Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) paveikto 2012.gada 3.ceturksnī

(2012.gada 1.jūlijs – 2012.gada 30.septembris)

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 trešajā darbības 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 vairāku mērķētu uzbrukumu incidentus, kā arī Latvijā izvietotos robotu tīklu komand- un kontroles centrus.

Pārskata periodā pasaulē tika atklāti vairāki jauni robotu tīkli, kas palielināja inficēto IP adrešu daudzumu visu valstu tīklos. Īpašu apdraudējumu izraisīja jaunatklātu JAVA un Internet Explorer programmu ievainojamību izmantošana datoru inficēšanā. Šie uzbrukumi skāra arī vairākas valsts iestādes, kur uzbrucēji sekmīgi inficēja datorus, apejot antivīrusu programmas. Vērojama tendence, ka uzbrucēji izmanto gan jaunatklātas kritiskas ievainojamības masveida infekcijās, gan līdz 2 gadiem vecas ievainojamības (tās izmanto vairums robotu tīklu uzturētāju).

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto IP adrešu skaitu Latvijā. Jūlijā šis skaits ir bijis 2715, augustā – 2386, septembrī – 3012. Liela daļa no šiem datoriem ir dažādu robotu tīklu sastāvdaļas. Inficēto IP adrešu skaita pieaugums septembrī skaidrojams ar augusta beigās atklāto JAVA ievainojamību, kas tiek plaši izmantota datorvīrusu izplatīšanai, kā arī ar jauniem atklātiem robotu tīkliem, kas sniedz plašāku informāciju par inficētām gala iekārtām, un ar mācību gada sākumu, kad vairāk jauniešu sāk aktīvi izmantot datorus.

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 tiks slēgts ar tiem elektronisko sakaru pakalpojumu komersantiem (turpmāk - ESK), kas vēlas sadarboties ar šīm abām organizācijām. Tie ESK, kas paraksta saprašanās memorandu, var lietot kvalitātes zīmi „Atbildīgs interneta pakalpojumu sniedzējs". Atbildīgs interneta pakalpojumu sniedzējs ir kvalitātes zīme, kuru var saņemt ESK, kurš:

1. 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.
2. Sadarbojas ar Net-Safe Latvia Drošāka interneta centru, lai nodrošinātu iespējami ātru nelegālā satura izņemšanu no publiskas aprites internetā.
3. Pēc klientu pieprasījuma nodrošina bezmaksas interneta satura filtru uzstādīšanu atbilstoši Elektronisko sakaru likumam.

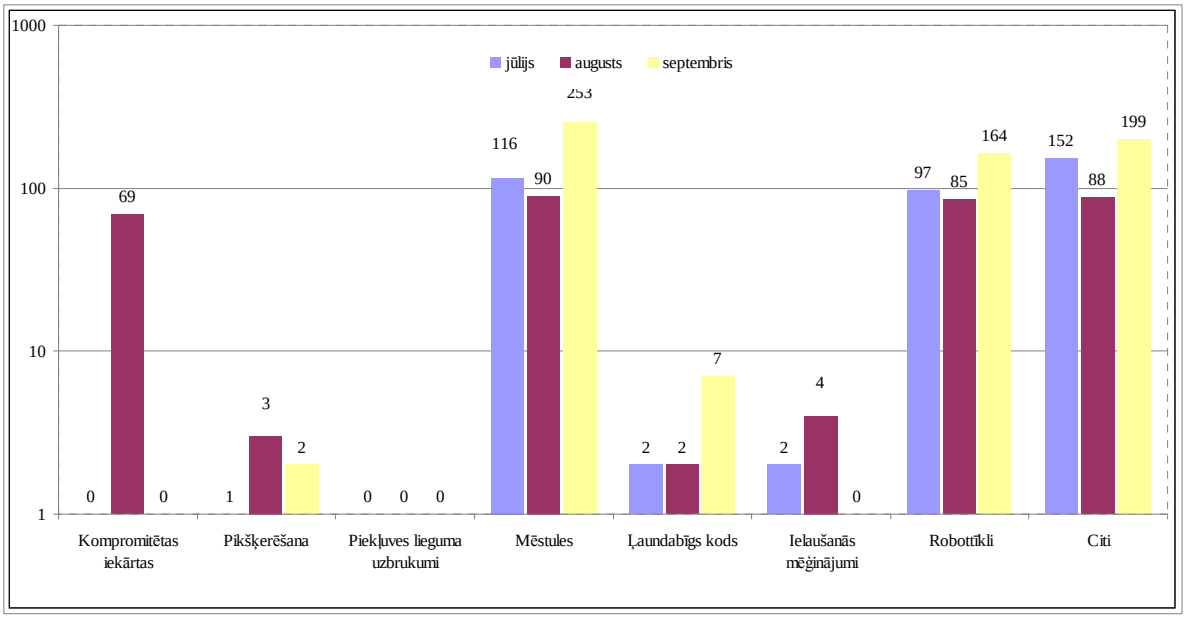
Septembrī ir uzsākta saprašanās memorandu parakstīšana. Līdz septembra beigām ir tikuši pilnībā parakstīti 3 saprašanās memorandi, bet 5 citi ir parakstīšanas procesā. Kvalitātes zīmes atklāšanas pasākums ir paredzēts 30.oktobrī. Ir izstrādāts arī kvalitātes zīmes vizuālais noformējums:

Paralēli CERT.LV turpina sarunas ar citiem ESK, lai arī tie pieņemtu no CERT.LV un apstrādātu informāciju par inficētajām IP adresēm. Pašlaik šo informāciju saņem 16 interneta pakalpojumu sniedzēji (IPS) / organizācijas, un lielākā daļa šos datus izmanto, lai informētu gala lietotājus un palīdzētu tiem risināt incidentus.
Būtisks robotu tīklu izplatības iemesls ir nezinošs lietotājs. Lai mazinātu apdraudējumu, ko rada lietotāju nezināšana, CERT.LV, papildus sadarbībai ar IPS, strādā arī pie tiešas lietotāju izglītošanas, organizējot IT drošības seminārus, informējot par drošas datora lietošanas un informācijas aprites pamatnoteikumiem un par mobilo iekārtu drošību. CERT.LV vada izglītojošos pasākumus gan IT profesionāļiem, gan iestāžu un organizāciju darbiniekiem, kuru ikdienas darbs ir saistīts ar informācijas tehnoloģiju izmantošanu, gan dodas vizītēs uz skolām un augstākajām mācību iestādēm.
Nozīmīga aktivitāte ir arī Esidross.lv portāla attīstība, kurā lietotāji var iegūt informāciju par dažādiem IT drošības aspektiem vienkāršā, nespeciālistiem saprotamā valodā, un uzzināt jaunumus par aktuāliem apdraudējumiem, kā arī pārbaudīt, vai viņa IP adrese nav inficēto sarakstā.

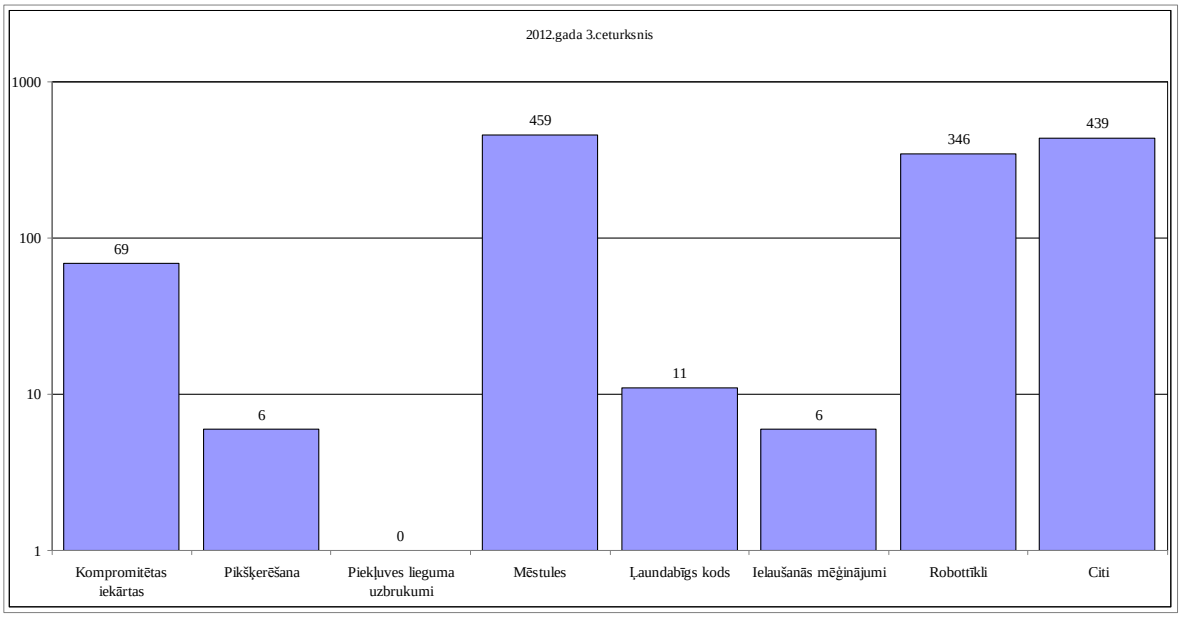
2. Uzdevums: **Sniegt atbalstu informācijas tehnoloģiju drošības incidentu novēršanā vai koordinēt to novēršanu.**

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis **1336** augstas prioritātes incidentus un reģistrējis **52066** zemas prioritātes incidentus, par daļu no kuriem ESK ir informējis savus gala lietotājus.

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

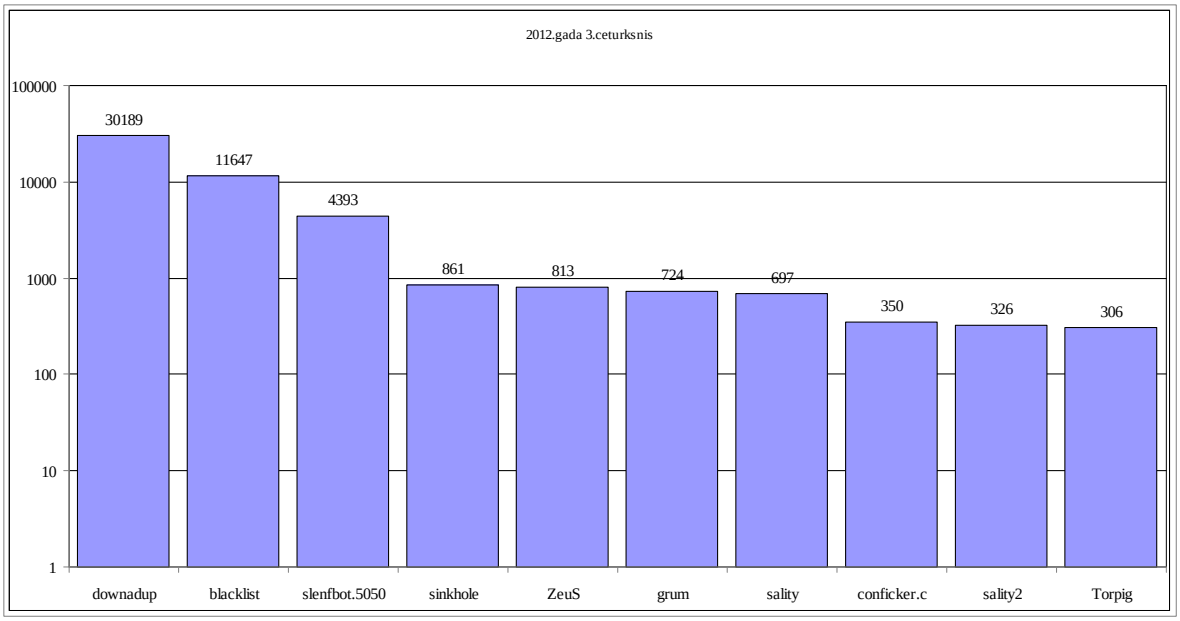


1.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



2.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2012.gada 1.jūlija līdz 30.septembrim.

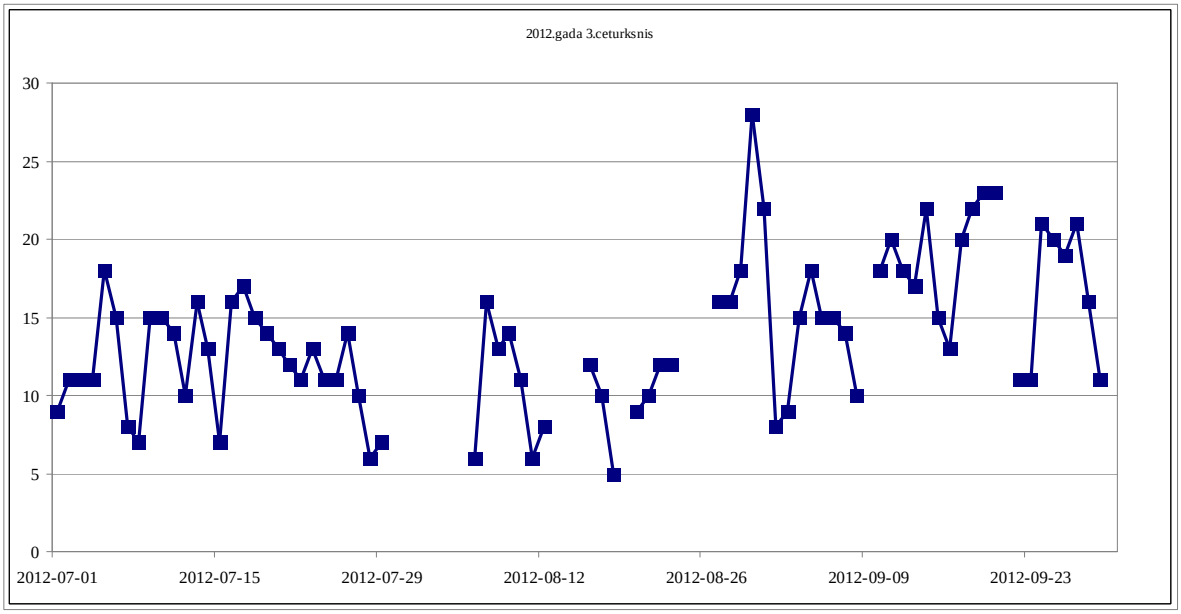
3.diagrammā redzami CERT.LV reģistrētie zemas prioritātes incidenti, to sadalījums pa infekciju tipiem – 10 populārākās infekcijas (kopā tiek apkopota informācija par 57 dažādu infekciju).



3.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.

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



4.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.

- CERT.LV saņēma ziņojumu par potenciālu DoS uzbrukumu valsts iestādes mājas lapai. Tuvākā izpētē tika konstatēts, ka lapas darbības ātruma samazināšanos izraisa satura kopēšanas programma, kas neveic kaitīgas darbības.

- Kāda novada pašvaldības mājas lapai tika konstatēti ielaušanās mēģinājumi. Kaitējums netiek konstatēts.
- CERT.LV saņēma informāciju no vairākām ārzemju CERT komandām par incidentu, kurā iesaistītas IP adreses no Latvijas. Tika koordinēta incidenta risināšana.
- CERT.LV konstatēja konkrētas IP adreses valsts iestādes tīklā, kuras bija inficētas ar ļaundabīgu programmatūru. Infekciju izdevās identificēt un savlaicīgi neitralizēt.
- Pēc incidenta pieteikuma saņemšanas no valsts iestādes par identificēto ārzemju resursu, kas tiek izmantots e-pasta lietotāju paroļu zādzībai, tiek panākta kaitnieciskā resursa atslēgšana.
- CERT.LV identificēja inficētas darbstacijas kādas organizācijas tīklā, kas darbojās kā robotu tīkla sastāvdaļa. Incidents tika novērsts.
- CERT.LV sniedza atbalstu un konsultēja incidenta risināšanas procesā kādu valsts iestāde. Šī iestāde piedzīvoja nopietnu uzbrukumu mājas lapai.
- CERT.LV panāca pikšķerēšanas lapas atslēgšanu, kas bija orientēta uz lētticīgu e-pasta lietotāju kontu informācijas zādzībām.
- CERT.LV veica ievainojamību meklēšanu kādam valsts iestādes portālam. Tika identificētas vairākas koda injekciju (Reflected XSS) ievainojamības, par kurām tika informētas atbildīgās personas.
- CERT.LV saņēma informāciju par diviem dažādiem namu pārvaldes (apsaimniekotāju) tiešsaistes projektiem, kurus kāds iedzīvotājs sajaucis un nodevis savus datus vienam projektam, lai arī tos vajadzēja nodot otram. Minētie projekti/portāli: https://e-parvaldnieks.lv/ (īpašnieks SIA "Rīgas namu pārvaldnieks") un http://eparvaldnieks.lv/ (īpašnieks it kā SIA "Namu apsaimniekošana"). Sūdzība tika saņemta par http://eparvaldnieks.lv. Par abiem portāliem ir informēta Datu Valsts inspekcija. Tā kā nākotnē paredzama arvien plašāka tiešsaistes sistēmu izmantošana dažādu maksājumu veikšanai un privātpersonas datu apstrādei, iespējams, ir nepieciešams šādu projektu darbības valstisks regulējums, lai nodrošinātu skaidrus un nepārprotamus projekta mērķus un darbības principus, ļaujot lietotājam nekļūdīgi noteikt, kādus datus par sevi jānorāda un kas un kādā veidā tos tālāk izmantos.
- CERT.LV saņēma pieteikumu no kādas bankas par krāpnieciskiem e-pastiem, kas sūtīti tās darbiniekiem. Krāpnieku izmantotie pasta konti tika pieteikti e-pasta servisu turētājiem kā kaitīgi.
- CERT.LV saņēma incidenta pieteikumu no privātas kompānijas par uzbrukumiem kompānijas tīmekļa lapai. CERT.LV sniedza detalizētas rekomendācijas konkrētās situācijas risināšanai un koordinēja incidenta risināšanu, sazinoties ar iesaistītajām pusēm ārvalstīs.
- Tika uzlauzta kādas pašvaldības mājas lapa. Iemesls - kļūdas satura vadības sistēmā.
- Tika konstatēts automatizēts ievainojamību meklēšanas uzbrukums kādas valsts iestādes sistēmai. Uzbrukums bija nesekmīgs, CERT.LV veica incidenta risināšanu un koordinēšanu.
- Tika konstatēts datorvīrusu izplatīšanas mēģinājums, kā starpnieku izmantojot kādas organizācijas tīmekļa lapu. Incidents tika operatīvi novērsts.
- Kādas valsts iestādes IDS tika konstatēts mēģinājums veikt servera un lapas ievainojamu komponentu meklēšanu. Uzbrukums bija nesekmīgs un nebija vērsts tieši pret valsts iestādi, bet bija daļa no automatizētas tīkla skenēšanas, kas tika veikta no Ķīnas un Taivānas IP adresēm.
- CERT.LV konsultēja kāda novada pašvaldību par mājas lapas drošību, kā arī veica tai automatizētus testus.
- Izmantojot JAVA ievainojamību CVE-2012-4681, vairākās Latvijas valsts un privātajās organizācijās izplatījās ZEUS saimes datorvīruss. Atbildīgās personas tika informētas un uzsākta inficēto datoru atrašana un salabošana.

- CERT.LV saņēma lūgumu palīdzēt privātpersonai, kas tiek šantažēta, draudot izplatīt privātus datus. CERT.LV konsultēja privātpersonu par iespējamajiem problēmas risinājumiem.
- CERT.LV saņēma pieteikumu par uzbrukumu kādam no kādas valsts iestādes serveriem. CERT.LV palīdzēja nodrošināt komunikāciju starp tīkla uzturētājiem un servera administratoriem.
- CERT.LV sadarbojās ar ebay.com drošības speciālistiem, lai novērstu incidentu, kurā iesaistīts kāds Latvijas serveris. Incidentā tika pārkāptas ebay.com autortiesības, kā arī, iespējams, izveidots mehānisms, kā krāpties ar Google meklētāja rezultātiem, kas saistīti ar ebay.com.
- CERT.LV risināja IT drošības incidentu, ko pieteica kāda valsts iestāde. Viņi konstatēja aizdomīgu tīkla aktivitāti divu e-pasta serveru starpā. Pārbaužu rezultātā tika konstatēts, ka aizdomīgās darbības ir serveru programmatūras īpatnības noteiktos gadījumos un nav klasificējamas kā uzbrukums.
- Kādā pašvaldībā notika IT drošības uzbrukums IP telefonijas sistēmai. Uzbrucēji veica simtiem paaugstinātas maksas zvanus uz ārvalstu numuriem. Pašvaldības IT darbinieki problēmu konstatēja un ziņoja CERT.LV. Konstatētie drošības trūkumi tika novērsti. Uzbrukuma rezultātā tika radīti materiālie zaudējumi Ls 266,88 + PVN apmērā.
- CERT.LV saņēma Kaspersky lab ziņojumu par P2P (peer-to-peer) robotu tīkla "ZeroAccess" vienu no kontrolcentriem, kas izvietots Latvijā. CERT.LV turpina incidenta risināšanu.

CERT.LV ir uzsācis kompromitēto tīmekļa vietņu serveru un pašu tīmekļa vietņu izķēmošanas gadījumu uzskaiti. Jūlijā tika kompromitēti 11 tīmekļa vietņu serveri un izķēmotas 24 tīmekļa vietnes (1 atradās uz FreeBDS servera, pārējās 23 uz Linux), augustā tika kompromitēti 13 tīmekļa vietņu serveri un izķēmotas 41 tīmekļa vietne (1 no tām atradās uz FreeBSD servera, 2 uz Windows, bet pārējās uz Linux), septembrī tika kompromitēti 12 tīmekļa vietņu serveri un izķēmotas 43 tīmekļa vietnes (42 atradās uz Linux serveriem, 1 nezināma). Kopā ceturksnī tika kompromitēti 36 tīmekļa vietņu serveri un izķēmotas 108 tīmekļa vietnes.

Pārskata periodā CERT.LV ir analizējis mērķētos uzbrukumus un tajos izmantoto ļaunatūru, kā arī veicis informācijas sistēmu un tīmekļa aplikāciju ievainojamību skenēšanas iekārtu ieviešanu un funkcionalitātes pārbaudi. Tāpat CERT.LV testēja zemas-mijiedarbes urķuslazda (low-interaction Honeypot) risinājumus.

Pārskata periodā CERT.LV informēja pakalpojumu sniedzējus un citas iesaistītās puses par konstatētajām kritiskām ievainojamībām DNS serveros. Apzināto, ievainojamo DNS serveru saraksts ir CERT.LV un Latvijas domēnu reģistra NIC.LV ciešas sadarbības rezultātā realizētā pētījuma rezultāts. Lielākā daļa apzināto līdz pārskata beigām ir ņēmuši vērā CERT.LV norādījumus un sniegto informāciju, novēršot konstatētās kritiskās ievainojamības. Kopumā tika apziņoti vairāk nekā 100 DNS serveru īpašnieki, no tiem 55% serveru līdz pārskata perioda beigām ir savesti kārtībā.

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

CERT.LV tīmekļa vietnē, redzamā vietā, regulāri tiek publicēta informācija par jaunākajām ievainojamībām un vīrusiem. Šī www.cert.lv lapas daļa ir visapmeklētākā. Pārskata perioda laikā tai ir bijuši kopā 5077 apmeklētāji. Kopā CERT.LV mājas lapai bijuši 6495 apmeklējumi, 4717 unikāli apmeklējumi no 60 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 90,7 % apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicēti 26 jaunumi, publiskais darbības pārskats par 2012.gada 2.ceturksni, kā arī informācija par dažādiem pasākumiem, publikācijām un citiem notikumiem.

CERT.LV ir Twitter konts un tajā tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv. Pārskata perioda laikā tajā ir publicētas 35 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu http://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 8 jauni raksti, portālu apmeklējuši 6692 apmeklētāji. Publicētie raksti:

- Kas jāzina, lai droši lietotu „facebook.com"?
- Kas ir atvērtā un slēgtā koda programmatūra?
- Droša mājas bezvadu tīkla konfigurācija
- Mac OS drošība
- Yahoo uzlauzts – publiskoti neskaitāmi lietotājvārdi un paroles
- Surogātpasts jeb spams
- PDF formāts – ērts, bet vai drošs?
- Ko ļaundaris var iegūt no uzlauzta datora?

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

Pārskata perioda laikā CERT.LV organizēja Risku analīzes semināru, kā arī pasniedza vairākus Informācijas drošības izpratnes seminārus dažādās vietās. Notika arī LV-CSIRT grupas pārveidošanas darba grupas sanāksmes un jaunizveidotās Drošības ekspertu grupas (DEG) pirmā sanāksme.

Sīkāka informācija par paveikto:

- 30.jūlijā CERT.LV sniedza informāciju ziņu aģentūrai LETA par mērķētiem IT uzbrukumiem Latvijā. Informācija tika publicēta portālā nozare.lv un to pārpublicēja visi lielākie ziņu portāli, piem. diena.lv, "Kāda Latvijas ministrija piedzīvojusi mērķtiecīgu hakeru uzbrukumu".
- 30.jūlijā LTV raidījums „Panorāma" filmēja sižetu par IT drošības uzbrukumiem Latvijā. 31.jūlijā tika rādīts sižets par FIB meklētajiem "hakeriem" ar CERT.LV vadītājas komentāriem, savukārt 5.augustā tika rādīts sižets par mērķētiem IT uzbrukumiem.
- CERT.LV sniedza ieteikumus žurnālam „Cosmopolitan" par tēmu "kā izvairīties no nevēlamu fotogrāfiju vai cita privātā materiāla nokļūšanas internetā un kas būtu jādara, ja tas tomēr ir noticis." Komentāri tika publicēti septembra Cosmopolitan publikācijā rakstā „Vai Tu vari kļūt par upuri kailfoto skandālam?"
- 16.augustā notika Drošības ekspertu grupas dibināšanas sanāksme.
- 3.septembrī CERT.LV pārstāvis runāja ar Radio-4, atbildot uz vispārīgiem jautājumiem par novērotajiem uzbrukumiem Latvijā un haktīvistiem.
- 5.septembrī CERT.LV intervēja TV raidījums „Nekā personīga", sižets par problēmām ar interneta banku autentificēšanās mehānismu izmantošanu portālos tika rādīts 9.septembrī. CERT.LV pārstāvis komentēja situāciju, kā arī apstiprināja, ka balstoties uz CERT.LV veiktajiem testiem autentifikācijas mehānisms patiešām ir nedroši implementēts un to ir iespējams apiet, kā arī pie noteiktiem apstākļiem lietot svešu identitāti. CERT.LV uzsvēra, ka risks NAV tikai teorētisks. Par atklātajām ievainojamībām CERT.LV bija ziņojis iesaistītajām pusēm vairākus mēnešus pirms "Nekā personīga" raidījuma sižeta.

- 6.septembrī Ziedot.lv birojā CERT.LV stāstīja bērniem par drošu datoru lietošanu un uzvedību virtuālajā vidē.
- 11.septembrī CERT.LV piedalījās Latvijas Radio raidījumā „Labrīt" un komentēja par vispārējo situāciju valstī IT drošības jomā.
- 11.septembrī CERT.LV noturēja Informācijas drošības izpratnes semināru Rundāles pilī. Seminārā piedalījās 45 dalībnieki no Rundāles pašvaldības un Rundāles pils.
- 13.septembrī notika pirmā Drošības ekspertu grupas sanāksme, kurā tika apspriestas problēmas saistībā ar Interneta banku autentificēšanās mehānismu izmantošanu dažādos portālos.
- CERT.LV pārstāvis 17.septembrī Latvijas Universitātē uzstājās ar prezentāciju „Drošība caur sadarbību – IT drošības likums, CERT.LV, citi spēlētāji" Datorikas fakultātes studentiem kursa "Informācijas sistēmu drošība" ietvaros. Lekcijā piedalījās ~35 studenti.
- 19.septembrī CERT.LV piedalījās Latvijas Radio raidījumā „Zināmais nezināmajā", kur stāstīja par drošu maksājumu karšu izmantošanu iepirkumiem internetā.
- 19.septembrī CERT.LV piedalījās ISACA Latvijas nodaļas regulārajā sanāksmē un apsprieda problēmas saistībā ar Interneta banku autentificēšanās mehānismu izmantošanu dažādos portālos.
- 20.septembrī CERT.LV Centrālā finanšu un līgumu aģentūrā novadīja Informācijas drošības un izglītības programmas semināru. Seminārā piedalījās 92 Centrālā finanšu un līgumu aģentūras darbinieki.
- 24.septembrī notika pirmais CERT.LV un DEG (Drošības ekspertu grupas) kopēji rīkotais praktiskais seminārs par IT risku pārvaldību. Interese par semināru bija ļoti liela - pieteicās vairāk kā 70 dalībnieku. 24.09.2012. pirmie 24 dalībnieki apguva zināšanas iespējamo risku novērtēšanā un novēršanā. Nākamā grupa seminārā piedalīsies 16.10.2012.

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:

- Sniegts atzinums VARAM darba dokumentam „Informācijas komunikāciju tehnoloģiju pārvaldības koncepcija".
- Sniegta konsultācija kādai vidusskolai par IT drošības noteikumu izstrādi un ieviešanu.
- 18.jūlijā CERT.LV pārstāvis piedalījās kā pieaicināts eksperts Saeimas Juridiskās komisijas sēdēs par grozījumiem likumā "Par tautas nobalsošanu un likumu ierosināšanu".
- CERT.LV sniedza konsultāciju drošības prasību definēšanai programmatūras iepirkumā kādai valsts iestādei.
- 4.septembrī CERT.LV pārstāvis piedalījās LR Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisijas sēdē, kurā tika apspriesti un pieņemti ierosinātie grozījumu IT drošības likumā.
- 12.septembrī notika tikšanās ar Valsts izglītības attīstības aģentūras Informācijas un karjeras atbalsta departamenta vecāko eksperti, lai apspriestu profesijas aprakstu „Informācijas sistēmu drošības pārvaldnieks". Diskusijas rezultātā tika izveidots informatīvs buklets.

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 30.septembrim CERT.LV ir apkopojis informāciju par 518 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību, kā arī par institūciju tīkliem un mājas lapām. 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 70 inficētām IP adresēm.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 „Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam" nosaka kārtību kādā Elektronisko sakaru komersantiem (ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. CERT.LV ir izskatījusi visus saņemtos plānus un nosūtījusi atbildes elektronisko sakaru komersantiem. 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.

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:

- 26.jūlijā notika CERT.LV un Latvijas pārstāves ENISA tikšanās.
- Jūlijā notika sadarbība ar Kaspersky Lab Rumānijas nodaļu ļaunatūras pētniecībā.
- Jūlijā notika sadarbība ar CERT.EE ļaunatūras pētniecībā.
- Jūlijā noslēgts saprašanās memorands ar Kazahstānas CSIRT komandu KZ-CERT.
- CERT.LV septembrī ir parakstījis saprašanās memorandu ar Azerbaidžānas CSIRT komandu cert.gov.az.
- Jūlijā tika uzsākta informācijas apmaiņas sadarbība ar Austrijas CSIRT vienību CERT.AT.
- Pārskata periodā notika sadarbība ar Ukrainas valsts CERT un Luksemburgas valsts CERT vienībām kāda incidenta risināšanā.
- CERT.LV pārstāvis strādāja pie ENISA Cyber Europe 2012 (CE2012) IT drošības mācību tehniskā pamata scenārija izstrādes un dalības plānošanas, piedalījās dažādās sanāksmēs un telekonferencēs, lai varētu sekmīgi sagatavoties Latvijas dalībai šajās mācībās.
- CERT.LV gatavojās piedalīties NATO mācībās „Cyber Coalition 2012" (CC2012), pārskata periodā notika iepazīšanās ar mācību scenāriju un citas aktivitātes.
- 24-25.septembrī CERT.LV pārstāvis piedalījās NATO Science and Technology Organisation (STO) simpozijā "Cyber Defence and Information Assurance".
- CERT.LV piedalījās TF-CSIRT sanāksmē, kas notika 27. un 28. septembrī Ļubļanā, Slovēnijā, ar prezentāciju par interneta pakalpojumu sniedzēju, drošības speciālistu un sabiedrības iesaisti drošākas interneta vides veidošanā un nodrošināšanā. CERT.LV izpelnījās atzinību no starptautisko kolēģu puses gan par uzsākto iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs", gan par Drošības ekspertu grupas izveidošanu.

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

- Pārskata perioda laikā notika vairākas sanāksmes ar Latvijas Drošāka interneta centra un Latvijas Interneta asociācijas pārstāvjiem, lai izveidotu un saskaņotu saprašanās memorandu ar ESK un kvalitātes zīmi "Atbildīgs interneta pakalpojumu sniedzējs".
- Pārskata periodā notika vairākas "Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas" (DEG) darba grupas sanāksmes, lai izveidotu Grupas statūtus un ētikas kodeksu. 16.augusta sanāksmē šie dokumenti tika saskaņoti un grupa nodibināta. Tajā tika nolemts likvidēt esošo LV CSIRT grupu un turpmāk darboties DEG. Ir izveidots arī DEG logo.
- CERT.LV ir uzlabojis veidu, kādā portāla www.esidross.lv apmeklētājiem tiek parādīts brīdinājums par to, ka viņu IP adrese ir inficēto sarakstā, kā arī papildināta informācija, ko cietušais saņem katrā individuālajā gadījumā.
- CERT.LV regulāri uzlabo un papildina informāciju savā mājas lapā, ir tikušas izveidotas atsevišķas sadaļas „Atbildīgs interneta pakalpojumu sniedzējs”, „Drošības ekspertu grupa”.

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