitralizēšanai.

VAIRĀK INFORMĀCIJAS:

- **Cisco VPN ievainojamība:** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

KIBERLAIKAPSTĀKĻI

PAKALPOJUMA PIEEJAMĪBA	LIETU INTERNETS	DATU NOPLŪDE	ĻAUNATŪRA UN IEVAINOJAMĪBAS	KRĀPŠANA
Būtiski incidenti netika reģistrēti	Jauns Mirai ļaunatūras paveids	Pietiek.com datu noplūde	Cisco un Telegram ievainojamības	Viltus loterijas

Politiskajā kibertelpā izskan ziņas par Krievijas saistību ar destruktīvo kiberuzbrukumu - ,,NotPetya''

2017. gada jūnijā visā pasaulē izplatījās vīruss „NotPetya". Vīrusa izplatības kampaņa tika veikta, lai bojātu uzņēmumu, iestāžu un privātpersonu datus, nevis izspiestu naudas līdzekļus. Latvijā cietušo skaits bija neliels, un pārsvarā skāra uzņēmumus, kam filiāles atradās Ukrainā. Kaut arī cietušo skaits bija mazs, nodarīto postījumu apmērs – nopietns. Vislielākos zaudējumus vīruss sagādāja Ukrainai, inficējot vairākus tūkstošus datoru, kas tika izmantoti gan publiskajā, gan privātajā sektorā . Vīruss tālāk no Ukrainas izplatījās uz Eiropas, Krievijas un ASV uzņēmumiem. **Kopumā zaudējumi mērāmi vairākos miljardos ASV dolāru.**

Lielbritānijas Nacionālais kiberdrošības centrs pēc veiktās analīzes ar augstu ticamību norāda, **ka tieši Krievijas bruņotie spēki ir atbildīgi par postošo kiberuzbrukumu – „NotPetya".** Ņemot vērā lielo pārliecību, š.g. 15.februārī Lielbritānijas valdība arī publiski izteica savu spriedumu, vainojot notikušajā kiberuzbrukumā Krievijas valdību. Lielbritānijas paziņojumam tajā pašā dienā pievienojās arī ASV.

Lielbritānijas Ārlietu ministrijas valsts ministrs Tariks Ahmeds norādīja, ka kiberuzbrukums, kas šķietami maskēts aiz kriminālās noziedzības plīvura, patiesībā radīts ar apzinātu mērķi - iznīcināt. Primārais uzbrukuma mērķis - Ukrainas kritiskā infrastruktūra. Lielbritānija arī aicināja Krieviju uzņemties atbildību par notikušo, un izteica brīdinājumu, kā šāda veida kiberuzbrukums nevar palikt bez „starptautiskām sekām".

Vairāk informācijas:

- **Lielbritānijas paziņojums par Krievijas saistību ar „NotPetya"**: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Dati un drošība, ,,Strava'' lietotnes pamācošais piemērs

„Strava" ir vingruma tīmekļa vietne, sociālais tīkls un mobilā lietotne, kura tiek izmantota, lai dalītos ar fizisko treniņu rezultātiem, piemēram, skriešanā vai velobraukšanā. Lietotne ievāc treniņu maršrutu GPS koordinātas. Lietotājiem pēc treniņa ir iespēja dalīties ar saviem rezultātiem ar citiem lietotājiem.

2017. gada nogalē „Strava" publicēja aktivitāšu karti (heatmap), kurā **apkopoti aptuveni 27 milj. lietotāju veiktie maršruti**, laika posmā no 2015. līdz 2017. gadam. „Strava" apgalvo, ka kartē iekļautas tikai tās aktivitātes, kam lietotājs nav iestatījumos liedzis piekļuvi vai publicitāti. Attiecīgi kartē neparādās to lietotāju dati, kas privātuma uzstādījumos izvēlējušies palikt neredzami.

2018. gada sākumā kāds divdesmit gadus vecs students no Austrālijas, pētot publicēto „Strava" karti, pamanīja, ka tajā skaidri iezīmējas ASV militāro objektu atrašanās vietas tādās valstīs kā Sīrija un Afganistāna. Precīzāk, ir novērojami karavīru pārvietošanās paradumi militārās bāzes zonā. Attiecīgi no tā ir izsecināms, ka „Strava" lietotne plaši tiek izmantota militāro spēku aprindās, kur karavīri publiski dalās ar saviem treniņu rezultātiem. **Tas nozīmē, ka citkārt sensitīva un potenciāli valsts drošībai nozīmīga informācija, ir kļuvusi šobrīd plaši pieejama.** Svarīgi arī atzīmēt faktu, ka šāda veida informācija, pat ja netiktu nepārdomāti publicēta, joprojām atrastos „Strava" un citu līdzīgu pakalpojumu sniedzēju rīcībā. Proti, ja kādam izdotos ielauzties „Strava" sistēmā, tad arī viņam šī informācija būtu pieejama.

Tas liek vēlreiz aizdomāties par to, cik svarīgi ir šodien pārdomāt gan savu, gan darbinieku rīcību digitālajā vidē un kādu informāciju tajā varam vai nevaram atļauties publicēt. Piemēram, ASV Jūras kājnieku korpusam kopš 2016. gada ir skaidri noteikts reglaments attiecībā uz „privātajām pārnēsājamajām fitnesa ierīcēm". Šāda veida ierīces ir aizliegts izmantot gadījumos, ja tās var pieslēgties un izmantot WiFi vai mobilos datus, ja tajās ir pieejamas – video / audio ierakstīšanas, fotografēšanas un mikrofona funkcijas. Nepietiek tikai ar šo funkciju „atslēgšanu".

Arī Latvijā aizvien biežāk tiek piekopta pozitīvā prakse gan privātajā, gan publiskajā sektorā - pirms svarīgām sanāksmēm, kurās tiek pārspriesta sensitīva informācija – atstāt viedtelefonus ārpusē vai tiem speciāli paredzētā vietā. **Tomēr CERT.LV šajā riska zonā aicina iekļaut ne tikai telefonus, bet arī citas viedierīces, piemēram, tos pašus viedpulksteņus, kam bieži vien ir iestrādātas līdzīgas funkcijas kā viedtelefoniem.**

VAIRĀK INFORMĀCIJAS:

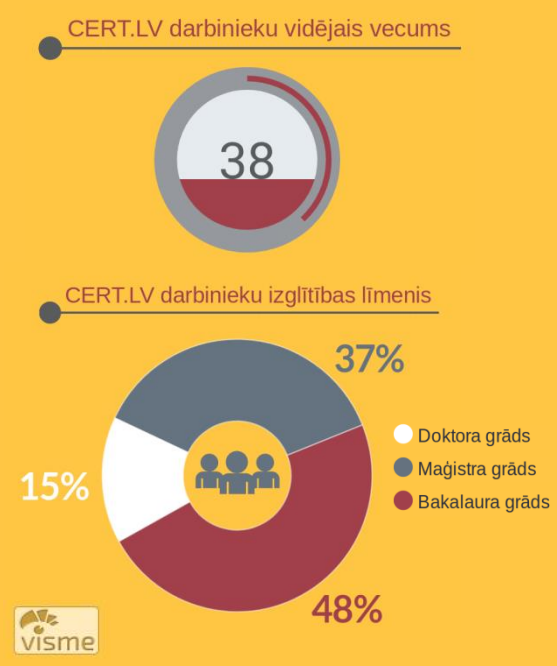
- **„Strava" iezgaismo karavīru pārvietošanās ceļus militārajās bāzēs:** http://www.bbc.com/news/technology-42853072
- **„Strava" atklāj militāro objektu lokāciju:** https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban

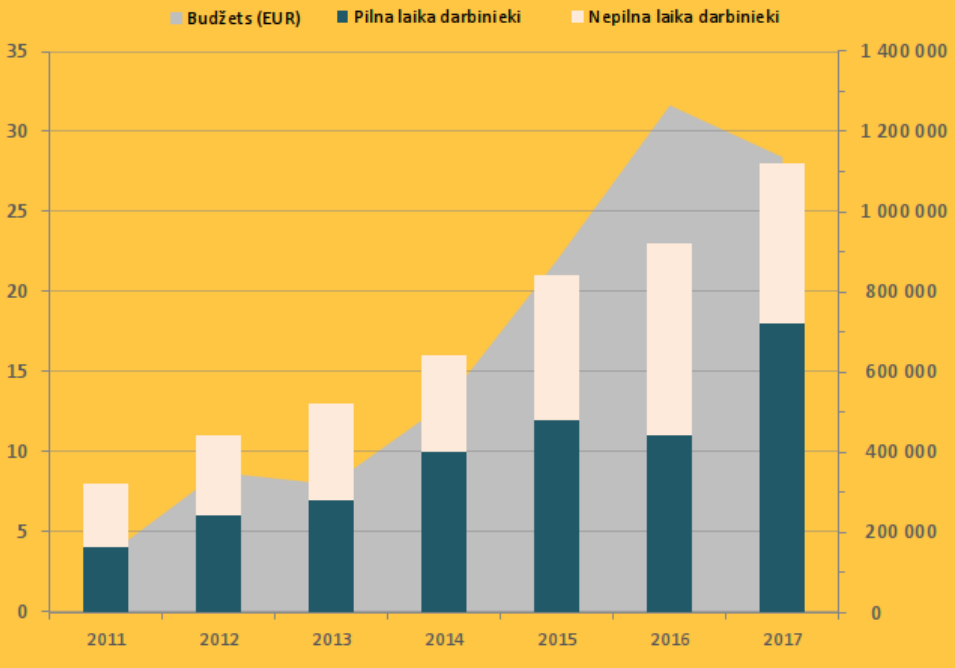
VILTUS LOTERIJAS

CERT.LV februāra vidū saņēma vairākas sūdzības, ziņojumus un jautājumus no interneta lietotājiem par viltus loterijām ar iespējām saņemt vērtīgus laimestus, piemēram, **iPhone par 1$ vai Eurojackpot miljoniem vērtu laimestu.** Šādu akciju rīkotāji izsūta vēstules e-pastā vai kā telefona īsziņas ar paziņojumu par ievērojamo laimestu un, lai to saņemtu, lūdz iesniegt dažādus personas datus. Piedevām, ziņojumā par iPhone iegūšanu, vietnes pašā apakšā bija grūti pamanāma atruna, ka ar šo lietotājs abonē vietnes servisu un pēc 7 izmēģinājuma dienām **tiks iekasēta ikmēneša abonēšanas maksa 49.99 $ apmērā**.

PADOMS: Sekojiet līdzi pakalpojumu sniegšanas noteikumiem, rūpīgi pārdomājiet informācijas sniegšanas nepieciešamību! Tāpat aicinām būt uzmanīgiem un sekot līdzi, kur, kādus un kam jūs norādāt savus personas datus! Jo īpaši tad, ja loterijas biļetes pat neesat iegādājušies. Zelta likums – jūsu dati, jūsu darīšana, citiem tos neatklājiet!

SKAITĻI UN FAKTI





MARTA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: "Ieteikumi sociālo tīklu drošai lietošanai"

Sociālie tīkli, piemēram, Snapchat, Facebook, Twitter, Instagram un LinkedIn ir lieliski resursi, kas ļauj jums tikties un komunicēt ar cilvēkiem visā pasaulē. Tomēr šīs iespējas slēpj arī riskus. Riskus ne tikai jums, bet arī jūsu ģimenei, draugiem un darba devējam.

Pilna raksta versija pieejama: https://cert.lv/uploads/201803-OUCH-March-Latvian.pdf

KIBERSTĀSTI

• • •

Pirmajā stāstā CERT.LV vēlas uzteikt kādu pozitīvu piemēru. Februārī kāda Latvijas pašvaldības pie CERT.LV vērsās ar lūgumu veikt ielaušanās testu konkrētās pašvaldības jaunās mājas lapas testa versijai. Pirms mājaslapas uzlikšanas produkcijā jeb publicēšanas, pašvaldība vēlējās pārliecināties, vai visi drošības aspekti ir ievēroti un nav atstāti neparedzēti „caurumi". CERT.LV veica ielaušanās testu un konstatēja vienu kritisku ievainojamību. Pēc CERT.LV sniegtajām rekomendācijām ievainojamība tika novērsta.

• • •

CERT.LV saņēma no kāda lietotāja ziņojumu par krāpniecisku e-pastu, kas sūtīts ar mērķi izkrāpt finanšu līdzekļus no lietotāja. E-pasts tika saņemts angļu valodā it kā no kāda ļaundara, kas uzdevās par kriminālu hakeru grupējumu no Korejas ar nosaukumu „uiideBunnY squad". Ļaundaris e-pastā apgalvo, ka viņa grupējums ir it kā uzlauzis kādu „18+" vietni, kuru apmeklējis arī lietotājs. Apmeklējuma brīdī hakeri esot ierakstījuši gan uz lietotāja datora ekrāna notiekošo, gan nofilmējuši viņu caur web kameru. Tāpat ļaundaris apgalvoja, ka viņi piekļuvuši arī lietotāja kontaktu sarakstam. Attiecīgi tika draudēts, ka ierakstītie video materiāli tiks nosūtīti lietotāja kontaktiem, ja lietotājs nesamaksās 290 dolārus, izmantojot kriptovalūtu. E-pasta noslēgumā sekoja instrukcija, kā veikt pārskaitījumus kriptovalūtā. CERT.LV informēja lietotāju, ka šis ir krāpnieciska rakstura e-pasts un ļaundaru prasības nekādā gadījumā pildīt nevajag. Tāpat CERT.LV aicināja nepublicēt savu e-pasta adresi publiskās vietnēs un izmantot e-pasta filtrus, lai dzēstu nevēlamas vēstules.

• • •

Nākamais stāsts uzskatāmi parāda, kā strādā un tiek izmantota sociālā inženierija. Kāda ārzemēs dzīvojoša latviete sazinājās ar CERT.LV un atklāja, ka uztraucas par savu drošību, saistībā ar Facebook iepazītu vīrieti, kas, spriežot pēc saņemtās informācijas, nav ES pilsonis. Sieviete CERT.LV rīcībā nodeva abu saraksti lietotnē Viber tālākai analīzei. Vīrietis sarakstē atklāja, ka viņš ir atraitnis un viens pats audzina savu meitu. Meitai no mirušās sievas tēva atstāts paprāvs mantojums 4,8 milj. $ vērtībā. Līdzekļus iespējams saņemt tikai meitas aizbildnim, kas, protams, viņš pats nevar būt, jo it kā 3 mēnešus atradies slimnīcā komā un līdz ar to, laikam zaudējis aizbildniecību. Cik noprotams no sarakstes, kas notikusi sliktā angļu valodā no vīrieša puses, tad ļaundaris piedāvājis sievietei kļūt par meitas aizbildni un par to saņemt 25% no mantojuma. Vīrietis sarakstē izmantoja glaimus, mīlestības apliecinājumus, piesauca dievu un likteni. Viņš pieprasīja finansiālu palīdzību dokumentu kārtošanai un viņas datus, ko sieviete arī labticīgi iedeva. Pēc tam, kad vīrietis vairs nedeva ziņu, latviete nobijās un uzrakstīja, ka dati neesot korekti un viņa esot sazinājusies ar savu advokāti. Sarakste atsākās nu jau skarbākos toņos un ar apvainojumiem par melošanu un neuzticēšanos. CERT.LV noskaidroja, ka no sievietes ļaundarim izdevies iegūt vārdu, uzvārdu, telefona numuru, e-pastu, dzimšanas datus un iespējams adresi. Finansiāli zaudējumi nav nodarīti. CERT.LV paskaidroja, ka vīrieša rīcībā nodotie dati ir publiski, un kaitējumu nodarīt nevar. Tāpat CERT.LV ieteica nobloķēt vīrieti Viber un Facebook, un neatbildēt uz viņa mēģinājumiem sazināties, kā arī ziņot Facebook administrācijai par viņa profilu. Turpmāku draudu gadījumā ieteikums vērsties vietējā policijā.

„NOMORERANSOM" PROJEKTS

„No More Ransom" projekta mērķis ir palīdzēt bez maksas atgūt datus šifrējošo izspiedējvīrusu upuriem. Tā ir platforma www.nomoreransom.org, kas ļauj pārliecināties, vai upura dati nav atgūstami bez maksas. Platformā šobrīd pieejami jau 52 atslēgu rīki atšifrēšanai, kas ir pielāgojami 84 plaši izplatītām ļaunatūru saimēm. Pateicoties šim projektam, jau vairāk nekā 35 000 cilvēku visā pasaulē ir izdevies atgūt savus datus bez maksas, kas ir kavējis kibernoziedzniekus gūt peļņu vairāk nekā 10 milj. EUR vērtībā.

Šifrējošie izspiedējvīrusi joprojām ir aktuāli. Arī CERT.LV periodiski saņem sūdzības un informāciju no fiziskām un juridiskām personām par nošifrētām ierīcēm un failiem.

Plašāka informācija par projektu: www.nomoreransom.org

CERT.LV LEPOJAS

„CROSSED SWORDS 2018" MĀCĪBAS LATVIJĀ

Š.g. janvāra beigās un februāra sākumā NATO apvienotais kiberaizsardzības izcilības centrs (NATO CCD CoE) sadarbībā ar CERT.LV pirmo reizi Latvijā organizēja tehniskās kiberaizsardzības mācības "Crossed Swords 2018". Šogad mācību mērogs, salīdzinot ar citiem gadiem, bija daudz plašāks, tehniski sarežģītāks un izaicinošāks. Mācības aptvēra vairākus ģeogrāfiskus atrašanās punktus, iesaistot tajās gan informācijas tehnoloģiju (IT) kritiskās infrastruktūras uzturētājus, gan militārās vienības. Mācībās piedalījās vairāk kā astoņdesmit kiberdrošības ekspertu no piecpadsmit NATO CCD CoE dalībvalstīm.

DALĪBA „GARAGE 48"

Šogad 16.februārī Rīgā notikušajā mini kiberdrošības hakatonā Garage48 mentora statusā iejutās arī CERT.LV IT drošības speciālists Ivo Ķutts. Garage48 kopā pulcēja speciālistus no dažādām jomām, to vidū bija gan kiberdrošības speciālisti un analītiķi, programmētāji, uzņēmēji, projektu vadītāji, pilna laika studenti u.c. Pasākuma pirmajā posmā dalībnieki nāca klajā ar 6 interesantām idejām, no kurām tālāk tika attīstītas tikai 3 idejas jeb izveidotas 3 konkurējošas komandas. Mentoru uzdevums bija komandām palīdzēt ar padomiem un ieteikumiem pie izvēlētās idejas attīstīšanas.

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

19.-25. **MARTS** - Digitālā nedēļa

20. **MARTS** - Digitālās drošības diena (Piedalās CERT.LV eksperts)

20. **MARTS** – „Kibernakts 2018"

21. **MARTS** - IT drošības seminārs "Esi drošs"

11.-13. **APRĪLIS** - RIPE apmācības LIR biedriem:

- **11.04.** NCC Basic IPv6 Training Course
- **12.04.** RIPE NCC IPv6 Security Training
- **13.04.** RIPE NCC Measurements and Tools Training Course

23.-27. **APRĪLIS** – Locked Shields 2018 mācības

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