Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) paveikto 2012.gada 4.ceturksnī

(2012.gada 1.oktobris – 2012.gada 31.decembris)

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

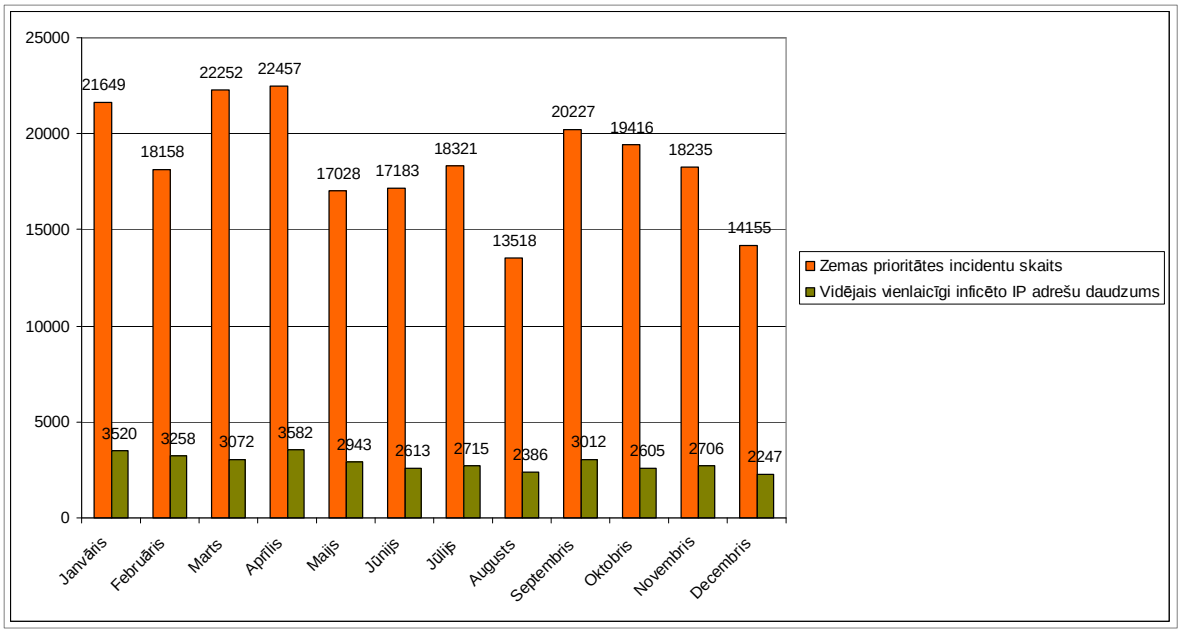
1. Uzdevums: **Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.**

2012.gada ceturtajā ceturksnī CERT.LV novēroja gan dažādus augstas bīstamības incidentus, gan arī lielu skaitu zemas prioritātes incidentu, kur datori bija inficēti ar dažādiem vīrusiem un bija kļuvuši par robotu tīklu (*botnet*) sastāvdaļām. Robotu tīkli joprojām ir visizplatītākā problēma ne tikai Latvijā, bet arī visā pasaulē. No augstas prioritātes incidentiem CERT.LV turpina izmeklēt Latvijā izvietotos robotu tīklu komandu un kontroles centrus.

Pārskata perioda laikā Latvijā ievērojami aktivizējās tā saucamais „Policijas vīruss", kas nobloķē lietotāja datoru un it kā policijas vārdā liek maksāt naudu. Vairāki desmiti lietotāju ir krituši par šī vīrusa upuri un samaksājuši pieprasītās summas. Kopējais inficēto lietotāju skaits ir vēl daudz lielāks un mērāms vairākos simtos. Aktuāla bijusi arī mājas lapu izķēmošana, gada beigās šo incidentu skaits ir ievērojami pieaudzis. Uzbrukumi mājas lapām tika veikti kampaņveidā. Šie uzbrukumu viļņi lielos apjomos skāra populāras, atvērtā koda satura rediģēšanas sistēmas "WordPress" un "Joomla", kuras lietotāji bija atstājuši novārtā, nesekojot līdzi atjauninājumiem. No uzbrukumiem cieta arī citi tiešsaistes projekti, kur uzbrukuma vektors galvenokārt ir bijis SQL injekcija, neatbilstoša konfigurācija un nepiemērota paroļu izvēle.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto IP adrešu skaitu Latvijā. Oktobrī šis skaits ir bijis 2605, novembrī – 2706, decembrī - 2247. Liela daļa no šiem datoriem ir dažādu robotu tīklu sastāvdaļas.

1.diagrammā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2012.gada laikā.



1.diagramma – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2012.gadā.

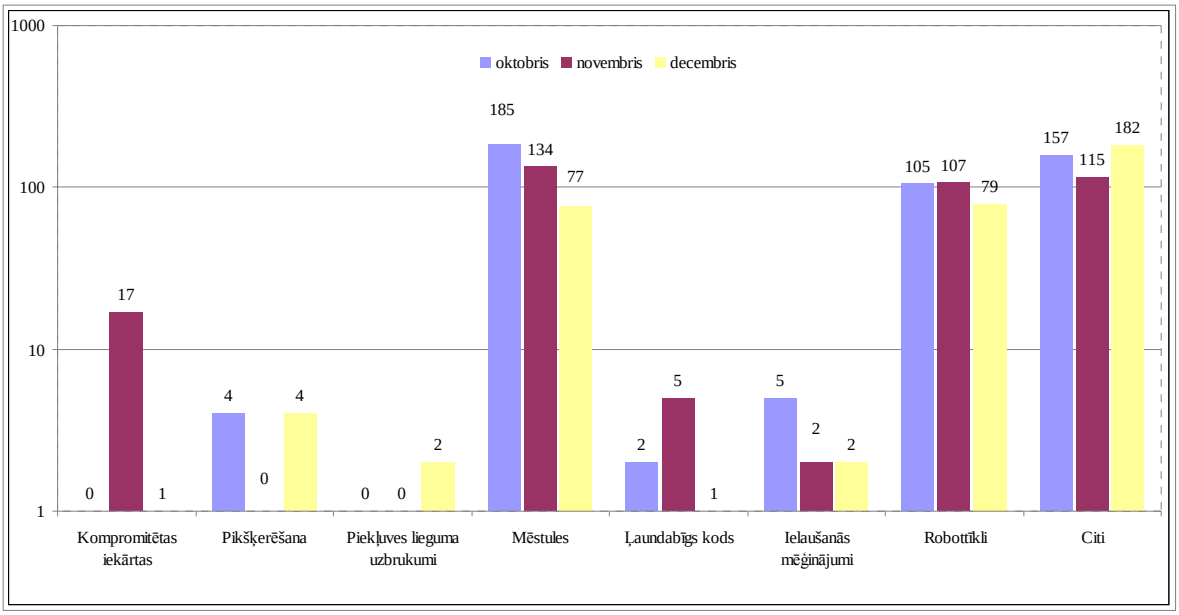
Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar tiem elektronisko sakaru pakalpojumu komersantiem (turpmāk - ESK), kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Memorands paredz, ka ESK sadarbojas ar CERT.LV un informē gala lietotājus par to, ka viņu datori ir inficēti ar kādu no datorvīrusiem un/vai kļuvuši par robotu tīklu sastāvdaļu, kā arī, sadarbībā ar Net-Safe Latvia Drošāka interneta centru, nodrošina iespējami ātru nelegālā satura izņemšanu no publiskas aprites internetā. Šīs iniciatīvas atklāšanas pasākums notika 2012.gada 30.oktobrī, līdz pārskata perioda beigām iniciatīvai ir pievienojušies 11 ESK, vēl 4 gatavojas parakstīt saprašanās memorandu. Tikai aktīvi iesaistot ESK ir iespējams uzlabot kopējo situāciju valstī.

Atbildīgie IPS 2012.gada beigās:
LU aģentūra "LU Matemātikas un informātikas institūts" SigmaNet datu centrs un akadēmiskais tīkls, SIA IZZI, SIA LATNET Serviss, SIA Datu tehnoloģiju grupa, SIA Interneta pasaule, SIA SPX, SIA ILVA Ltd., Latvijas Universitāte (LANET), SIA Versija, SIA Garm Technologies, SIA Compitex.

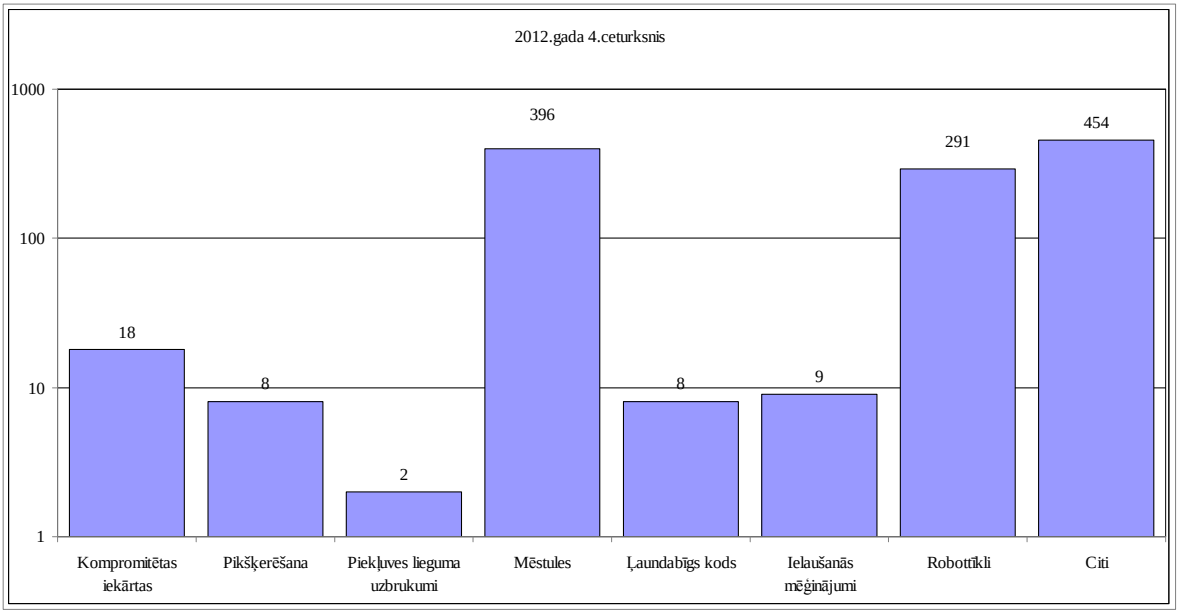
2. Uzdevums: **Sniegt atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinēt to novēršanu.**

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis **1186** augstas prioritātes incidentus un reģistrējis **64944** zemas prioritātes incidentus, par daļu no kuriem ESK ir informējis savus gala lietotājus.

2.diagrammā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (diagrammas ir logaritmiskā mērogā). 3.diagrammā redzams augstas prioritātes incidentu kopskaits pārskata periodā.

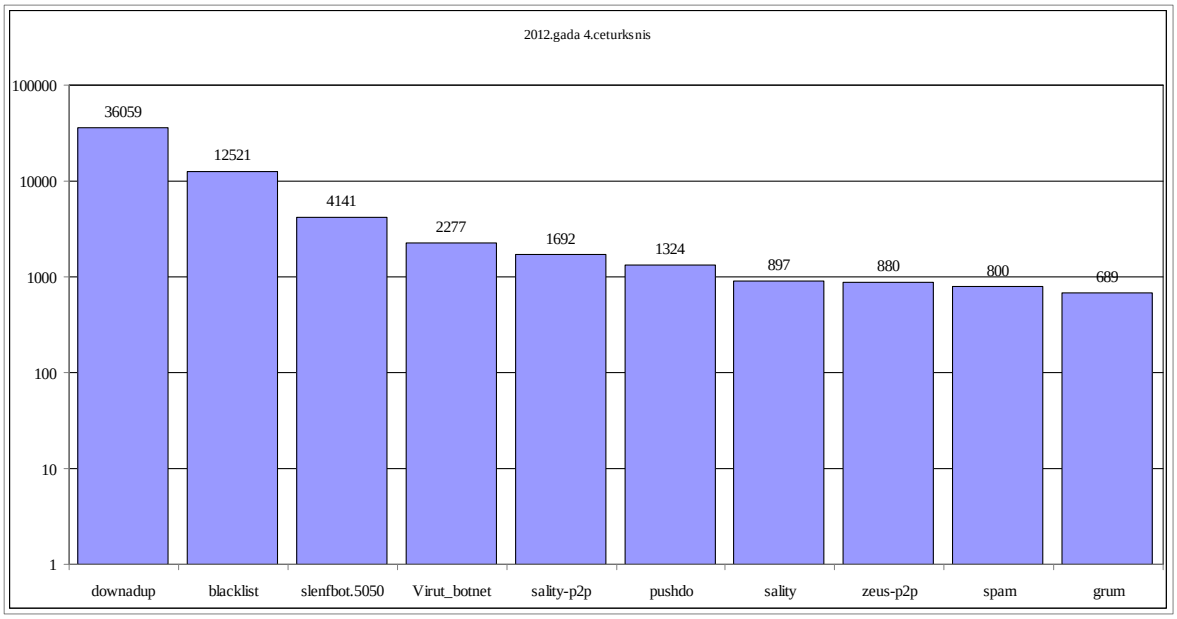


2.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



3.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2012.gada 1.oktobra līdz 31.decembrim.

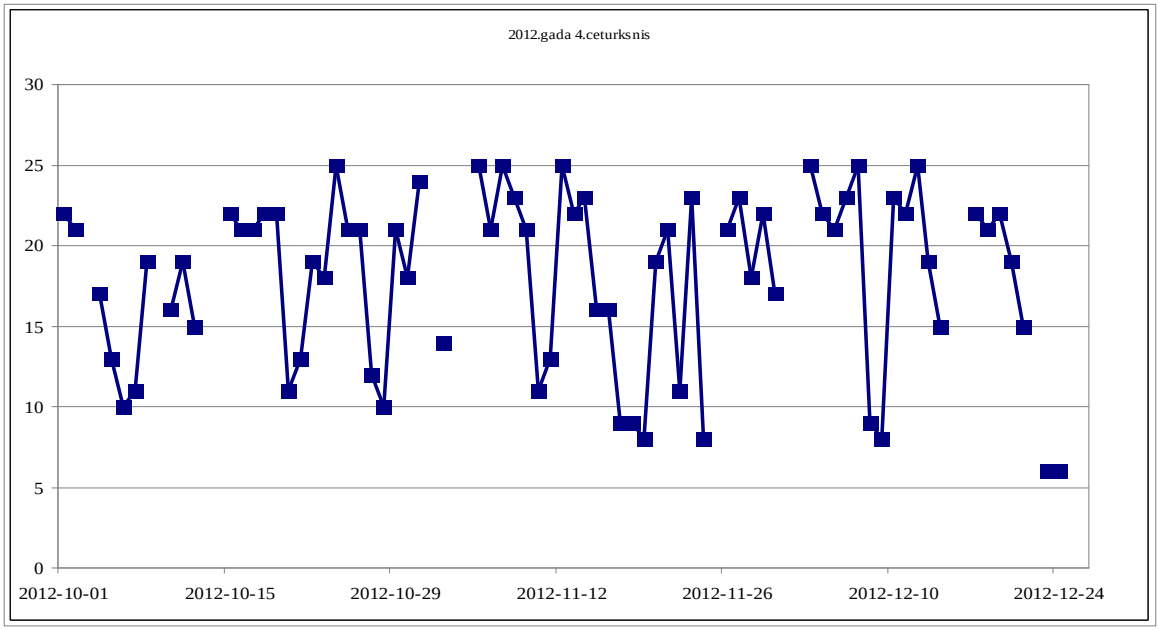
4.diagrammā redzami CERT.LV reģistrētie zemas prioritātes incidenti, to sadalījums pa infekciju tipiem – 10 populārākās infekcijas (kopā tiek apkopota informācija par 57 dažādām infekcijām).



4.diagramma – CERT.LV reģistrētie zemas prioritātes incidenti – 10 populārākās infekcijas.

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.

5.diagrammā ir redzams, cik inficētu valsts un pašvaldību institūciju IP adreses bijušas katras dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem.



5.diagramma – Valsts un pašvaldību institūciju IP adrešu skaits, kas reģistrētas pārskata perioda incidentu ziņojumos.

Pārskata perioda laikā CERT.LV ir sadarbojies ar dažādām valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem, kā arī citām organizācijām konkrētu, dažādas bīstamības incidentu risināšanā. Zemāk aprakstīti daži incidentu piemēri anonimizētā veidā

- Oktobra sākumā CERT.LV saņēma pirmās ziņas par lokalizētu „Policijas vīrusa" versiju, kas izmanto Latvijas Valsts policijas simboliku. Mēneša laikā tika konstatēti daudzi inficēšanās gadījumi, CERT.LV sagatavoja un publicēja brīdinājumus, kā arī instrukcijas par to, kā no šī vīrusa atbrīvoties. Daudziem vīrusa upuriem tika sniegtas telefoniskas konsultācijas. Šī vīrusa aktivitāte saglabājās un palielinājās visa pārskata perioda laikā. Īpaši liela aktivitāte un jaunas šī vīrusa versijas tika novērotas decembra otrajā pusē, kad būtiski pieauga arī vīrusa upuru telefonzvani CERT.LV diennakts palīdzības dienestam.
- CERT.LV konstatēja mēģinājumus izkrāpt Facebook kontu informāciju, viltotās vēstules teksts bija noformēts samērā labā latviešu valodā un domāts latviešu auditorijai.
- Pēc Patērētāju tiesību aizsardzības centra lūguma CERT.LV sazinājās ar mājas lapu uzturētājiem, pie kuriem izvietota finanšu piramīdas MMM-2012 lapas, un lūdza tās slēgt.
- CERT.LV konstatēja kāda novada pašvaldības mājas lapas izķēmošanas faktu un par to brīdināja pašvaldību. Lapa tika salabota. Izķēmošana notika, izmantojot kompromitētu legāla lietotāja kontu, kura parole tika nozagta ar vīrusa palīdzību.
- Kādas pašvaldības mājas lapa vairākas stundas nebija pieejama. Problēmas cēlonis - konfigurācijas kļūda jaunajā lapas aizsardzības programmā. Pēc CERT.LV brīdinājuma tika sākta lapas atjaunošana.
- CERT.LV panāca Latvijā izvietoto ZEUS un SpyEye komandu un kontroles centra atslēgšanu.
- Kādas bankas speciālisti konstatēja uzbrukuma mēģinājumus no Norvēģijas IP adrešu apgabalā esošas IP adreses. Pēc papildus izpētes tika konstatēts, ka tiek veikts saskaņots ievainojamību testēšanas (*penetration testing)* mēģinājums, par kuru nebija informēti visu līmeņu darbinieki. Šis incidents ir uzskatāms arī par sekmīgu modrības testu bankas darbiniekiem.
- Pret CERT.LV mājas lapu tika veikts piekļuves atteices uzbrukums. Ar dažādu intensitāti tas turpinājās vairākas dienas.
- CERT.LV saņēma incidenta ziņojumu par privātas kompānijas mājas lapas uzlaušanu un tās resursu izmantošanu viltotas ING SWE Belgium intrnetbankas uzturēšanai ar mērķi izkrāpt bankas klientu autentifikācijas datus. Kaitīgais saturs tika padarīts nepieejams. Kompānijas mājas lapa tika kompromitēta, uzbrucējam uzminot FTP servisa paroli, kas bija izvēlēta neatbilstoši vāja.
- CERT.LV saņēma incidenta pieteikumu no kādas valsts iestādes par notiekošu uzbrukumu e-pasta serverim no IP adreses Francijā. Uzbrukuma mērķis bija piemeklēt autentifikācijas kombinācijas iestādes darbinieku e-pasta kontiem. Atbildīgā persona veica nepieciešamās darbības uzbrukuma atvairīšanai. CERT.LV sazinājās ar Francijas CERT komandu. . Iesaistītās valsts iestādes pārstāvis ir informēts par nepieciešamajām darbībām turpmākai lietas virzīšanai, atbilstoši Francijas likumdošanai.
- Oktobra otrajā pusē tika konstatēta jauna „Policijas vīrusa" latviskā versija. CERT.LV atjaunoja aprakstus par datoru „ārstēšanu" no šī vīrusa.
- CERT.LV NetFlow datu analīzes rezultātā konstatēja no interneta rekursīvi pieejamu DNS serveri kādas valsts iestādes tīklā, kam, iespējams, veikts uzbrukums. Par incidentu tika informēta iestādes atbildīgā persona. Trūkumi tika novērsti nekavējoties.

- Oktobrī CERT.LV, sadarbojoties ar mitināšanas (*hosting*) pakalpojumu sniedzēju, strādāja pie ZEUS robotu tīkla komandu un kontroles centra identificēšanas. CERT.LV saņēma robotu tīklu kontrolējošā servera datus analīzei. Kontrlocentra darbība ir apturēta.
- CERT.LV saņēma incidenta ziņojumu par uzbrukuma mēģinājumiem kādas universitātes resursiem. Uzbrukumā iesaistītās IP adreses ir apzinātas un informētas atbilstošās ārvalstu CERT komandas. Uzbrukumā iesaistītās mašīnas ir robotu tīkla sastāvdaļa.
- Oktobrī CERT.LV veica atkārtotus drošības testus vairākām valsts iestāžu mājas lapām, kas iepriekš identificētas kā ievainojamas. Trīs gadījumos trūkumi joprojām nebija novērsti un, izmantojot atklātās ievainojamības, bija iespējams iegūt kontroli pār failu sistēmu, kā arī iespēju izķēmot mājas lapu, vai izgūt visu informāciju no tās datu bāzēm. CERT.LV sagatavoja un nosūtīja oficiālas vēstules attiecīgo iestāžu vadītājiem.
- CERT.LV saņēma brīdinājumu par datorvīrusa izplatīšanu no kādas tīmekļa lapas Latvijā. Tika brīdinātas atbildīgās personas, lapa tika salabota. Jau ilgstoši ir novērojama tendence, kad uzlauztās lapas, piekļuve serveriem un to resursiem tiek pārdotas. Vēlāk tās izmanto citi kibernoziedznieki ļaunatūras izplatīšanas kampaņās.
- CERT.LV palīdzēja mājas lapu izstrādātājam atrast ievainojamības Joomla! CMS lapās, kas tika izmantotas, lai tajās ievietotu kaitīgu kodu datorvīrusu izplatīšanai.
- CERT.LV sniedza skaidrojumus par kādas lapas nepieejamības gadījumiem.
- CERT.LV saņēma ziņojumu par aizdomām, ka pret kādas valsts iestādes mājas lapas serveri tiek veikts DDoS uzbrukums. Tika sniegta palīdzība žurnālfailu izpētē un tika atrasti neparastās aktivitātes cēloņi.
- Kādai pašvaldībai tika sniegta konsultācija IT drošības politikas dokumentu uzlabošanai.
- Tika konstatēts personas datu izkrāpšanas mēģinājums, izmantojot viltotu "Draugiem.lv" darba piedāvājumu lapu. CERT.LV iesaistījās incidenta risināšanā.
- CERT.LV sniedza palīdzību interneta krāpšanas upurim, kas tika apkrāpts, izmantojot sludinājumus ss.lv.
- Tika saņemts ziņojums par DDoS uzbrukumu kādai mājas lapai. Lai atvairītu uzbrukumu, IT speciālisti veica mājas lapas pārcelšanu. Tā kā DNS ieraksti netika savlaicīgi sagatavoti un domēna DNS ierakstiem bija noteikts ilgstošs derīguma laiks, kas traucēja ātri nomainīt atbildīgos DNS un WWW serverus, traucējumi mājas lapas darbībā turpinājās arī pēc tam, kad DDoS uzbrukumi bija beigušies. CERT.LV palīdzēja sakārtot DNS ierakstus, lai atjaunotu normālu sistēmu darbību.
- CERT.LV palīdzēja iespējama SMS krāpniecības mēģinājuma izmeklēšanā, organizējot sadarbību divu Latvijas banku starpā.
- Tika sniegta konsultācija personai, kuras dati izkrāpti ar "Nigērijas vēstuļu" shēmas palīdzību. Savus finanšu līdzekļus persona nebija vēl zaudējusi.
- Decembra otrajā pusē tika novēroti masveida uzbrukumi Latvijas tiešsaistes lapām, kuras tiek uzturētas uz Joomla! satura rediģēšanas sistēmas. Uzbrukumu intensitāte pieaug un turpinās arī 2013.gada janvārī. CERT.LV veica uzbrukumu analīzi un publicēja rekomendācijas publiskos resursos, kā arī sagatavoja preses relīzi medijiem. Vairāk informācijas par šo uzbrukumu kampaņu iespējams atrast CERT.LV mājas lapā: https://cert.lv/resource/show/290

- Tika saņemts ziņojums no kādas ārzemju CSIRT komandas par vairākiem Latvijas datoriem, kas iesaistīti DDoS uzbrukumā. CERT.LV brīdināja šo serveru uzturētājus un palīdzēja novērst sekas.
- Notika masveida mājas lapu izķēmošanas gadījumi, kuros cieta arī kādas valsts iestādes lapa, CERT.LV palīdzēja novērst incidentu.

Cita veida sadarbība ar dažādām iestādēm ir norādīta pie 8.punkta.

CERT.LV ir sācis uzskaitīt arī uzlauzto un izķēmoto mājas lapu gadījumus. Šādu gadījumu skaits oktobrī bija 30, novembrī – 104, decembrī – 91. Vairāk nekā 90% no visiem uzlauztajiem serveriem darbojas uz Linux/Unix platformām.

Oktobrī tika pabeigta ievainojamo DNS serveru turētāju apziņošana. 60% problēmas bija novērsuši. Ievainojamie DNS serveri valstī tika apzināti NIC.LV un CERT.LV kopīgi veiktā, apjomīgā pētījumā.

Pārskata periodā CERT.LV testēja zemas-mijiedarbes urķuslazda (low-interaction Honeypot) risinājumus, lai izvēlētos piemērotāko Latvijas apstākļiem.

3. Uzdevums: **Uzturēt sabiedrībai pieejamā veidā atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu.**

CERT.LV tīmekļa vietnē tiek publicēta gan informācija par jaunākajām ievainojamībām un vīrusiem, gan arī cita informācija par aktuāliem notikumiem un apdraudējumiem. Pārskata periodā vispopulārākā bija lapa par jaunākajām ievainojamībām un vīrusiem, tai seko CERT.LV sagatavota informācija par „Policijas vīrusa" apkarošanas praksi un mehānismiem. Kopā CERT.LV mājas lapai bijuši 16838 apmeklējumi, 12313 unikāli apmeklējumi no 61 valsts. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 92,56 % apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 42 ziņas un preses relīzes, publiskais darbības pārskats par 2012.gada 3.ceturksni, kā arī informācija par dažādiem pasākumiem, publikācijām un citiem notikumiem.

CERT.LV ir divi Twitter konti un tajos tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv un http://twitter.com/datorologs. Pārskata perioda laikā certlv kontā tika publicētas 116 ziņas, kontam pievienojušies 75 jauni sekotāji un 115 reizes certlv ziņa ir tikusi „retvītota" jeb padota tālāk. Datorologs kontā pārskata periodā tika publicētas 11 ziņas, kontam pievienojās 25 jauni sekotāji un 3 reizes datorologs ziņas ir padotas tālāk.

CERT.LV uztur arī pieaugušo izglītošanas portālu http://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 12 jauni raksti, portālu apmeklējuši 17320 (12456 unikāli) apmeklētāji. Publicētie raksti:

1. "Kāds piekļuvis manam e-pastam!"
2. "Privātā dzīve internetā"
3. Pārpublicēts raksts no laacz.lv "Paroļu nebūšanas jeb nomaini savu paroli. Tagad."

4. "Rīks IDRE (Informācijas Drošības Risku Eksperts)"
5. "Bloķētu datoru glābšana un portatīvie antivīrusi"
6. "Robotu tīkls jeb „zombiju armija”"
7. "Drošība par velti. Rakstu grupa par risinājumiem"
8. "iPhone drošība"
9. "Smilšu kaste jeb buferzona"
10. "Backup jeb datu rezerves kopijas"
11. "Antivīruss avast! Free Antivirus"
12. „Datu drošība uzņēmumā”.

Pārskata periodā bijušas arī uzstāšanās televīzijā un radio, dažādas publikācijas presē un portālos. Sīkāka informācija:

1) Publikācijas presē:
   - 10.oktobris - intervija ar laikraksta "Diena" žurnālistu par datu noplūdes iespējām no Gmail kontiem;

2) Intervijas un ziņas radio:
   - 23.oktobris - CERT.LV uzstājās Latvijas radio 1 ar 3 minūšu sižetu par „Policijas vīrusu”;
   - 29.oktobris - CERT.LV piedalījās Latvijas radio 1 raidījumā „Zināmais nezināmajā”, lai pastāstītu gan par iniciatīvu „Atbildīgs Interneta pakalpojumu sniedzējs”, gan arī par datoru inficēšanas veidiem un aktuālo „Policijas vīrusu”;
   - 27.decembris – ziņa Latvijas radio portālā un ziņu izlaidumos par „Policijas vīrusa” jaunāko versiju „Latvijā datorus brīvdienās bloķējis "Policijas vīruss"”;

3) Sižeti televīzijā:
   - 2.novembris - CERT.LV pārstāvis piedalījās Latvijas televīzijas raidījumā „Labrīt, Latvija!”, kur atbildēja uz jautājumiem par IT drošības situāciju Latvijā, stāstīja par to, kā pasargāt datoru no inficēšanās un informēja par „Policijas vīrusu”;
   - 28.novembris - CERT.LV pārstāvis piedalījās TV5 raidījumā „Kriminal+” un sniedza informāciju par „Policijas vīrusu”;
   - 14.decembris - CERT.LV pārstāvis piedalījās TV3 sižetā par „Hackfest Valmiera 2012” un IT drošību raidījumā „Bez tabu”;

4) Ziņas portālos:
   - 7.decembris – raksts par Ministru kabineta IT vingrinājumu „Ministru kabinetā simulē IT traģēdiju” Dienas Bizness portālā db.lv;
   - 11.decembris – raksts par drošāku pirmssvētku iepirkšanos internetā „Pārāk vilinoši piedāvājumi internetā visticamāk ir krāpšana” portālā TVnet;
   - 11.decembris – raksts par drošāku pirmssvētku iepirkšanos internetā „Ja piedāvājums šķiet neticami labs, tad, visdrīzāk, tā ir krāpšana” portālā Apollo;
   - 27.decembris – raksts par jaunāko „Policijas vīrusa” versiju „Brīvdienās plosījies "Policijas vīruss"” portālā Apollo;
   - 27.decembris – raksts par jaunāko „Policijas vīrusa” versiju „Brīvdienās plosījies «Policijas vīruss»” portālā TVnet;
   - 27.decembris – raksts par jaunāko „Policijas vīrusa” versiju „Svētkos "policijas vīruss" apkrāpis iedzīvotājus” Latvijas Avīze portālā la.lv;
   - 27.decembris – raksts par jaunāko „Policijas vīrusa” versiju „Svētku brīvdienās izkrāpj naudu ar Policijas vīrusa palīdzību” portālā Bizness.lv;
   - 27.decembris – raksts par jaunāko „Policijas vīrusa” versiju „Svētkos "policijas vīruss" apkrāpis iedzīvotājus” Neatkarīgā Rīta Avīze portālā nra.lv;

- 30.decembris – informatīva ziņa „«CERT.LV»: kiberuzbrukumi valsts iestādēm notiek katru dienu” portālā TVnet;
- 30.decembris – informatīva ziņa „"CERT.LV": iedzīvotāju zināšanas par IT drošību uzlabojas” portālā Kasjauns.lv;
- 30.decembris – informatīva ziņa „Visbiežāk kiberuzbrukumi valsts iestādēm iespējami novecojušas programmatūras dēļ” LTV mājas lapā.

4. Uzdevums: **Veikt pētniecisko darbu, organizēt izglītojošus pasākumus, apmācību un mācības informācijas tehnoloģiju drošības jomā.**

Pārskata perioda laikā CERT.LV kopā ar ISACA Latvija nodaļu organizēja Rudens IT drošības konferenci, kopā ar Valmieras pilsētas pašvaldību – konkursu „Hackfest Valmiera 2012”, kā arī IT drošības vingrinājumu Ministru Kabinetam, „Esi drošs-2” semināru, NetFlow un Risku analīzes semināru, kā arī citus pasākumus. Informācijas drošības izpratnes semināri tika pasniegti dažādās vietās, notika divas DEG (Drošības ekspertu grupas) sanāksmes.

Sīkāka informācija par paveikto:

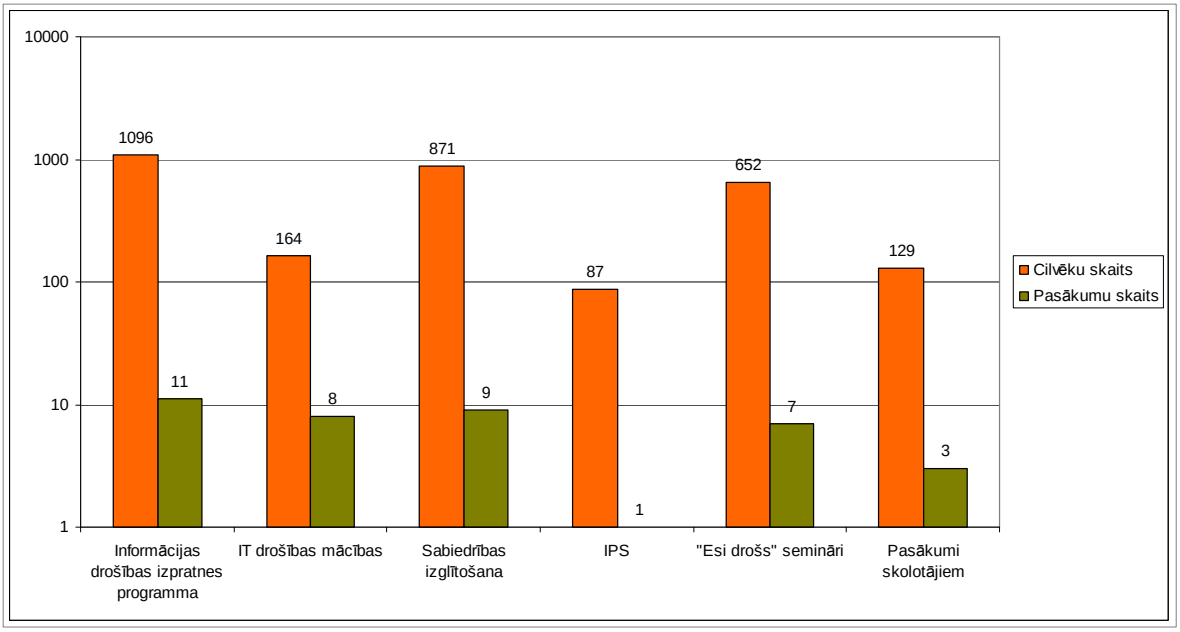
- 4.oktobrī CERT.LV piedalījās ENISA organizētajās IT drošības mācībās „Cyber Europe 2012”, notika cieša sadarbība ar citām organizācijām no Latvijas, kas piedalījās šajās mācības. CERT.LV pārstāvis vadīja un koordinēja mācību scenārija izpildi no ENISA mācību vadības centra.
- 10.oktobrī 20 skolnieki no Cēsu 1. pamatskolas viesojās pie CERT.LV. Skolnieku mērķis bija uzzināt, kā aizsargāt savu datoru, savu mobilo telefonu un sevi pašu digitālajā laikmetā.
- 12.oktobrī notika NetFlow seminārs, piedalījās 20 dalībnieki.
- 16.oktobrī notika Risku pārvaldības seminārs, tajā piedalījās 19 dalībnieki no valsts un pašvaldību iestādēm.
- 17. oktobrī Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisijas deputāti izbraukuma sēdē tikās ar CERT.LV un Nacionālās informācijas tehnoloģiju (IT) drošības padomes pārstāvjiem. Tikšanās notika CERT.LV telpās.
- 19.oktobrī CERT.LV noturēja semināru (4 mācību stundas) Ventspils 1.ģimnāzijā.
- 30.oktobrī notika iniciatīvas „Atbildīgs Interneta pakalpojumu sniedzējs” atklāšana. Pasākumā piedalījās ~20 cilvēki, ziņas pēc pasākuma tika publicētas LETA, Zparks, BNS, kā arī bija sižets Latvijas radio 4.
- 31.oktobrī-1.novembrī Daugavpilī CERT.LV kopā ar Daugavpils universitāti organizēja divus seminārus - Informācijas drošības izpratnes programmu un „Esi drošs-1” semināru, abus seminārus apmeklēja vairāk nekā 100 dalībnieku.
- 5.novembrī CERT.LV nolasīja izglītojošu lekciju Latvijas Universitātes studentiem par dažādiem veidiem, kā datori parasti tiek inficēti.
- 7.novembrī CERT.LV vadīja semināru jaunajiem datorzinību speciālistiem Jelgavas tehnikumā.
- 7.novembrī CERT.LV piedalījās NBS Sakaru skolas kursā, izpildot mācību IT drošības uzbrukumu un novadot nodarbību par iekšēja uzbrucēja radītu drošības apdraudējumu informācijas sistēmai
- 8.novembrī CERT.LV kopā ar ISACA Latvija nodaļu rīkoja IT drošības konferenci, kurā piedalījās arī ar vairākām prezentācijām. Konferencei bija pieteikušies vairāk nekā 300

dalībnieki, tā notika LU aulā. Konferences programmā bija 11 prezentācijas, 2 no tām cieši saistītas ar CERT.LV aktualitātēm un paveikto.

- 9.novembrī CERT.LV vadīja semināru Rīgas izglītības un informatīvi metodiskā centra (RIIMC) skolotājiem.
- 13.-16.novembrī CERT.LV piedalījās NATO krīzes vadības mācībās "CMX 12" un IT drošības mācībās "Cyber Coalition 12", kurās tika veicināta starptautiskā (NATO dalībvalstu un partnera nāciju līmeņa) sadarbība un testēta stratēģiskā līmeņa krīzes vadība dalībvalstīs starptautisku IT drošības uzbrukumu gadījumā.
- 21.novembrī CERT.LV Eiropas Komisijas TAIEX (Technical Assistance and Information Exchange) programmas ietvaros Palestīnas delegācijai sniedza prezentāciju par IT drošības situāciju Latvijā.
- 1-2.decembrī Valmieras pilsētas pašvaldība sadarbībā ar CERT.LV rīkoja konkursu IT drošības entuziastiem un profesionāļiem „Hackfest Valmiera 2012". Šāds pasākums, sadarbībā ar kādu pašvaldību, tika Latvijā rīkots pirmo reizi un viens no tā mērķiem bija palīdzēt Valmieras pilsētas pašvaldībai identificēt trūkumus savās IT sistēmās. CERT.LV piedalījās konkursa uzdevumu izveidē, kā arī tehniskās infrastruktūras konfigurēšanā un projektēšanā. Konkursam tika izveidoti četri dažādas sarežģītības uzdevumi, no kuriem divi bija radīti tieši šim konkursam un divi kā kopijas reālām Valmieras pašvaldības sistēmām. Konkursā aktīvi piedalījās 16 dalībnieki, kuriem tika dotas 24 stundas, lai veiktu dažāda veida uzbrukumus un ielaušanās mēģinājumus izveidotajā IT infrastruktūrā. Konkursa laikā veiktie uzbrukumi un konstatētie IT infrastruktūras drošības trūkumi katram dalībniekam bija jādokumentē. Pieraksti un paveiktais konkursa laikā tika vērtēti ekspertu komisijā, kas noteica konkursa uzvarētājus. Būtiskākie ieguvumi no šī pasākuma ir:
  - kāda visā pasaulē lietota IT produktā atklāta, līdz šim nezināma, ievainojamība. Par atklāto ievainojamību Valmieras pilsētas pašvaldība informēja izstrādātājus;
  - studentu iesaistīšana un motivēšana ar specbalvu;
  - lielisks sadarbības piemērs, kurā sadarbojās valsts un publiskais sektors, nodrošinot balvu fondu.

  Visu iesaistīto pušu sadarbības produktivitāti novērtēja gan CERT.LV, gan Valmieras pašvaldība, kā arī uzņēmēju pārstāvji.
- 4.decembrī CERT.LV organizēja IT drošības semināru „Esi drošs-2", tajā piedalījās 85 pārstāvji no Valsts un pašvaldību iestādēm, kā arī citām organizācijām, viņi noklausījās 6 prezentācijas, 2 no tām tieši par CERT.LV būtiskiem jautājumiem.
- 7.decembrī pirmo reizi Latvijā notika Ministru kabineta līmeņa informācijas tehnoloģiju (IT) vingrinājums, kurā tika veikta liela mēroga IT drošības incidentu simulācija. Vingrinājuma mērķis bija izspēlēt un pārbaudīt rīcības un lēmumu pieņemšanas sistēmu IT drošības krīžu gadījumu gatavībai. Vingrinājums ļāva ne tikai plašāk iepazīt un izprast apdraudējumus nacionālajai drošībai 21.gadsimtā, bet arī palielināt Latvijas gatavību atvairīt IT uzbrukumus. Vingrinājumu organizēja CERT.LV kopā ar LR Satversmes aizsardzības biroju.
- Decembrī CERT.LV strādā pie tehnisko IT drošības mācību organizēšanas "Sniega Vētra 2013", kas norisināsies 30.- 31.01.2013.
- Pārskata periodā reizi mēnesī notika DEG sanāksmes.

8.diagrammā redzams kopējais pasākumu skaits un apmācīto cilvēku skaits kopš CERT.LV darbības uzsākšanas 2011.gadā līdz 2012.gada decembrim.



8.diagramma – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits.

5. Uzdevums: **Sniegt atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas tehnoloģiju jomā, ievērojot normatīvajos aktos noteiktos datu apstrādes ierobežojumus.**

Dažāda veida sadarbība un atbalsts:

- CERT.LV pārstāvis piedalījās sanāksmē Satiksmes ministrijā par e-paraksta jautājumiem.
- 17.oktobrī CERT.LV telpās notika Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisija izbraukuma sēde.
- 11.oktobrī tika izsludināti grozījumi likumā "Par tautas nobalsošanu, likumu ierosināšanu un Eiropas pilsoņu iniciatīvu". Pārskatīta un papildināta sagatavotā iniciatīvu atbalsta vākšanas tiešsaistes sistēmu sertifikācijas instrukcija. Pārskata periodā saņemtas jau pirmās interesentu vēstules par šo tēmu.
- CERT.LV pārstāvis piedalījās Ārlietu ministrijas organizētajā sanāksmē par Eiropas pilsoņu iniciatīvu veicināšanas pasākumiem Latvijā un Eiropā, izskatot vienotas platformas izveidi vienkāršotai iniciatīvu atbalsta vākšanai tiešsaistē.
- CERT.LV piedalījās Latvijas IT drošības stratēģijas sanāksmē.
- CERT.LV piedalījās Saeimas Juridiskās komisijas sēdē par grozījumiem likumā "Par tautas nobalsošanu un likumu ierosināšanu".
- CERT.LV piedalījās Tieslietu ministrijas rīkotajā sanāksmē-diskusijā par ES direktīvas 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu ieviešanu.
- CERT.LV pārstāvis piedalījās Aizsardzības ministrijas un VARAM rīkotajā sanāksmē un diskusijā par "Fizisko personu elektroniskās identifikācijas likuma" projektu.

6. Uzdevums: **Uzraudzīt, kā valsts un pašvaldību institūcijas un elektronisko sakaru komersanti izpilda Informācijas tehnoloģiju drošības likumā noteiktos pienākumus.**

IT drošības likumā noteikts, ka Valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2012.gada 31.decembrim CERT.LV ir apkopojis informāciju par 529 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību.

CERT.LV regulāri informē Valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā inficētas. Pārskata periodā CERT.LV ir bijusi informācija par 91 inficētu IP adresi.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. CERT.LV ir izskatījis iesniegtos plānus un nosūtījis atbildes vēstules ar vērtējumu. CERT.LV ir sācis individuāli pa telefonu sazināties ar ESK un mudināt viņus iesniegt rīcības plānus, kā arī piedāvājis palīdzību neskaidrību gadījumos. CERT.LV arī strādā pie Rīcības plāna parauga sagatavošanas, jo uzskata, ka tas varētu palīdzēt mazajiem ESK izveidot savus plānus.

Viens no ESK, SIA LATNET Serviss, savā mājas lapā http://www.ls.lv sadarbībā ar CERT.LV veic pārbaudi un paziņo, ja lietotāja, kas pieslēdzies viņu mājas lapai, IP adrese inficēta ar datorvīrusu. CERT.LV vēlas šādu sadarbību paplašināt arī ar citiem IPS un portāliem.

7. Uzdevums: **Sadarboties ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām).**

Visa perioda laikā ir notikusi aktīva sadarbība ar citu valstu informācijas tehnoloģiju drošības incidentu novēršanas vienībām, gan lūdzot palīdzību un informāciju par incidentiem, kas notiek Latvijā, gan palīdzot ar citās valstīs notikušu incidentu risināšanu.

CERT.LV pārstāvji pārskata periodā piedalījušies sekojošās konferencēs un semināros, kā arī veikuši citus uzdevumus:

- CERT.LV un visa Latvijas komanda (dažādas organizācijas) piedalījās ENISA Cyber Europe 2012 mācībās. Pirms un pēc mācībām tika rīkotas organizatoriskās sanāksmes.
- CERT.LV pārstāvji piedalījās "XVI Conference on Telecommunications and IT Security - Secure 2012", kas notika Varšavā, Polijā.
- 25.oktobrī CERT.LV pārstāvis piedalījās ENISA rīkotajā telekonferencē par paredzēto pētījumu Risku analīzes metodēs.
- CERT.LV piedalījās NATO krīzes vadības mācībās "CMX 12" un IT drošības mācībās "Cyber Coalition 12", kurās tika veicināta starptautiskā (NATO dalībvalstu un partnera nāciju līmeņa) sadarbība un testēta stratēģiskā līmeņa krīzes vadība dalībvalstīs starptautisku IT drošības uzbrukumu gadījumā. CERT.LV pārstāvis piedalījās CC12 mācību koordinēšanā un izpildē.
- CERT.LV pārstāvis novembrī vadīja vienu no četriem TRANSITS kursu moduļiem (Operational module for CSIRTs), kas notika Prāgā, Čehijā.

- CERT.LV pārstāvis, kopā ar Aizsardzības Ministrijas pārstāvjiem, piedalījās 3 Baltijas valstu IT drošības mācībām veltītā plānošanas konferencē “EUCOM and Baltic States Cyber Workshop”. Šīs - pirmās plānošanas konferences rezultātā tika identificēti 3 Baltijas valstīm kopīgie vingrinājumu virzieni un mērķauditorija.
- 11-12. decembrī CERT.LV pārstāvji piedalījās piektajā Baltijas valstu informācijas tehnoloģiju (IT) drošības politiku koordinācijas sanāksmē, kas notika Tallinā, Igaunijā. CERT.LV pārstāvji uzstājās ar vairākām prezentācijām un aktīvi iesaistījās diskusijās.
- 11-14.decembrī Rīgā notika BAITSE (Baltic Academic IT Security Exchange) projekta sanāksme, CERT.LV piedalījās šīs sanāksmes organizēšanā un vadībā. Projekta kopējais mērķis ir izstrādāt maģistru mācību kursu "Informācijas tehnoloģiju drošības ievainojamību testēšanā un pārvaldībā".

8. Uzdevums: **Veikt citus normatīvajos aktos noteiktos pienākumus.**

- 12.oktobrī Satiksmes ministrijā notika Latvijas Komercbanku asociācijas (LKA), Latvijas atvērto tehnoloģiju asociācijas (LATA), Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas (LIKTA), ISACA Latvijas nodaļas, Latvijas Interneta asociācijas (LIA) un Latvijas Tirdzniecības un rūpniecības kameras (LTRK) tikšanās ar CERT.LV vadītāju un Nacionālās informācijas tehnoloģiju drošības padomes priekšsēdētāju sanāksmē par sadarbību informācijas tehnoloģiju drošības jautājumos.
- Sadarbība ar Latvijas Drošāka interneta centru saprašanās memoranda ar IPS un zīmes "Atbildīgs interneta pakalpojumu sniedzējs" izveidē un atklāšanā.
- 24.oktobrī CERT.LV pārstāvji piedalījās Santa Monica Networks rīkotajā Security Day 2012.
- 28.decembrī CERT.LV vadītāja Baiba Kaškina saņēma Atzinības rakstu par ieguldījumu informācijas tehnoloģiju drošības attīstībā no Satiksmes ministra A.Roņa.

Noslēgums.

CERT.LV pateicas Satiksmes ministrijai par lielisko sadarbību un atbalstu visā sadarbības laikā.

Pārskatu sagatavoja – Līga Besere
e-pasts: liga.besere@cert.lv