Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi 2015. gadā

2015

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

2015. gadā Latvijas iedzīvotāji vairakkārt cieta no starptautiskām uzbrukumu kampaņām, zaudējot naudu vai savu privāto informāciju. Arī šogad kiberuzbrukumu galvenais dzinējspēks bija nelegāla finansu līdzekļu iegūšana.
Kopumā kiberuzbrukumu tendences ar katru gadu paliek arvien satraucošākas. Incidenti tiek rūpīgāk mērķēti uz specifiskām lietotāju grupām - uzņēmējiem, grāmatvežiem, Gmail lietotājiem, ar mērķi panākt lielāku ticamību un līdz ar to iespējamību, ka lietotājs tiks inficēts.

Latvijas iedzīvotāji 2015. gadā visvairāk saskārās ar "banku" vīrusiem un šifrējošiem izspiedējvīrusiem. Arī notikušajās starptautiska mēroga datu noplūdēs ir bijuši vairāki tūkstoši Latvijas iedzīvotāju datu ieraksti.

Aizvadītās Latvijas prezidentūras Eiropas Savienības Padomē laikā liela daļa valsts iestāžu bija mērķētu uzbrukumu upuri. Izplatīti bija DDoS uzbrukumi, ievainojamību meklēšana jeb taustīšanās un ļaunatūras izplatīšanas kampaņas. Atsevišķi uzbrukumi bijuši sekmīgi, piemēram, uzbrucējam izdevās traucēt tieslietu sektora darbu, pielietojot DDoS uzbrukumus.

Pārskata periodā izaicinājumus dažādu tīmekļa vietņu uzturētājiem un lietotājiem sagādāja CMS ievainojamības. Statistika rāda, ka Latvijā apmēram 50% vietņu tiek kompromitētas atkārtoti, kas nozīmē, ka to īpašnieki pēc incidenta atjauno vietni, taču neizlabo drošības trūkumus. Kompromitētās vietnes visbiežāk izmanto kā resursu vīrusu izplatīšanai, mēstuļu piegādei un citu uzbrukumu pēdu slēpšanai, retāk izķēmo.

CERT.LV veica pētījumu par Krievijas interneta troļļu aktivitātēm Latvijas ziņu portālu komentāru sadaļās, kur ar provokatīviem komentāriem un saitēm tiek veikti mēģinājumi inficēt lietotāju datorus. Pētījuma rezultāti tika atspoguļoti IT drošības konferencē "Kiberšahs. Stratēģija un taktika", kas notika 1. oktobrī.

2015. gadā izplatītākie incidentu veidi bija mēstules, ielaušanās mēģinājumi un vīrusu infekcijas.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 2927 augstas prioritātes incidentus un reģistrēja 606956 zemas prioritātes incidentus.

Pārskata periodā CERT.LV piedalījās 103 pasākumos, izglītojot 6680 cilvēkus par IT drošības tēmām.

1. Incidentu apstrāde

Pārskata periodā vērienīgākais drošības incidents bija „CTB Locker" šifrējošā vīrusa izplatīšanas kampaņa. Uzbrukumu mērķis bija inficēt datorus ar vīrusu, kurš sašifrē datorā esošos failus, prasot izpirkuma maksu. Vīruss tika izsūtīts vairākās kampaņās, galvenokārt ar mēstuļu palīdzību. Lielākai ticamībai vīrusu saturoši e-pasti tika izsūtīti šaurām lietotāju grupām, piemēram, juristiem, grāmatvežiem, valsts un pašvaldību iestāžu darbiniekiem.
CERT.LV aicināja interneta lietotājus rūpīgi izvērtēt e-pasta saturu un to pielikumus, lai nekļūtu par krāpnieku upuriem.

Pārskata periodā vairāku Latvijas banku klienti piedzīvoja "banku" trojāna uzbrukumus. Tie pārsvarā bija uzbrukumi, ar mērķi inficēt lietotājus ar ļaunatūru, kas zog naudu no lietotāju kontiem. Vīrusi galvenokārt tika izplatīti caur inficētiem e-pastu pielikumiem, kā arī citos veidos.

"Banku" trojāna kampaņu ietvaros CERT.LV veica uzbrukumu kampaņas analīzi. Izpēte atklāja, ka vīruss ir modificēts atvasinājums no Zbot trojan saimes ar WEB injekciju funkcionalitāti, kas nelīdzinās iepriekšējām Zbot variācijām. Trojan.Zbot, saukts arī par Zeus vīrusu, ir viens no izplatītākajiem vīrusiem šādās kampaņās. Vīruss mēģina nozagt konfidenciālu informāciju no inficēta datora. Tas var arī lejupielādēt konfigurācijas failus un atjauninājumus no interneta. Vīruss maina sistēmas informāciju un pārtver bankas datus, taču var tikt pielāgots, lai vāktu jebkāda veida informāciju.

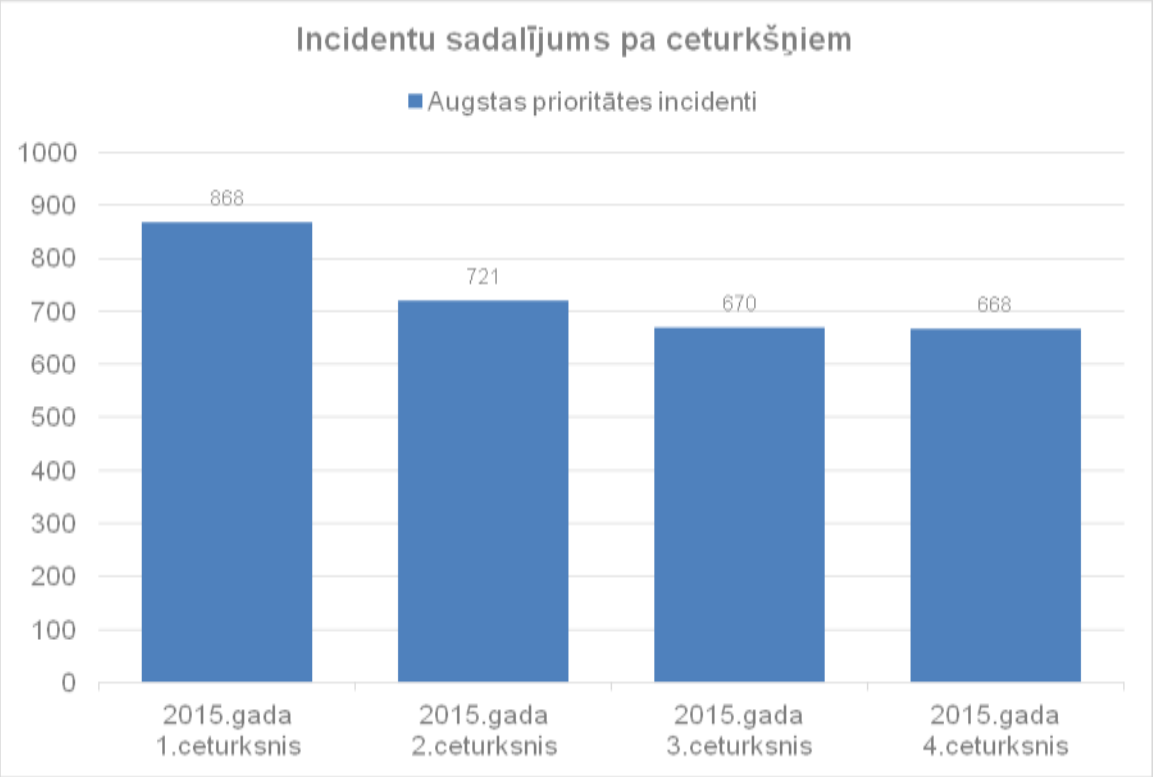
Visa gada garumā notika uzbrukumu kampaņa "DDoS 4 Bitcoin". Kampaņa tika realizēta, pret Latvijā strādājošām komercbankām un lieliem uzņēmumiem, veicot apjomīgus DDoS uzbrukumus, ar mērķi izspiest naudu. Pēc uzbrukuma sekoja draudi, ka tiks veikti vēl lielāka apjoma uzbrukumi un tiks radīti potenciāli traucējumi, ja netiks samaksāts par to, lai uzbrukumi neturpinātos.
Šādi incidenti ir signāls, ka uzņēmumiem jāpārdomā drošības politika un jāseko tās izpildei. CERT.LV sniedza rekomendācijas iespējamo uzbrukumu mērķorganizāciju IKT vides stiprināšanai un ieteica nekomunicēt ar krāpniekiem un nemaksāt prasīto summu.

1.1. Augstas prioritātes incidenti

CERT.LV apkopo informāciju par notikušajiem augstas prioritātes incidentiem, (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).

2015. gadā CERT.LV apstrādāja 2927 augstas prioritātes incidentus.

CERT.LV saņem ziņojumus no iestādēm, sadarbības partneriem, un lietotājiem, kas vēršas pēc palīdzības un konsultācijām, ja pamana kādu neparastu notikumu.
Lai arī incidentu skaitam ir tendence mazināties, jāatzīmē, ka iestādes arvien biežāk vēršas pie CERT.LV tieši nopietnu un komplicētu incidentu gadījumos.



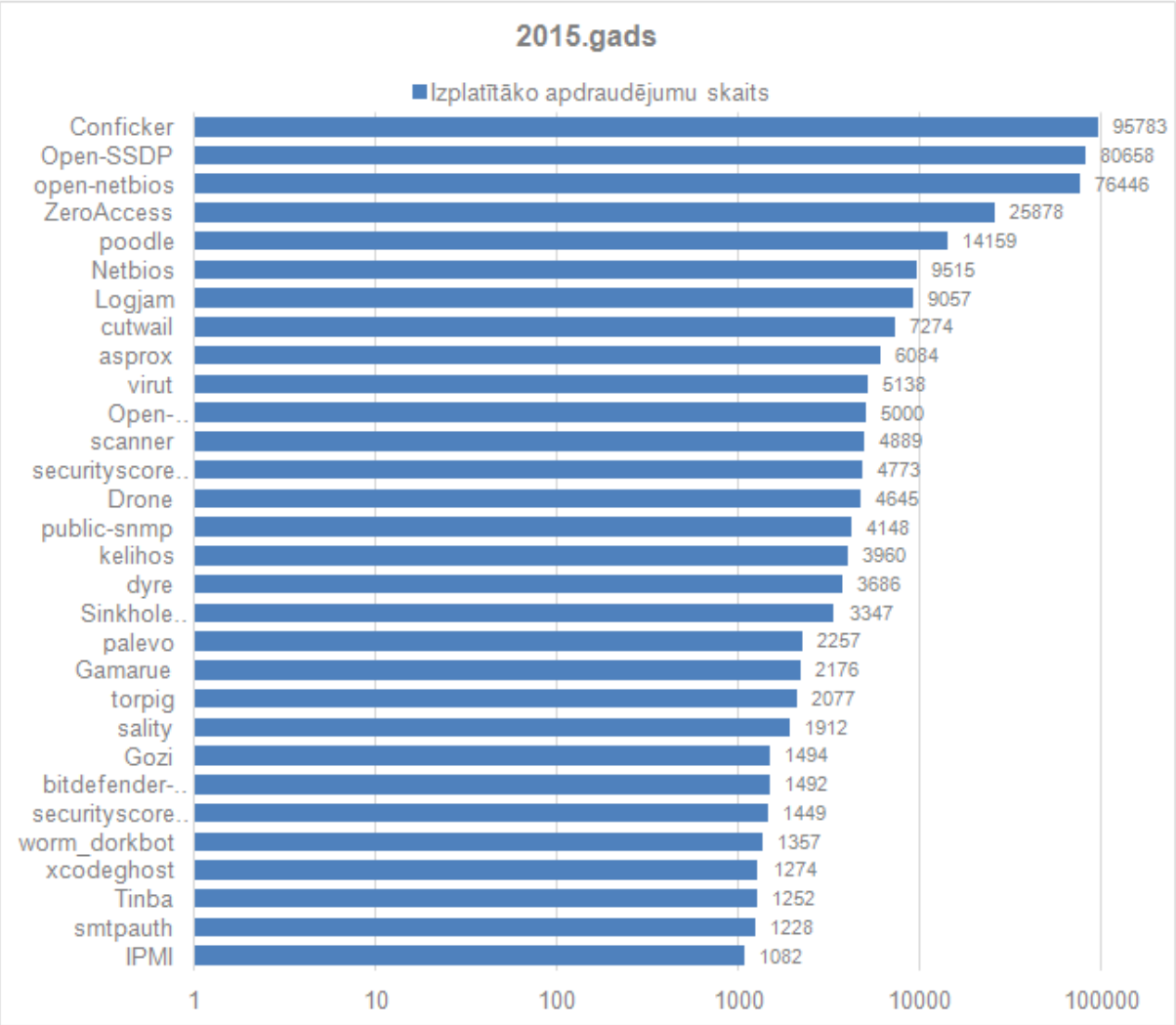
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem.

Lielākais incidentu apjoms tika reģistrēts gada pirmajā ceturksnī, kurā notika vairākas šifrējošo vīrusu kampaņas.

Lai novērstu sevišķi bīstamus incidentus, CERT.LV regulāri brīdināja valsts un pašvaldību iestādes par aktuālajām vīrusu kampaņām, ievainojamībām un politiski nozīmīgiem datumiem, kad iestādēm jāpievērš pastiprināta uzmanība iestādes IT infrastruktūrai.

1.2. Zemas prioritātes incidenti

2015.gadā CERT.LV reģistrēja un apstrādāja 606956 zemas prioritātes incidentus. Tie ir galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūta mēstules, kā arī nedroši konfigurētas iekārtas).



2.attēls - CERT.LV reģistrētie zemas prioritātes incidenti 2014.gadā pa apdraudējumu tipiem.

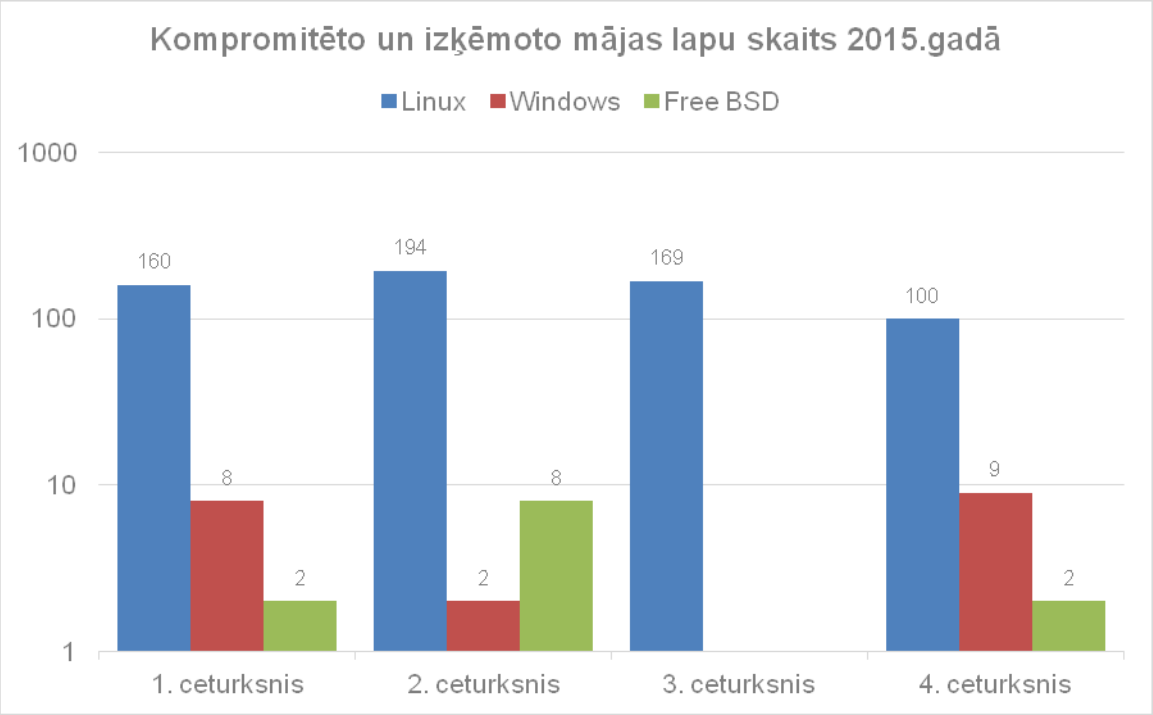
Latvijā joprojām ir salīdzinoši lieli „Conficker" vīrusa infekcijas rādītāji. Statistika liecina, ka lielākā daļa ar šo vīrusu inficētie datori lieto novecojušu Microsoft Windows XP operētājsistēmu, turklāt netiek lietota arī pretvīrusu programmatūra. Šis vīruss uzskatāms par novecojušu, kā arī no tā var diezgan vienkārši atbrīvoties, taču inficēto datoru īpašnieki nepūlas to darīt, padarot savu datoru par vīrusu perēkli un apdraudējumu citiem datorlietotājiem.

Nemainīgi augstas izplatības pozīcijas saglabā lielais nedroši konfigurēto ierīču skaits, kas statistikā atzīmēts kā open-ssdp un open-netbios servisi (pakalpojumi, kas nodrošina servisu apziņošanu un atpazīšanu tīklā, kā arī saziņas iespējas starp iekārtām lokālā tīkla ietvaros).
Visbiežāk šie servisi atrodas uz nedroši konfigurētiem mājas maršrutētājiem un WiFi iekārtām, kuras tiek lietotas ar ražotāja sagatavoto konfigurāciju, kas ir ērti, taču nebūt ne droši, sniedzot potenciālajiem uzbrucējiem ērtu iespēju piekļūt tīklā esošajiem datoriem un izmantot tos tālākās nelikumīgās darbībās vai veikt datu zādzību.
Bieži vien šo iekārtu funkcionalitāte tiek nesankcionēti izmantota, lai veiktu DDoS uzbrukumus citiem tīkliem. Nedroši konfigurētas iekārtas arvien vairāk tiek izmantotas kā starpniekserveri noziedzīgu darbību slēpšanai.

CERT.LV sadarbojas ar lielāko daļu Latvijas interneta pakalpojuma sniedzēju un iniciatīvas "Atbildīgs interneta pakalpojuma sniedzējs" ietvaros informē par inficētām iekārtām gala lietotājus. Gandrīz 70% no CERT.LV rīcībā esošās informācijas ar atbildīgo interneta pakalpojuma sniedzēju starpniecību tiek sekmīgi nogādāta līdz gala lietotājam kopā ar instrukcijām, kā atbrīvoties no kaitīgās programmatūras.

Kompromitētas vietnes

CERT.LV uzskaita uzlauzto un izķēmoto mājaslapu gadījumus. 2015. gadā tika uzlauztas un izķēmotas 654 mājaslapas.



3. attēls – Kompromitēto mājas lapu skaits 2015. gadā.

2015. gada decembrī tika atklāta kritiska Joomla satura vadības sistēmas ievainojamība. Apzinot apdraudējuma ietekmi, .lv domēnu zonā tika pārbaudīti apmēram 700 000 domēna vārdi. No tiem 13 000 izmanto Joomla satura vadības sistēmu.

CERT.LV apzināja valsts pārvaldē un citur Latvijā esošos Joomla projektus, lai brīdinātu par apdraudējumu un koordinētu ievainojamību novēršanu. Valsts sektorā tika atklāti vairāki desmiti šādu vietņu.

Pēc CERT.LV novērojumiem, Latvijā aptuveni 50% no kompromitētām tīmekļa vietnēm tiek kompromitētas atkārtoti, kas norāda uz resursu turētāju un/vai administratoru paviršo attieksmi pret drošības ielāpu ieviešanu. Lielā daļā gadījumu kompromitētā lapa tiek atjaunota no rezerves kopijām ar tām pašām vecajām ievainojamībām. Ir tikai laika jautājums (no dažām dienām līdz nedēļai), kad uzbrucējs atkal izmanto tos pašus "vārtus", pa kuriem ienācis iepriekš.

2. Nozīmīgākie incidenti 2015. gadā

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

Izspiedējvīrusi

- Janvārī Latvijā un citās ES valstīs ar lielu vērienu sāka izplatīt „CTB Locker" izspiedējvīrusu. Noziedzīgie grupējumi kampaņu izvērsa vairākos piegājienos. Izplatība notika galvenokārt caur e-pasta vēstulēm, kas noformētas pareizā latviešu valodā, izliekoties par parādu piedzinējiem vai valsts iestādēm. Pielikumā bija arhīvs, kurš saturēja izpildāmo failu ar paplašinājumu .scr vai .exe. Atverot pielikumu un izpildot kaitīgo programmu, datorā esošie faili tika šifrēti un upurim tika pieprasīta samaksa 2 Bitcoin (~ 600 EUR) par sašifrēto datu atgūšanu. Atgūt sašifrētos datus no inficētas iekārtas nemaksājot ir teju neiespējami.

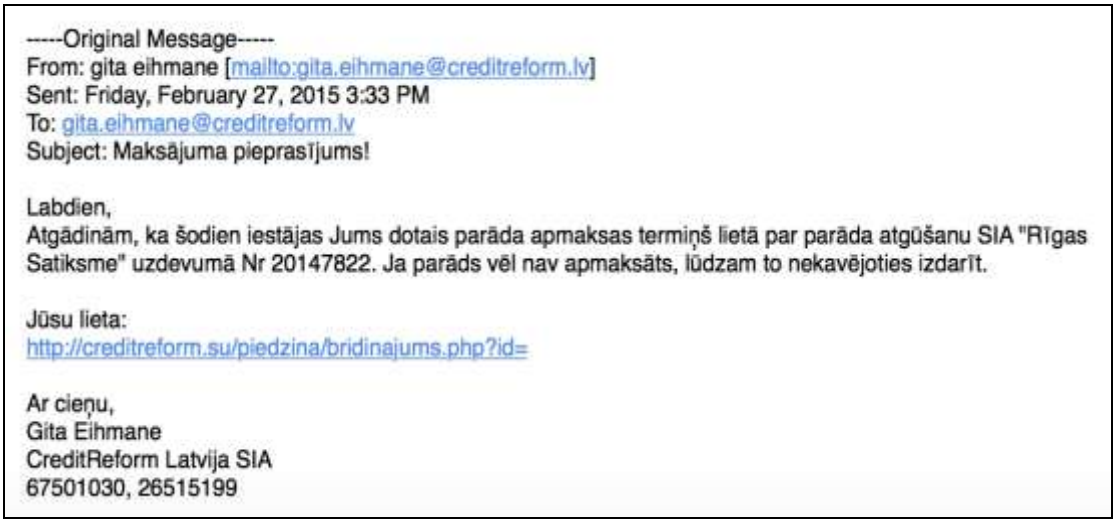
  Vīrusa ekrānšāviņš:

  Incidenta risināšanas ietvaros CERT.LV veica vairāku kontrolcentru bloķēšanu, tika ieviesti mēstuļu atpazīšanas mehānismi un notika aktīva informācijas apmaiņa ar sadarbības partneriem Eiropā.

  Vairākas valsts iestādes būtiski cieta no vīrusa radītajām sekām, zaudējot datus. CERT.LV norādīja uz nepilnībām, kas šīm iestādēm jānovērš, lai situācija neatkārtotos un apdraudējuma ietekme tiktu mazināta.

- Februārī šifrētājvīrusu kampaņai pievienojās e-pasti, noformēti kā parādu piedziņas firmas paziņojumi, kas saturēja saites uz „CTB Locker" datorvīrusu. E-pasts tika sūtīts no

leģitīmas adreses, kas visdrīzāk, tikusi kompromitēta.



-----Original Message-----
From: gita eihmane [mailto:gita.eihmane@creditreform.lv]
Sent: Friday, February 27, 2015 3:33 PM
To: gita.eihmane@creditreform.lv
Subject: Maksājuma pieprasījums!

Labdien,
Atgādinām, ka šodien iestājas Jums dotais parāda apmaksas termiņš lietā par parāda atgūšanu SIA "Rīgas Satiksme" uzdevumā Nr 20147822. Ja parāds vēl nav apmaksāts, lūdzam to nekavējoties izdarīt.

Jūsu lieta:
http://creditreform.su/piedzina/bridinajums.php?id=

Ar cieņu,
Gita Eihmane
CreditReform Latvija SIA
67501030, 26515199

- Martā CERT.LV veica incidenta pārbaudi, kura ietvaros radās aizdomas, ka nesankcionēti iegūts saraksts ar e-pasta adresēm, uz kurām vēlāk uzbrucēji izsūtīja „CTB Locker" vīrusu. Vienā no „CTB Locker" uzbrukuma kampaņām ~80% saņēmēju izrādījās grāmatveži vai cilvēki, kas saistīti ar grāmatvedību.
- Decembrī parādījās jauns izspiedējvīrusa paveids - TeslaCrypt. Lai inficētu lietotājus, tika izplatīti e-pasti ar XLS dokumentā esošu makrovīrusu, kuru iespējojot, notika lietotāja datu šifrēšana. Lai atgūtu šifrētos datus, tika pieprasīta izpirkuma maksa caur QIWI pārskaitījumu sistēmu. Kampaņas mērķis bija krieviski runājoši grāmatveži.
- Decembrī Latvijā tika konstatēti vairāki šifrējošā izspiedējvīrusa CryptoWall 4.0 gadījumi. Lietotāji tika inficēti, apmeklējot vāji aizsargātu un/vai kompromitētu mājas lapu. Vīruss izmantoja neatjauninātas vai citādi ievainojamas komponentes, piemēram, Adobe Flash, Java vai Microsoft Windows.
- Decembra beigās vairāki nelieli Latvijas internetveikali cieta no Linux Encoder šifrēšanas vīrusa. Uzturētāji lapas atjaunoja no rezerves kopijām.

Ļaunatūras izplatīšana

- Janvāra sākumā Latvijā tika identificēts ZeuS robotu tīkla kontrolserveris. Tas bija izveidots uz uzlauzta tīmekļa servera, kas uzturēja novecojušu Wordpres tīmekļa vietni. CERT.LV atklāja, ka upuru skaits, kuru kontrolē serveris, ir 32, taču neviens no tiem neatradās Latvijā. Tika informētas attiecīgo valstu CERT vienības. Robotu tīkla kontrolcentrs sadarbībā ar Valsts policiju tika likvidēts.
- Aprīlī CERT.LV konstatēja pirmos „Dyre Wolf trojan" infekcijas gadījumus Latvijā.
- Aprīlī parādījās pirmie gadījumi, kad kādas iestādes darbiniekiem tika iesūtīts datorvīruss, izmantojot inficētus Microsoft Word dokumentus, kas saturēja kaitīgus *macro* skriptus. Darbinieki tika brīdināti, mēģinājums inficēt datorus neizdevās.
- Jūlijā CERT.LV identificēja 62 uzlauztas tīmekļa vietnes, kas inficēja apmeklētāju datorus, izmantojot "Angler exploit kit" rīkus. Mazāk kā puse šo resursu bija .lv domēnu zonā, taču visi tika uzturēti uz Latvijas IP adresēm. Resursu turētāji tika informēti un uzsāka

darbu pie tīmekļa vietņu labošanas vai slēgšanas. Lielākā daļa uzlauzto vietņu tika uzturētas uz novecojušas Worpdpress vai Joomla satura vadības sistēmas.

- Septembrī CERT.LV apturēja Latvijā uzturētu Android OS ļaunatūras kontrolcentru. Kaitīgā programmatūra pārsvarā tika mērķēta pret Spānijas banku klientu Android viedierīcēm.
- Oktobrī caur e-pastiem tika izplatīts datorvīrusa instalators "Upatre". Tas, inficētas iekārtas gadījumā, ar Microsoft Outlook programmas palīdzību, izplata sevi tālāk visām upura e-pasta kontaktpersonām. Cieta arī vairākas valsts iestādes. Oktobra beigās atkārtoti tika izplatīts liels daudzums surogātpasta, ar pielikumā esošu "Upatre" datorvīrusu instalatoru. Tika inficēti arī vairāku pašvaldību datori. Tādējādi tika mēģināts izplatīt internetbanku apzagšanai domāto "Dyre" datorvīrusu.
- Oktobrī vairākās .LV zonas lapās tika konstatētas kļūdas, kas ļāva veikt SQL injekciju uzbrukumu. Lapu īpašnieki tika informēti.

"DDoS 4 Bitcoin" kampaņas

- Maijā CERT.LV saņēma informāciju par organizētām DDoS uzbrukumu kampaņām ar mērķi izspiest naudu. Uzbrucēji izsūtīja e-pastu organizācijai, draudot veikt DDoS uzbrukumu, ja netiks samaksāts no 20 līdz pat 100 Bitcoin. Uzbrucēji apgalvoja, ka viņu rīcībā ir resursi, lai organizētu līdz pat 400 Gbps apjomīgu uzbrukuma datu plūsmu. Vairākos gadījumos noziedzīgais grupējums veica iebiedēšanas uzbrukumus, kas sasniedza 50 Gbps, bet pārsvarā, ja upuris nesāka komunicēt un neatbildēja uz draudiem, nopietnāks uzbrukums netika uzsākts. CERT.LV informēja valsts iestādes un lūdza ziņot par šādiem gadījumiem.
- Oktobrī atkārtoti notika vairāki apjomīgi DDoS uzbrukumi Latvijā strādājošām komercbankām. Uzbrukumus organizēja „DDoS 4 Bitcoin" un "Armada" kibernoziedznieku grupējumi.

Pikšķerēšanas kampaņas

- Aprīlī kādas bankas vārdā tika izsūtīti e-pasti, kas saturēja saiti uz pikšķerēšanas vietni. CERT.LV informēja iesaistīto resursu turētājus. Atklājās, ka kaitīgās lapas izvietotas, izmantojot novecojušu Wordpress satura vadības sistēmu versiju ievainojamības.
- Nedrošas tīmekļa vietnes tika izmantotas pikšķerēšanas uzbrukumu veikšanai pret Brazīlijas banku klientiem. Latvijas domēnu zonā [.lv] esošas tīmekļa vietnes bija iesaistītas Brazīlijas bankas CAIXA klientu datu izkrāpšanā, uzturot pikšķerēšanas resursus. Visas iesaistītās tīmekļa vietnes bija kompromitētas.
- CERT.LV kopā ar bankām strādāja pie incidentu risināšanas, kuros Latvijas interneta lietotājiem masveidā tika izsūtītas pikšķerēšnas e-pasta vēstules, ar aicinājumiem apmeklēt tīmekļa vietni, kas izskatās līdzīgi internetbanku vietnēm. Uzbrukuma mērķis – izkrāpt lietotāju datus. CERT.LV panāca kaitīgo resursu aizvēršanu dažu stundu laikā. Neviena lietotāja konts necieta uzbrukumā. Uzbrukumā tika iesaistīti inficēti serveri.
- Masveidā tika izsūtīti e-pasti it kā Paypal tiešsaistes maksājumu sistēmas vārdā, ziņojot par konta bloķēšanu. Lai apstiprinātu savu identitāti un atrisinātu it kā radušās

problēmas, upuris tika aicināts apmeklēt uzbrucēju sagatavotu Paypal vietnes līdzinieku un veikt pieslēgšanos sistēmai. Ja upuris veica autentifikācijas mēģinājumu, tad lietotājvārds un parole nonāca uzbrucēju rīcībā.

Kaitīgas baneru apmaiņas vietnes

- Leģitīmu vietņu neatjauninātas vai kompromitētas baneru apmaiņas programmas, cuar kurām tiek izplatīta ļaunatūra, ir visnenovērtētākā problēma Latvijas interneta vidē. Diemžēl tā ir grūti atklājama, jo pašas vietnes ne vienmēr kontrolē caur tām sūtīto reklāmu saturu. Inficētus banerus izplatījuši gan populāri ziņu portāli, gan privātpersonu uzturētas un veidotas vietnes.
- Aprīlī tika atklāts, ka neatjaunināta servera dēļ kāda portāla reklāmas izplatīšanas programmā tika ievietots kaitīgs baneris, kas apmeklētāju datoriem mēģināja piegādāt datorvīrusu. Servera īpašnieki tika brīdināti, reklāmu izplatīšanas sistēma tika atslēgta līdz atjaunināšanai.
- Kāds iepazīšanās portāls pārsūtīja apmeklētājus uz Policijas vīrusa web versiju saturošu vietni. Kā noskaidrojās, portāls lietoja ārvalstu baneru apmaiņas sistēmas, pār kurām viņiem nebija nekādas kontroles. Uzbrucējiem, kompromitējot šo baneru sistēmu, izdevās piegādāt kaitīgu kodu visām tīmekļa vietnēm, kas lietoja ievainojamo baneru sistēmu.

Uzbrukumi, saistībā ar Latvijas Prezidentūru ES

- Janvārī pret tieslietu sektoru tika vērsts apjomīgs DDoS uzbrukums, kura ietekmē tika būtiski traucēta sektora institūciju un tīmekļa vietņu darbība. CERT.LV veica incidenta tehnisko analīzi, kuras rezultātā izdevās noskaidrot arī patieso uzbrukuma avotu neskatoties uz to, ka tas tika slēpts ar tehnoloģiskām metodēm.
- CERT.LV atmaskoja vērienīgu *typosquat* domēnu infrastruktūru. Daļa no tās bija uzturēta, lai iegūtu ar Latvijas prezidentūru ES padomē saistīto informāciju. Izmeklēšanas tehniskā informācija tika nodota tiesībsargājošām iestādēm.

3. Sadarbības un komunikācijas pasākumi

Jūlijā CERT.LV sāka publicēt iknedēļas ziņas par IT drošības incidentiem, atspoguļojot kiberdrošības aktualitātes Latvijā un pasaulē.

Oktobrī CERT.LV rīkoja kiberdrošības brokastis mediju pārstāvjiem par aktuālākajiem apdraudējumiem, kas skar interneta lietotājus un iespējām, kā pasargāties no jaunākajiem vīrusiem un krāpšanas shēmām interneta vidē.
Pasākums pulcēja 16 dažādu mediju pārstāvjus, tika sniegtas vairākas intervijas radio un TV, kā arī tika publicēti raksti presē un ziņu portālos. Pasākums notika Eiropas Kiberdrošības mēneša ietvaros.

Gada laikā stabili pieaug sekotāju skaits populārajās sociālo tīklu platformās Twitter un Facebook.
Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1430.
CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 268.

Gadījumos, kad CERT.LV saņem informāciju, ka izsūtīts liels skaits ar inficētām mēstulēm, sociālie mediji ir efektīvs veids, kā ātri brīdināt datorlietotājus. Arī ziņu portāli bieži publicē informāciju uzreiz pēc CERT.LV ziņu parādīšanās sociālajos tīklos, tādējādi paātrinot komunikāciju lietotāju vidū.

Pārskata periodā CERT.LV iesaistījās informatīvajās kampaņās. Viena no tām bija AS „Swedbank" digitālās drošības izstāde "7 zelta likumi tavu datu drošībai internetā". Paralēli izstādei, AS „Swedbank" rīkoja semināru ciklu "7 zelta likumi tavu datu drošībai internetā", kuru vadīja Swedbank drošības eksperti. Tāpat notika sadarbība ar LMT, Latvijas Komercbanku asociāciju, SIA DPA, DNB Latvijas barometru un LIKTA.

CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. Kopā CERT.LV lapai bijuši 92,778 unikāli apmeklējumi jeb sesijas.

CERT.LV turpināja uzturēt arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus un atbildot uz lietotāju komentāriem.

4. Izglītojošie pasākumi

2015. gadā CERT.LV turpināja rīkot izglītojošus pasākumus par drošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem, studentiem un citiem interesentiem.

Gada lielākais pasākums bija ikgadējā IT drošības konference „Kiberšahs. Stratēģija un taktika virtuālajā vidē", kas notika 1. oktobrī Latvijas Nacionālajā bibliotēkā. Konferenci klātienē apmeklēja 499 dalībnieki, savukārt interneta tiešraidi vēroja 2000 unikāli lietotāji.
Nozīmīgākās tēmas bija kiberterorisms, mobilo ierīču drošības izaicinājumi, interneta troļļi, drošas programmatūras izstrādes principi.
Konference tika organizēta sadarbībā ar ISACA Latvijas nodaļu. Pasākumu atbalstīja SIA DEAC, SIA „Latvijas Mobilais Telefons" un NIC.

CERT.LV organizētie pasākumi IT drošības speciālistiem

No 5.- 6. martam CERT.LV un Zemessardzes Kiberaizsardzības vienība rīkoja tehniskās mācības „Marta migla". Mācību mērķis bija pārbaudīt dalībnieku prasmes IT infrastruktūras aizsardzībā, IT drošības uzbrukumu atklāšanā un novēršanā. Mācībās piedalījās 59 dalībnieki.

29. aprīlī CERT.LV rīkoja semināru "Esi drošs - 2". Seminārā tika apskatītas tādas tēmas kā izmaiņas IT drošības likumā, mobilo iekārtu lietošanas riski, „whitelist" saraksta izmantošana, aizsardzībai pret vīrusiem un piekļuves lieguma uzbrukumi ES prezidentūras laikā. Semināru atbalstīja SIA DSS un LMT. Pasākumu apmeklēja 254 dalībnieki, savukārt semināra tiešraidi vēroja 249 unikālie apmeklētāji.

30. jūlijā CERT.LV rīkoja semināru "Moderno operētājsistēmu ekspluatācijas pamati", kas bija paredzēts IT drošības speciālistiem ar priekšzināšanām, piedāvājot iespēju veikt virkni praktiskus uzdevumus. Seminārā piedalījās 12 dalībnieki.

No 4. līdz 6. augustam CERT.LV sadarbībā ar ENISA rīkoja semināru "Pierādījumu vākšana un artefakti digitālajā vidē". Semināra dalībnieki iepazinās ar mobilo iekārtu incidentu veidiem un to risināšanu, pierādījumu vākšanu un artefaktu analīzi digitālajā vidē. Semināru apmeklēja 34 dalībnieki.

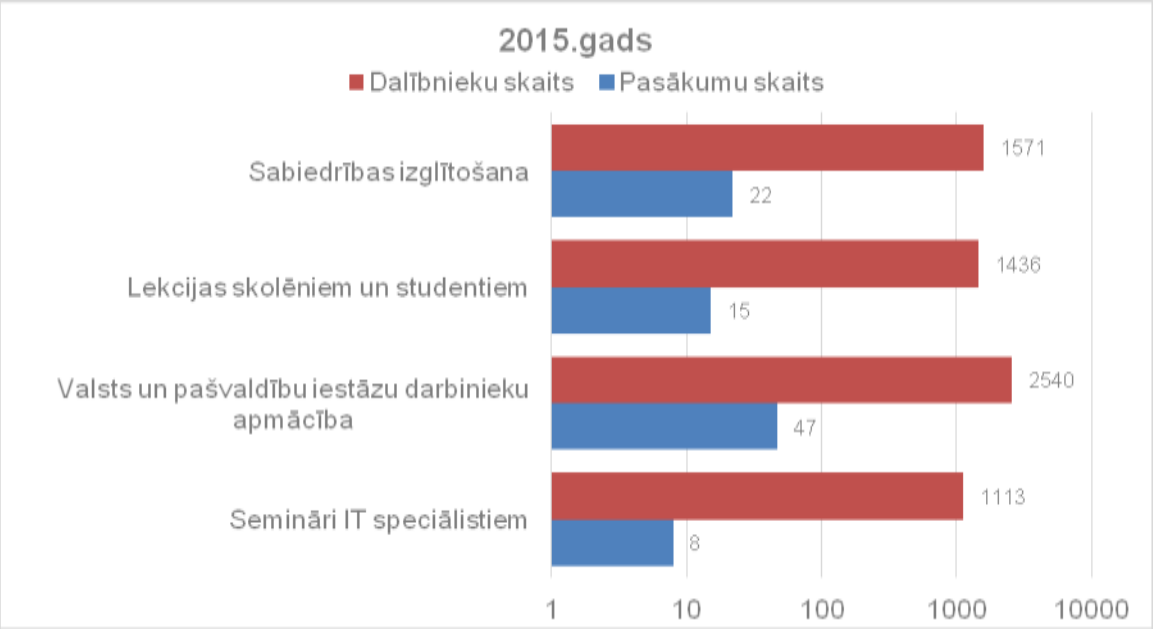
3. decembrī CERT.LV rīkoja otro semināru "Esi drošs". Seminārā tika prezentētas tādas tēmas kā aktualitātes IT drošības jomā, bezvadu tīklu drošības aspekti, SSL/TLS protokolu drošības izaicinājumi, datu drošība mākonī un sociālās inženierijas stresa testi iestādēs. Semināru apmeklēja 199 dalībnieki no valsts un pašvaldību iestādēm.

CERT.LV prezentācijas par IT drošību

CERT.LV arī šogad piedāvāja noklausīties lekciju par IT drošības aktualitātēm, iespējām sevi pasargāt no izplatītākajiem apdraudējumiem, izmantojot praktiskus piemērus. Lekcijas paredzētas skolēniem, skolotājiem, iestāžu darbiniekiem, vadītājiem un citiem interesentiem.
Šī gada laikā būtiski pieauga interesentu skaits, kas vēlas noklausīties lekciju, tāpat ir iestādes, kas aicina CERT.LV pārstāvi runāt atkārtoti, uzlabojot iestādes drošības kultūru.

Lai iegūtu izpratni par iestāžu darbinieku drošības paradumiem internetā un veiktu izplatītāko risku analīzi, 2015. gada sākumā CERT.LV uzsāka valsts un pašvaldību iestāžu darbinieku aptauju. Aptaujā piedalījās 771 respondents no 20 iestādēm. Rezultāti tika prezentēti CERT.LV konferencē.

Kopā 2015. gadā CERT.LV par IT drošību tika izglītoti 6680 dalībnieki, kuri piedalījās 103 dažādos pasākumos. Lielākā auditorija bija valsts un pašvaldību iestāžu darbinieki.



4.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2015. gadā.

Sabiedrības izglītošana

No 2015. gada 23.marta līdz 27. martam CERT.LV iesaistījās "E-prasmju nedēļas 2015" aktivitātēs. 25.martā CERT.LV organizēja ikgadējo „Datorologa akciju", kuras ietvaros iedzīvotājiem bija iespēja veikt bezmaksas datora pārbaudi. Otra akcija notika 28. oktobrī.

Tāpat CERT.LV pārstāvji uzstājās ar prezentācijām dažādos sadarbības partneru pasākumos - konferencēs, diskusijās un sanāksmēs.

5. Sadarbība ar valsts iestādēm

CERT.LV 2015. gadā piedalījās dažādu darba grupu darbībā, likumprojektu izstrādē un sniedza konsultācijas IT drošības jautājumos dažādām valsts iestādēm.

Sadarbība ar Aizsardzības ministriju

Regulāri notika tikšanās ar ministrijas Valsts sekretāru un komunikācija ar Nacionālās kiberdrošības politikas koordinācijas nodaļu.
CERT.LV iesaistījās Aizsardzības ministrijas darba grupā par atbildīgas ievainojamību atklāšanas politikas ieviešanu.

CERT.LV piedalījās Aizsardzības ministrijas darba grupā par MK noteikumu Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" izstrādi.
2015. gada 28. jūlijā šie noteikumi tika apstiprināti. Tie nosaka valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā tiek nodrošināta valsts un pašvaldību institūciju IKT sistēmu atbilstība šīm prasībām.

Latvijas Prezidentūra ES Padomē

CERT.LV ar Aizsardzības ministrijas un nozares atbalstu veica lielus sagatavošanās darbus, lai prezidentūra noritētu pēc iespējas gludāk un netiktu traucēts iestāžu darbs pat apjomīgu uzbrukumu gadījumos. Tika sagatavota aizsardzības infrastruktūra un veikti vairāk kā 100 ielaušanās testi, kuru rezultātā atklāti un novērsti būtiski drošības trūkumi.

Prezidentūras norises laikā īpaša gatavība reaģēt bija Prezidentūras sākumā, 16.martā, 9.maijā, Austrumu partnerības samita un Digitālās asamblejas laikā. Šajos datumos CERT.LV darbojās paaugstinātas gatavības režīmā, pievēršot īpašu uzmanību kibertelpas situācijas un izmaiņu uzraudzībai.

Citi sadarbības partneri

CERT.LV sadarbojās ar Zemessardzes Kiberaizsardzības vienību, kopīgi piedaloties dažādās tehniskajās mācībās, kā arī nodrošinot vienībai virtuālu treniņu vidi drošības incidentu risināšanas pilnveidei. CERT.LV atbalsta arī vienības biedrus drošības pētniecībā, veicinot atbildīgas ievainojamību atklāšanas praksi. Šīs aktivitātes ietvaros ir atklātas vairākas ievainojamības.

CERT.LV turpināja atbalstīt Drošības ekspertu grupas (DEG) darbību, kas nodrošina diskusiju forumu IT drošības speciālistiem gan no privātā, gan valsts sektora. DEG sanāksmes notika reizi mēnesī.

6. Starptautiskā sadarbība

Pārskata periodā CERT.LV stiprināja sadarbību ar citu valstu IT drošības incidentu novēršanas vienībām un starptautiskām organizācijām.
CERT.LV speciālisti uzstājās ar prezentācijām starptautiskās konferencēs, semināros un apguva jaunas prasmes tehniskajās mācībās. Tāpat virkne starptautisku pasākumu notika Prezidentūras ietvaros.

Sadarbība ar CERT kopienu

CERT.LV pārstāvji pārskata periodā piedalījās TF-CSIRT un FIRST tehniskajos semināros. Turpinājās sadarbība ar Trusted Introducer servisa nodrošinātājiem, uzsākot CERT.LV gatavošanos starptautiskajai Trusted Intrducer sertifikācijai.
CERT.LV vadītāja B. Kaškina 2015.gadā bija TF-CSIRT grupas vadītāja un vadīja visas TF-CSIRT un Trusted Introducer sanāksmes.

Sadarbība ar ENISA

Daudzveidīga sadarbība notika ar Eiropas Tīkla un informācijas drošības aģentūru, piemēram, rīkojot seminārus un mācību kursus

No 11. līdz 12. maijam CERT.LV kopā ar ENISA organizēja starptautisku semināru "CERTs in Europe", kurā piedalījās dalībnieki no 20 valstīm. Seminārs fokusējās uz dažādu valstu pieredzi, saistītu ar prezidentūru Eiropas Savienības Padomē un Tīklu un informācijas drošības direktīvu.

13. maijā ENISA un Aizsardzības ministrija Rīgā organizēja konferenci Latvijas prezidentūras ES padomē ietvaros par atbildīgu ievainojamību atklāšanu. CERT.LV pārstāvis konferencē uzstājās ar prezentāciju un piedalījās paneļdiskusijā.

16. jūnijā CERT.LV pārstāvis piedalījās ENISA organizētajā „EU28 Cloud Security Conference: Reaching the Cloud Era in the European Union", kas notika Rīgā. Tāpat CERT.LV pārstāvji piedalījās "ENISA Train the Trainers" seminārā Tallinā, Igaunijā.

CERT.LV aktīvi iesaistījās ENISA organizētājās kiberdrošības mācībās "Cyber Europe 2014" trešajā - stratēģiskajā fāzē, kas notika no 2015. gada februārī, Briselē, Beļģijā.

Sadarbība ar NATO CCDCoE

CERT.LV pārstāvji sadarbojās ar NATO Cooperative Cyber Defence Centre of Exelence.
Nozīmīgākais pasākums bija starptautiskās kiberdrošības mācības "Locked Shields 2015", kuras notika no 22. līdz 24. aprīlim. Latvijas - Lietuvas apvienotā komanda 16 komandu konkurencē ieguva 4. vietu, savukārt juridiskajā komponentē komanda bija otra labākā.

No 25. līdz 29. maijam CERT.LV pārstāvji piedalījās CCDCoE organizētajā CyCON konferencē Tallinā, Igaunijā.
Tāpat tika papildinātas zināšanas un prasmes NATO CCDCoE rīkotajos mācību kursos par IT drošības tēmām.

Starptautiskie pasākumi

2015. gadā CERT.LV pārstāvji piedalījās starptautiska līmeņa pasākumos, lai veicinātu sadarbību un apgūtu jaunas zināšanas un prasmes.

Nozīmīgākie pasākumi:

- „One Conference" Nīderlandē.
- FI-ISAC (European FI-Information Sharing and Analysis Center) sanāksme Nīderlandē.
- 2ND BALTIC – U.S. Seminar on Critical Energy Infrastructure Protection and Cybersecurity.
- CERT.LV pārstāvja dalība Aizsardzības ministrijas organizētā vizītē Japānā, ministrijas Valsts sekretāra delegācijas sastāvā.
- Vispasaules Nacionālo CERTu sanāksme un FIRST konference Vācijā.
- CERT-EU konference Beļģijā.

Starptautiskās kiberdrošības mācības

No 24. februārim līdz 26. februārim CERT.LV piedalījās ENISA organizētājās kiberdrošības mācībās "Cyber Europe 2014" trešajā - stratēģiskajā fāzē Briselē, Beļģijā.
Mācību mērķi bija Eiropas IT drošības krīžu pārvaldības procedūru un mehānismu testēšana, valsts līmeņa IT drošības kapacitātes uzlabošana un sadarbības izpēte starp valsts un privāto sektoru. Mācības notika trīs posmos jeb fāzēs.

No 22. aprīļa līdz 24. aprīlim notika lielākās starptautiskās tehniskās kiberdrošības mācības "Locked Shields 2015", kuras organizēja NATO CCDCoE. Latvijas komandu veidoja CERT.LV, Zemessardzes Kiberaizsardzības vienība, kiberdrošības eksperti no privātā sektora un Lietuvas CERT kiberdrošības eksperti.
Mācību mērķis bija sagatavot speciālistus mainīgajai kiberdrošības videi, izmantojot reālas tehnoloģijas un uzbrukumu metodes.
Latvijas-Lietuvas apvienotā komanda 16 komandu konkurencē ieguva 4. vietu.

No 16. līdz 20. novembrim norisinājās ikgadējās NATO "Cyber Coalition 2015" treniņmācības, kurās piedalījās ap 600 kiberdrošības ekspertu no NATO un tās partneru dalībvalstīm, tai skaitā arī Latvijas pārstāvji no CERT.LV, Zemessardzes Kiberaizsardzības vienības un Nacionālajiem bruņotajiem spēkiem.

Plašāka informācija par CERT.LV uzdevumu izpildi pieejama CERT.LV mājaslapā:
https://cert.lv/section/show/48

Atskaiti sagatavoja:
CERT.LV Sabiedrisko attiecību projektu vadītāja Svetlana Amberga, tālrunis 67085851,
e-pasts svetlana.amberga@cert.lv

2016. gada 15. martā