



CERT.LV aktualitātes

Rīga, 2018. gada 21. marts



“Esi drošs” programma

- 13:30-13:40 CERT.LV aktualitātes - Baiba Kaškina, CERT.LV**
- 13:40-14:00 Eiropas tīklu un informācijas sistēmu drošības direktīvas ieviešana Latvijā**
Sanita Žogota, Aizsardzības ministrija
- 14:00-15:00 Vispārīgā datu aizsardzības regula un drošība**
Katrīna Sataki, NIC.LV, Iveta Skujiņa, CERT.LV
- 15:00-15:30 Kafijas pauze**
- 15:30-16:00 Cinītis, vezums un procesora optimizācija - Kārlis Podiņš, CERT.LV**
- 16:00-16:30 Mākoņdatošana un drošība. Iespējas un riski, t.sk. valsts mākoņdatošanas kontekstā - Juris Pūce, Analytica**
- 16:30-17:00 CERT.LV un NIC.LV DNS ugunsmūris - Varis Teivāns, CERT.LV**



Par semināru

- **WIFI PIEEJA:**
 - SSID: Bank Citadele
- **TIEŠRAIDE**
- **APLIECINĀJUMI:**
 - Elektroniski 22.martā



CERT.LV – 7 gadi





„Crossed Swords 2018”

- NORISE: 29.01. - 02.02.2018
- DALĪBNIEKI: < **80** kiberdrošības eksperti
no **15** NATO CCD CoE dalībvalstīm
- VAIRĀKI GEOGRĀFISKIE ATRAŠANĀS PUNKTI
- (IT) KRITISKĀS INFRASTRUKTŪRAS UZTURĒTĀJI
+ MILITĀRĀS VIENĪBAS



Mēneša ziņas

- PIEEJAMAS ELEKTRONISKI
- SVARĪGĀKO ZINU APKOPOJUMS
- SKAITLI UN FAKTI
- KALENDĀRS
- KIBERLAIKAPSTĀKĻI
- KIBERSTĀSTI

MĒNEŠA ZINU IZLAIDUMS NR. 01/2018

JANVĀRI AKTUĀLI:

- E-VESELĪBA UGUUNKRISTĪBĀS
- JAUNI RISKI, KAS BALSTĪT IEKĀRTU PAMATFUNKCIONALITĀTĒ
- KRIPTOVALŪTA – PIEVILCIS „BURĒĀNS” LAUINĀTĀRĀS IESRADĀŠĀJĒM
- VILTOU REŽĪNU VILNIS
- SKAITLI UN FAKTI
- KIBERSTĀSTI

E-VESELĪBA UGUUNKRISTĪBĀS

Šis gads iesākās trauksmīni, ar zinu par uzbrukumiem veselības aprūpes kvalitātes un efektivitātes uzlabošanas programmai e-veselība. Pirmatnējā izpēte apiecīnāja, ka 16.janvāri e-veselības sistēma piedzīvoja pārslodzes uzbrukumu (DDoS). Šāda uzbrukuma mērķis ir padarīt sistēmu nepieejamu, bet datu noplūde nenotiek.

Šādām uzbrukumam var tikt paklauta jebkura sistēma. Uzbrukuma ietekmes mazināšanai pirms sistēmas nodokinas ekspluatāciju sistēmai vēlams nodrošināt aizsardzību pret DDoS uzbrukumiem, kā arī vēlams izstrādāt rīcības plānu situācijai, kad uzbrukumu neizdots atvairīt un tā sekas būtu jutamas lietotājiem.

KIBERLAIKAPSTĀKĻU

PAKALPOJUMA PIĘEJAMĪBA	LIEU INTERNETS	DATU NOPLŪDE	LAUINĀTĀRA UN IEVAINOJAMĪBAS	KRĀŠANA
Uzbrukumi e-veselības sistēmai	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Meltdown un Spectre ievalnojamības	Viltoju režīnu vilnis

JAUNI RISKI, KAS BALSTĪT IEKĀRTU PAMATFUNKCIONALITĀTĒ

2017. gada nogali un 2018. gada sākumu izleimēja vairākas nopietnas, datoru un procesoru darbību ietekmējošas ievalnojamības: **aparātprogrammatūras (firmware)** līmena ievalnojamība IntelME (CVE-2017-5705 ildz CVE-2017-5712) un „dzelzis” (hardware) līmena ievalnojamības Meltdown (CVE-2017-5754) un Spectre (CVE-2017-5753 un CVE-2017-5715), kuru visi kopīgā raksturīgā izleime – tās sniedz iespēju uzbrucējiem pārņemt vadību pār datorsistēmu un palikt nepamanītiem.

Ievelnojamību labojumi šādās situācijās nav vienkārši, jo nepieciek tikai ar mikroprocesoru ražotāju (piem., Intel, AMD, ARM u.c.) izlaistiem atjauninājumiem, tie jāpielāgo katra iekārtu ražotāja dažādo produktu vajadzībām. Tās var izraisīt neparedzētas izmaiņas iekārtu darbībā, piemēram, neprognozējamu restartēšanos (Intel sākotnēji izlaists Spectre ielāps) vai pat darbības pilnīgu

MĒNEŠA ZINU IZLAIDUMS NR. 02/2018

CERT.LV
informāciju izveido
veicināt
veicināt
veicināt
veicināt

ESIS

CERT.LV dzimšanas diena! Šogad aprīt jau 7 gadu
o mums uzticas, mūsos ieklausīs un kļūst arī
piendzīgam teju 30 cilvēku kolektīvam. Kaut arī
vielās izdodas!” B. Kašķina, CERT.LV vadītāja.

par jauno ievalnojamību, ar kuru janvāra beigās nāca
ainājamība konstatēta Cisco ASA (Adaptive Security)
tajās tika drošības iekārtās. Ar apdraudēto produktu
pie drošības padomiem (Security Advisories), ievadot
SA-0101.

nodod iespēju attīlināti pārņemt kontroli pār iekārtu,
sniedz jaundariem iespēju traučēt iekārtas darbu, to
sākotnējā rezultātā var tikt atteikts ienākošais VPN

Cisco produktiem, pārliecīgāties, vai tas nav iekļauts
iskā grupā, tad aicinām izmantot Cisco piedāvātos
nības neutralizēšanai.

content/CiscoSecurityAdvisory/cisco-sa-2018-129-as1

IDE

LAUINĀTĀRA UN IEVAINOJAMĪBAS	KRĀŠANA
Cisco un Telegram ievalnojamības	Viltus loterijas

1 no 5



Digitālā nedēļa 2018

- **DIGITĀLĀS DROŠĪBAS DIENA - 20. MARTS**
 - Diskusija “Drošība un pārliecība digitālajā vidē” – piedalās CERT.LV eksperts
 - KIBERNAKTS 2018 – diskusijā piedalās CERT.LV eksperts
- **SEMINĀRS «ESI DROŠS» – 21. MARTS**
- **PAR CITĀM AKTIVITĀTĒM:** <http://eprasmes.lv/>



CERT.LV un NIC.LV DNS ugunsmauris



Brīdinājums: Launatūra

Brīdinājums

Tīmekļa vietne, kuru vēlējāties apmeklēt, iespējams satur vai izplata launatūru (malware). Piekļuve vietnei tika ierobežota.

Ja uzskatāt, ka piekļuve ierobežota nepamatoti, lūdzu informējiet CERT.LV, sūtot e-pastu uz cert@cert.lv. E-pastā iekļaujiet šu paskaidrojumu, kāpēc piekļuvi vietnei nevajadzētu ierobežot, un pievienojiet arī zemāk redzamo tehnisko informāciju:

Klienta IP: 192.168.1.200
Pieprasītais domēns: testtesttest222.lv
Pieprasītais ports: 80
URL: /evil.exe
Piekļuves laiks (EET): 2018-03-21 09:46:22 EET

[Kopēt brīdinājuma informāciju](#)

Lai saņemtu plašāku informāciju, sazinieties ar savas organizācijas IT nodalju.



Aktuālie pasākumi

- **14. JŪNIJS - KRITISKĀS INFRASTRUKTŪRAS SEMINĀRS**
- **9. OKTOBRIS - KIBERŠAHS 2018**
 - Aprīlī aicināsim pieteikt referātus konferencei

A close-up photograph of an owl's face, focusing on its large, bright yellow eyes with dark pupils. The owl's feathers are a mix of brown, black, and white, appearing textured and slightly ruffled. The background is a soft-focus green.

Paldies!

cert@cert.lv

<https://www.cert.lv>

