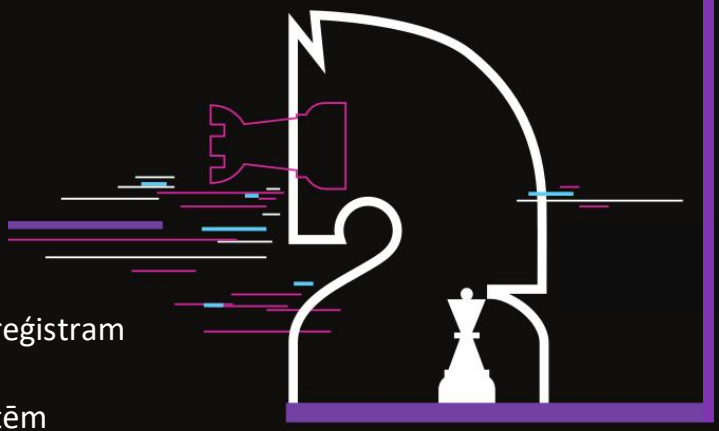
WWW.CERT.LV

OKTOBRA APSKATS:

- Veiksmīgi aizvadīts „Kiberšahs 2018”
- Oktobrī 564 aktivitātes 35 Eiropas valstīs
- Uzmanību: „#Atkrāpies!”
- Profesijas un izglītība jeb atvērtās durvis LUMII
- Atskats uz 6. oktobra vēlēšanām
- Nesankcionētas pieslēgšanās mēģinājums CSDD reģistram
- CERT.LV meklē papildspēkus
- Krāpnieciska loterija ar Ed Sheeran koncerta biļetēm



VEIKSMĪGI AIZVADĪTS „KIBERŠAHS 2018”

“Kiberšahs 2018” runātāji un sesiju moderatori

9.oktobrī, viesnīcā *Raddisson Blu Latvija* norisinājās IT drošības konference "Kiberšahs 2018", kuru rīkoja CERT.LV un ISACA Latvijas nodaļa sadarbībā ar LMT, dots. un Eiropas Savienību (konference daļēji tiek līdzfinansēta no CEF projekta “Improving Cyber Security Capacities in Latvia” (INEA/CEF/ICT/A2017/1528784)).

Šogad konferences galvenā uzmanība tika pievērsta procesu novērošanai un analīzei, interneta gala lietotāja uzvedības modeļiem tiešsaitē, veiksmīgai risku vadībai un jaunākajām tehnoloģijām un risinājumiem nozarē. Konferenci klātienē apmeklēja 500 IT drošības ekspertu, bet tiešraidē pasākumam sekoja gandrīz 4 reizes lielāka auditorija, ap 2000 skatītāju.

Visiem interesentiem konferences tiešraides ieraksts ir pieejams vietnēs straume.lmt.lv, www.cert.lv un facebook.com/certlv/.

OKTOBRĪ 564 AKTIVITĀTES 35 EIROPAS VALSTĪS

EIROPAS KIBER-DROŠĪBAS MĒNESIS

Jau sesto gadu oktobris visā Eiropā tiek saukts par Eiropas kiberdrošības mēnesi. Šajā laikā pasākumu saturs un aktivitātes tiek organizētas, lai veicinātu sabiedrības izpratni par kiberdrošības jautājumiem, lai rosinātu nopietnāku attieksmi pret draudiem, kas saistīti ar virtuālo vidi. Iniciatīvas pilotversija bija 2012.gadā, kad piedalījās vien 8 dalībvalstis. Ar 2013.gadu arī Latvija aktīvi piedalās.

Šogad oktobra sākumā, saglabājot jau pēdējos gados iedibināto tradīciju un atzīmējot Kiberdrošības mēnesi, CERT.LV rīkoja ikgadējo starptautisko kiberdrošības konferenci „Kiberšahs 2018” IT drošības jomas ekspertiem. Tāpat CERT.LV pārstāvji piedalījās vairākās diskusiju grupās, uzstājās seminārā “KIBERDROŠĪBA? Tā ir arī mazā biznesa problēma!”, konferencē „DSS ITSEC”, kā arī oktobrī tika atzīmēta CERT.LV pievienošanās Latvijā aizsāktajai pretkrāpšanas kustībai #Atkrāpies!

Eiropas kiberdrošības mēnesi organizē Eiropas Tīklu un informācijas drošības aģentūra (ENISA) sadarbībā ar Eiropas Komisiju. Informācija par Kiberdrošības mēneša aktivitātēm Eiropā ir pieejama Eiropas Kiberdrošības mēneša tīmekļa vietnē https://cybersecuritymonth.eu/

Novembra OUCH!

Ikmēneša informācijas drošības biļetens ikvienam

Biļetena tēma: Vai esmu „uzlauzts”?

Lai cik droši jūs šķietami arī justos kibertelpā, tieši tāpat kā vadot automašīnu, agrāk vai vēlāk arī te var notikt negadījums. Raksta pilnajā versijā ir ieteikumi, kā noteikt, vai jūs kāds ir uzlauzis, un, ja tas tā ir noticis, ko tādā gadījumā darīt? Jo ātrāk jūs atklāsiet, ka ir noticis kas nelāgs, jo lielāka iespēja ir atrisināt problēmu.

Pilna raksta versija pieejama: https://cert.lv/uploads/201811-OUCH-November-Latvian.pdf

Uzmanību: “#Atkrāpies!”

Oktobrī CERT.LV oficiāli pievienojās arī Latvijā aizsāktajai pretkrāpšanas kustībai **#Atkrāpies!** Tās mērķis ir vienoti ar dažādām valsts iestādēm, uzņēmējiem, sabiedriskām organizācijām un sabiedrību virzīties uz “nulles toleranci” pret krāpšanos un negodīgām darbībām **t.sk. krāpnieciska rakstura e-pastiem, sociālo inženieriju, viltus mājas lapām un citām nelikumīgām darbībām kibertelpā.** Kustībai pievienojušās jau vairāk nekā 45 dažādas valsts pārvaldes iestādes un nevalstiskās organizācijas.

Plašāka informācija par kustību pieejama: http://atkrapies.lv/

Profesija un izglītība jeb atvērtās durvis LU MII

23.oktobrī LU MII ēkā viesojās Kalnciema vidusskolas pedagogi, skolēni un *Erasmus+* sadarbības partneri no Francijas, Itālijas, Horvātijas un Polijas, kopā pulcējot 45 skolēnus vecumā no 15-18 gadiem un 7 pedagogus. Projekta mērķis bija iepazīties ar profesijām, kas saistītas ar matemātiku un/vai datorzinātni. CERT.LV iepazīstināja ar sevi, stāstot par organizācijas pamatuzdevumiem, mērķiem un parādīja, cik liela nozīme IT uzņēmumā ir arī citām profesijām, kā piemēram, sabiedriskajām attiecībām.

Kiberlaikapstākļi

				
Pakalpojuma pieejamība	**Lietu internets**	**Datu noplūde**	**Ļaunatūra un ievainojamības**	**Krāpšana**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Saņemta info. par vairākām ievainojamībām valsts un pašvaldību iestāžu mājas lapās	Ed Sheeran koncerta biļešu krāpniecība

Krāpnieciska loterija ar Ed Sheeran koncerta biļetēm

CERT.LV oktobrī saņēma vairākus ziņojumus **par krāpniecisku loteriju lietotnē WhatsApp**, kas sola iespēju iegūt divas bezmaksas biļetes uz Ed Sheeran koncertu Lucavsalā. Taču vienīgais, ko šajā "loterijā" patiesi var iegūt, ir paliels mobilā telefona rēķins. Aicinām būt vērīgiem, uzticēties informācijai tikai oficiālās tīmekļa vietnēs, no oficiāliem pasākuma organizatoriem (L Tips Agency) un oficiāliem biļešu izplatītājiem (bilesuserviss.lv).

Plašāka informācija par krāpniecību pieejama: https://cert.lv/lv/2018/10/krapnieciska-loterija-ar-ed-sheeran-koncerta-biletem-lietotne-whatsapp

Kiberstāsti

Joprojām aktuāli, par ko liecina saņemto ziņojumu skaits, ir krāpnieciski e-pasti, kuros krāpnieks apgalvo, ka zina saņēmēja paroli, datorā ir uzinstalējis vīrusu un ir uzfilmējis video, kurā saņēmējs apmeklē pieaugušajiem domātas tīmekļa vietnes. Lai video materiāls netiktu publiskots, ļaundaris pieprasa samaksu. Šādi izspiešanas mēģinājumi CERT.LV redzeslaukā parādījās jau vasarā. Ļaundari izmanto publiski pieejamas e-pasta/paroles kombinācijas, kas iegūtas no lielu servisu (Linkedin, Dropbox utt.) un dažādu mazāku tīmekļa forumu datu noplūdēm, visbiežāk - vairākus gadus vecām. Saņemot šādu e-pastu, nepieciešams nomainīt kompromitēto paroli visos resursos, kur tā vēl tiek izmantota. Pašu izspiešanas vēstuli ieteicams ignorēt, nekādas e-pastā minētās darbības ar lietotāja datoru nav notikušas, un tajā nav uzstādīti kādi speciāli datorvīrusi.

• • •

Oktobrī tika saņemti vairāki detalizēti ziņojumi no kāda zviedru kiberdrošības pētnieka *Kasper Karlsson* par vairākām vidēji kritiskām un vienu ļoti kritisku ievainojamību valsts un pašvaldību institūciju vietnēs. Kritiskākā no ievainojamībām sniegtu ļaundarim iespēju piekļūt vairākām resursa datubāzēm, kas satur viegli atšifrējamu informāciju arī par lietotājiem un to piekļuves datiem. Pētnieks pārstāv Zviedrijas IT konsultāciju uzņēmumu "Omegapoint" un darbojas, ievērojot atbildīgu ievainojamību atklāšanas principus. Visi ziņojumos norādītie resursi tika apzināti un aicināti novērst atklātās ievainojamības. Lielākā daļa no tām tikušas operatīvi novērstas, pārējās vēl tiek labotas. Kā pateicību par sniegto ieguldījumu un pozitīvo piemēru, CERT.LV sagatavoja un nosūtīja pētniekam oficiālu atzinības vēstuli.

• • •

Tika saņemts ziņojums par kādu uzlauztu pašvaldības vietni, kurā ievietoti ļaundabīgi skripti, kas pārvirza apmeklētājus uz citu vietni. CERT.LV sazinājās ar minēto pašvaldību un lūdza dzēst pievienoto saturu, kā arī salabot vietnes/servera drošību, tai skaitā – atjaunot vietnes CMS programmatūru un tās spraudņus, lai novērstu šāda veida gadījumus nākotnē. Sniegtās rekomendācijas tika ņemtas vērā, un vietne salabota.

Atskats uz 6. oktobra vēlēšanām

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; tos izdevās veiksmīgi atvairīt.**

Katru gadu IT drošības incidentu apdraudējuma līmenis ir ar pieaugošu tendenci, ar vai bez vēlēšanām. **Šogad, salīdzinot ar citiem vēlēšanu gadiem, tika veikts visapjomīgākais darbs,** lai Latvija varētu pēc iespējas labāk reaģēt uz kiberdraudiem un mazināt identificētos IKT riskus, kas saistīti ar vēlēšanu procesu. CERT.LV ar kolēģiem Vēlēšanu drošības koordinācijas grupā ir veikusi ievērojamu sagatavošanās darbu, kā arī līdz vēlēšanām veikusi virkni ielaušanās testus un sniegusi drošības uzlabošanas tehniskās vadlīnijas, kuras lielākā daļa iesaistīto iestāžu sekmīgi ieviesa un atklātos trūkumus novērsa.

Pamanāmākais incidents vēlēšanu laikā bija sociālā tīkla Draugiem.lv sākumlapas izķēmošana. 6. oktobra pēcpusdienā, apmeklējot Draugiem.lv portālu, lietotāji saskarās ar provokatīvu ainu – Krievijas himnu fonā, un attēliem ar Krievijas armiju, prezidentu un karogu. Izķēmotā lapa tika aizvērta 20 minūšu laikā un portāla darbība atjaunota pāris stundu laikā.

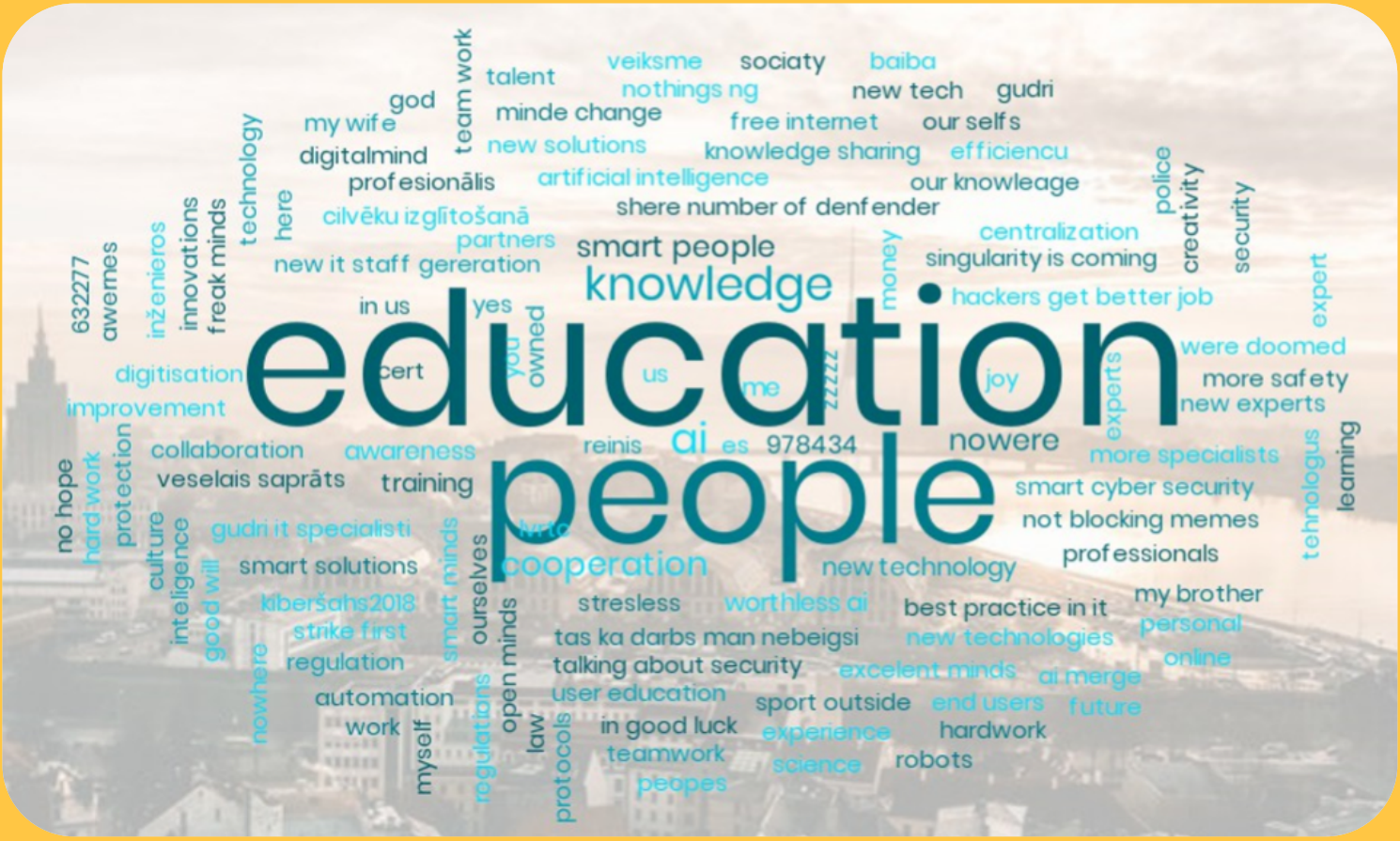
Nesankcionēta s pieslēgšanās mēģinājums CSDD reģistram

CSDD darbinieki saskārās ar kādas personas nesankcionētu mēģinājumu piekļūt Transportlīdzekļu reģistram un centieniem veikt naudas izspiešanu. Sadarbībā ar Valsts policiju iespējamais vainīgais tika aizturēts. Aizturētajai personai nebija izdevies piekļūt CSDD reģistrā esošajiem datiem un nav notikusi datu noplūde. Izmantotā ievainojamība e-CSDD portālā ir apzināta un novērsta.

Pret personu uzsākts kriminālprocess pēc Krimināllikuma 183.panta pirmās daļas, 241.panta trešās daļas, un 15.panta ceturtās daļas, proti, par informācijas sistēmas darbības traucēšanas mēģinājumu un izspiešanas mēģinājumu mantkārīgos nolūkos.

STATISTIKA: KĀDI FAKTORI VARĒTU UZLABOT KIBEDROŠĪBAS NĀKOTNI?

***Aptauja veikta kiberdrošības konferences „Kiberšahs 2018" laikā. Atbildes snieguši 212 apmeklētāji.**



CERT.LV KOMANDA MEKLĒ PAPILDSPĒKUS

CERT.LV komanda meklē papildspēkus – **IT drošības incidentu apstrādes un novēršanas speciālistu**, un **IT sistēmu administratoru darbam ar Linux**. Plašāka informācija par abām vakancēm pieejama šeit: https://cert.lv/lv/par-mums/vakances

Ja atbilsti lielākajai daļai prasību un vēlies ar entuziasmu risināt tehniskus izaicinājumus, piesakies, rakstot uz vakance@cert.lv. Ja neesi drošs, vai gribi pieteikties, atnāc ar mums vispirms iepazīties, rakstot uz vakance@cert.lv.

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

29. **NOVEMBRIS -** LIKTA 20. gadskārtējā konference

06. **DECEMBRIS –** IT drošības seminārs „Esi drošs"

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