Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2016

2016. gada 4. ceturksnis (01.10.2016. – 31.12.2016.)

Pārskatā iekļauta vispārpieejama informācija, tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums

2016. gada 4. ceturksnī CERT.LV reģistrēja un apstrādāja 677 augstas prioritātes incidentus un 255 184 zemas prioritātes incidentus.

Pārskata periodā notikušajiem incidentiem raksturīga iezīme ir kiberuzbrucēju rūpīga sagatavošanās pirms uzbrukuma veikšanas. Ir novērots lielāks mērķētu uzbrukumu apjoms, kuros uzbrucēji ir veikuši priekšizpēti un noskaidrojuši uzņēmuma vai iestādes vadītāju, kura vārdā izsūtīt krāpniecisku e-pastu, kā arī noskaidrojuši uzņēmuma vai iestādes grāmatvedi un tā e-pastu, kam krāpniecisko sūtījumu adresēt.

Pārskata periodā tika novērota arī intensīva šifrējošā izspiedējvīrusa Locky izplatīšanas kampaņa, kurā bija arī vairāki cietušie gan no uzņēmumu, gan privātpersonu vidus.

Līdz šim nebijis notikums ir lietu interneta (IoT) robotu tīkla veiktais masīvais DDoS uzbrukums, kurš uz dažām stundām padarīja nepieejamas daudzas populāras globālā tīmekļa vietnes. Latvijā tika identificēti vairāki simti ievainojamu iekārtu, kas varētu būt daļa no 100 000 inficēto IoT iekārtu, kas piedalījās pirmajā globālajā lietu interneta uzbrukumā.

Pārskata periodā notika gada lielākais IT drošībai veltītais pasākums Latvijā - CERT.LV un ISACA Latvijas nodaļas ikgadējā konference “Kiberšahs 2016”. Pasākumu apmeklēja gandrīz 600, bet pieteicās vairāk nekā 700 dalībnieki. Konference uzsāka arī Eiropas Kiberdrošības mēneša aktivitātes Latvijā. Eiropas Kiberdrošības mēneša ietvaros CERT.LV rīkoja arī Datorologa akciju, kurā visiem interesentiem bija iespēja pārbaudīt sava datora vai mobilās iekārtas “veselību”, un Mediju brokastis, kurās mediju pārstāvji tika informēti par Kiberdrošības mēneša norisi un IT drošības aktualitātēm Latvijā.

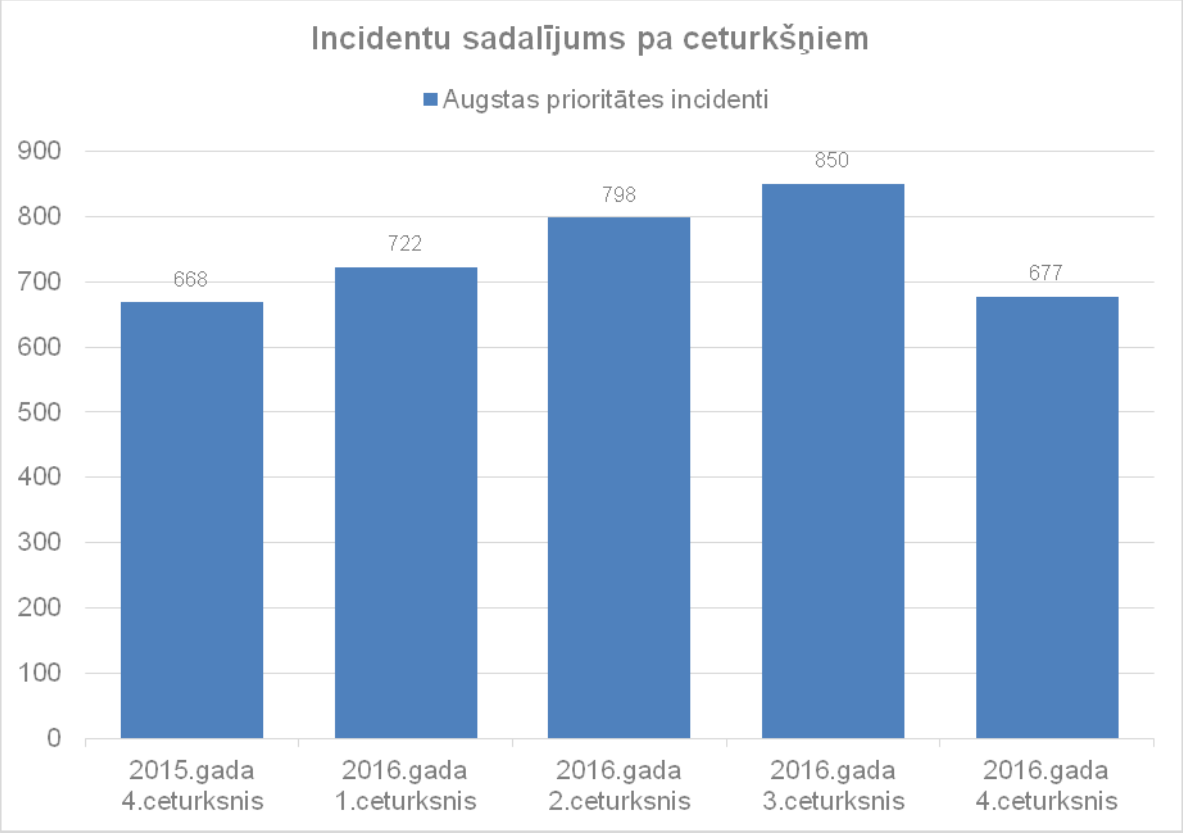
Decembrī CERT.LV sadarbībā ar Aizsardzības ministriju organizēja kiberdrošības mācības "Kiberdzirnas 2016". Tajās piedalījās valsts un pašvaldību iestāžu vadītāji un par informācijas tehnoloģiju drošību atbildīgie darbinieki no 23 institūcijām. Mācību mērķis bija veicināt institūciju vadītāju izpratni par kiberdrošības incidentiem, to iespējamām sekām, kā arī nepieciešamo rīcību kiberdrošības incidentu novēršanai.

Pārskata periodā CERT.LV par IT drošību izglītoja 3295 cilvēkus, iesaistoties 47 izglītojošos pasākumos, ievietoja 30 jaunas ziņas vietnē www.cert.lv, piedalījās 11 radio pārraidēs un 9 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

CERT.LV ik mēnesi apkopo informāciju par notikušajiem incidentiem, iedalot incidentus augstas prioritātes (visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai ko ir paziņojis cilvēks, nevis automātisks ziņotājs) un zemas prioritātes (galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūta mēstules) incidentos.

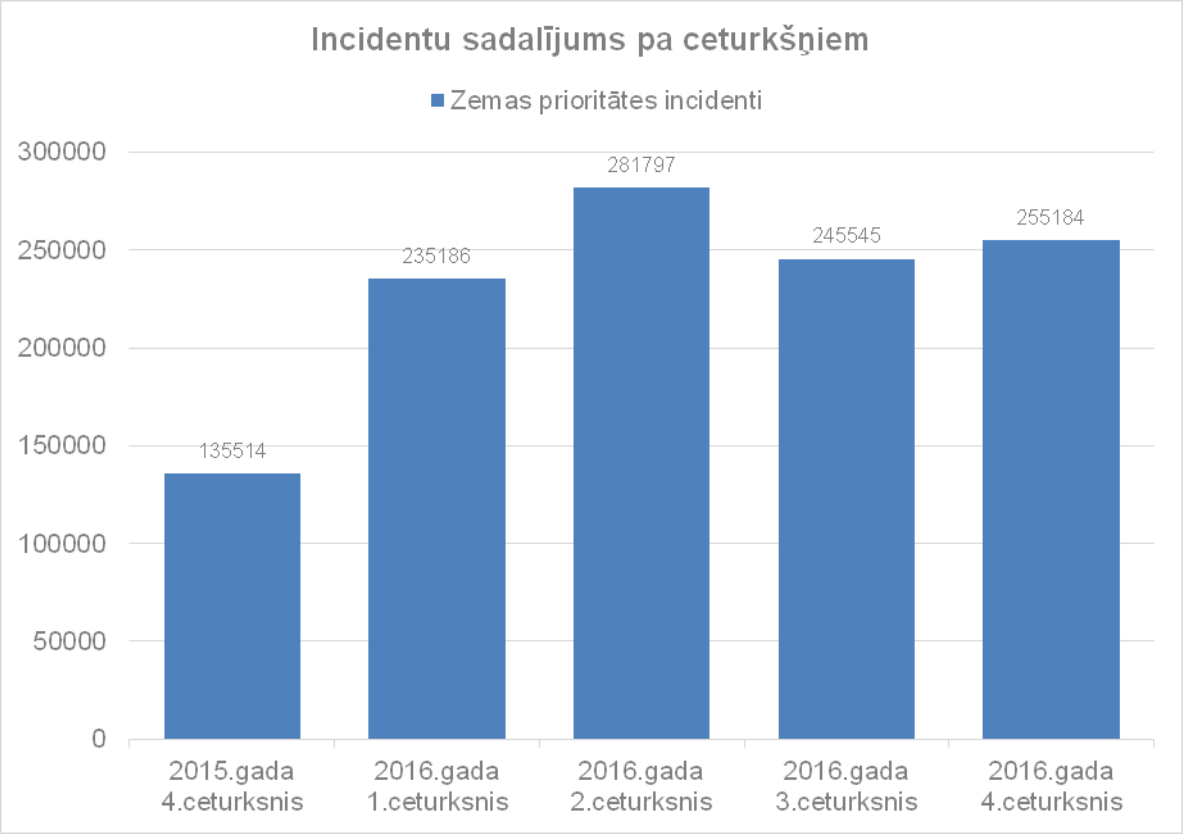
2016. gada 4. ceturksnī CERT.LV apstrādāja 677 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 850 augstas prioritātes incidenti, bet 2015. gada 4. ceturksnī 668 augstas prioritātes incidenti.



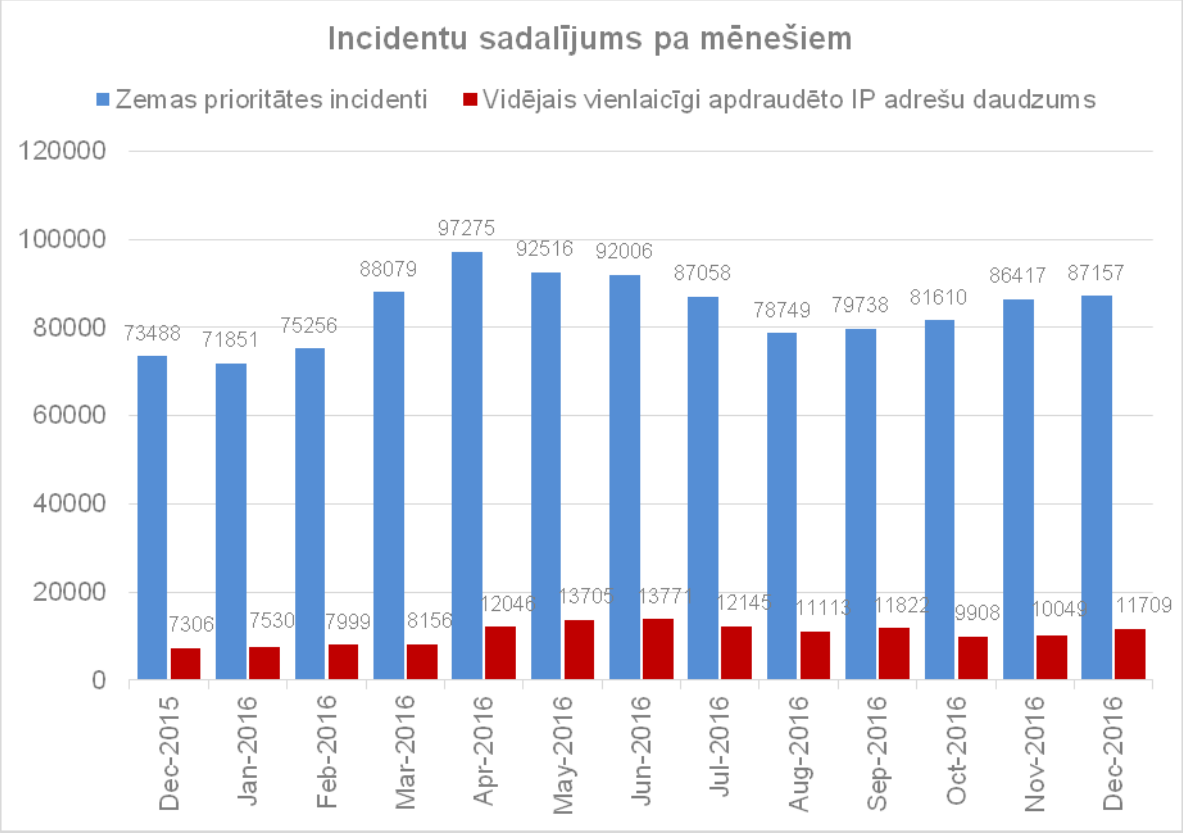
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2015. un 2016. gadā.

Pārskata periodā, neskatoties uz aktīvajām krāpniecisko e-pastu un ļaunatūras izplatīšanas kampaņām, ir vērojams kritums reģistrēto un apstrādāto augstas prioritātes incidentu apjomā, salīdzinot ar iepriekšējo pārskata periodu. To varētu skaidrot ar grūtībām savlaicīgi atklāt apkrāpšanas vai inficēšanas faktu. To, ka notikusi krāpšana vai viņu iekārta ir inficēta, incidentos iesaistītie upuri bieži konstatē tikai vairākas nedēļas vai pat mēnešus pēc incidenta, jo kibernoziedznieki prasmīgi slēpj sava nodarījuma pēdas.

2016. gada 4. ceturksnī CERT.LV reģistrēja 255 184 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 245 545 zemas prioritātes incidenti, bet 2015. gada 4. Ceturksnī 135 514 zemas prioritātes incidenti.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2015. un 2016.gadā.



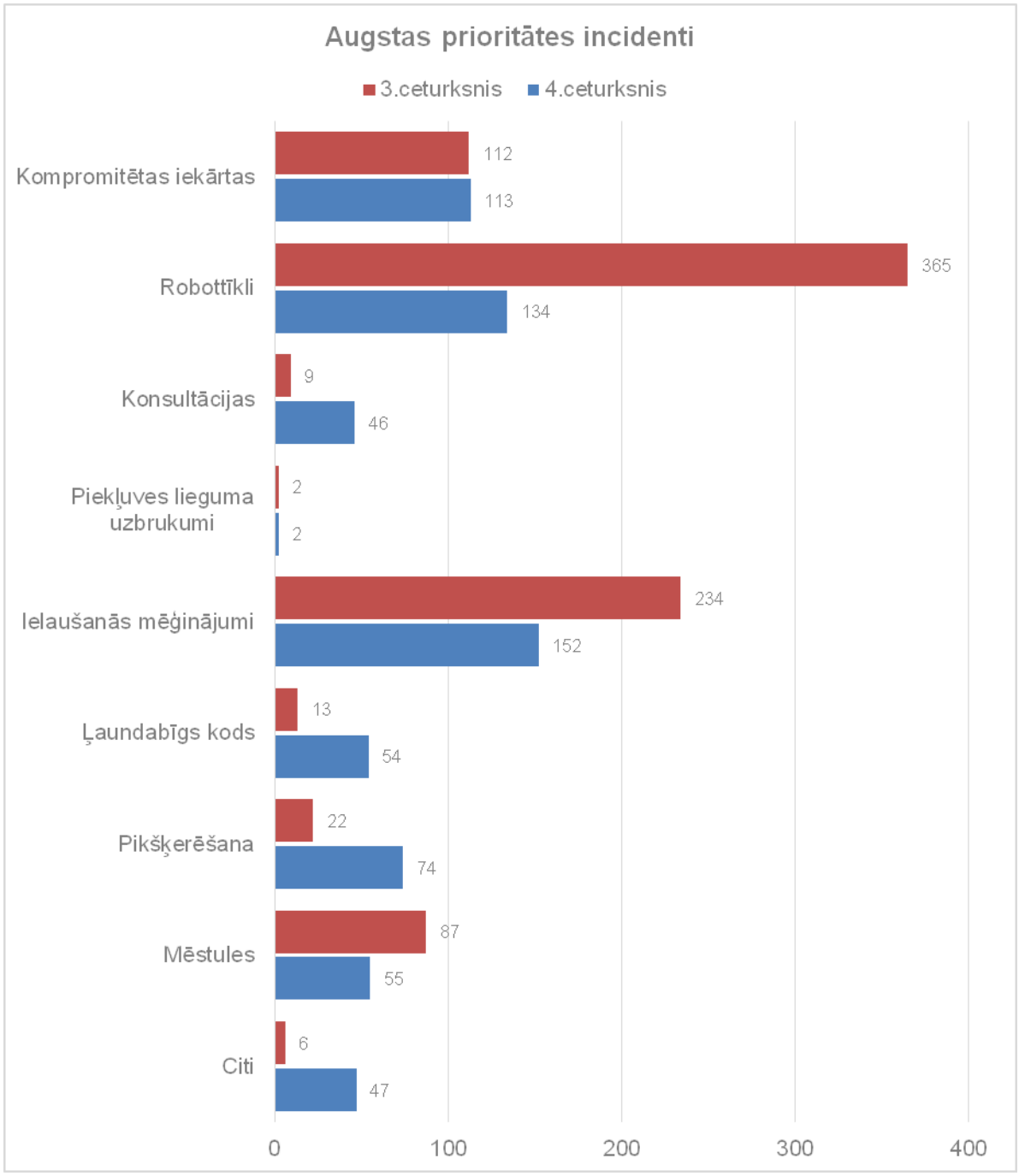
3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi apdraudēto IP adrešu daudzums 2015. un 2016. gadā.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi apdraudēto unikālo IP adrešu skaitu Latvijā, kas pārskata periodā nav būtiski mainījies, salīdzinot ar iepriekšējo pārskata periodu.

Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar IPS, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS kopskaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

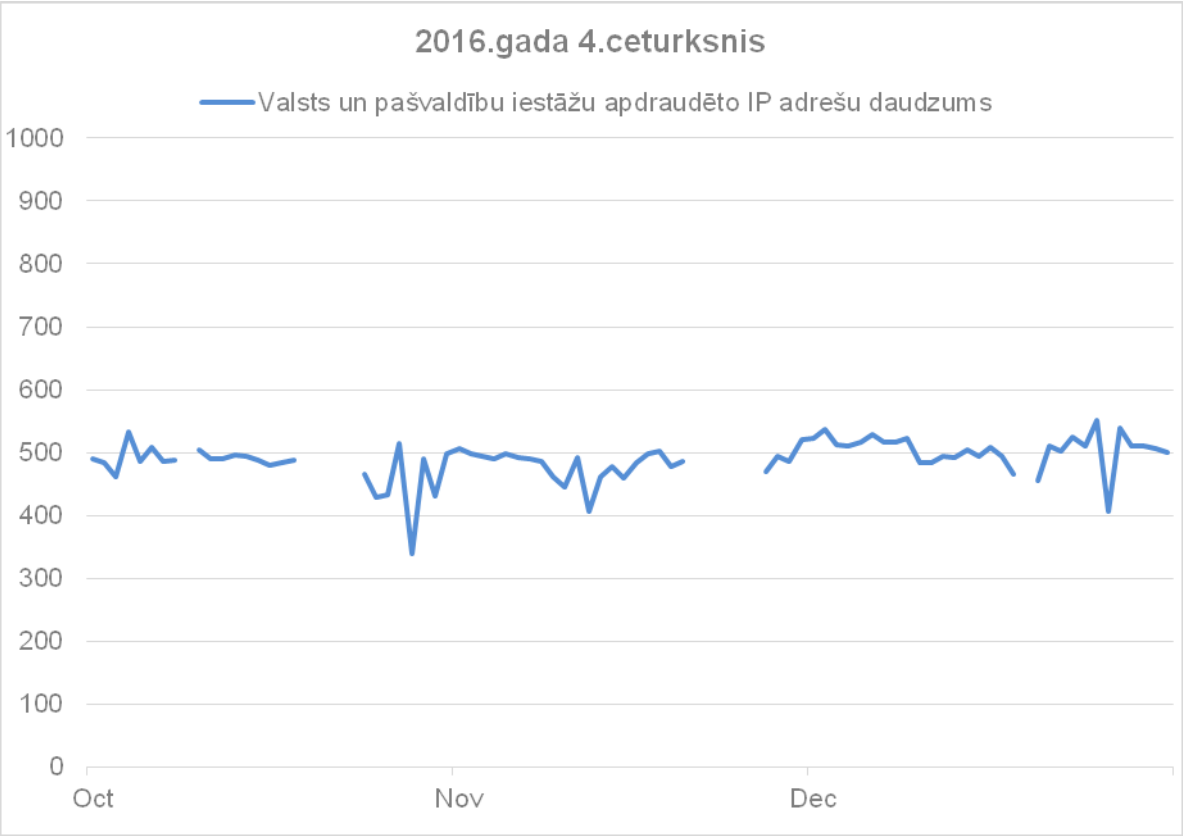
Pārskata periodā CERT.LV reģistrēja un apstrādāja 677 augstas prioritātes incidentus.



4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2016. gada 3. un 4. ceturksnī.

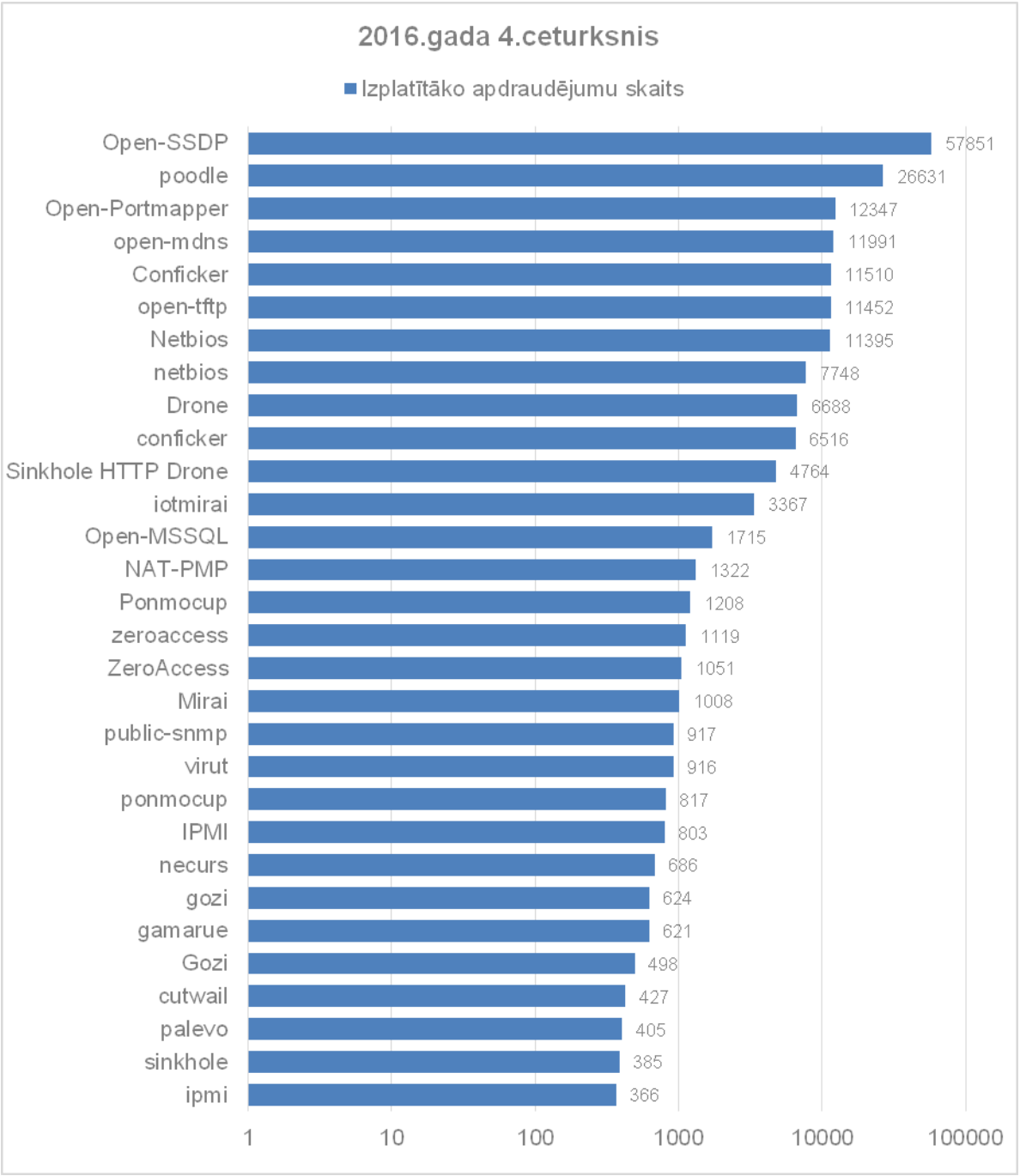
CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:



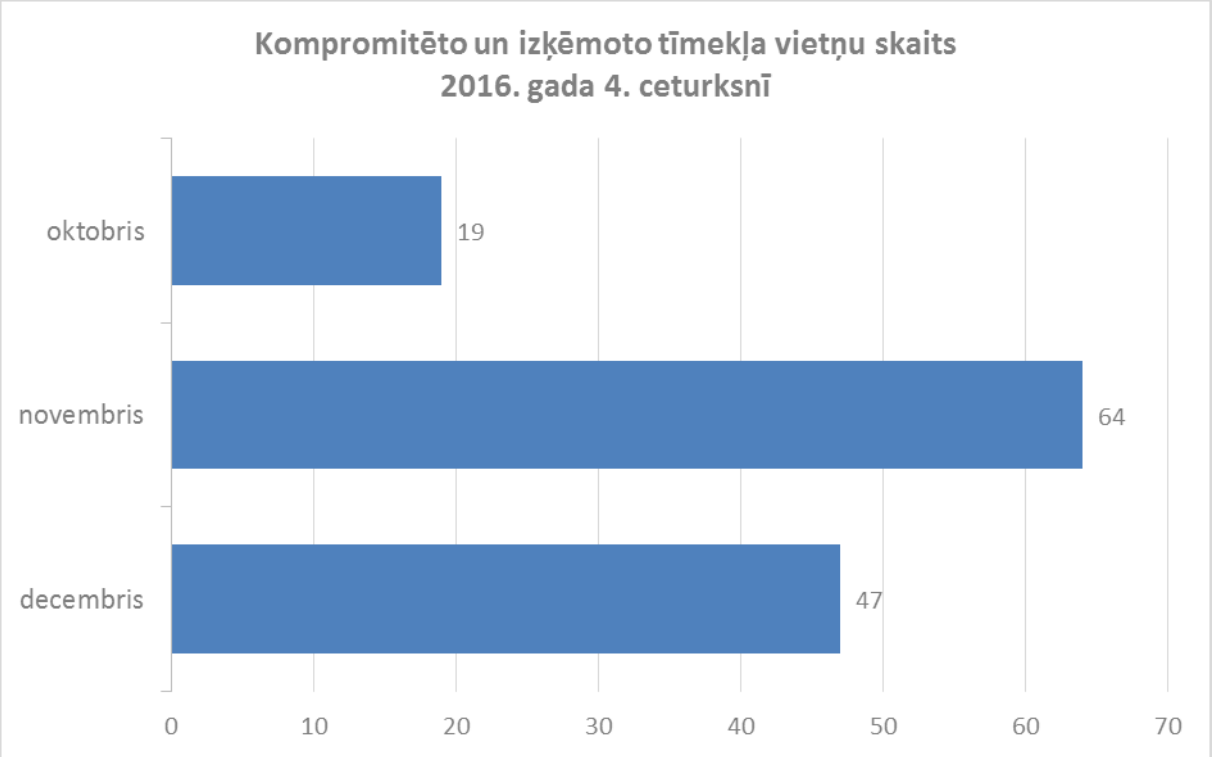
5.attēls - Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2016.gada 4.ceturksnī.

2016. gada 4. ceturksnī CERT.LV reģistrēja 255 184 zemas prioritātes incidentus.



6.attēls – CERT.LV reģistrētie zemas prioritātes incidenti no 2016. gada 1. oktobra līdz 31. decembrim pa apdraudējumu veidiem.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 130 kompromitētas un izķēmotas tīmekļa vietnes. No visām izķēmotajām vietnēm 127 gadījumos vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet 3 gadījumos Windows.



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2016. gada 4. ceturksnī.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā.

Svarīgākie CERT.LV risinātie drošības incidenti pārskata periodā:

- Pārskata periodā tika veiktas drošības pārbaudes 119 valsts un pašvaldību tīmekļa vietnēs. Būtiskas ievainojamības tika atklātas 20 valsts un pašvaldību resursos. CERT.LV informēja par ievainojamībām vietņu uzturētājus un koordinēja ievainojamību novēršanu.

  Par ievainojamībām vēl divās valsts un pašvaldību tīmekļa vietnēs CERT.LV informēja IT drošības speciālists Nils Putniņš sadarbībā ar uzņēmumu *Influent Solutions* un *Digital Security Alliance* biedrību, ievērojot atbildīgas ievainojamību atklāšanas (RDP) pamatprincipus. Apdraudējumu izdevās operatīvi novērst.

- Oktobra sākumā vairāki *Facebook* lietotāji no Latvijas kļuva par kaitīgās programmas *Slinky* upuri. Tā masveidā izplatījās, lietotājiem neapdomīgi instalējot aplikāciju, kas uzdeva sevi par profila statistikas attēlošanas rīku. Kaitīgā programma veica dažāda satura ierakstus lietotāju vārdā un nākotnē varētu tikt izmantota arī ļaunatūras izplatīšanai.

- Oktobrī tika atklāti pieci .LV domēnus izmantojoši internetveikali, kuru lapās, izmantojot populārajā interneta veikalu platformā *Magento* esošu ievainojamību, kibernoziedznieki bija ievietojuši kaitīgu kodu, kas vāca maksājuma formās ievadītos kredītkaršu datus. CERT.LV izsūtīja brīdinājumus šo resursu īpašniekiem par lapas koda atjaunināšanu. Kibernoziedznieki kopumā bija kompromitējuši vairāk kā 4900 interneta vietņu dažādās valstīs.

- 10.10. Kāda valsts iestāde saņēma e-pastu it kā pašas iestādes vārdā bez sūtījuma teksta, bet ar arhivētu (.zip) HTML failu pielikumā, kurš saturēja Cerber šifrējošo vīrusu. E-pasta filtri kaitīgo sūtījumu bloķēja.
- 18.10. Kāda uzņēmuma tīmekļa vietnē tika konstatēta nešifrēta HTTP savienojuma izmantošana lojalitātes karšu klientu informācijas pārraidē. HTTPS savienojums netika nodrošināts. Pēc CERT.LV brīdinājuma uzņēmums savu vietni salaboja, un tā tagad nodrošina šifrētu HTTPS savienojumu.
- 18.10. Tika konstatēta SQL injekcijas ievainojamība kādas valsts iestādes tīmekļa vietnē. Lapas uzturētāji tika brīdināti. Ievainojamība tika novērsta.
- 21.10. Kādai iestādei tika nosūtīta informācija par ievainojamībām viņu uzturētajā infrastruktūrā. Ziņojums par ievainojamībām tika saņemts atbildīgas ievainojamību atklāšanas procesa ietvaros. CERT.LV koordinēja ievainojamību novēršanu.
- 21.10. Lietu interneta (IoT) robotu tīkls Mirai veica masīvu DDoS uzbrukumu DNS pakalpojuma nodrošinātājam Dyn. Uzbrukums uz dažām stundām padarīja nepieejamas daudzas Dyn klientu vietnes, tādas kā Twitter, Reddit, Github, Soundcloud, Spotify u.c.

  Tiek lēsts, ka uzbrukumā piedalījās 100,000 inficētas IoT iekārtas. Latvijā tika identificēti vairāki simti iekārtu, kuras varētu būt piedalījušās šāda tipa uzbrukumos. Mirai robotu tīkls tika izveidots, pateicoties lielam skaitam nedroši konfigurētu IoT iekārtu, kurās uzbrucēji izmantoja sen zināmas ievainojamības un noklusējuma paroles.

  Eksperti uzskata, ka nākotnes DDoS uzbrukumi varētu sasniegt 10 Tb/s, kas ir pietiekami, lai spētu padarīt internetu nepieejamu kādā no valstīm.
- 24.10. Tika veikti kiberuzbrukumi divām interneta izsoļu vietnēm, iegūstot komerciāla rakstura informāciju, klientu personas un maksāšanas līdzekļu datus un informāciju par darījumu summām, kā arī izkropļojot resursu saturu, kas padarīja interneta vietnes nepieejamas. Vainīgos aizturēja Valsts policija, sadarbojoties ar CERT.LV.
- 25.10. Tika uzlauzts kādas valsts iestādes darbinieka e-pasts un no šī e-pasta izsūtītas krāpnieciskas mēstules *Apple* lietotāju datu izkrāpšanai. E-pasta uzturētājs tika brīdināts, problēma tika novērsta.
- 25.10. Kādas pašvaldības tīmekļa vietne tika uzlauzta, un tajā ievietotas saites uz ļaunatūras izplatīšanas vietnēm. CERT.LV identificēja vairākas bojātas tīmekļa vietnes sadaļas, kurās ievietots ļaundabīgs kods. Pēc CERT.LV brīdinājuma lapa tika iztīrīta, atjaunināta un pārcelta uz citu serveri.
- 27.10. Tika saņemta informācija par nešifrēta HTTP savienojuma izmantošanu klientu datu pārraidei kāda uzņēmuma vietnē. CERT.LV brīdināja vietnes uzturētāju. Pēc brīdinājuma HTTPS savienojums tika nodrošināts.
- 29.10. Uzbrucēji izķēmoja divu valsts iestāžu mājaslapas. Izmantojot SQL injekcijas, tajās tika ievietoti politiski motivēti paziņojumi arābu valodā. Abas lapas bija izvietotas vienā koplietošanas serverī. Citas šajā serverī esošās lapas izķēmotas netika. Lapu saturs tika atjaunots no rezerves kopijām.

- 31.10. Virkne .lv tīmekļa vietņu tika iesaistītas uz apmeklētāju ierīcēm vērstos uzbrukumos, izplatot *FakejQuery* trojāni. Vietnes tika uzturētas uz novecojušām satura vadības sistēmu (*Joomla*, *Wordpress*, *Drupal*) versijām un bija ērti izmantojamas kā platforma uzbrukumiem. CERT.LV apzināja inficētās vietnes un koordinēja incidentu risināšanu.
- 01.11. CERT.LV saņēma ziņu par veiksmīgu šifrējošā izspiedējvīrusa uzbrukumu kādā valsts iestādē. Darbiniekam, atverot e-pasta pielikumā esošo arhīva (.zip) failu, kas saturēja Windows skripta failu (.wsf), vīruss nošifrēja visus dokumentus uz lokālās darbstacijas un daļu dokumentu uz darbstacijai pievienotā failservera. Vīrusu izdevās apturēt, atslēdzot darbstaciju no tīkla. Faili tika atjaunoti no rezerves kopijām. Šis incidents saistīts ar vairākas dienas aktīvo *Locky* saimes izspiedējvīrusu izplatīšanas kampaņu.
- 09.11. Tika uzlauzta kādas valsts iestādes tīmekļa vietne. Lapā tika nesankcionēti nomainīts saturs, izmantojot ievainojamības novecojušā satura vadības sistēmas *Joomla* versijā. CERT.LV brīdināja uzturētājus, lapa tika salabota.
- 09.11. CERT.LV saņēma informāciju par viltus loteriju, kas tika nesankcionēti rīkota it kā kādas bankas vārdā izlozējot mobilo telefonu, un bija paredzēta bankas lietotāju datu izkrāpšanai. CERT.LV nav informācijas, ka kāds lietotājs būtu šajā incidentā cietis. CERT.LV sazinājās ar vietnes uzturētājiem un kaitīgais saturs no vietnes tika izņemts.
- 10.11. Masveidā tika izsūtītas vēstules latviešu valodā par it kā nesamaksātu parādu. Pielikumos esošie faili saturēja datorvīrusu, kas paredzēts informācijas zagšanai un finanšu transakciju pārtveršanai no inficētā datora. Uzbrucēju sagatavotais kods tika izplatīts .zip arhīva pielikumos ar .wsf (Windows Script File) instrukcijām. CERT.LV ieteica ierobežot šādu failu piegādes, atvēršanas un izpildīšanas iespējas.
- 11.11. CERT.LV saņēma vairākus ziņojumus par krāpšanas mēģinājumiem, kuros no uzņēmumiem mēģināja izkrāpt naudu ar uzņēmuma vadītāja vārdā sūtītu viltotu e-pastu. Krāpnieki pirms tam veikuši rūpīgu uzņēmumu mājas lapu izpēti, lai noskaidrotu uzņēmuma struktūru, uzņēmuma vadītāju, vadītāja e-pastu un uzņēmuma grāmatvedi, kuram adresēt viltoto sūtījumu. Lai attaisnotu kļūdaini sagatavoto tekstu, krāpnieki aizbildinājās ar bojātu klaviatūru. CERT.LV aicina būt uzmanīgiem un rūpīgi izvērtēt saņemtos e-pastus pirms tiek veiktas jebkādas finansiālas darbības. Ja e-pasti ir neprofesionāli sagatavoti, tajos ir steidzamības vai slepenības aspekts, drošāk ir veikt telefona zvanu un pārliecināties, vai šāds e-pasts tiešām ir sūtīts.
- 11.11. Sniegta konsultācija kādai valsts iestādei par mājas lapas drošības aspektiem un to, kā izvērtēt izstrādātāju un viņu piedāvāto satura vadības sistēmu atbilstību konkursa nolikumam.
- 16.11. Tika saņemts ziņojums par viltus tīmekļa vietni. Vietne nesankcionēti tika izveidota kādas kompānijas vārdā. Uzņēmumam savas tīmekļa vietnes nav, tas izmanto tikai e-pastu, tāpēc uzņēmuma pārstāvis vērsās policijā ar aizdomām par iespējamu viltus lapas izmantošanu “CEO krāpšanā”. CERT.LV ieteica uzņēmumam brīdināt savus klientus, ka jebkādus e-pastus tā vārdā, kuros pieprasīts mainīt maksājuma saņēmēja kontu, nepieciešams papildus pārbaudīt, sazinoties ar uzņēmumu pa telefonu.

- 21.11. Pret kāda uzņēmuma datortīklu no 20. līdz 21. novembrim tika veikts apjomīgs DDoS uzbrukums, kurš tika ierobežots, atslēdzot uzņēmuma tīklu no ārzemju interneta. Uzbrukuma organizatori sazinājušies ar uzņēmuma vadību un izteikuši vēlmi iegūt kontroli pār uzņēmuma daļām. Uzņēmums atteicās ar viņiem komunicēt, taču atkārtoti DDoS uzbrukumi uzņēmumam nesekoja.
- 23.11. Kāds lietotājs, atsaucoties uz Facebook pamanītu reklāmu, samaksāja vairāk kā 100 EUR viltotā e-veikalā www.canadagoosemallhut.com. Veikals no kredītkartes noņēma ne tikai summu par nepiegādāto preci, bet arī vairāk kā 15EUR dažādas papildu „komisijas" maksas. Krāpnieciskā vietne tika slēgta. Apkrāptajam pircējam CERT.LV ieteica sazināties ar savas kredītkartes izdevējbanku, lai risinātu naudas atgūšanas jautājumus.
- 29.11. Kāda Latvijas uzņēmuma tīmekļa vietnē tika uzturēta pikšķerēšanas lapa, kas bija domāta kādas Brazīlijas bankas lietotāju datu izkrāpšanai. Kaitīgā lapa tika izvietota, izmantojot ievainojamības satura vadības sistēmā. Lapa bija sasniedzama tikai no Brazīlijas IP adresēm. Pēc CERT.LV brīdinājuma lapas uzturētājs to slēdza.
- 29.11. Kādas valsts iestādes darbiniekam tika atsūtīts e-pasts par rēķinu. E-pasta pielikums saturēja MS Excel failu ar Macro komandu, kas pēc atvēršanas datorā lejuplādē šifrējošo vīrusu *Locky*. Darbinieks tika brīdināts par kaitīgo saturu. Vīruss netika aktivizēts.
- 29.11. Kādas tīmekļa vietnes uzturētāji savā Facebook kontā saņēma vēstuli, kurā pieprasīti 400 USD un draudēts dzēst viņu mājas lapu, ja nauda netiks samaksāta. Uzbrucējs, nesaņemot prasīto summu, lapu tiešām izdzēsa. Lapa tika atjaunota no rezerves kopijām un uzlabota to uzturošā servera drošība. Dati par šo izspiešanas mēģinājumu nodoti policijai.
- 30.11. Izmantojot viltus rēķinus, kādam uzņēmumam tika izkrāpti vairāki maksājumi. Krāpnieki izmantoja *backdoor* vienā no uzņēmuma datoriem un pieslēdzās uzņēmuma e-pastam. Informācija par krāpniecību nodota policijai.
- 01.12. Tika konstatētas nesankcionētas satura izmaiņas kādas valsts iestādes tīmekļa vietnē. Izmaiņu veikšana bija iespējama arī neautorizētam lietotājam, ja tika veikta labošanas rīkjoslas izsaukšana. Lapas uzturētāji veica izmaiņas piekļuves tiesībās un novērsa atklāto drošības caurumu.
- 02.12. Kāda Latvijas tīmekļa vietne tika izmantota šifrējošā datorvīrusa izplatīšanā. Kaitīgi e-pasti ar saiti uz šo tīmekļa vietni tika izsūtīti Zviedrijas datorlietotājiem. Vīruss interneta vietnē tika ievietots, izmantojot ievainojamības novecojušā satura vadības sistēmas *Joomla* versijā. CERT.LV sazinājās ar vietnes īpašnieku, kas slēdza vietnei piesaistīto domēnu, kuru neplānoja turpmāk izmantot.
- 05.12. Mobilās aplikācijas Watsapp lietotāju vidū tika izplatīta saite uz viltus loteriju www.faceb00ks.com/laimesrats. Ja lietotājs izvēlējās iesaistīties piedāvātajās aktivitātēs, viņam tika paziņots, ka ir laimēts un nepieciešams ievadīt tālruņa numuru laimesta saņemšanai. Ievadot tālruņa numuru un neizlasot atrunu zem ievades lauka, lietotājs veica reģistrēšanos maksas pakalpojumam.
- 06.12. Tika sašifrēts kādas valsts iestādes darbinieka dators. Darbinieks atvēra inficētu e-pastu ar augstas ticamības saturu no reāli eksistējošas e-pasta adreses, kas

tika sūtīts, izmantojot eksistējošu pasta grupu. Dators bija pieslēgts pie bezvadu tīkla, kurš bija izolēts no lokālā datortīkla, rezultātā citi datori netika ietekmēti.

- 12.12. Tika atklāta drošības nepilnība kādas valsts iestādes informācijas sistēmā. Nepilnība noteiktos apstākļos ļāva autentificētam lietotājam piekļūt citu lietotāju parolēm. Nepilnību atklāja iestādes par IT drošību atbildīgā persona. Tika veikta nepilnības novēršana un visu sistēmas lietotāju paroļu maiņa.
- 15.12. Tika saņemta informācija no vairākām valsts iestādēm un organizācijām par personalizētiem krāpnieciskiem e-pastiem, kas iestādes vadītāja vārdā tika nosūtīti iestādes grāmatvedim un aicināja veikt steidzamu maksājumu 11 985 EUR apmērā uz Lielbritāniju.
- 15.12. Tika saņemta informācija no kādas valsts iestādes par intensīviem atkārtotiem mēģinājumiem iesūtīt sistēmā šifrējošo vīrusu *Locky*. Iesūtīšanas mēģinājumi bijuši neveiksmīgi. Tos bloķēja izmantotais ugunsmūra risinājums.
- 20.12. DoS uzbrukuma rezultātā tika traucēta kāda portāla darbība. Incidenta analīzes rezultātā tika konstatēts, ka resursu pārslodzi radīja ievainojamību skenera izmantošana no kaitnieciskas IP adreses. CERT.LV ieteica uzlabot portāla aizsardzību, lai šādu skeneru izmantošana no vienas IP adreses neradītu DoS situācijas.
- 30.12. Saņemts ziņojums no kādas valsts iestādes par vairākiem simtiem atkārtotu mēģinājumu no vienas IP adreses veikt kaitniecisku informācijas ievadi tīmekļa vietnes ievades laukos. Uzbrukumu mēģinājumi bijuši neveiksmīgi. Par incidentu informēta Valsts policija.

CERT.LV pasākumi incidentu novēršanai:

- 06.12. CERT.LV izsūtīja informāciju valsts un pašvaldību iestādēm par *Android* mobilo iekārtu analīzes rezultātā atklāto nedrošo iekārtu sarakstu un apdraudējumu specifiku.
- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās iknedēļas ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

3. Mobilo ierīču ļaunatūras pētniecība.

Mobilā ļaunatūra kļūst arvien aktuālāks apdraudējums. Par to liecina gan CERT.LV saņemtie ziņojumi, gan sabiedrības un mediju interese par mobilo ierīču drošības jautājumiem, gan arvien pieaugošais mobilo ierīču skaits, kas pie CERT.LV speciālistiem nonāk Datorologa akciju laikā.

Līdz šim CERT.LV eksperti saskārušies tikai ar tādu mobilo ļaunatūru, kas nav specifiska Latvijai, bet tas ir tikai laika jautājums, līdz parādīsies arī mobilā ļaunatūra, kas tiks mērķēta tieši uz Latvijas mobilo iekārtu lietotājiem. Lai pilnvērtīgi sagatavotos jaunās mobilās ļaunatūras analīzei, CERT.LV turpina darbu pie laboratorijas veidošanas un ļaunatūras analizēšanas.

Pārskata periodā CERT.LV saņēma vairākus lūgumus izvērtēt atsevišķu mobilo aplikāciju lietošanas drošību. CERT.LV sniedza ieteikumus par drošu aplikāciju izvēli, lejupielādi un lietošanu.

Biežākie mobilie apdraudējumi pārskata periodā bija lietotāju saņemti paziņojumi par it kā konstatētām problēmām mobilajā iekārtā, kuru risināšanai lietotājam tiek piedāvāts lejupielādēt kādu mobilo lietotni, kura, ja lejupielādēta no oficiālā PlayStore, var aprobežoties tikai ar reklāmu rādīšanu, bet, ielādēta no neoficiālām tīmekļa vietnēm, var nodarīt būtisku kaitējumu iekārtas un datu drošībai.

Papildu apdraudējums pārskata periodā bija lietotāju apkrāpšana ar paaugstinātas maksas pakalpojumu starpniecību. Lietotāji saņēma paziņojumus par laimestu loterijā vai ziņojumu par it kā konstatētu infekciju viņu mobilajā iekārtā, un tika aicināti sūtīt īsziņu (SMS), lai pieteiktos laimestam vai lejupielādētu antivīrusu, bet, neiepazīstoties ar pakalpojuma nosacījumiem, veica paaugstinātas maksas pakalpojuma abonēšanu.

4. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību).

Informācija par CERT.LV sadarbību ar medijiem

26. oktobrī Eiropas Kiberdrošības mēneša ietvaros CERT.LV organizēja Mediju brokastis, kurās mediju pārstāvji tika informēti par Kiberdrošības mēneša norisi un IT drošības aktualitātēm Latvijā.

1) **Intervijas un ziņas radio:**
   - 10.10. komentārs MixFM radio par Aizsardzības ministrijas ieviesto fakultatīvo padziļināto IT nodarbību programmu skolās
   - 19.10. intervija LR4 ziņām par Datorologa akciju un biežāk pieļautajām lietotāju kļūdām
   - 24.10. komentārs LR1 raidījumā "Kā labāk dzīvot" par to, kā darbiniekiem pašiem nekļūt par "algotiem" hakeriem un neapdraudēt uzņēmumu?
   - 26.10. komentārs LR1 ziņām par Kiberdrošības mēnesi un IT drošības aktualitātēm
   - 27.10. intervija LR4 raidījumam "Doma laukums" par DSS konferenci un IT drošības situāciju Latvijā
   - 28.10. intervija LR1 raidījumam "Aktuāli" par IT drošības situāciju un aktuālākajiem apdraudējumiem
   - 29.10. telefonintervija Latvijas Radio par portatīvo datoru webkameru aizlīmēšanas pamatotību
   - 07.11. komentārs LR1 raidījumam "Pēcpusdiena" par aktuālākajiem IT drošības apdraudējumiem valsts un pašvaldību iestādēs
   - 30.11. komentārs LR4 ziņām par e-veselības projektu un tā drošību
   - 09.12. komentārs LR1 ziņām par kaitnieciskiem e-pastiem un krāpšanām pirmssvētku laikā
   - 16.12. intervija LR4 raidījumam "Doma laukums" par lietu interneta veiktajiem uzbrukumiem un krāpnieciskajiem e-pastiem, kas mērķēti uz grāmatvežiem

2) **Sižeti televīzijā, tiešraides:**
   - 12.10. intervija LTV7 ziņām par jaunsardzes ieceri apmācīt jauniešus par "baltajiem" hakeriem
   - 19.10. telefonintervija LTV raidījumam "Rīta panorāma" par Eiropas Kiberdrošības mēnesi un Datorologa akciju
   - 26.10. intervija TV3 par uzlauztām videokamerām un atbildīgu ievainojamību atklāšanu
   - 27.10. intervija LTV raidījumam "Panorāma" par iekārtu ērtumu un drošības aspektu trūkumiem
   - 06.11. sižets TV3 ziņās par IT drošību valsts un pašvaldību iestādēs
   - 27.11. komentārs TV3 raidījumam "Nekā personīga" par ķīnā ražotu iekārtu – telefonu un novērošanas kameru – drošības nepilnībām
   - 15.12. intervija LNT raidījumam "900 sekundes" par gada aktualitātēm un svarīgākajiem apdraudējumiem pirmssvētku periodā

- 16.12. intervija TV3 ziņām par lietu internetu (IoT) un tā drošības aspektiem
- 21.12. komentārs TV3 ziņām par policijas izmeklēto kiberuzbrukumu diviem interneta izsoļu namiem

3) Informācija par CERT.LV tīmekļa vietnēm:

Pārskata periodā vietnē https://www.cert.lv publicētas 30 ziņas. Populārākā bija ziņa ar uzaicinājumu pieteikties IT drošības seminārам "Esi drošs", kurai ir 1487 unikāli skatījumi. Otra populārākā bija ziņa bija par konferenci "Kiberšahs", kuru skatījuši 1437 unikāli apmeklētāji. Trešā populārākā bija Kontaktu sadaļa ar 1218 unikāliem skatījumiem. Kopā CERT.LV mājaslapai bijuši 17,084 lapu skatījumi, kurus veido 9,805 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 12,725 apmeklējumi, no tiem 10,271 unikāli apmeklējumi.

CERT.LV turpina tulkot un portālā www.esidross.lv publicēt OUCH! ikmēneša izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts). Pārskata periodā publicēti 3 jauni OUCH! numuri.

Portālā esidross.lv publicētie raksti:

- Četri soļi drošībai
- Lekciju kursa "Kibernoziedznieku vēsture" video (3. daļa)
- Lekciju kursa "Kibernoziedznieku vēsture" video (4. daļa)
- Ļaunprogrammatūras izplatās mobilajās ierīcēs. Pasargā mobilās ierīces no kibernoziedzniekiem!
- Mākoņa droša izmantošana
- Lekciju kursa "Kibernoziedznieku vēsture" video (5. daļa)Droša atbrīvošanās no mobilās iekārtas

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1615.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 473.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 68.
- Sociālajā tīklā Google+ https://www.google.com/+CertLv ir 26 sekotāji.

Pēdējos divos ceturkšņos stabili pieaug sekotāju skaits populārajās sociālo tīklu platformās Twitter un Facebook, taču www.draugiem.lv un Google+ tas saglabājas nemainīgs.

5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

4. oktobrī CERT.LV pārstāvis piedalījās Digitālās drošības alianses (DDA) rīkotajā preses konferencē, ar kuru tika uzsākta kampaņa “Mirklis pirms klik”, kas tika vērsta uz uzņēmējiem ar mērķi veicināt darbinieku izglītošanu par digitālās drošības jautājumiem.

6. oktobrī notika gada lielākais IT drošībai veltītais pasākums Latvijā - CERT.LV un ISACA Latvijas nodaļas ikgadējā konference “Kiberšahs 2016”. Pasākumu apmeklēja gandrīz 600, bet pieteikušies bija vairāk nekā 700 dalībnieki. Konference uzsāka arī Eiropas Kiberdrošības mēneša aktivitātes Latvijā.

19. oktobrī Eiropas Kiberdrošības mēneša ietvaros noritēja kārtējā CERT.LV organizētā Datorologa akcija, kuras laikā jebkurš interesents varēja atnest savu datoru, planšetdatoru vai viedtālruni uz bezmaksas pārbaudi pie Datorologa – datordrošības speciālista – un “izārstēt”, ja tas būtu nepieciešams, kā arī saņemt konsultāciju par drošu interneta lietošanu. Drošības ekspertiem no CERT.LV pievienojās arī eksperti no SIA "Stream Networks" un SIA "Lattelecom". SIA "Lattelecom" ir to interneta pakalpojumu sniedzēju vidū, kas ieguvuši arī kvalitātes zīmi "Atbildīgs interneta pakalpojumu sniedzējs”.

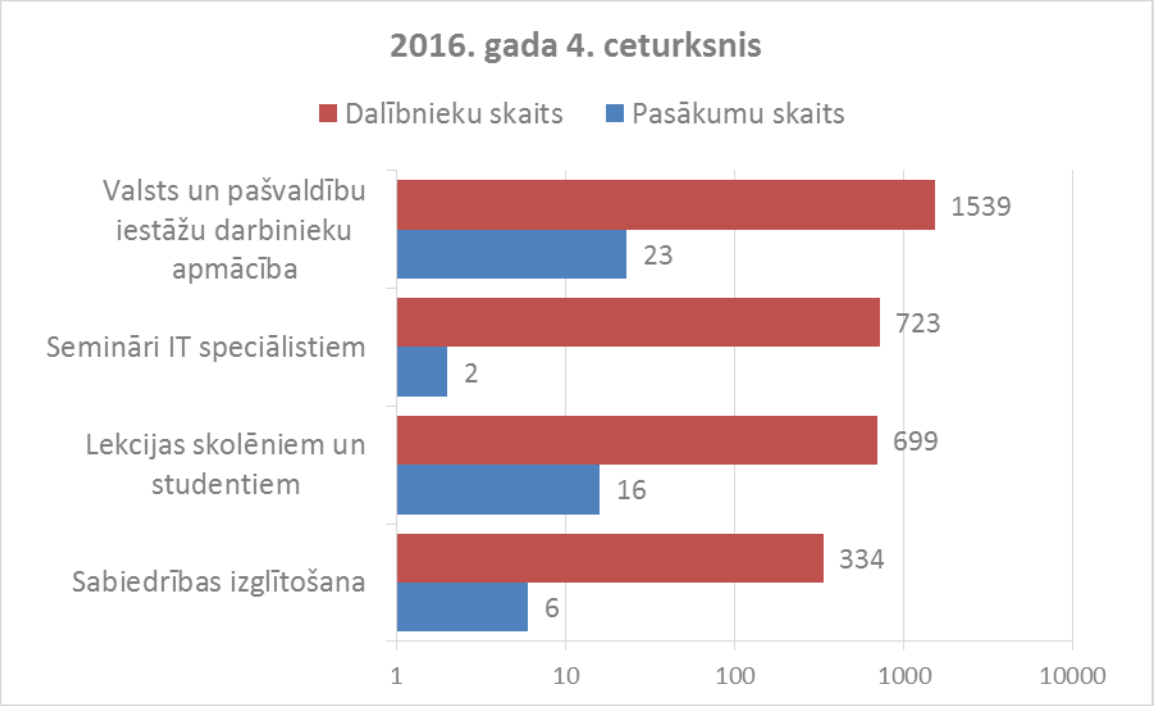
27. oktobrī CERT.LV pārstāvji uzstājās ar prezentācijām "IoT security driven by hacker & cybercrime community" un "Responsible disclosure process – Latvian approach" konferencē “DSS ITSEC 2016”.

24. novembrī CERT.LV pārstāvis piedalījās videomateriāla filmēšanā "Amigo iniciatīvas laimīgām ģimenēm" video cikla "Kā būt par vecāku 21.gadsimtā?" ietvaros, stāstot par drošu informācijas un komunikāciju tehnoloģiju lietošanu.

1. decembrī CERT.LV pārstāvis piedalījās LIKTA organizētajā konferencē un e-komercijas sesijā sniedza atbildes uz jautājumiem, kas saistīti ar IT drošību.

8. decembrī CERT.LV sadarbībā ar Aizsardzības ministriju organizēja kiberdrošības mācības "Kiberdzirnas 2016", kurās piedalījās valsts un pašvaldību iestāžu vadītāji un par informācijas tehnoloģiju drošību atbildīgie darbinieki no 23 institūcijām. Mācību mērķis bija veicināt institūciju vadītāju izpratni par kiberdrošības incidentiem, to iespējamām sekām, kā arī nepieciešamo rīcību kiberdrošības incidentu novēršanai.

Pārskata periodā CERT.LV par IT drošību izglītoja 3295 cilvēkus, iesaistoties 47 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2016. gada 4. ceturksnī.

6. *Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā.*

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 05.10. Tikšanās ar Kiberaizsardzības vienību par sadarbību.
- 13.10. DEG sanāksme.
- 18.10. Ministru kabineta sēde par grozījumiem Informācijas tehnoloģiju drošības likumā un Krimināllikumā.
- 28.10. Tikšanās Aizsardzības ministrijā par Kiberjaunsardzes projektu.
- 01.11. Tikšanās Aizsardzības ministrijā par IT drošības mācībām "Kiberdzirnas 2016".
- 01.11. Tikšanās Aizsardzības ministrijā par MK noteikumu nr. 442 ieviešanu.
- 11.11. un 16.11. Tikšanās Aizsardzības ministrijā par izmaiņām IT drošības likumā saistībā ar atbildīgu ievainojamību atklāšanu.
- 08.12. DEG sanāksme.

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2. punktā.

7. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu.

IT drošības likums nosaka, ka valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. CERT.LV ir izstrādājis rīcības plāna paraugu, lai palīdzētu mazajiem ESK izveidot savus plānus, un izsūtījis informāciju par šo paraugu tiem ESK, kuri līdz šim nav izstrādājuši un iesnieguši CERT.LV rīcības plānu elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.

Uz pārskata perioda beigām informācija ir saņemta no 64 ESK. 59 ESK ir iesnieguši rīcības plānu, bet 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no tiem 1 ESK nodevis visu ārpakalpojumā citam ESK.

Viens no ESK oktobrī iesniedza atjaunotu rīcības plānu. Nākamajā pārskata periodā plānots izsūtīt atgādinājumu visiem ESK par nepieciešamību veikt rīcības plānu atjaunošanu.

Pārskata periodā CERT.LV nav saņēmis nevienu ziņojumu no ESK par drošības vai integritātes pārkāpumiem, kas būtiski ietekmējuši elektronisko sakaru tīkla darbību vai pakalpojumu sniegšanu un atbilst Informācijas tehnoloģiju drošības likuma (ITDL) 9.panta pirmās daļas 2.punktam.).

Pārskata periodā CERT.LV nav konstatējis apdraudējumus, kuru atrisināšanai būtu nepieciešams slēgt galalietotājam piekļuvi elektronisko sakaru tīklam (ITDL 9.panta pirmās daļas 5.punkts).

Attiecībā uz ITDL 6^1 panta izpildi, pārskata periodā nav saņemts neviens ziņojums.

8. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

Oktobra sākumā kopā ar pārējiem mācību dalībniekiem notika intensīvi sagatavošanās darbi ENISA organizētajām IT drošības mācībām "Cyber Europe 2016". Mācības notika 13.-14. oktobrī. Latvijas pusē tās koordinēja CERT.LV. Mācību norise vērtējama kā veiksmīga, iespējami uzlabojumi sadarbībā starp valsts un privāto sektoru.

Pārskata periodā tika uzsākta arī gatavošanās NATO organizētajām kiberdrošības mācībām "Locked Shields" un "Crossed Swords", kā arī notika dalība mācībās "Cyber Coalition".

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 06.10. IT drošības mācību "Cyber Europe 2016" komunikāciju pārbaude;
- 12.10. Gala pārbaudes pirms IT drošības mācībām "Cyber Europe 2016";
- 13.-14.10. Starptautiskās IT drošības mācības "Cyber Europe 2016";
- 02.-04.11. Sadarbības tikšanās Prāgā ar Čehijas valdības CERT vienību;
- 08.-10.11. CERT.LV pārstāvis piedalās "3rd Informal CSIRT Network Meeting" Hāgā, Nīderlandē;
- 09.-11.11. un 16.-18.11. CERT.LV pārstāvis piedalījās Clarified security organizētajās mācībās "Web Application Security";
- 14.-25.11. CERT.LV sadarbības vizīte pie Polijas CERT Polska;
- 20.-23.11. CERT.LV pārstāvji piedalās GEANT rīkotajos TRANSITS kursos Prāgā un CERT.LV pārstāvis pasniedz vienu no kursa moduļiem ("*Operational module*");
- 24.-27.11. CERT.LV pārstāvis piedalījās ar prezentāciju "*IOT insecurity and important role of Responsible Vulnerability Disclosure Policy - real life experience and lessons learned during vulnerability resolution coordination with Chinese CERTs and Vendors*" IT drošības ekspertu sanāksmē "4GH" Nīderlandē;
- 28.11.-02.12. CERT.LV pārstāvis piedalījās ar prezentāciju "*CERT.LV activities, role in Latvia and globally*" ENISA un International Telecommunication Union (ITU) rīkotajā pasākumā "ITU-ENISA Regional Cybersecurity Forum", kas notika Sofijā, Bulgārijā;
- 28.11. – 03.12. CERT.LV sadarbībā ar MilCERT un Kiberaizsardzības vienību piedalījās NATO kiberdrošības mācībās "Cyber Coalition 2016";
- 28.11.-03.12. CERT.LV pārstāvis piedalījās NATO CCDCOE organizētajos kursos "International Law of Cyber Operations" Tallinā, Igaunijā;
- 05.-09.12. CERT.LV pārstāvis piedalās MISP kursos Cīrihē, Šveicē;
- 12.12. Telekonference ar projektu "CyberGreen" par sadarbību;
- 27.-31.12. CERT.LV pārstāvji piedalās CCC (Chaos Computer Club) organizētajā "33C3" konferencē Hamburgā, Vācijā.
  Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 13.10. CERT.LV pārstāvis sniedza interviju LU studentam bakalaura darba izstrādei par kibernoziegumiem no kriminoloģijas skatupunkta, aplūkojot sarežģītākās problēmām, ar kurām nākas saskarties, pildot darba pienākumus;
- 01.12. CERT.LV pārstāvis sniedza interviju LU studentei kursa darba izstrādei par personas datu drošību un aizsardzību.

10. Ar Elektroniskās identifikācijas uzraudzību saistīto pienākumu izpilde.

Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums "Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību noteikto'' CERT.LV ir uzsācis noteikto funkciju veikšanu.

Iepriekšminēto funkciju izpildei veikto darbu uzskaitījums:

- CERT.LV pārstāvēja elektroniskās identifikācijas uzraudzības komiteju Eiropas Komisijas rīkotajā seminārā *„eIDAS Trust Services: 6 months on after the switch over*" par uzticamības pakalpojumiem eIDAS regulas kontekstā;
- CERT.LV pārstāvis piedalījās ENISA izveidotās darba grupas, kas saistīta ar informācijas un komunikācijas tehnoloģiju produktu sertifikācijas vadlīniju izstrādes jautājumiem ES līmenī, virtuālajās sanāksmēs, kā arī pēc saskaņošanas ar Aizsardzības ministriju sniedza Latvijas redzējumu par minētajiem jautājumiem;
- CERT.LV pārstāvji iesaistījās Fizisko personu elektroniskās identifikācijas likumā noteikto Ministru kabineta noteikumu izstrādes procesā, tehnisko un organizatorisko prasību definēšanā kvalificētiem un kvalificētiem paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzējiem;
- CERT.LV pārstāvji piedalījās LVRTC organizētā sanāksmē par iespējamajiem riskiem, kas rastos, ja sertificēts uzticamības pakalpojumu sniedzējs pārtrauktu savu darbību. Ar Ministru kabineta sēdes protokollēmumu Elektroniskās identifikācijas uzraudzības komitejai uzdots izveidot un sešu mēnešu laikā no nolikuma apstiprināšanas iesniegt Ministru kabinetā informatīvo ziņojumu par minēto jautājumu;
- CERT.LV pārstāvji savas kompetences ietvaros asistēja Datu valsts inspekcijas atbildīgajiem darbiniekiem Latvijas uzticamības saraksta (*LV Trust List*) aktualizācijā un publicēšanā;
- CERT.LV rīkotajā seminārā "Esi drošs" CERT.LV pārstāvis sniedza prezentāciju par Elektroniskās identifikācijas komiteju, tās mērķiem un uzdevumiem, kā arī saistošo Latvijas un Eiropas Savienības likumdošanu elektroniskās identifikācijas un uzticamības pakalpojumu jomā;

- Sanāksmē ar Latvijas Nacionālā akreditācijas biroja (LATAK) pārstāvjiem sniedza savu redzējumu par atbildības sadalījumu kvalificētu elektroniskās identifikācijas un sertificētu uzticamības pakalpojumu sniedzēju uzraudzībā.

11. Papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas Interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2016. līdz 31.12.2016. ir saņēmusi un izvērtējusi 128 ziņojumus. No tiem 37 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 25 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 16 ziņojumos konstatēta personas goda un cieņas aizskaršana un 4 ziņojumos konstatēta naida kurināšana un rasisms. Par finanšu krāpšanas mēģinājumiem internetā saņemti 9 ziņojumi, 8 ziņojuma saturs nav bijis pretlikumīgs, 29 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 4 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 33 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

2017. gada 16. februārī
Sagatavotājs – Līga Besere
Tālrunis: 67085888
E-pasts: liga.besere@cert.lv