CERT.LV DARBĪBAS PĀRSKATS

2024

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Satura rādītājs

Kopsavilkums

Latvija saglabā augstu kibernoturības līmeni, neraugoties uz ievērojamu kiberapdraudējumu skaita pieaugumu, to sarežģītību un intensitāti. Kibertelpā joprojām vērojami finansiāli un ģeopolitiski motivēti kiberuzbrukumi. Kiberuzbrucēji aktīvi izmanto cilvēku neuzmanību un tehnoloģiju ievainojamības, gudri pielietojot pikšķerēšanu, skenēšanu, vāju autentifikāciju un mērķētu ļaunatūras piegādi.

2024. gada 4. ceturksnī sasniegts vēsturiski augstākais kiberapdraudējumu līmenis Latvijā. CERT.LV reģistrēto ziņojumu skaits (418 325) salīdzinājumā ar 3. ceturksni ir audzis par 3% un salīdzinājumā ar attiecīgo periodu pērn – par 25%.

Kiberdrošības situāciju joprojām nosaka ģeopolitiskā spriedze un ideoloģiskie konflikti pasaulē. Kiberapdraudējumi Latvijā, tajā skaitā arī finansiāli motivēti, galvenokārt ir saistāmi ar Krieviju atbalstošiem kiberuzbrucējiem. Biežāka interese par Latvijas IKT infrastruktūru vērojama arī no kiberuzbrucējiem, kas, iespējams, saistāmi ar Ķīnu, liecinot par jaunu pavērsienu Ķīnas atbalstīto kiberuzbrucēju realizētās kiberoperācijās.

Kiberuzbrucēji lielākoties izmanto DDoS uzbrukumus, dažādas ievainojamības, internetā nedroši eksponētas iekārtas un sarežģītas sociālās inženierijas taktikas, lai traucētu pakalpojumu sniegšanu, inficētu neatjauninātas iekārtas, veiktu kiberspiegošanu un zagtu datus.

Fiksētie kiberuzbrukumi kopumā nav radījuši būtisku ietekmi uz sabiedrības drošību un būtiskajiem un svarīgajiem pakalpojumiem, kas norāda uz efektīvu aizsardzības pasākumu kopumu. Taču kiberuzbrukumu veidi, to intensitāte un komplicētība attīstās ļoti strauji. Ir svarīgi turpināt darbu un ieguldījumus kibernoturības un aizsardzības risinājumos, lai pilnvērtīgi aizsargātu tīklu un informācijas sistēmas. Nepieciešams turpināt vairot gala lietotāju izpratni, gan sniedzot informāciju par aktuālo situāciju, kiberapdraudējumiem un ievainojamībām, gan veicinot labu kiberhigiēnas praksi.

CERT.LV DNS ugunsmūris, starptautiskās kiberdrošības draudu medības un pieaugoša valsts pārvaldes iestāžu darbinieku izpratne par kiberhigiēnu veido stingru pamatu stiprākai aizsardzībai.

Latvijas kibertelpas stiprināšanu turpina veicināt Nacionālās kiberdrošības likums (NKDL), kas stājās spēkā 2024. gada 1. septembrī, paplašinot to organizāciju loku, uz kurām attiecas būtiski papildinātās Eiropas Parlamenta un Padomes tīklu un informācijas sistēmu direktīvas 2022/2555 (NIS2) prasības.

Būtiskāko kiberapdraudējumu dinamika un tendences

2024. gada 4. ceturksnī kvantitatīvo rādītāju ziņā kiberapdraudējumu TOP 5 ierindojas konfigurācijas nepilnības, ļaundabīgs kods, informācijas vākšana, ielaušanās mēģinājumi un krāpšana. Salīdzinot ar šo pašu periodu pirms gada, lielākais pieaugums ir šādos apdraudējuma veidos:

- informācijas vākšana (+98%),
- konfigurācijas nepilnības (+28%),
- krāpšana (+25%)
- ielaušanās mēģinājumi (+4%).

Ievainojamību izmantošana joprojām ir viens no galvenajiem piekļuves punktiem kiberuzbrukumos, lai iefiltrētos sistēmās un nozagtu vērtīgus datus. Līdztekus tiek izmantotas sen zināmas konfigurācijas nepilnības plaši lietotos produktos un jaunatklātas ievainojamības, lai iekļūtu organizāciju iekšējos tīklos un nesankcionēti piekļūtu sensitīvai informācijai. Cilvēciskais faktors un vāju paroļu izmantošana arī rada nopietnus riskus, ļaujot pikšķerētājiem apdraudēt pat labi aizsargātas sistēmas.

Konfigurācijas nepilnību, internetā nedroši eksponētu iekārtu, kas ļauj piekļūt sistēmām un datiem, īpatsvars pieaug. Tas norāda uz tehnoloģiju un sistēmu pieaugošo sarežģītību, padarot tās grūtāk pārvaldāmas un konfigurējamas, turklāt organizācijām joprojām trūkst kvalificētu kiberdrošības speciālistu.

Kvantitatīvo rādītāju ziņā DDoS uzbrukumu skaits ir samazinājies, vienlaikus tie ir kļuvuši sarežģītāki, koncentrētāki un jaudīgāki, padarot tos potenciāli "sāpīgākus". Neraugoties uz pieaugošo kiberuzbrukumu intensitāti, to ietekme bija maznozīmīga, kas norāda uz Latvijas augsto kibernoturību.

Pieaug ar datu noplūdēm saistītie kiberdraudi tām organizācijām, kas glabā fizisko personu datus. 4. ceturksnī notika vēsturiski ievērojamākais datu izgūšanas incidents Latvijā, kad kiberuzbrucējiem bija izdevies piekļūt uz "ZZ Dats" uzturētā servera esošai datubāzei. Šis incidents tiešā veidā ietekmējis 42 Latvijas pašvaldības. Tā rezultātā ir apdraudēta personas datu drošība, kas var tikt izmantota turpmāk mērķētā pikšķerēšanā pret iedzīvotājiem.

Krāpšanas gadījumos izkrāptās naudas apmēri turpina augt, krāpniekiem izmantojot arvien efektīvākas sociālās inženierijas metodes un mākslīgā intelekta instrumentus. Visizplatītākās finansiāli motivētās krāpniecības bija saistītas ar sūtījumu piegādes tematiku. Lai arī šo krāpšanas gadījumu skaits bija liels, to nodarītie zaudējumi ir salīdzinoši nelieli. Lielāka ietekme bija telefonkrāpniecībām un viltus investīciju platformām. Vairumā gadījumu telefonkrāpnieki uzdevās par banku, valsts un tiesībsargājošo iestāžu pārstāvjiem. CERT.LV saņemtie ziņojumi liecina, ka iedzīvotājiem ne vienmēr ir skaidra izpratne par iestāžu oficiālo komunikāciju, kā rezultātā krāpniekiem tiek izpausta personīga informācija un nodoti maksājumu karšu un bankas kontu dati.

Kvantitatīvo rādītāju ziņā ļaundabīga koda izraisītu kiberincidentu skaits ir samazinājies, kas norāda uz efektīviem aizsardzības mehānismiem, taču apdraudēto unikālo IP adrešu skaits joprojām saglabājas augsts. Pikšķerēšana ir iecienītākā metode ļaunatūru izplatīšanai, izmantojot sociālos medijus un populāras e-pasta mārketinga platformas.

CERT.LV pakalpojumu attīstība un efektivitāte

DNS ugunsmūris: 2024. gada 4. ceturksnī DNS ugunsmūra lietotāji tika pasargāti no kaitīgu vietņu apmeklēšanas **459 213** reizes, pārvirzot galalietotāju uz CERT.LV brīdinājuma vietni. Tas ir par **344%** vairāk nekā 3. ceturksnī. Kopš 2024. gada rudens ir pieejama DNS ugunsmūra mobilā lietotne, kas ir ērti lejupielādējama un aktivizējama mobilajās iekārtās "Android" un "iOS" lietotājiem. Lietotne ne tikai pasargā no tieši Latvijā aktuālās krāpnieciskās kampaņās izmantotu ļaunprātīgu saišu apmeklēšanas, bet arī bloķē telefonzvanus no numuriem, ko CERT.LV ir identificējusi kā krāpnieciskus. Lietotne sniedz atgriezenisko saiti par novērstajiem apdraudējumiem.

Agrās brīdināšanas sistēma (ABS): Pārskata periodā ABS ģenerēto brīdinājumu skaits kopskaitā bija **2,4 miljardi** jeb par pusmiljonu vairāk nekā 2024. gada 3. ceturksnī. Tas ir skaidrojams ar plaša mēroga pikšķerēšanas un datorvīrusiem saistītu brīdinājumu skaita pieaugumu. ABS ik mēnesi fiksē vidēji **6 000** augstas prioritātes kiberapdraudējumus (incidenti ar augstu bīstamības potenciālu) valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs.

Draudu medību operācijas: Stiprinot Latvijas kibertelpu, līdz pārskata beigām CERT.LV kiberdrošības draudu medību operācijās analīze veikta jau **150 000** gala iekārtās dažādās publiskā sektora iestādēs un IKT kritiskās infrastruktūras organizācijās. Aptuveni **20%** gadījumu infrastruktūrā tika konstatēta citu valstu atbalstītu kiberuzbrucēju klātbūtne un citi būtiski kiberapdraudējumi, kurus mērķa organizācijām pēc veiktajām draudu medībām bija iespēja novērst, pieņemot datos balstītus lēmumus.

Neraugoties uz augsto kiberapdraudējumu intensitāti, Latvija ne tikai veiksmīgi stāv pretī pieaugošiem izaicinājumiem, bet ir kļuvusi par piemēru daudzām citām valstīm, saglabājot līdera lomu Eiropā apjomīgu kiberdrošības draudu medību jomā. Sadarbībā ar Kanādas bruņotajiem spēkiem CERT.LV izveidoja unikālu Draudu medību rokasgrāmatu, kurā iekļautas rekomendācijas draudu medību veikšanai, kā arī tika novadīts nozīmīgs pirmais seminārs starptautiskajiem partneriem, daloties ar līdzšinējo pieredzi.

IT sistēmu drošības testi: 2024. gada 4. ceturksnī CERT.LV speciālisti veica **4** drošības testus un **7** pikšķerēšanas uzbrukumu simulācijas dažādās publiskā sektora iestādēs un IKT kritiskās infrastruktūras organizācijās. To laikā tika konstatētas un novērstas dažādas ievainojamības, tostarp kritiskas, kā arī tika trenētas šo organizāciju darbinieku kiberhigiēnas prasmes.

Drošības operāciju centrs (SOC): Turpinās SOC attīstīšana un jaunu klientu piesaiste. Uz pārskata perioda beigām SOC uzraudzīto iekārtu skaits klientu infrastruktūrā sasniedza **5 290**, proaktīvi un profesionāli nodrošinot kiberapdraudējumu un kompromitētu sistēmu atpazīšanu. Reģistrēti vairāk nekā **392 000** drošības telemetrijas trauksmes ziņojumi, no kuriem **650** bija kritiski.

Koordinēta ievainojamību atklāšana (CVD): Pārskata periodā CVD platformā drošības pētnieku skaits palielinājās par **13%**, aktīvas iestāžu programmas pieauga par **20%** un ievainojamību ziņojumu skaits – par **23%**. CVD ziņošanas prakse palīdz savlaicīgāk uzzināt par ievainojamībām un koordinēt ievainojamību izpēti un to novēršanu, tādējādi efektīvāk organizēt pasākumus kibertelpas aizsardzībai.

Apmācības un izglītojošie pasākumi kiberdrošības jomā: Pārskata periodā īstenoti **74 (+57)** pasākumi ar kopskaitā **15 593 (+7 806)** dalībniekiem, veicinot kiberdrošības kultūru iedzīvotāju un organizāciju vidū un stiprinot kibernoturību.

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Latvija turpina veiksmīgi demonstrēt augstu kibernoturību, neraugoties uz vēsturiski līdz šim augstāko kiberapdraudējumu līmeni, nopietniem izaicinājumiem un kiberuzbrukumu intensitāti.

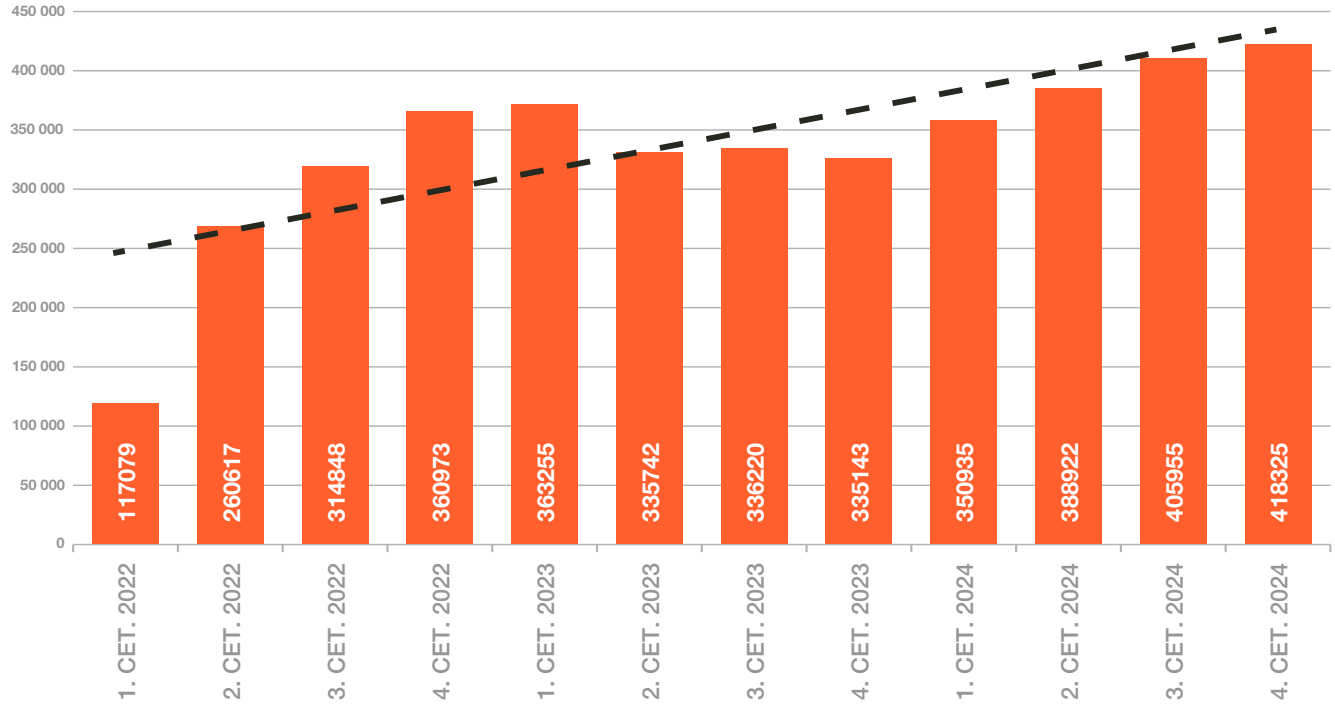
Kvantitatīvo rādītāju ziņā 2024. gada 4. ceturksnī kiberapdraudējumu TOP 5 ierindojās konfigurācijas nepilnības, kam seko ļaundabīgs kods, informācijas vākšana, ielaušanās mēģinājumi un krāpšana (2. attēls).

Reģistrēto apdraudēto unikālo IP adrešu lielāko skaitu (267 933) veido "citi" kiberapdraudējuma veidi ar "Shadowserver" fiksētiem maznozīmīgiem apdraudējumiem, kas ir saistīti ar individuālu lietotāju iekārtām un plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem organizācijām.

2024. gada 4. ceturksnī sasniegts vēsturiski augstākais apdraudēto unikālo IP adrešu skaits Latvijā, kas liecina par ievērojamu kiberapdraudējumu pieaugumu un intensitāti.

CERT.LV reģistrēto ziņojumu skaits ir audzis salīdzinājumā ar 3. ceturksni par 3% un salīdzinājumā ar 2023. gada 4. ceturksni par 25%.

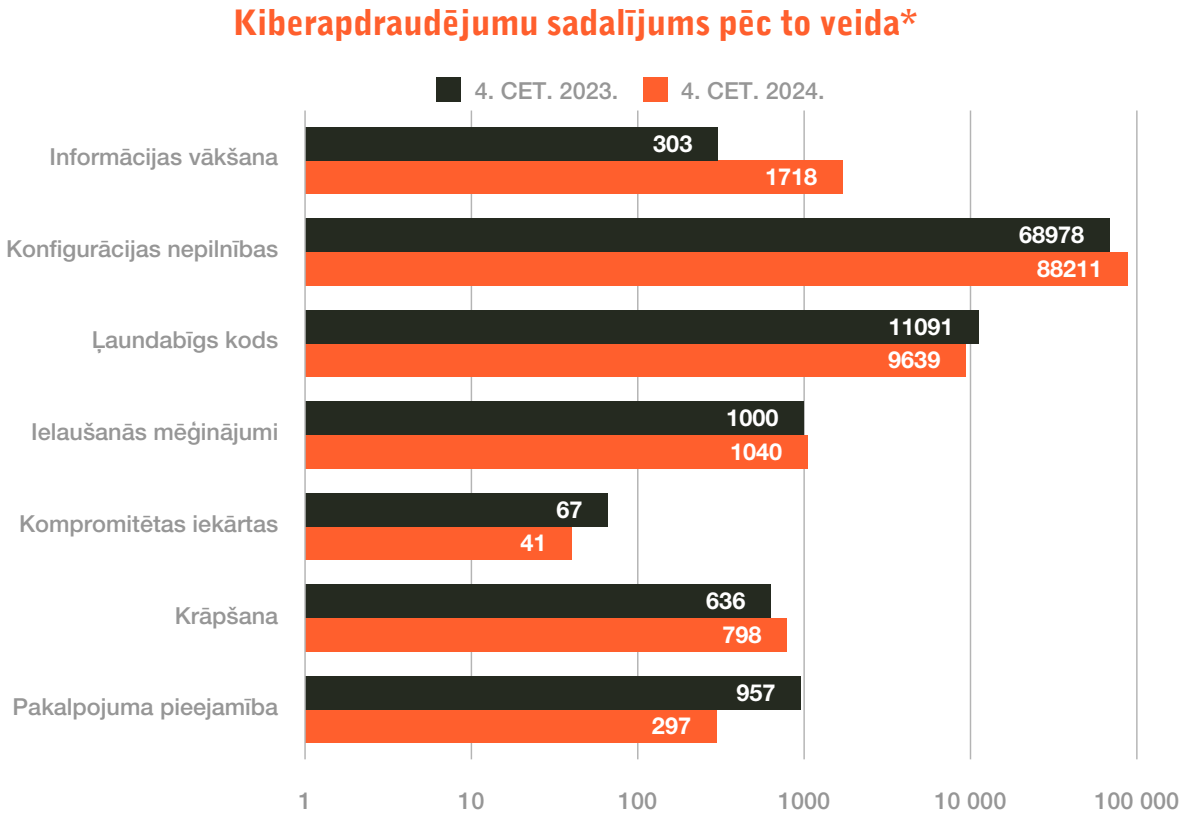
Kiberapdraudējumu dinamika pa ceturkšņiem



1. attēls. Apdraudētās unikālās IP adreses pa ceturkšņiem 2022. - 2024. gadā

Kiberapdraudējuma veids (apdraudēto unikālo IP adrešu skaits)	Izmaiņas pret 2024. gada 3. ceturksni	Izmaiņas pret 2023. gada 4. ceturksni
Konfigurācijas nepilnības (88 211)	+ 1%	+ 28%
Ļaundabīgs kods (9 639)	- 19%	- 13%
Informācijas vākšana (1 718)	+ 467%	+ 98%
Ielaušanās mēģinājumi (1 040)	+ 6%	+ 4%
Krāpšana (798)	- 38%	+ 25

CERT.LV aktīvi sadarbojas ar valsts un privātajiem uzņēmumiem, lai palīdzētu atvairīt kiberuzbrukumus un stiprinātu vispārējo kiberdrošību. Publiskā un privātā sektora organizācijas Latvijā aizvien aktīvāk ziņo par kiberincidentiem un ievainojamībām, kā arī arvien biežāk izmanto CERT.LV atbalstu. Tas liecina par pieaugošu uzticības līmeni starp organizācijām un CERT.LV komandu kiberdrošības stiprināšanā.



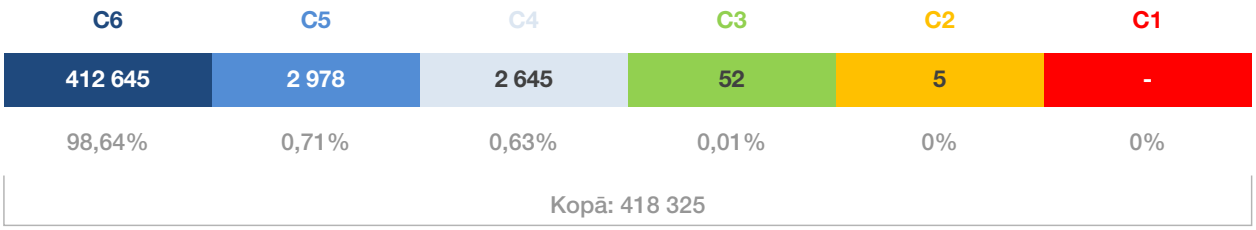
2. attēls. Apdraudēto unikālo IP adrešu skaita salīdzinājums pēc kiberapdraudējuma veida.

*Grafikā nav iekļauti - Cits, Informācijas drošība un Kaitīgs saturs.

Latvijas kibertelpas stiprināšanu turpina veicināt Nacionālās kiberdrošības likums (NKDL), kas stājās spēkā 2024. gada 1.septembrī, paplašinot to organizāciju loku, uz kurām attiecas būtiski papildinātās Eiropas Parlamenta un Padomes direktīvas (NIS2) prasības.

Apdraudētās unikālās IP adreses pēc svarīguma un ietekmes

CERT.LV reģistrētie kiberapdraudējumi tiek klasificēti no zemākās (C6) līdz augstākajai (C1) kategorijai. Pārskata periodā C1 kategorijas jeb nacionāla līmeņa apdraudējumi nav fiksēti. C2 kategorijā, kas ietver augstas nozīmes apdraudējumus, tika reģistrētas 5 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. C3 jeb nozīmīgi apdraudējumi ar plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 52 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem.



3. attēls. 4. ceturksnī apdraudēto unikālo IP adrešu sadalījums kategorijās pēc apdraudējuma ietekmes.

Lielākais kiberapdraudējumu īpatsvars fiksēts maznozīmīgu apdraudējumu kopā C6, kas ir saistīti ar plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem.

Kiberuzbrukumi tika vērsti pret valsts iestādēm, kā arī finanšu, transporta, enerģētikas, telekomunikācijas nozaru pakalpojumu sniedzējiem, taču tie neradīja būtisku vai ilgstošu ietekmi uz attiecīgo pakalpojumu vai resursu pieejamību.

Konfigurācijas nepilnību rezultātā, internetā nedroši eksponētu iekārtu, kas ļauj piekļūt sistēmām un datiem, īpatsvars pieaug. Tas norāda uz tehnoloģiju un sistēmu pieaugošo sarežģītību, padarot tās grūtāk pārvaldāmas un konfigurējamas, turklāt organizācijām joprojām trūkst kvalificētu kiberdrošības speciālistu. Kvantitatīvo rādītāju ziņā DDoS uzbrukumu skaits ir samazinājies, vienlaikus tie ir kļuvuši sarežģītāki, koncentrētāki un jaudīgāki, padarot tos potenciāli "sāpīgākus". Neraugoties uz pieaugošo kiberuzbrukumu intensitāti, to ietekme bija maznozīmīga.

2024. gada 4. ceturksnī reģistrētie būtiskākie kiberincidenti, kiberapdraudējumi un ievainojamības detalizētāk aplūkoti šī pārskata 2. nodaļā, ietverot arī praktiskus ieteikumus drošības uzlabošanai.

Galvenās kiberapdraudējumu tendences

Kiberapdraudējums – jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas.

Latvija turpina piedzīvot politiski motivētus kiberuzbrukumus pret atsevišķiem resursiem valsts un privātajā sektorā. Latvijas kibertelpā galvenokārt bija vērojami kiberuzbrucēji, kuru darbības potenciāli varētu būt saistītas ar Krieviju, tajā skaitā arī finansiāli motivēti uzbrukumi, taču arvien biežāk interese par Latvijas infrastruktūru vērojama arī no uzbrucējiem, kas iespējams saistāmi ar Ķīnu. Maznozīmīga klātbūtne Latvijas kibertelpā vērojama arī no uzbrucējiem, kas varētu tikt saistīti ar Baltkrieviju un Ziemeļkoreju. Ar Baltkrieviju iespējami saistāmo uzbrucēju aktivitātes pārklājas ar Krievijas interesēm, bet ar Ziemeļkoreju potenciāli saistāmās operācijas vērstas uz finanšu līdzekļu ieguvi.

Ievainojamību izmantošana joprojām ir viens no galvenajiem piekļuves punktiem gan valstu atbalstītiem kiberoperāciju grupējumiem, gan finansiāli motivētiem kibernoziedzniekiem, lai iekļūtu sistēmās un nozagtu vērtīgus datus. Cilvēciskais faktors un vāju paroļu izmantošana arī rada nopietnus riskus, ļaujot pikšķerētājiem apdraudēt pat šķietami labi aizsargātas sistēmas.

Kiberuzbrucēji arvien biežāk izmanto konfigurācijas nepilnības, lai piekļūtu sistēmām un datiem. Konfigurāciju nepilnību pieaugums norāda uz to, ka tehnoloģiju un sistēmu sarežģītība pieaug, padarot tās grūtāk pārvaldāmas un konfigurējamas. Organizācijām trūkst resursu, lai efektīvi pārvaldītu un konfigurētu sarežģītas sistēmas un veiktu regulāras pārbaudes.

Pieaug ar datu noplūdēm saistītie kiberdraudi, kas galvenokārt vērsti pret organizācijām, kas glabā fizisko personu datus. Tas uzsver nepieciešamību pēc pastāvīgas, rūpīgas sistēmu pārvaldības un regulāras drošības pārbaudes. Būtiski ir parūpēties par visiem organizācijas uzraudzībā esošiem digitālajiem resursiem, regulāri tos atjaunot.

Krāpšanas gadījumos izkrāptās naudas apmēri turpina augt, krāpniekiem izmantojot arvien efektīvākas sociālās inženierijas metodes un mākslīgā intelekta instrumentus. Latvijas Finanšu nozares asociācijas apkopotie dati par krāpšanas gadījumiem liecina, ka Latvijas iedzīvotājiem ik mēnesi, pašiem apstiprinot maksājumus, kopumā tiek izkrāpti 1-1,5 miljoni eiro.

Joprojām tiek izmantotas vājas paroles un netiek lietota vairāku faktoru autentifikācija. Šī problēma eksistē gan pakalpojumu ņēmēju, gan pakalpojumu sniedzēju pusē, lai gan tehniskie risinājumi pastāv jau gana ilgi.

CERT.LV saņemtie ziņojumi liecina, ka iedzīvotājiem ne vienmēr ir skaidra izpratne par iestāžu oficiālo komunikāciju, kā rezultātā krāpniekiem tiek izpausta personīga informācija un nodoti maksājumu karšu un bankas kontu dati.

2. TOP kiberincidenti un apdraudējumi: atbalsts un ieteikumi to novēršanā

CERT.LV, valstī lielākā kiberapdraudējumu datu apkopotāja, ik mēnesi apstrādā un analizē vairākus miljonus ienākošo signālu. Reģistrējot un uzturot informāciju par kiberdrošības apdraudējumiem, CERT.LV sniedz publiskā un privātā sektora organizācijām, kā arī fiziskām personām atbalstu kibericidentu risināšanā un novēršanā, ja incidentā iesaistīta Latvijas IP adrese vai .lv domēns.

Kiberincidents – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.

CERT.LV atzinīgi vērtē gan kiberdrošības kopienas dalībnieku ziņojumus "Mattermost" platformā, gan iedzīvotāju iesaisti, kuri identificē krāpnieciskas un kaitīgas e-pasta vēstules un saites, ziņojot un pārsūtot tās uz e-pastu cert@cert.lv, lai pasargātu citus. Veicinot un padarot ziņošanu ērtāku, ieviests telefona numurs krāpniecisku SMS pārsūtīšanai: +371 23230444 (telefona zvani netiek apstrādāti).

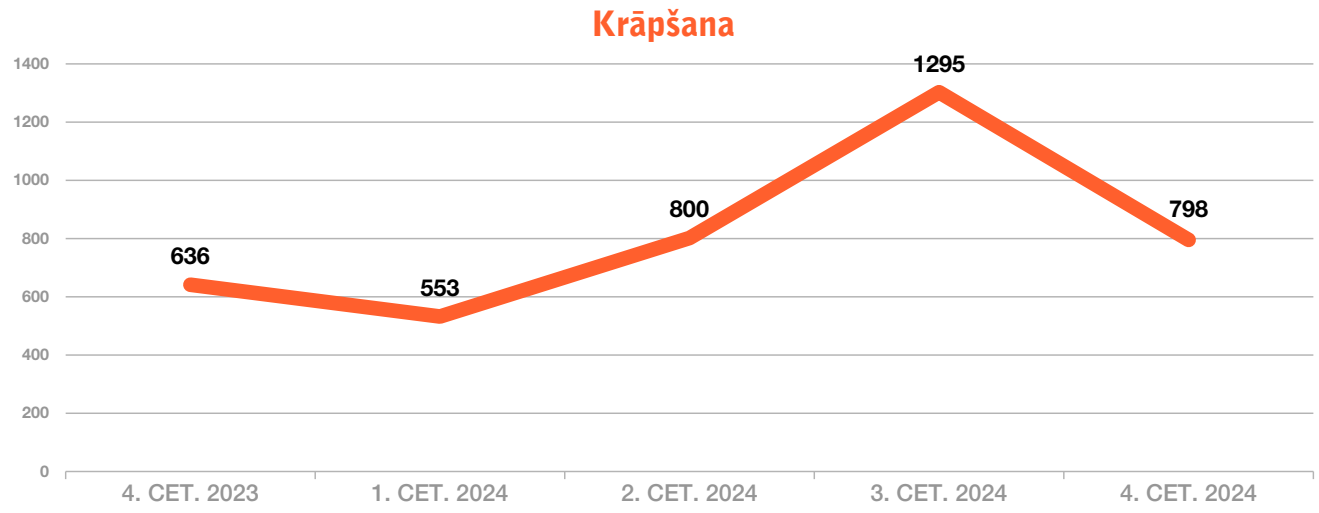
Apkopojot saņemtos ziņojumus, kaitnieciskie domēna vārdi tiek ievietoti aktīvās aizsardzības rīkā – DNS ugunsmūrī, kas ik dienu jau 5 gadus bez maksas pasargā no tieši Latvijā aktuālajām krāpnieciskās kampaņās izmantotām ļaundabīgām saitēm, vietnēm un kaitīga satura. Novembrī ieviestā mobilā lietotne palīdz arī pret identificētiem krāpnieku telefonu zvaniem.

2.1. Krāpšana

Salīdzinājumā ar 2024. gada 3. ceturksni pārskatā periodā CERT.LV reģistrēto krāpšanas gadījumos apdraudēto unikālo IP adrešu skaits ir samazinājies par 38%. Salīdzinājumā ar pagājušā gada 4. ceturksni – pieaugums par 25%.

Pārskata periodā CERT.LV un Latvijas Fakti veiktajā iedzīvotāju aptaujā 18% no respondentiem, kas cietuši krāpšanā, atzina, ka krāpnieku lamatās iekrituši steigas dēļ, 18% noticēja krāpniekiem, jo iepriekš nebija dzirdējuši par attiecīgo krāpšanas veidu, bet 32% saņemtās ziņas vai zvana saturs šķita ticams, tāpēc bija pārliecināti, ka komunicē ar atbilstošo organizāciju.

Kopumā 70% respondentu atbildēja, ka jūtas droši internetā, kaut gan puse aptaujāto atzina, ka varētu būt kiberuzbrukumu mērķis. Tikai nedaudz vairāk par 20% novērtēja savas zināšanas par kiberdrošību virs vidējā.



4. attēls. Apdraudēto unikālo IP adrešu skaits

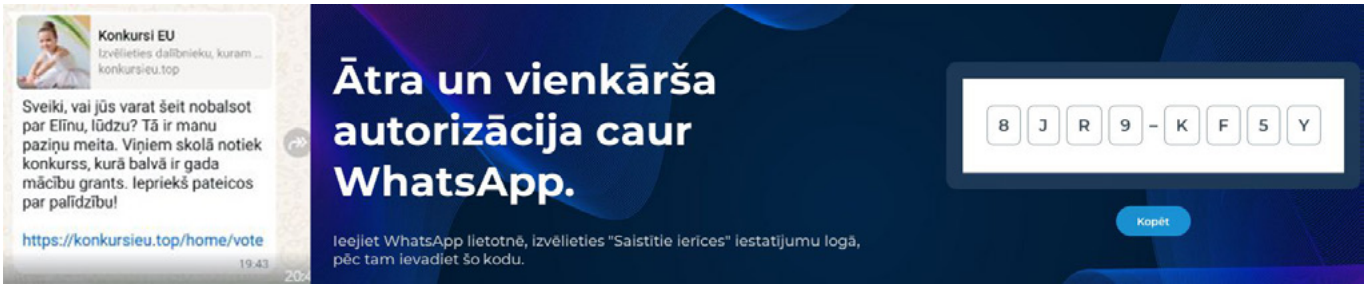
Izplatītākie krāpšanas veidi:

Pikšķerēšana un smikšķerēšana

Krāpnieki sūta maldinošus ziņojumus e-pastā un īsziņās ar viltus saitēm, maskējoties ar pazīstamu organizāciju nosaukumu, lai iegūtu personas datus un piekļuvi finanšu kontiem.

Pārskata periodā novērotas apjomīgas pikšķerēšanas kampaņas, maskējoties ar finanšu pakalpojumu sniedzēju (it īpaši "SEB banka", "Luminor banka", "Citadele banka", "Paysera") vārdu. Krāpnieki nereti aicina atjaunināt tiešsaistes banku vai rada viltus pārliecību, ka upura bankas kontā esošie līdzekļi ir apdraudēti, un pieprasa veikt steidzamas darbības, lai it kā apdraudētos naudas līdzekļus pasargātu.

Novembrī masveidā tika saņemti ziņojumi par krāpniekiem, kas saziņas lietotnē "WhatsApp" sūtīja ziņas, aicinot konkursa ietvaros balsot par paziņu bērnu, taču patiesais krāpnieku nolūks bija nozagt "WhatsApp" kontu. Zīmīgi, ka novembrī ieviešot DNS ugunsmūra mobilo lietotni, šīs vienas kampaņas ietvaros 23 615 reižu tika novērsti iedzīvotāju mēģinājumi atvērt šo ļaunprātīgo saiti, tādējādi novirzot cilvēkus uz drošu piezemēšanās vietni. Par līdzīgu kampaņu krievu valodā CERT.LV brīdināja arī 2024. gada jūnijā, taču šoreiz krāpnieki saziņai izmantoja latviešu valodu.



Attēlā ekrānšāviņš ar krāpniecisko "WhatsApp" ziņu piemēriem.

Turpinās viltus ziņas it kā "Latvijas Pasts", DHL un citu kurjerpakalpojumu sniedzēju vārdā, mudinot lietotājus apstiprināt sūtījuma saņemšanas laiku vai precizēt piegādes adresi. Lielākoties tiek izplatīts viltus SMS vai īsziņas "WhatsApp"platformā.

Decembrī aktivizējās krāpnieki ar viltus īsziņām par it kā piemērotu sodu, uzdodoties par Ceļu satiksmes drošības direkciju. Šīm īsziņām tika pievienotas krāpnieciskas saites, kuras atverot, tiek prasīts autentificēties ar bankas datiem.

Pēc ilgākas pauzes 4. ceturksnī CERT.LV atkal tika saņemti iedzīvotāju ziņojumi par krāpnieciskām īsziņām, kas it kā nākušas no Tiesas.lv un Elietas.lv.

Telefonkrāpšanas gadījumi jeb vikšķerēšana

Krāpnieki joprojām izliekas par valsts iestāžu, banku vai uzņēmumu darbiniekiem, lai iegūtu personas datus vai piekļuves kodus, izmantojot dažādas psiholoģiskas metodes, kas var ietekmēt pilnīgi jebkuru.

Pārskata periodā vairāki iedzīvotāji saņēma zvanus šķietami no "Smart-ID" operatoriem vai "Latvenergo" pārstāvjiem, kas apgalvoja, ka nepieciešama elektrības skaitītāju nomaiņa – krāpnieku mērķis bija izgūt "Smart-ID" piekļuves kodus. Viltvārži uzdevās arī par mobilo sakaru operatoriem "Latvijas Mobilais Telefons", "Tele2" vai "Bite Latvija", lai izvilinātu personas datus it kā identitātes apstiprināšanai. Tika apgalvots, ka beigsies līgums ar operatoru, un lai novērstu SIM kartes slēgšanu, tika pieprasīts steidzami veikt maksājumu. Nereti šajā shēmā tika iesaistīti arī viltus policisti vai viltus bankas darbinieki.

Kā jauna tendence oktobrī fiksēti krāpnieku uzaicinājumi pievienoties "WhatsApp" grupām no nezināmiem numuriem. Krāpnieku mērķis - krāpniecisku saišu izplatīšana, upura iesaistīšana ar kriptovalūtas pseidotirdzniecību saistītās peļņas shēmās, vai vienkārši potenciālā upura telefona numura pārbaude turpmākai izmantošanai citās krāpniecības kampaņās.

Viltus tīmekļvietnes un sociālo mediju izmantošana

Krāpnieki turpina pilnveidot viltus vietnes, lai, maldinot lietotājus, iegūtu viņu datus vai izkrāptu naudu. Šīs vietnes imitē reālas tīmekļvietnes, piemēram, banku, tiešsaistes veikalu vai pakalpojumu sniedzēju lapas, lai izskatītos uzticamas. Lai piesaistītu upuri, krāpnieki sūta pikšķerēšanas e-pasta vēstules vai īsziņas ar saitēm uz viltus vietnēm, kā arī izmanto reklāmas meklētājprogrammās. Kad lietotāji ievada savus datus viltus vietnēs, krāpnieki iegūst piekļuvi viņu personīgajai informācijai, bankas kontiem vai maksājumu karšu datiem, ko pēc tam izmanto krāpnieciskām darbībām.

Skaudrs piemērs tam bija maksājumu karšu datu pikšķerēšana ar viltus aptauju anketām caur "Facebook" reklāmām, maskējoties ar "SEB banka" vārdu. Tāpat novērotas intensīvas pikšķerēšanas kampaņas ar "Microsoft", "DocuSign", "Paysera", "inbox.lv" viltus lapām, kur paroļu zagšanas nolūkā ar krāpnieciskām saitēm tika pievilināti neuzmanīgie lietotāji.

Novērotas jaunas krāpšanas shēmas, kurās krāpnieki izmantoja viltus vietnes, lai iegūtu maksājumu karšu datus. Spilgts gadījums bija oktobrī, kur krāpnieks uzstāja uz līguma parakstīšanu, izmantojot viltus "eparaksts.lv" vietni. Viltus lapā tika attēlots paziņojums, ka dokumenta atvēršana ir par maksu, tā cenšoties iegūt upura norēķinu karšu datus.

Attēlā ekrānšāviņš ar piemēru eparaksts.lv viltus vietnei.

Krāpnieki aktīvi izmanto sociālos medijus, piemēram, "Facebook" un "Instagram", lai izplatītu krāpnieciskas saites uz viltus interneta veikaliem un viltus reklāmas, kas īpaši saasinās "melno piektdienu", pirmssvētku iepirkšanās un Ziemassvētku periodā.

Izplatās viltus tīmekļvietnes, kur sola neiedomājamas atlaides vai iespējas investīcijām. Šādu vietņu atšķiršana no īstām kļūst arvien sarežģītāka. Piemēram, daudzi iedzīvotāji ziņoja par viltus "RD Electronics" vietni, kas "ķēra uz āķa" neuzmanīgos pircējus, novirzot uz pikšķerēšanas lapu. Spilgts gadījums bija arī "Delfi" klons, kas tika nopublicēts vairākās "Facebook" grupās, izmantojot vairākus botu kontus. "Delfi" klons ar domēna vārdu delfiauto.lv centās pārdot kriptovalūtu tirdzniecības programmatūru, un uzmanības piesaistīšanai tika izmantoti attēli ar sabiedrībā pazīstamām personām, piemēram, Latvijas Valsts prezidentu.

Šādas shēmas ir īpaši bīstamas, jo tās izmanto pazīstamu zīmolu, personu un pakalpojumu vārdus, lai radītu uzticību un maldinātu lietotājus, apietu drošības pasākumus un izkrāptu naudu no neuzmanīgiem lietotājiem.

Mērķēta pikšķerēšana

Attīstoties tehnoloģijām, kiberuzbrucēji arvien gudrāk pielāgo ziņojumus, lai izskatītos pārliecinošāk, pamatojoties uz konkrētu informāciju par organizāciju, personu vai konkrētu mērķi. Lai iepazītu savu mērķi, tiek izmantota brīvi pieejamās informācijas vākšana (OSINT).

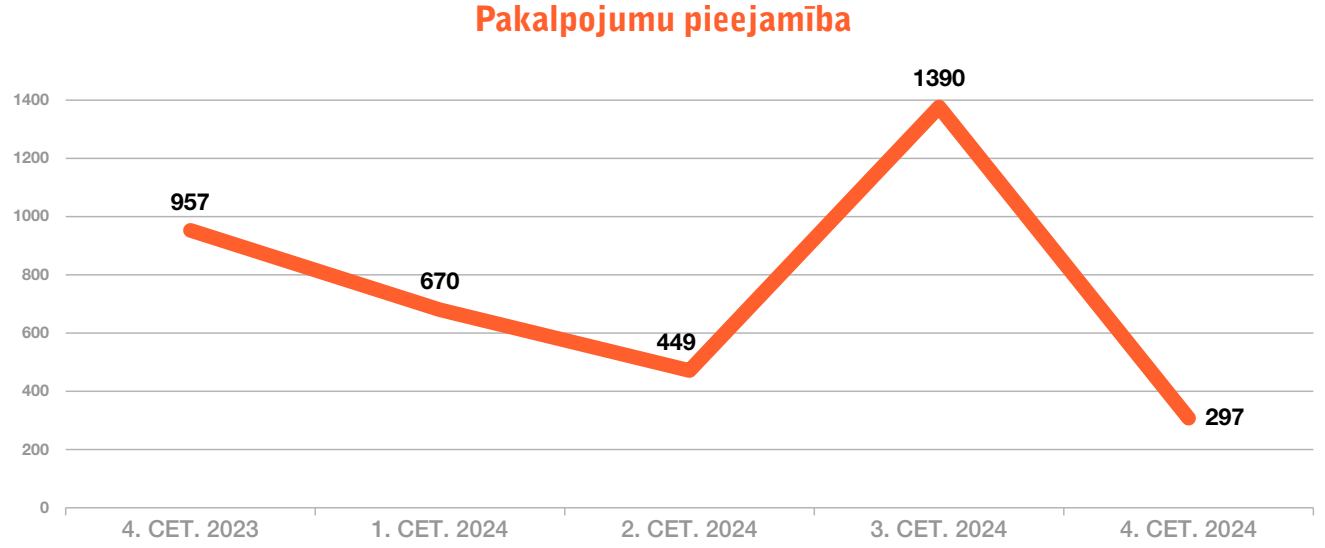
Arī uzņēmumi cieš no krāpniekiem, jo īpaši grāmatveži ar piekļuvi uzņēmuma kontiem un pilnvarām veikt maksājumus. Krāpnieki mēģina izkrāpt finanšu līdzekļus, izmantojot, piemēram, viltus rēķinus un maksājumu pieprasījumus. Īpaši tas pastiprinās gada nogalē, kad uzņēmumi ir aizņemti ar finanšu pārskatiem, padarot tos neaizsargātākus pret šādiem kiberuzbrukumiem.

10 IETEIKUMI DROŠĪBAI

1. Pārbaudīt avotus un datu precizitāti, kritiski izvērtējot saņemtās ziņas patiesumu un sūtītāja e-pasta adresi un saturu, rūpīgi pievērst uzmanību valodas kļūdām un stilam.
2. Regulāri un savlaicīgi atjaunināt viedierīču un iekārtu operētājsistēmas un lietotnes!
3. Neievadīt informāciju uznirstošajos logos un neklikšķināt uz saitēm tajos!
4. Neklikšķināt uz saites, ja nav pārliecības, ka saite ved uz vietni, kas saistīta ar uzticamu vēstules sūtītāju! Šaubu gadījumā zvanīt uz organizācijas oficiālo tālruni un pārbaudīt.
5. Papildu aizsardzībai izmantot divu faktoru autentifikāciju: tas pasargās no konta pārņemšanas, pat ja uzbrucējs būs ieguvis jūsu paroli!
6. Nekādā gadījumā nesūtīt citām personām attēlus vai video ar bankas kartēm vai personu apliecinošiem dokumentiem!
7. Nepakļauties krāpnieku prasībām viedierīcēs instalēt attālinātas piekļuves programmatūru (AnyDesk, TeamViewer, HopToDesk, AeroAdmin u.c.)!
8. E-pasta administratoriem nepieciešams konfigurēt DMARC un SPF pārbaudes ienākošajiem e-pastiem, lai ierobežotu viltoto vēstuļu saņemšanu. Plašāk: https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-izejoso-e-pastu-viltosanu
9. Izmantot CERT.LV un NIC.LV nodrošināto bezmaksas aktīvo aizsardzības pakalpojumu – https://dnsmuris.lv/, lai pasargātu sevi un darbiniekus no krāpniecisku vietņu apmeklēšanas.
10. Ziņot par krāpnieku aktivitātēm un ļaundabīgām vietnēm, pārsūtot kaitīgos e-pastus uz cert@cert.lv vai arī pārsūtot krāpnieciskas SMS un telefonu numurus uz +371 23230444 (telefona zvani netiek apstrādāti) tādējādi pasargājot citus DNS ugunsmūra lietotājus.

2.2. Pakalpojuma pieejamība

Kvantitatīvo rādītāju ziņā, salīdzinot ar 2024. gadu 3. ceturksni un pagājušā gada 4. ceturksni, DDoS uzbrukumu skaits ir samazinājies, apjomam ievērojami sarūkot, bet to kvalitāte un jauda pieaug. DDoS kļūst arvien sarežģītāki, koncentrētāki un jaudīgāki.



5. attēls. Apdraudēto unikālo IP adrešu skaits

Tas norāda uz tendenci ieguldīt vairāk resursu mazākā DDoS kiberuzbrukumu skaitā, lai padarītu tos efektīvākus.

Apjomīgākais DDoS uzbrukums sasniedza 200 gigabitus sekundē (Gbps) pret vienu mērķi, bet ilgstošākais bija 10 dienas nepārtraukts uzbrukums.

Neraugoties uz pieaugošo uzbrukumu intensitāti, to ietekme bija maznozīmīga, kas norāda uz Latvijas augsto kibernoturību un centralizētā aizsardzības pakalpojuma efektivitāti.

Mērķu izvēlē vērojama neapšaubāma tendence – orientēties uz valsts pārvaldes iestādēm un IKT kritisko infrastruktūru. Atsevišķos gadījumos joprojām vērojama slikti izpētītu mērķu izmantošana, piemēram, Skultes ostas domēns, kas regulāri nokļūst dažādos DDoS mērķu sarakstos. Tas varētu būt skaidrojams ar kādas haktīvistu grupas sākotnēji sagatavoto ne pārāk kvalitatīvo mērķu sarakstu, kas ik pa brīdim atkal nonāk apritē.

Tomēr jaunākas tendences rāda, ka uzbrucēji veic arvien rūpīgāku mērķu izlūkošanu, izpētot sistēmu, ar kuru nāksies saskarties, un citus faktorus, kas varētu ietekmēt uzbrukumu, lai efektīvāk sasniegtu vēlamo pārslodzi/ pakalpojuma nepieejamību.

DDoS uzbrukumos aktīvi tiek izmantotas tīklā vai internetam pieslēgtas nedroši konfigurētas, novecojušas vai nepareizi pieslēgtas iekārtas. Sākot no televizoriem līdz apkures katliem un solārajām sistēmām, kuras nereti nav uzstādījis pats lietotājs, bet gan pieslēdzis pakalpojuma sniedzējs, ignorējot labās prakses principus.

Kiberuzbrucēji DDoS uzbrukumā izmanto Latvijā esošas ievainojamas iekārtas, lai apietu ierobežojumus, piemēram, ģeobloķēšanu, kas mazina uzbrukuma ietekmi, ierobežojot piekļuvi konkrētajam resursam no noteiktām valstīm vai reģioniem. Attiecīgi šādu neatjaunināt u iekārtu uzturētāji rada kiberdrošības apdraudējumu gan sev, gan apkārtējiem.

DDoS uzbrukumi pārslogo mērķsistēmas ar pārmērīgu datplūsmu, padarot to pakalpojumus īslaicīgi nepieejamus. Haktīvistu grupējumi izmanto robottīklus un citus resursietilpīgus rīkus, lai traucētu tīmekļa vietņu funkcionalitāti un pieejamību. Šādus uzbrukumus izmanto kā politiskās izpausmes un propagandas rīkus plašākā ģeopolitiskā konfliktā, kas ir daļa no pieaugošās tendences, kad kibernoziedznieku grupas apvienojas ar valsts interesēm, lai apdraudētu IKT kritisko infrastruktūru un raidītu politiskus vēstījumus.

Pakalpojumatteices uzbrukumi bankām

2024. gada oktobrī tika novēroti intensīvi pakalpojumatteices uzbrukumi vairākām bankām. Tika ietekmētas banku sistēmas, un klientiem bija grūtības ielogoties internetbankā vai mobilajā lietotnē, veikt maksājumus vai karšu norēķinus, tādējādi īslaicīgi radot uzbrukumā ietekmēto pakalpojumu pieejamības traucējumus banku klientiem.

Krimas platformas samits Latvijā norisinās bez ievērojamiem kiberuzbrukumiem

No 23. līdz 24. oktobrim Rīgā notika Starptautiskās Krimas platformas 3. parlamentārais samits ar nolūku izcelt Krievijas agresijas globālo ietekmi un pastrādātos noziegumus. Šis samits ir svarīgs solis Ukrainas atbalstīšanā, un ir pozitīvi, ka tas noritēja bez būtiskiem pakalpojumatteices traucējumiem. CERT.LV veica platformas resursu monitorēšanu gan pirms, gan pasākuma laikā, lai būtu gatavībā un nodrošinātu efektīvu rīcību pret potenciāliem kiberuzbrukumiem.

IETEIKUMI DROŠĪBAI

1. Apzināt publiskos kritiskos resursus, kuri varētu būt pakļauti DDoS uzbrukumam.
2. Pieslēgt monitoringu, lai pamanītu, ka kritiskais resurss nav sasniedzams no interneta.
3. Izveidot papildu interneta pieslēgumu, lai spētu piekļūt tīkla iekārtu vadībai laikā, kad interneta kanāls un iekārtas ir pārslogotas.
4. Pārliecināties, ka ir zināmas un testētas metodes, kā noskaidrot tehniskas detaļas par uzbrukumu: mērķis, uzbrukuma veids (piemēram, *netflow*/ugunsmūra žurnālfaili).
5. Izstrādāt un notestēt rīcības plānu, kā rīkoties uzbrukuma laikā:
   - Pieslēgt DDoS aizsardzību, ko nodrošina interneta pakalpojumu sniedzējs. Latvijā DDoS aizsardzības pakalpojumus piedāvā Aizsardzības ministrija sadarbībā ar VAS LVRTC, SIA "TET" un citi pakalpojumu sniedzēji;
   - Pēc pieprasījuma interneta pakalpojumu sniedzējs var izfiltrēt/ierobežot lieko datu plūsmu automātiski vai manuāli;
   - Migrēt atsevišķas svarīgākās sistēmas aiz DDoS aizsardzības uz mākoņpakalpojumu satura piegādes tīkliem (*Content Delivery Network*), piemēram, "Cloudflare", "Microsoft Azure", "Google", "AWS";
   - Filtrēt piekļuvi resursam pēc ģeolokācijas, atstājot piekļuvi svarīgākajiem klientiem vai tikai Latvijas IP adrešu diapazoniem.

2.3. Ievainojamības un konfigurācijas nepilnības

CERT.LV regulāri veic visaptverošu monitoringu, pētot ievainojamību (CVE) ainavu, kas ir sasaistāma ar eksponētiem servisiem/iekārtām un informē par aktuālajiem kiberapdraudējumiem.

CVE (Common Vulnerabilities and Exposures) ir standartizēta sistēma, kas identificē un nosauc drošības ievainojamības programmatūrā un aparatūrā, piešķirot tām unikālus identifikatorus, tā padarot vienkāršāku dažādu sistēmu un datu bāzu ievainojamību izsekošanu un atsauci uz tām.

Ievainojamība – IKT vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam.

2024. gada 4. ceturksnī CERT.LV izplatīja brīdinājumus par 9 jaunatklātām kritiskām CVE ievainojamībām, sniedzot norādījumus par atjauninājumiem un to uzstādīšanu.

Atbilstoši FIRST CVSS metodoloģijai, ievainojamības ar vērtējumu no 9.0 līdz 10, ir kritiskākas, jo tām ir augsts izmantošanas potenciāls, radot ievērojamus riskus sistēmām un datiem.

Neatlieciet drošības atjauninājumus, jo kiberuzbrucēji vispirms ķeras pie visvieglākajiem mērķiem. CERT.LV aicina sekot līdzi izstrādātāju norādījumiem un laicīgi atjaunināt programmatūras uz jaunāko pieejamo versiju. Ar visiem aktuālajiem brīdinājumiem var iepazīties cert.lv vietnē: https://cert.lv/lv/incidenti/bridinajumi

CERT.LV vietnē publicētie brīdinājumi par ievainojamībām 2024. gada 4. ceturksnī

CVE	Ietekmētie produkti	Apraksts
CVE-2024-9680	Firefox un Thunderbird	14. oktobris – Kritiska "nulles dienas" ievainojamība, kuras rezultātā var tikt izpildīts patvaļīgs kods uz ietekmētajām sistēmām. Ievainojamībai piešķirts kritisks vērtējums (CVSS: 9.8/10) tās potenciālās ietekmes un vienkāršuma dēļ. Skartās programmatūras ietekmētās versijas ir pakļautas uzlaušanas riskam.
CVE-2024-38812, CVE-2024-38813	VMware vCenter Server un Cloud Foundation	23. oktobris - Atklātās ievainojamības sniedz uzbrucējam iespēju veikt attālinātu koda izpildi un eskalēt tiesības līdz root lietotājam, tādējādi pārņemot ievainojamo sistēmu. Attālinātai koda izpildei uzbrucējam nepieciešama piekļuve VMware vCenter.
CVE-2024-47575	Fortinet FortiManager un FortiManager Cloud	24. oktobris - Atklāta kritiska "nulles dienas" ievainojamība, kas nodrošina iespēju centralizēti veikt attālinātu iekārtu pārvaldību. Izmantojot šo ievainojamību, neatentificēts uzbrucējs var panākt attālinātu patvaļīgu kodu un komandu izpildi ievainojamajās iekārtās, kas izmanto FortiManager, kā arī izgūt sensitīvus datus. Ievainojamībai piešķirts kritisks vērtējums (CVSS: 9.8/10)
CVE-2024-48990 CVE-2024-48991 CVE-2024-48992 CVE-2024-10224 CVE-2024-11003	Ubuntu Server	21. novembris - Linux distributīvos izmantotā utilītprogrammā Needrestart atklātas piecas augsta riska ievainojamības, kas sistēmā autentificētam uzbrucējam ļauj iegūt priviliģēta līmeņa tiesības (root). Šīs ievainojamības skar plaši izmantoto Ubuntu Server operētājsistēmu, jo Needrestart utilītprogramma tajās nereti ir uzstādīta jau pēc noklusējuma.

*CVSS: nozares standarta datorsistēmu drošības ievainojamību nopietnības novērtēšanas metodoloģija, palīdzot organizācijām noteikt prioritāti, kuras ievainojamības novērst vispirms.

Daudzas no nepilnībām ir saistītas ar tīmeklī izvietotu sistēmu ievainojamībām, kas bieži vien ir galvenais mērķis uzbrucējiem, kuri meklē nesankcionētu piekļuvi. Pastāvīga tendence ir ievainojamību izmantošana tīmekļa satura pārvaldības sistēmās, ugunsmūros, VPN un maršrutētājos.

Ņemot vērā ievainojamību lielo skaitu un izaicinājumus, ar kuriem ik mēnesi saskaras produktu izstrādātāji un lietotāji, kā arī to, ka lielām organizācijām ir sarežģīti veikt savlaicīgu atjauninājumu uzstādīšanu, ļoti ticams, ka ievainojamību izmantošana arī turpmāk būs viens no galvenajiem piekļuves punktiem gan valstu atbalstītiem kiberoperāciju grupējumiem, gan finansiāli motivētiem kibernoziedzniekiem, lai iefiltrētos sistēmās un nozagtu vērtīgus datus.

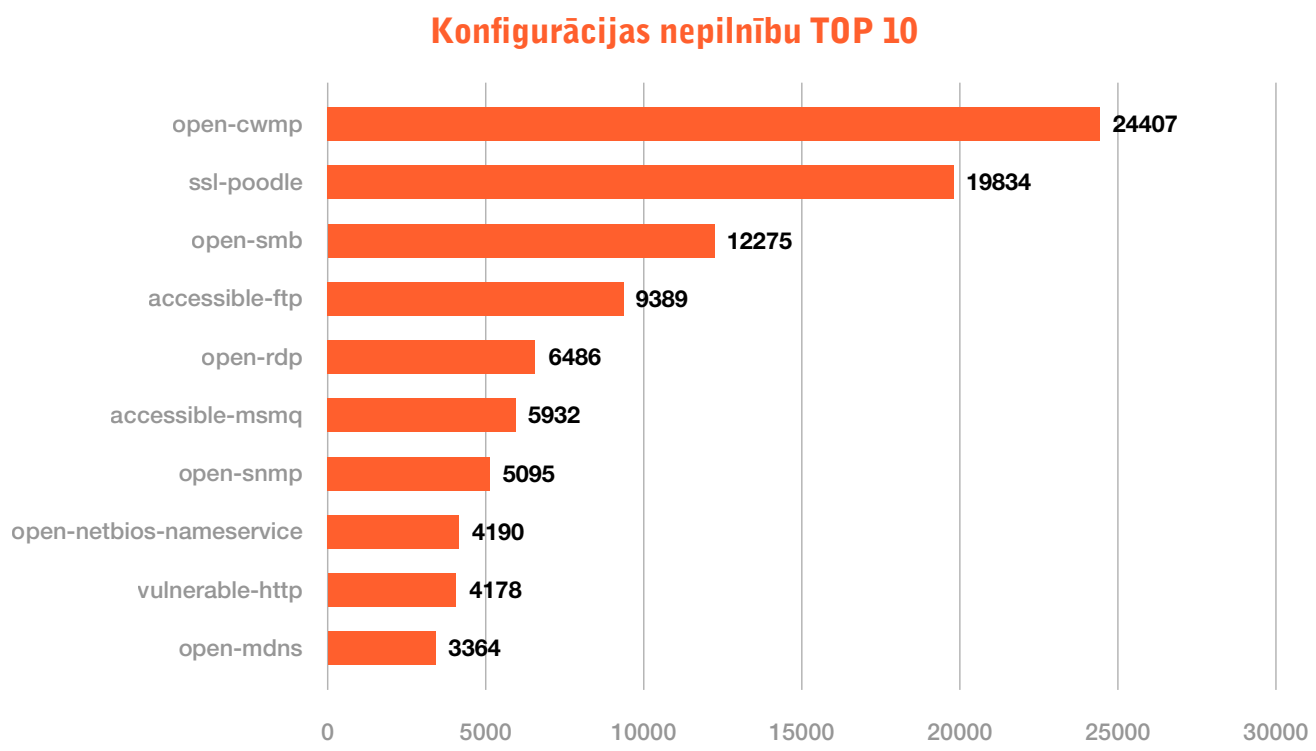
Konfigurācijas nepilnības joprojām rada ievērojamus riskus

2024. gada 4. ceturksnī konfigurācijas nepilnību TOP 10 saraksta augšgalā līderis ir *Open-cwmp* – pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu kā maršrutētāju vai VoIP telefonu pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla. Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, izmantojot VPN.

Konfigurācijas nepilnības aizvien veido lielāko daļu no visiem CERT.LV reģistrētajiem apdraudējuma veidiem Latvijas kibertelpā. Turklāt to skaits turpina augt, uzrādot augšupejošu tendenci un sasniedzot vēsturiski augstāko rādītāju – 88 211 apdraudētas unikālas IP adreses.

Ievainojamības, kas novērtētas kā "augstas" vai "kritiskas", var būt pieejamāks ieejas punkts uzbrucējiem, kuri vēlas uzlauzt sistēmas un piekļūt datiem. Šādi uzbrukumi var radīt finansiālus zaudējumus, kaitēt organizācijas reputācijai vai pat izraisīt sodus.

CERT.LV SOC nodrošina nepārtrauktu uzraudzību, ātru reaģēšanu uz incidentiem un proaktīvu draudu identificēšanu, palīdzot ātri atklāt un novērst drošības ievainojamības, samazinot risku un potenciālos zaudējumus.



6. attēls. TOP 10 Konfigurācijas nepilnības 2024. gada 4. ceturksnī

Joprojām liela daļa kiberuzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, tāpēc savlaicīga konfigurācijas nepilnību apzināšana un ievainojamību lāpīšana var būtiski uzlabot kiberdrošības situāciju.

Ievainojamību izmantošana arī turpmāk būs viens no galvenajiem piekļuves punktiem gan valstu atbalstītiem kiberoperāciju grupējumiem, gan finansiāli motivētiem kibernoziedzniekiem, lai iefiltrētos sistēmās un nozagtu datus.

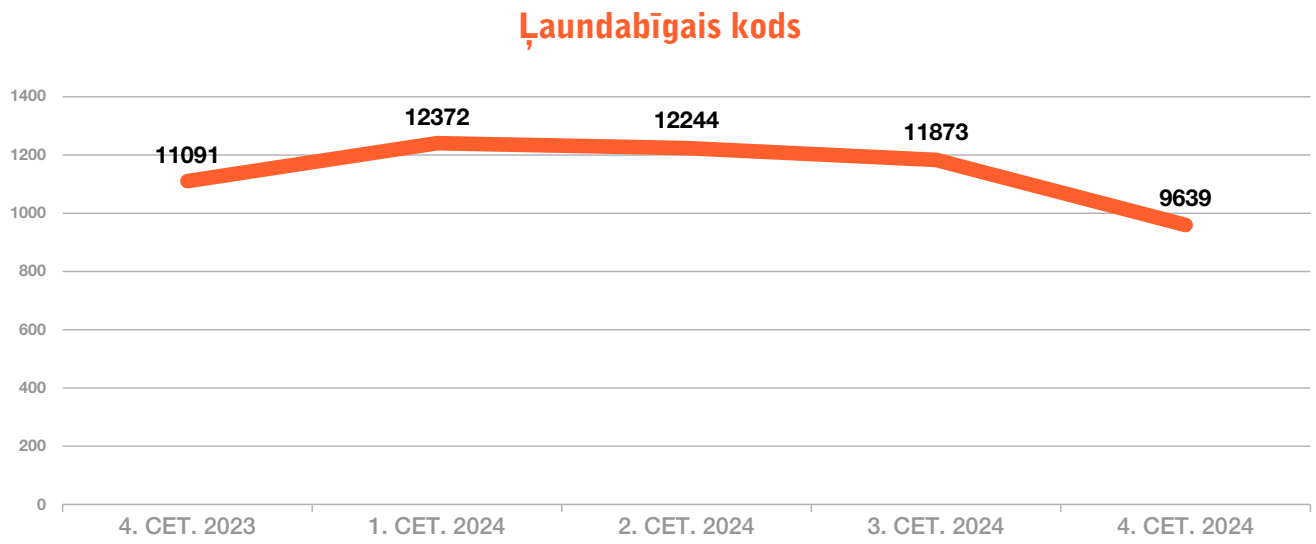
Svarīgi nodrošināt, ka visas sistēmas un programmatūra tiek regulāri atjauninātas ar jaunākajiem drošības ielāpiem. Nekavējoties ir jālabo ievainojamības, kas novērtētas kā "augstas" vai "kritiskas". Tomēr nevajadzētu ignorēt ievainojamības ar zemāku vērtējumu, jo tās bieži kalpo kā balsts vēlākos kiberuzbrukumu posmos.

IETEIKUMI DROŠĪBAI

1. **Servisu eksponēšana:** Pārskatīt un apzināt servisus, kas tiek nodrošināti. Neeksponēt servisus publiski, ja tas nav nepieciešams. Ja tas tomēr ir nepieciešams, veikt ierobežojošus pasākumus – piekļuve no konkrēta IP apgabala, VPN u.c.
2. **Regulāra IS atjaunināšana:** Regulāri un savlaicīgi atjaunināt programmatūru/ operētājsistēmas un citas trešo pušu komponentes, lai novērstu ievainojamības savlaicīgi.
3. **Tiesību/autorizāciju politika:** Izveidot stingras ierobežojošas politikas piekļuvju administrēšanas caurskatāmībai. Tiesības piešķirt pēc principa least privilege, nodrošinot lietotāju piekļuvi sistēmām un resursiem atbilstoši veicamajam darbam. Veikt regulāru auditu.
4. **Kiberuzbrukumu atklāšana/novēršana:** Savlaicīga kiberdraudu apzināšana nereti palīdz novērst pašu uzbrukumu vai tā tālāku eskalāciju. Nodrošināties ar agrīnās brīdināšanas sistēmu un/vai novēršanas sistēmām, lai identificētu un bloķētu nevēlamas aktivitātes.
5. **Drošības auditi:** Regulāri veikt vietnes auditus, kas iekļauj aktīvus un/vai pasīvus drošības skenēšanas pasākumus un aplikācijas koda auditu. Ja tas nav iespējams, piesaistīt ārpakalpojumus. Koordinētai ievainojamību atklāšanai ieteicams izmantot platformu cvd.cert.lv.
6. **Darbinieku apmācības:** Nodrošināt regulāras darbinieku apmācības kiberdrošības jautājumos, lai mazinātu sociālās inženierijas riskus, kas bieži vien ir uzbrukumu sākotnējā fāze.

2.4. Ļaundabīgs kods

2024. gada 4. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar ļaundabīgu kodu ir samazinājies par 19% salīdzinājumā ar 3. ceturksni un salīdzinājumā ar pagājušā gada 4. ceturksni to ir par 13% mazāk.



7. attēls. Apdraudēto unikālo IP adrešu skaits

TOP 5 biežāk pielietotās metodes sistēmu uzlaušanai un inficēšanai

- Pikšķerēšanas e-pasti;
- Publiski zināmu ievainojamību ļaunprātīga izmantošana;
- Eksponētu servisu ļaunprātīga izmantošana;
- Nopludināti lietotāju piekļuves dati;
- Automatizētie uzbrukumi.

Galvenie ļaunatūras tipi

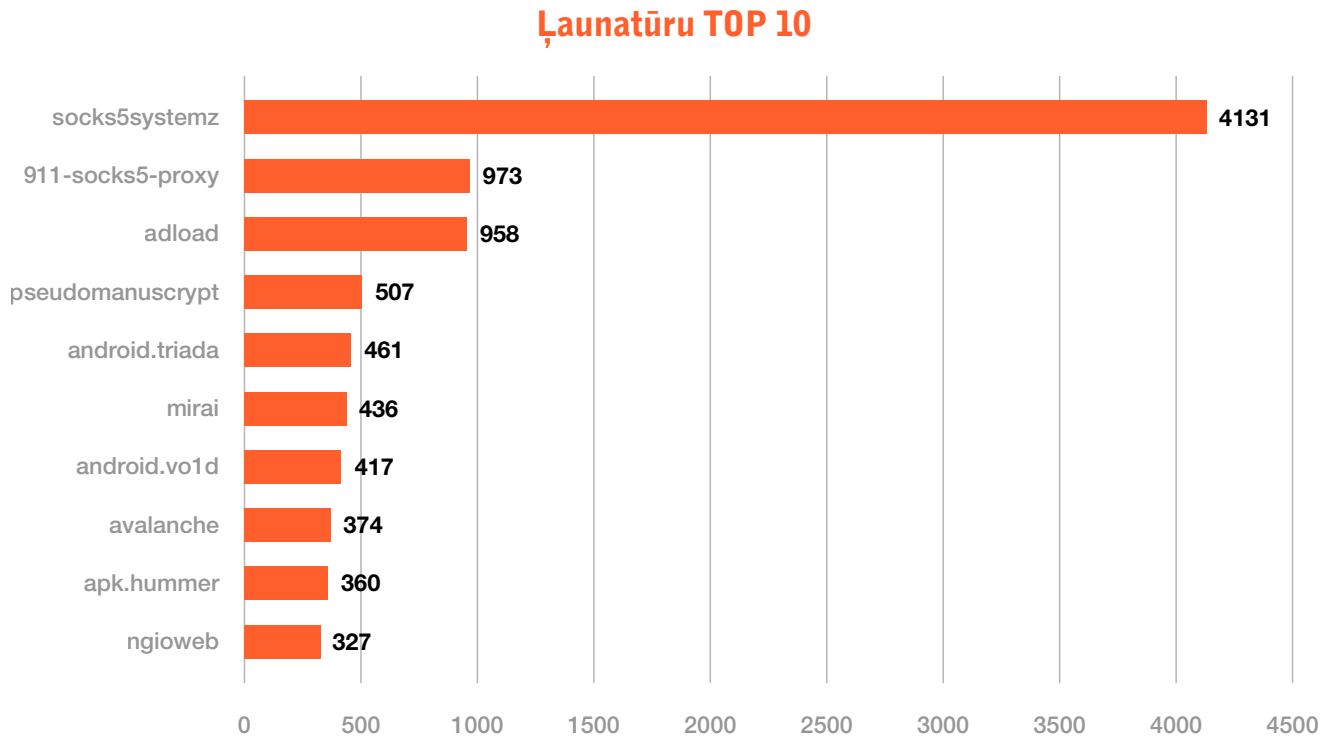
- Lietotāju datu zadzēji
- Botu tīkli
- Izspiedējvīrusi
- Attālinātās kontroles *trojāni* datu izgūšanai, infrastruktūras kompromitēšanai

Sociālā inženierija, izmantojot pikšķerēšanu, mudina lietotājus lejupielādēt ļaunprātīgu programmatūru.

Pikšķerēšana joprojām ir iecienītākā metode, vienlaikus uzlabojot savas stratēģijas, izmantojot sociālos medijus un populāras e-pasta mārketinga platformas.

Lai apietu korporatīvo aizsardzību, kiberuzbrucēji arvien vairāk pievēršas sociālajiem medijiem un saziņas platformām, piemēram, “WhatsApp”. Visticamāk, šī pieeja turpināsies arī turpmāk.

Kiberuzbrucēji joprojām aktīvi izmanto maldinošas pikšķerēšanas tīmekļa lapas. Arī tiešsaistes reklāmās iestrādāta ļaundabīga programmatūra paplašina uzbrukuma laukumu.



8. attēls. TOP 10 ļaunatūras 2024. gada 4. ceturksnī

Dažkārt kiberuzbrukumi ir oportūnistiski. Tomēr arvien biežāk kiberuzbrukumi tiek rūpīgi plānoti un to mērķis ir dati vai infrastruktūra, kam ir vislielākā ietekme uz upuru darbību. Kibernoziedznieki var vai nu zagt tieši no cietušajiem upuriem, vai pelnīt ar informāciju, kas ir nozagta no cietušajiem. Turklāt kibernoziedznieki arvien vairāk savstarpēji sadarbojas organizētās grupās, padarot tās par spēku, ar ko jārēķinās.

Ļaunatūras tiek izplatītas galvenokārt diviem mērķiem – lai izvilinātu datus vai gūtu peļņu. Atverot ļaundabīgo pielikumu, iekārta tiek inficēta ar ļaunatūru, kas ievāc lietotājvārdus, paroles, kriptovalūtu maciņu un to piekļuves informāciju u.tml., lai nosūtītu to uz uzbrucēja kontrolētu infrastruktūru.

Turpina pieaugt pret uzņēmumiem vērsto kiberuzbrukumu apjoms. Kompromitēti e-pasti vai lietotņu konti tiek aktīvi izmantoti, lai tālāk izplatītu ļaunatūras. Pikšķerēšanas e-pastos novērots paaugstināts kaitīgo pielikumu īpatsvars ar .html paplašinājumu, tostarp arī pikšķerēšanas shēmas, kur kaitīgajā pielikumā ir instrukcijas, kas mudina lietotāju izpildīt komandas, ielīmējot tās Windows "*run*" logā.

Ļaunprātīgi pielikumi e-pasta vēstulēs rada nopietnus drošības riskus

Lietotāju datu zadzēji un ļaunprātīgas programmatūras kļūst arvien sarežģītākas. Spilgts piemērs tam ir "Amazon" paziņojums 2024. gada oktobrī par bloķētiem domēniem, ko Krievijas hakeru grupa APT29 izmantoja mērķtiecīgos uzbrukumos valdības un militārajām organizācijām, lai nozagtu sensitīvu informāciju, izmantojot ļaunprātīgus attālinātās piekļuves protokola (RDP) savienojumu failus ar tādiem nosaukumiem kā "Zero Trust Security Environment Compliance Check.rdp".

E-pasta vēstulēs ar kaitīgu .html paplašinājumu ļaundari mudina izpildīt komandas Windows "*run*" logā. Tas ļauj kibernoziedzniekam izpildīt kodu jeb palaist programmu uz upura datora, lai nozagtu datus un informāciju, apdraudot upura sociālo tīklu vai e-pasta kontus.

Kā jauna tendence novērota mākslīgā intelekta attēlu ģeneratora izmatošana, kur bildes lejupielādei liek izpildīt komandas Windows "*run*" logā, tā paverot iespēju vīrusam ievākt upura datus.

Vēl viens uzskatāms kaitīga pielikuma piemērs, kas tika novērots pārskata periodā, ir viltus e-pasta vēstule ar uzņēmuma "CNC Baltic" vārdu. Vēstule pielikumā saturēja arhīva (.zip) datni ar Lokibot datorvīrusu lietotājvārdu, paroļu u.c. nozīmīgu datu iegūšanai.

Jauna krāpniecības shēma, izmantojot viltus klientu apkalpošanas tālruņa numuru

Parādījusies jauna krāpnieciska shēma, kurā lietotāji saņem it kā īstu "PayPal" e-pasta vēstuli ar rēķinu, aicinot apmaksāt it kā saņemtu pakalpojumu/produktu, kurš realitātē nemaz nav pasūtīts. Rēķinā ir norādīts viltots "PayPal" klientu apkalpošanas dienesta numurs, uz kuru aicina lietotāju zvanīt, lai informētu par krāpšanas mēģinājumu. Zvanot uz viltoto klientu apkalpošanas numuru, krāpnieki mēģina iegūt "PayPal konta piekļuvi, finanšu informāciju - kredītkartes vai bankas piekļuves datus. Dažos gadījumos lietotāji tiek mudināti instalēt ļaunprātīgu programmatūru, kas var nozagt sensitīvus datus vai nodrošināt attālinātu piekļuvi datoram, lai krāpnieki tālāk varētu veikt vēl citas kaitnieciskas darbības.

Turpinās izspiedējvīrusu uzbrukumi

2024. gada oktobrī par izspiedējvīrusa uzbrukuma upuri kļuva pārtikas ražotājs – kāda alus darītava Latvijā. Uzbrucēji piekļuva sistēmām, izmantojot attālināto pārvaldības rīku (remote desktop) un sašifrēja datus. Lai ātrāk atjaunotu sistēmu darbību, uzņēmums nolēma samaksāt prasīto izpirkuma summu. CERT.LV sniedza atbalstu kiberuzbrukuma izvērtēšanā.

Lietotāju datu zadzēji, ļaunprātīgas programmatūras, kas izzog personas datus, kļūst arvien sarežģītākas un rada nopietnas bažas.

> Lai identificētu un likvidētu ļaunatūru, kā pirmais solis ir nekavējoties pārbaudīt datoru ar antivīrusa programmatūru. Nākamais solis ir nomainīt paroles un pārbaudīt kontus, jo pastāv iespēja, ka kriptovalūtu iegūšana nav vienīgā ļaunatūras veiktā darbība.

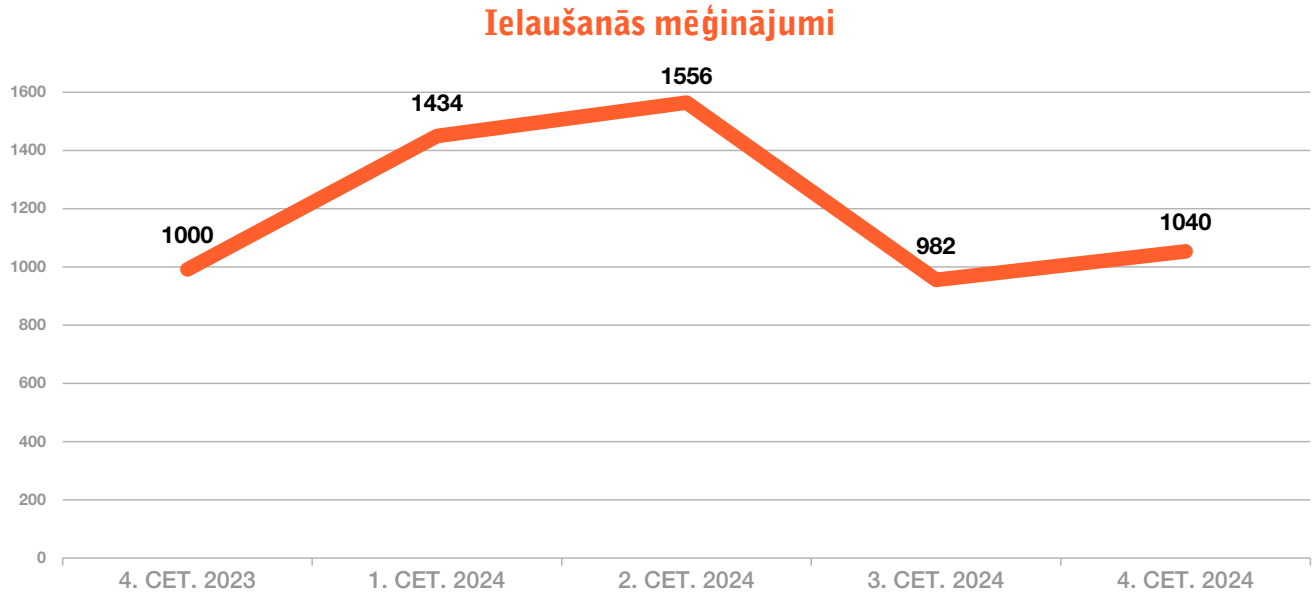
Visbiežāk lietotāju datu zadzēju ļaunatūras tiek mērķētas uz nedroši, lokāli glabāto autentifikācijas datu un paroļu zagšanu, proti, paroļu iegūšanu no tīmekļa pārlūka vai nešifrētiem failiem. Šāda veida ļaunatūra tiek izplatīta kā ļaundabīgs tīmekļa pārlūka spraudnis vai kā izpildfails, pievienots pie pikšķerēšanas e-pasta vēstules - šīs tendences, visticamāk, turpināsies.

Par kiberapdraudējumiem un vietnēm, kas izplata vīrusus, CERT.LV aicina ziņot uz e-pastu cert@cert.lv. Ļaunprātīgu aktivitāšu indikatori tiek operatīvi ievietoti DNS ugunsmūrī, lai pasargātu interneta lietotājus no ļaunprātīgu vietņu apmeklēšanas. Kā arī ir pieejams telefona numurs krāpniecisku SMS pārsūtīšanai: +371 23230444 (telefona zvani netiek apstrādāti).

2.5. Ielaušanās mēģinājumi

2024. gada 4. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits kiberapdraudējuma veidā – Ielaušanās mēģinājumi – ir audzis gan salīdzinājumā pret 3. ceturksni (+6%), gan pret pagājušā gada attiecīgo periodu (+4%).

Lielākajā daļā gadījumu tiek izmantota paroļu minēšanu (brute-force) pret dažādiem elektronisko sakaru komersantiem, valsts un pašvaldību iestādēm, kā arī privāto sektoru.



9. attēls. Apdraudēto unikālo IP adrešu skaits

Līdztekus tiek izmantotas sen zināmas konfigurācijas nepilnības plaši lietotos produktos. Tāpat, izmantojot jaunatklātas ievainojamības, kibernoziedznieki uzstājīgi meklē iespējas iekļūt organizāciju iekšējos tīklos, lai nesankcionēti piekļūtu sensitīvai informācijai vai nošifrētu iekārtas un pieprasītu maksu par datu atgūšanu.

Cilvēciskais faktors un vājas paroles situāciju vēl vairāk sarežģī, jo cilvēki bieži vien kļūst par pikšķerēšanas upuriem, apdraudot pat labi aizsargātas sistēmas.

Kiberuzbrukumi, tostarp ielaušanās mēģinājumi, galvenokārt apdraud sensitīvus datus. Viena no taktikām, ko kiberuzbrucēji veiksmīgi izmanto, ir ļaunprātīgu programmatūru slēpšana šķietami drošos ielāpos atjauninājumos, kas var nopietni apdraudēt organizācijas tīklu, turklāt neizraisot nekādus sistēmas brīdinājumus. Tas palielina laika starpību starp tīkla kompromitēšanas un ielaušanās fakta atklāšanu. Agrīna atklāšana ir lētāka nekā zaudējumu novēršana. IT drošības kiberapdraudējumu pazīmes (IoC) palīdz identificēt šādas darbības.

"Sarkanie karodziņi" – jeb biežākie IoC ir neparasta tīkla datu plūsma un lietotāju uzvedība, daudzi pieteikšanās mēģinājumi īsā laikā u.c. CERT.LV MISP platforma palīdzēs ātrāk atklāt un novērst kiberuzbrukumus un apdraudējumus, apkopojot un koplietojot apdraudējumu pazīmes.

IETEIKUMI DROŠĪBAI

1. Regulāri atjaunināt programmatūru sistēmas.
2. Izmantot spēcīgas autentifikācijas metodes – ieviest daudzfaktoru autentifikāciju (MFA) un nodrošināt stingru paroļu politiku.
3. Šifrēt sensitīvus datus gan pārsūtīšanas, gan glabāšanas laikā.
4. Veikt regulāras drošības pārbaudes un risku novērtējumus.
5. Izglītot darbiniekus par kiberdrošības jautājumiem.
6. Izstrādāt skaidru rīcības plānu kiberincidentu gadījumos un apmācīt darbiniekus.
7. Veikt regulāru datu rezerves kopēšanu.
8. Izmanot ugunsmūri un antivīrusu programmatūru.

2.6. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā iekārtu, tīmekļvietņu vai kontu kompromitēšanas gadījumos apdraudēto unikālo IP adrešu skaits salīdzinājumā ar pagājušā gada 4. ceturksni ir samazinājies par 39%, kā arī salīdzinājumā ar 2024. gada 3. ceturksni – samazinājies par 39%. Tas varētu liecināt par ieviestiem efektīvākiem drošības pasākumiem un tehnoloģijām, kas palīdz novērst kiberdraudus. Tomēr svarīgi ir turpināt uzlabot drošības pasākumus un apmācības par kiberdrošības labāko praksi, lai veicinātu šo pozitīvo tendenci.

Pielietotās metodes uzlaušanai:

- Pikšķerēšanas e-pasti;
- Publiski zināmas / jaunatklātas ievainojamības;
- Eksponēti servisi;
- Vāja paroļu pārvaldība un 2FA neesamība;
- Piegādes ķēdes;
- Automatizētie uzbrukumi;
- Kompromitēti lietotāju sociālo tīklu konti.

Cēloņi, kas liedz pašai mērķa iestādei efektīvi uzraudzīt infrastruktūru un reaģēt uz potenciāliem incidentiem:

- Nav centralizēta auditācijas pierakstu uzkrāšana un analīze.
- Tīkla segmentācijas un IT infrastruktūras inventarizācijas neesamība.
- Nepareizi konfigurēta SIEM (*Security Information and Event Management*) sistēma;
- Nepareizi konfigurēta vai neeksistējoša lietotāju tiesību pārvaldība un izpildāmo failu politika.

Izgaismojas kiberoperācijas, kurās uzbrukuma izcelsme, iespējams, saistāma ar Ķīnu

2024. gada oktobrī CERT.LV saņēma ziņojumu no kādas valsts sektora iestādes par ievainojamu "Ivanti" Cloud Services Appliance (CSA) serveri, kas tiek izmantots, lai nodrošinātu attālināto gala ierīču pārvaldību. Incidenta izmeklēšanas laikā tika konstatēts, ka uzbrucēji izmantoja programmatūras versiju ievainojamības piekļuvei, jo uz izmantošanas brīdi ievainojamības nebija publiski paziņotas no "Ivanti" puses, tāpēc drošības atjauninājumi nebija

pieejami. Tika konstatēts, ka uzbrucēji mēģināja piekļūt arī citām iestādes iekštīklā esošām iekārtām, tomēr, pateicoties infrastruktūrā izvietotiem drošības risinājumiem, uzbrucēju darbības tika pamanītas un deaktivizētas.

Kiberuzbrukuma izcelsme pārliecinoši saistāma ar Ķīnas atbalstītu kiberuzbrucēju grupu GALLIUM. Uzbrukuma tehniskie raksturojumi ļauj secināt, ka uzbrucēju mērķis Latvijā nebija nejaušs, un tas tika realizēts ar nolūku iekļūt dziļāk mērķa infrastruktūrā. CERT.LV turpina sniegt atbalstu kiberuzbrukumā skartajai iestādei ar visu pieejamo CERT.LV pakalpojumu spektru, lai turpmāk arvien uzlabotu infrastruktūras noturības spējas.

Datu noplūde no pašvaldību sistēmas – lielākā zināmā Latvijā

Laikā no 29. oktobra līdz 2. novembrim tehniskas kļūmes dēļ no Vienotās pašvaldību informācijas sistēmas noplūda ievērojams datu apjoms. Par incidentu paziņoja IT sistēmas izstrādātājs un uzturētājs SIA "ZZ Dats". Incidents tiešā veidā skāris 42 Latvijas pašvaldības (visas, izņemot Rīgas valstspilsētas pašvaldību). Kibernoziedznieki piekļuva gandrīz visu pašvaldību iedzīvotāju vārdiem, uzvārdiem, personas kodiem un deklarētajām adresēm, kā arī dažu pašvaldību darbinieku datiem un dokumentu aprakstiem. Kā norāda Datu valsts inspekcija, šī ir lielākā zināmā datu noplūde Latvijā.

Datu noplūde var radīt nopietnus riskus, ļaujot pikšķerētājiem ēsmu piemeklēt vēl precīzāk. CERT.LV aicina pašvaldību darbiniekus un iedzīvotājus būt piesardzīgiem un gataviem iespējamiem pikšķerēšanas mēģinājumiem un krāpnieciskiem e-pasta ziņojumiem. Saņemot e-pasta vēstules vai saziņas pieprasījumus, kas šķiet aizdomīgi, svarīgi ir pārliecināties, ka saziņa patiešām nāk no uzticama avota.

Datu noplūde Lietuvas elektroniskajā iepirkumu sistēmā reģistrētai informācijai skar arī Latvijas uzņēmumus

12. novembrī Lietuvas Publisko iepirkumu uzraudzības birojs publicēja paziņojumu par kiberuzbrukumu Lietuvas elektroniskajai iepirkumu sistēmai. Uzbrukuma rezultātā noplūdusi tajā reģistrēto uzņēmumu informācija: e-pasti un paroles. Saistībā ar šo kiberincidentu, CERT.LV saņēma informāciju par mērķētiem un pielāgotiem pikšķerēšanas uzbrukumiem Latvijas uzņēmumiem, kuri reģistrējušies Lietuvas Publisko iepirkumu sistēmā.

CERT.LV aicina Latvijas uzņēmumus būt modriem un ziņot cert@cert.lv, ja ir saņemtas aizdomīgas e-pasta vēstules šķietami no Lietuvas sadarbības partneriem, ar aizdomīgiem pielikumiem, lūgumu par datu atjaunošanu vai pieprasījumiem sniegt kādu papildu informāciju.

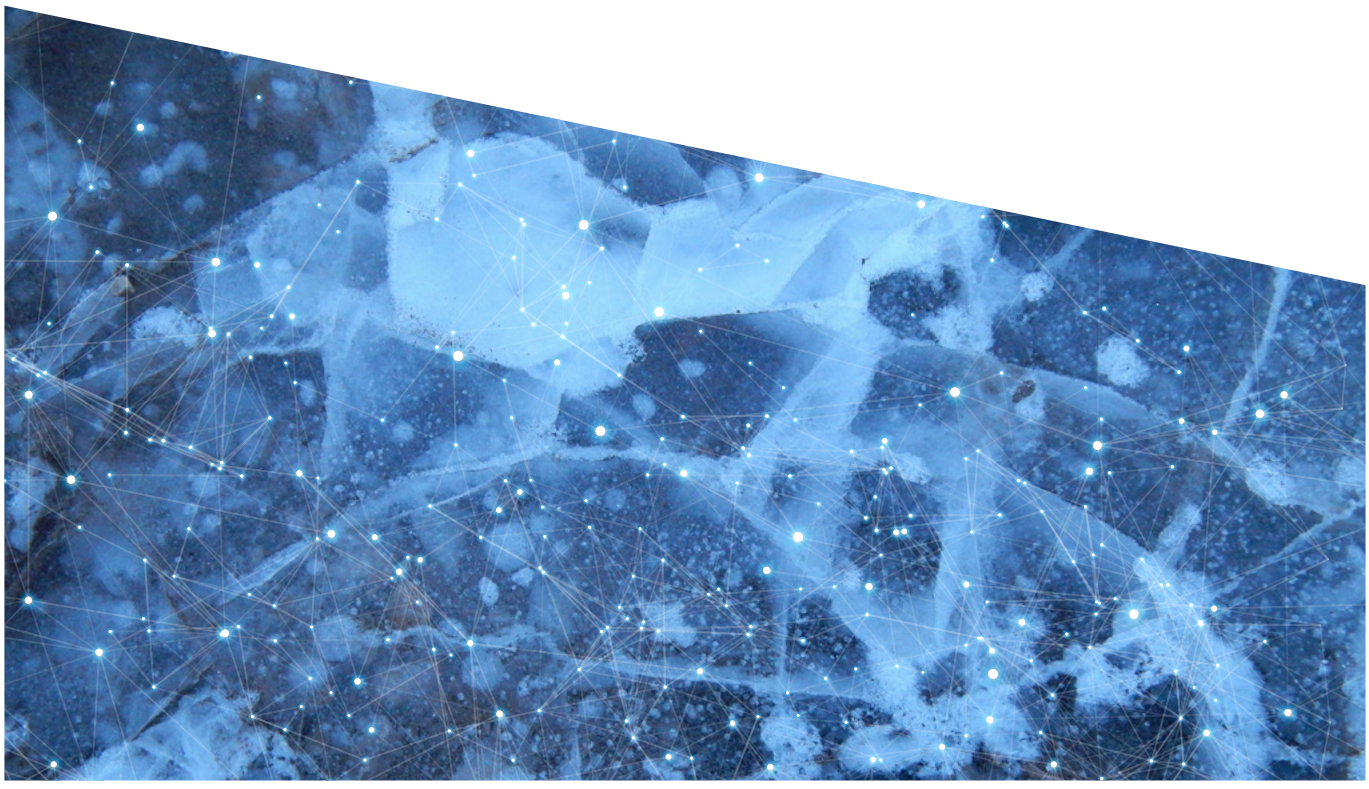
3 soļi, kā atpazīt pikšķerēšanas, smikšķerēšanas vai vikšķerēšanas mēģinājumus:

- pārbaudīt sūtītāja e-pasta adresi un pievienotās saites, vai tās sakrīt ar iestādes oficiālo adresi;
- nevērt vaļā pielikumus ar zip, rar, iso, exe vai rpd paplašinājumu, kas var saturēt kaitīgu saturu;
- pārbaudīt zvanītāja identitāti un informāciju, pašam piezvanot uz oficiālo iestādes numuru.

Pārskata periodā novērotie incidenti rāda, cik būtiski ir parūpēties par visiem iestādes uzraudzībā esošiem digitālajiem resursiem, regulāri tos atjaunot, un slēgt publiskai piekļuvei tos, kas vairs netiek aktīvi izmantoti. Ievainojamību un konfigurāciju nepilnību draudi uzsver nepieciešamību pēc pastāvīgas, rūpīgas sistēmu pārvaldības un regulāras drošības pārbaudes.

IETEIKUMI DROŠĪBAI

1. **Veikt paroļu uzglabāšanu šifrētā veidā**, piemēram, izmantojot paroļu pārvaldnieku.
2. **Izmantot divu faktoru autentifikāciju visur**, kur vien tas iespējams.
3. Saņemot e-pastu no personām, ar kurām tiek veikta regulāra komunikācija, pārbaudīt, vai tiek izmantots kāds no e-pasta kontiem, kuri figurē regulārajā komunikācijā. **Sistēmu administratoriem ieteicams izmantot DMARC, SPF un DKIM tehnoloģijas.**
4. Uzturot sistēmas, kurās pieejama iekšējās lietošanas informācija, **regulāri monitorēt eksponētos servisus**, it īpaši pie sistēmu atjauninājumu veikšanas.
5. Tīmekļa vietnēm, kurās iespējams norēķināties ar maksājumu kartēm, **veikt vietnes drošības auditu, ideālā gadījumā arī PCI sertifikāciju**.
6. Izmantojot "WordPress" vai cita veida atvērtā koda CMS, izvēlēties automātisko atjauninājumu iespēju vai **veikt regulārus atjauninājumus**. Rūpīgi izvērtēt uzstādītos spraudņus un to nepieciešamību.
7. Uzturot augstas nozīmības sistēmas vai tādas, kurās tiek glabāta informācija lielā apjomā, kas ir grūti atjaunojama, **obligāti izmantot ārējo rezerves kopiju uzturēšanu**.
8. Uzturot resursus, it īpaši informatīvus un/vai kur minētas konkrētas personas un tām piesaistītā informācija, ko iespējams izmantot jebkāda veida ļaundabīgos nolūkos, piemēram, pikšķerēšanā, norādot jau pieejamu informāciju, kur tas iespējams, **pieprasīt uzglabāt žurnālfailus**, kas satur informāciju par piekļuvi šiem resursiem un to saglabāšanu/lejupielādi, ja informācija tiek nodrošināta dokumentos ar lejupielādes iespēju.
9. Lai aizsargātu piegādes ķēdes no potenciālajiem draudiem, **rūpīgi pārbaudīt un izvērtēt**, vai **starpniekpakalpojuma** sniedzējs uztur augstu **kiberdrošības līmeni**, kā arī turpmāk veikt regulāru uzraudzību.
10. **Izmantot efektīvu aktīvo aizsardzību – DNS ugunsmūri** (https://dnsmuris.lv/), lai pasargātu no ļaunprātīgu vietņu apmeklēšanas.
11. **Plānot un organizēt regulāras darbinieku apmācības un zināšanu pārbaudi** vismaz reizi gadā. Regulāri informēt darbiniekus par biežāk iespējamajiem un šobrīd aktuālajiem kiberapdraudējumiem.



3. Kiberapdraudējumu prevencija

3.1. DNS ugunsmūris: aktīvā aizsardzība

Latvijā regulāri notiek kampaņveidīgas krāpnieciskas aktivitātes – gan novirzīšana uz viltus vietnēm bankas kontu, e-pasta vai sociālo tīklu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšana kibertelpā.
CERT.LV novēro šādas aktivitātes un operatīvi ievieto kampaņu indikatorus DNS ugunsmūrī. Aktīvā aizsardzība pasargā lietotājus no identificēto viltus vietņu apmeklēšanas, tos pārvirzot uz brīdinājuma vietni.
DNS ugunsmūra mobilā lietotne pasargā no kiberkrāpniekiem un viltvāržu zvaniem!
2024. gada rudenī DNS ugunsmūrim tika ieviesta mobilā lietotne. Pateicoties lietotnei, novembrī DNS ugunsmūris 23 615 reižu novērsa mēģinājumus uz iekārtām atvērt viltus saites, kas "WhatsApp" saziņas platformā tika izplatītās kādas krāpšanas kampaņas ietvaros, novirzot šādus pieprasījumus uz drošu piezemēšanās vietni (plašāk par DNS ugunsmūra popularizēšanas kampaņas rezultātiem skatīt 4. nodaļā).

DNS ugunsmūris un mobilā lietotne – aktīvās aizsardzības pakalpojums
Lietotāju pasargāšanai no kiberapdraudējumiem, tādiem kā krāpniecisku vai vīrusu izplatošu tīmekļvietņu apmeklēšanas, nodrošinot vienotu valstī noteikto ierobežojamo domēnu zonu apstrādi un izplatīšanu. Pakalpojumu bez maksas nodrošina CERT.LV un NIC.LV.

Plašāk: https://dnsmuris.lv/

4. ceturksnī kopskaitā DNS ugunsmūra pakalpojuma ietvaros:

- vairāk nekā 1,7 miljoni apstrādāto pieprasījumu;
- 459 213 reizes lietotāji pasargāti no ļaunprātīgu vietņu apmeklēšanas.

Nozīmīgākās aktīvās aizsardzības epizodes 4. ceturksnī

Brīdinājumi	Skaits
"WhatsApp" saziņas platformas izmantošana krāpšanas kampaņās	**23 615**
"Latvijas Pasts" tēla izmantošana viltus vietnes kampaņās	**7 045**
"Latvijas Mobilais Telefons" jeb LMT vārda izmantošana krāpnieciskās kampaņās	**4 959**
"SEB banka" tēla izmantošana viltus vietnes kampaņās	**2 544**
"Citadele banka" tēla izmantošana viltus vietnes kampaņās	**1 381**
AgentTesla ļaunatūra	**968**
Balada ļaunatūra, kas bija atrodama inficētās mājaslapās	**856**

CERT.LV aicina ikvienu Latvijas iedzīvotāju un organizāciju izmantot bez maksas pieejamo DNS ugunsmūra mobilo lietotni. Tā ne tikai pasargā no krāpniecisku un vīrusus izplatošu saišu vietņu apmeklēšanas, bet arī bloķē telefonzvanus no numuriem, ko CERT.LV būs identificējusi kā krāpnieciskus. Tāpat gadījumos, kad ļaunatūra jau ir inficējusi iekārtu, DNS ugunsmūris vai mobilā lietotne sniedz iespēju ātrāk identificēt šādas iekārtas un operatīvi veikt seku novēršanu. Mobilā lietotne sniedz arī atgriezenisko saiti par novērstajiem apdraudējumiem un iespēju sazināties ar CERT.LV. Lejupielādēt lietotni var, sekojot vienkāršai instrukcijai Android un iOS lietotājiem.

Līdz ar NKDL stāšanos spēkā no 2024. gada 1. septembra Elektronisko sakaru komersantiem ir noteikts pienākums izmantot CERT.LV uzturēto ierobežojamo interneta resursu sarakstu DNS RPZ (Response Policy Zone), un ierobežot

galalietotājiem piekļuvi tajā iekļautajiem interneta resursiem. CERT.LV uztur arī atsevišķu DNS RPZ zonu ar katras kompetentās iestādes veidoto sarakstu, kurā iekļauti resursi, kam atbilstoši normatīvajiem aktiem Latvijā jāierobežo piekļuve elektronisko sakaru tīklos.

CERT.LV piedāvā iespēju arī citiem uzņēmumiem un iestādēm, kas paši uztur savus DNS rekursīvos serverus, izmantot CERT.LV uzturētās DNS RPZ zonu sarakstus.

Par krāpnieku aktivitātēm un ļaundabīgām vietnēm CERT.LV aicina nekavējoties informēt Valsts policiju (https://www.vp.gov.lv/lv/ka-zinot-policijai), kā arī pārsūtīt kaitīgās e-pasta vēstules uz cert@cert.lv un krāpnieciskās īsziņas pārsūtīt uz tālruņa numuru +371 232 30 444, kas ir paredzēts tikai īsziņu pārsūtīšanai.

3.2. Sensoru tīkls

Kiberapdraudējumu agrās brīdināšanas sistēma ir CERT.LV nodrošināts pakalpojums, kas veic datu plūsmas anomāliju analīzi un kiberuzbrukumu pazīmju identificēšanu pakalpojuma saņēmēja infrastruktūrā.

CERT.LV pakalpojums ietver:

- nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu;
- brīdinājumu nosūtīšanu pakalpojumu saņēmējam par konstatētajiem augstas prioritātes kiberapdraudējumiem;
- regulāru CERT.LV aktuālo kiberapdraudējumu indikatoru atjaunošanu;
- pakalpojuma saņēmēju konsultēšanu un atbalstu.

CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu. Turpinās sensoru programmu nodrošinājuma darbības pilnveidošana.

Sensoru tīkls – agrās brīdināšanas sistēma (ABS)
Iestādēm un organizācijām, kurās tas ir uzstādīts, ļauj laicīgi pamanīt un atpazīt radušos kiberapdraudējumus, kā arī savlaicīgi reaģēt uz tiem, papildus nodrošinot daudzpusīgāku priekšstatu par apdraudējumu spektru.

Plašāk: https://cert.lv/lv/pakalpojumi

ABS ik mēnesi fiksē vidēji 6 000 augstas prioritātes kiberapdraudējumus (incidentus ar augstu bīstamības potenciālu) valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs.

2024. gada 4. ceturksnī ABS ģenerēto brīdinājumu skaits kopskaitā bija aptuveni 2,4 miljardi kas ir par pusmiljonu vairāk nekā 3. ceturksnī.

ABS ģenerēto augstas prioritātes kiberapdraudējumu brīdinājumu skaits pa CERT.LV signatūru grupām 4. ceturksnī

Apdraudējumi	Oktobris	Novembris	Decembris
Ar datorvīrusiem saistīti brīdinājumi	5696	10418	2559
Ar pikšķerēšanu saistīti brīdinājumi	904	1716	601
Ar potenciāli ļaunprātīgām vietnēm saistīti brīdinājumi	945	5019	1329
Ar robottīklu, krāpšanām, vīrusu indikatoriem saistīti brīdinājumi	6838	1454	962

3.3. Drošības operāciju centrs (SOC)

CERT.LV SOC pakalpojums centralizēti apkopo drošības telemetriju no klienta infrastruktūras, korelē notikumus klienta infrastruktūrā ar CERT.LV pieejamo kiberapdraudējumu indikatoru un zināšanu kopu, lai savlaicīgi identificētu, brīdinātu, apturētu kiberapdraudējumu vai kiberincidentu un novērstu tā kaitējumu.

Drošības operāciju centrs (SOC)
Aktīva un individuāli pielāgota kiberdrošības uzraudzība reāllaikā, lai identificētu, izmeklētu, novērstu apdraudējumus un kiberincidentus 24/7 režīmā.

Plašāk: https://cert.lv/lv/pakalpojumi

Pakalpojums ietver klienta drošības telemetrijas datu apstrādi un īslaicīgu uzglabāšanu CERT.LV infrastruktūrā Latvijas teritorijā, kā arī citas būtiskas priekšrocības.

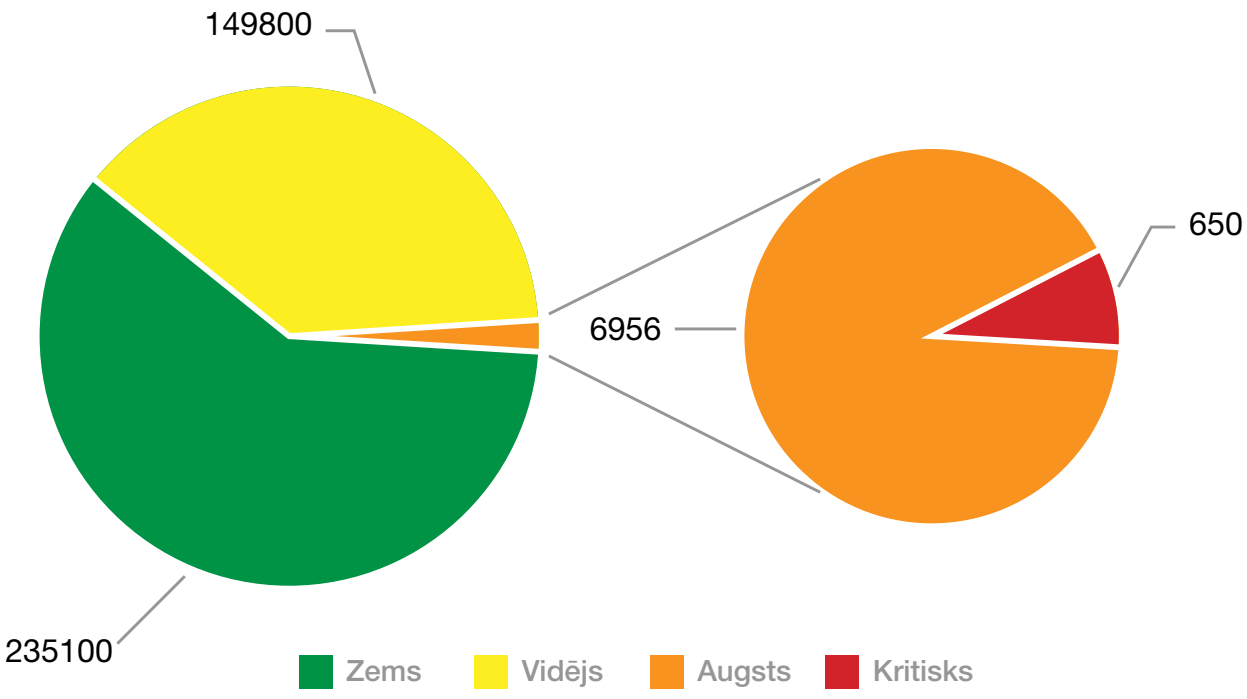
CERT.LV SOC klientiem ir nodrošināta:

- efektīva, centralizēta uzraudzība un iegūta pārredzamība 24/7 režīmā;
- operatīvi pamanīti un novērsti aktuālie kiberapdraudējumi;
- automatizēta aktīvā aizsardzība un prevencija;
- kiberincidentu izmeklēšana CERT.LV komandas vadībā;
- ērta piekļuve informācijas panelim un sekošana līdzi trauksmju ziņojumiem;
- ieteikumi un labā prakse infrastruktūras noturības stiprināšanai.

Pārskata perioda beigās SOC uzraudzīto iekārtu skaits klientu infrastruktūrā ir sasniedzis vairāk nekā 5200, reģistrējot vairāk nekā 392 000 drošības telemetrijas trauksmes ziņojumu, no kuriem 650 bija kritiski.

Lielāko daļu jeb 60% veidoja maznozīmīgi trauksmes ziņojumi, 38% vidējas pakāpes, 2% augstas pakāpes ziņojumu.

Drošības trauksmes ziņojumu sadalījums pēc to kritiskuma līmeņa



10. attēls. Drošības trauksmes ziņojumu skaits uz 2024. gada 4.cet. beigām

Turpinās SOC pakalpojumu attīstīšana un jaunu klientu piesaiste, paplašinot klientu loku atbilstoši NKDL un sekmējot efektīvāku aizsardzību un noturību pret kiberapdraudējumiem.

3.4. Pasākumi incidentu novēršanai

Rūpējoties par Latvijas kibertelpas drošību, CERT.LV piedāvā plašu ar kiberdrošību saistītu pakalpojumu klāstu būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem - Nacionālās kiberdrošības likuma (NKDL) subjektiem, tiešās un pastarpinātās pārvaldes iestādēm, atvasinātām publiskajām personām un citām valsts institūcijām, kā arī privāto tiesību juridiskajām personām, kas pilda valsts pārvaldes deleģētu uzdevumu un privāto tiesību juridiskajām personām.

Pārskata periodā NKDL subjektiem e-pasta vēstulēs tika izsūtīti brīdinājumi gan par novērotiem kiberapdraudējumiem, gan par 5 jaunatklātām kritiskām ievainojamībām, sniedzot norādījumus par atjauninājumiem un mudinot tos nekavējoties ieviest.

Ar būtiskāko CVE ievainojamību apkopojumu un analīzi, kas atklātas 4. ceturksnī, var iepazīties šīs atskaites 2. nodaļas 2.3. sadaļā.

Informācija par jaunatklātiem kiberapdraudējumiem un ievainojamībām tiek publicēta CERT.LV tīmekļa vietnē un sociālo tīklu "X" (@certlv), "Facebook" (@cert.lv) un "LinkedIn" kontos. Tāpat "Mattermost" saziņas platformā notiek regulāra informācijas apmaiņa starp CERT.LV, atbildīgajiem par IT drošību un citiem speciālistiem kiberdrošības kopienā.

3.5. Koordinēta ievainojamību atklāšana (CVD)

Pārskata periodā CERT.LV turpināja darbu pie CVD platformas attīstības un popularizēšanas, pildot koordinētas ievainojamību atklāšanas procesa koordinētāja un vidutāja, kā arī platformas izstrādātāja, uzturētāja un pārziņa lomu.

CVD platformā ir publicēta informācija par iestādēm, kuras brīvprātīgi iesaistījušās koordinētas ievainojamību atklāšanas procesā un noteikušas resursus, uz kuriem ievainojamību ziņošana attiecināma.

Koordinēta ievainojamību atklāšanas platforma (CVD)
Nodrošina iespēju pētniekam reģistrēt ziņojumu par novēroto ievainojamību, kā arī visiem iesaistītajiem (iestādei, pētniekam un CERT.LV) iepazīties ar iesniegto informāciju, savā starpā sazināties un sekot līdzi ievainojamību novēršanas gaitai.

Plašāk: https://cvd.cert.lv/

Platformā tiek reģistrēti ievainojamību ziņojumi un ar to apstrādi saistītā komunikācija starp iesaistītajām pusēm. Šāda ziņošanas prakse dod iespēju CERT.LV savlaicīgi uzzināt par ievainojamībām un pilnvērtīgi koordinēt ievainojamību izpēti un to novēršanu, tādējādi efektīvāk organizējot pasākumus Latvijas kibertelpas aizsardzībai.

2024. gada 4. ceturksnī CVD platformā pieauga gan drošības pētnieku skaits, gan aktīvas iestāžu programmas, gan platformā reģistrēto ievainojamību ziņojumu skaits.

Turpinās darbs, ieviešot pētnieku reitingu un profila informācijas pārvaldīšanas iespēju. Lai nodrošinātu efektīvāku ziņojumu apstrādi, CERT.LV aicina platformā reģistrēties visas iesaistītās puses, tādējādi paātrinot informācijas apmaiņu un padarot caurspīdīgāku saziņu ievainojamības izpētes un novēršanas laikā.

Uz pārskata perioda beigām platformā bija reģistrēti:

- Drošības pētnieki (aktīvi): 78 (+9)
- Aktīvas iestāžu programmas: 12 (+2)
- Ievainojamību ziņojumi: 116 (+22), tajā skaitā:
  - CERT.LV klientūras ievainojamības: 61 (+11)
  - uz konkrētām iestāžu programmām reģistrētās ievainojamības: 55 (+11)

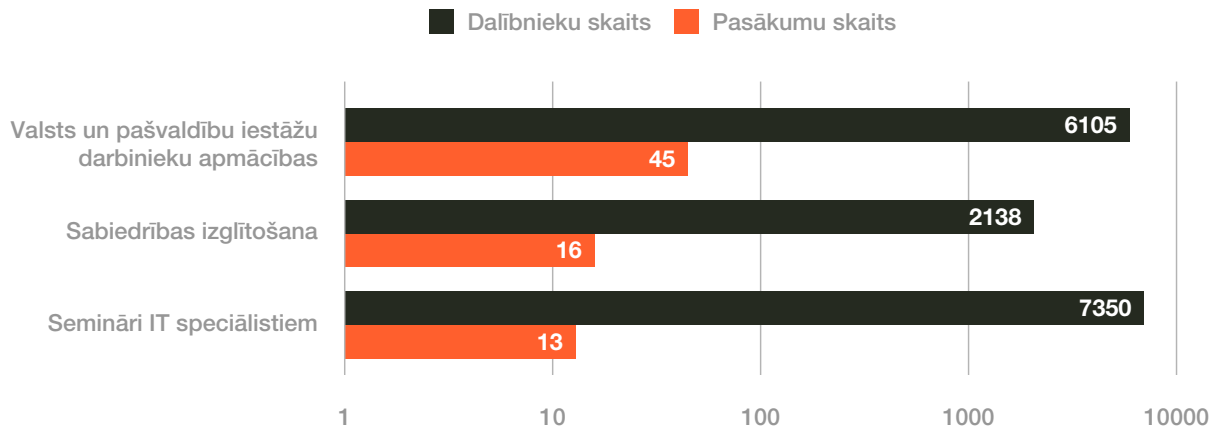
4. Komunikācija ar sabiedrību

4.1. Apmācības un izglītojošie pasākumi

Pārskata periodā CERT.LV komanda veica aktīvu darbu sabiedrības izglītošanā, gan organizējot, gan piedaloties dažādos tematiskos semināros, informējot par aktualitātēm kiberdrošības jomā, kā arī veicinot kiberhigiēnas labo praksi.

4. ceturksnī CERT.LV īstenoja 74 (+57) izglītojošus pasākumus par kiberdrošību un aktualitātēm, apmācot kopskaitā 15 593 (+7 806) dalībniekus.

Izglītojošo pasākumu un apmācīto personu skaits



11. attēls. Izglītojošo pasākumu un apmācīto personu skaits 2024. gada 4. ceturksnī

"KiberŠahs 2024" konference

No 1. līdz 3. oktobrim jau 11. reizi Rīgā norisinājās nozīmīgākā kiberdrošības konference Baltijā – "KiberŠahs 2024" (CyberChess 2024), lai pārrunātu un dalītos pieredzē par stratēģiski politiskiem un dziļi tehniskiem izaicinājumiem, kā arī par inovācijām un nākotnes jautājumiem. Oktobris tradicionāli Eiropā tiek atzīmēts kā kiberdrošības mēnesis, un šīs konferences norise mēneša pašā sākumā iezīmēja simbolisku startu plašākai diskusijai par kiberdrošības nozīmīgumu mūsdienu sabiedrībā. Konferenci organizēja CERT.LV, Aizsardzības ministrija un Nacionālais kiberdrošības centrs sadarbībā ar ISACA Latvijas nodaļu un LU MII.

Pulcējot vairāk nekā 500 kiberdrošības jomas profesionāļus klātienē un vairāk nekā 5 000 tiešsaistē no vairāk nekā 25 valstīm, 63 lektori, tajā skaitā arī runātāji no CERT.LV, 3 dienu garumā dalījās ar saviem pētījumiem un pieredzes stāstiem ar kiberdrošību saistītām tēmām jomās, īpaši pievēršot uzmanību cīņai ar pastāvošajiem kiberapdraudējumiem.

Konferences atklāšanā dalībniekus līdztekus ar Aizsardzības ministru Andri Sprūdu un Nacionālās Kiberdrošības centra ģenerāldirektoru Rolandu Heniņu uzrunāja arī CERT.LV vadītāja Baiba Kaškina.

Konferences galvenās skatuves - stratēģiski politiskās sesijas (#CyberChess) moderators bija pieredzējis starptautisku pasākumu vadītājs Oskars Priede, savukārt paralēlsesijas – #CyberStory, kas apkopoja ar nākotni un inovācijām saistītus tematus, un #CyberShok, kas bija veltīta dziļi tehniskiem pētījumiem un praktiskiem demonstrējumiem, – tajās notiekošās paneļdiskusijas vadīja CERT.LV pārstāvji Dana Ludviga un Dr. Bernhards Blumbergs.

Ar dziļi tehnisku, bet reizē saistošu prezentāciju svarīgākos kiberdrošības izaicinājumus un risinājumus, īpaši pievēršoties pieredzei par paveiktajām kiberdrošības draudu medībām, izklāstīja CERT.LV vadītājas vietnieks Varis Teivāns.

Konferences sesiju starplaikos CERT.LV kiberdrošības eksperts Kārlis Svilans moderēja paneļdiskusijas (raidierakstu sarunas) starp nozares ekspertiem – konferences lektoriem, tā raisot diskusijas par prezentācijās pausto un atklāto.

Pateicoties CERT.LV darbinieku aktivitātēm, sekojot līdz kiberdrošības nozares attīstībai pasaulē, konferences programmā bija iespējams piesaistīt starptautiskos ekspertus no 18 valstīm, kuri dalījās ar saviem pētījumiem un pieredzes stāstiem.

Praktisko semināru konferences pirmajā dienā par DNS ugunsmūra izstrādi un pielietojumu semināru vadīja CERT.LV Incidentu risināšanas nodaļas vadītājs Armīns Palms.

Jau piekto gadu CERT.LV kiberdrošības eksperti B. Blumbergs un K. Svilans līdztekus konferencei "KiberŠahs 2024" organizēja un sekoja līdz arī tiešsaistes kiberdrošības sacensībām Capture The Flag (CTF), kas ļāva sacensību dalībniekiem (70 komandas ar 186 spēlētājiem no 9 valstīm) stāties pretī dažādiem kiberdrošības izaicinājumiem tādās kategorijās kā, piemēram, kriptogrāfija, tīkla analīze, kriminālistika, binārais kods u.c. Pirms konferences tika organizēti vairāki tehniskie semināri, kas sniedza iespēju kiberdrošības profesionāļiem papildināt arī praktiskās zināšanas tādās jomās kā kiberincidentu izmeklēšanā, kiberuzbrukumu analīzē un kiberaizsardzības pilnveidošanā. "KiberŠahs 2024" noslēgumā B. Blumbergs sniedza apkopojumu par rezultātiem un komandu sniegumu.

Konferences materiāli pieejami tīmekļvietnē: https://cyberchess.lv/.

NCC-LV
LATVIJAS KIBERDROŠĪBAS KOORDINĀCIJAS CENTRS

Līdzfinansē Eiropas Savienība

Izglītojošs pasākums IT drošības speciālistiem

11. decembrī CERT.LV organizēja kiberdrošības semināru "Esi drošs" valsts un pašvaldību iestāžu atbildīgajiem darbiniekiem par IT drošību, būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un citiem interesentiem, kuri darbojas IT drošības jomā. Semināru atklāja CERT.LV vadītāja Baiba Kaškina. Atskatu uz 2024. gada notikumiem Latvijas kibertelpā sniedza CERT.LV vadītājas vietnieks Varis Teivāns. Aizsardzības ministrijas Kiberdrošības politikas departamenta direktors Edgars Kiukucāns akcentēja 2024. gadā paveiktos būtiskākos darbus. Seminārā tika aplūkotas tādas tēmas kā kiberdraudu simulācijas – ieguvumi par saprātīgu cenu; digitāla pasaule un kiberdrošība - paradumi un zināšanas skaitļos; DNS ugunsmūra attīstība un ieguvumi lietotājiem; jaunas kiberdrošības apmācību iespējas RTU ar Google.org atbalstu; mākslīgais intelekts – gudrāka drošība. Semināram tiešsaistē sekoja vairāk nekā 1350 dalībnieku. Semināra ieraksts: https://cert.lv/lv/2024/11/it-drosibas-seminars-esi-dross-11-decembri.

Praktiskās mācības, izspēlējot kiberdrošības incidentu izmeklēšanu

CERT.LV turpina savai klientūrai nodrošināt praktisku kiberincidenta izmeklēšanas izspēli, kur tās dalībniekiem tiek sniegta unikāla iespēja iejusties kiberdetektīvu lomā un interaktīvā veidā pētīt un analizēt kiberuzbrukuma gaitu starptautiskā uzņēmumā. Viens no izspēles centrālajiem uzdevumiem ir noskaidrot vainīgo, kurš ir atbildīgs par kiberuzbrukumu, kā arī pārrunāt tā sekas.

Pārskata periodā interaktīvas mācības ar CERT.LV speciālistu vadībā izspēlētu kiberdrošības incidentu spēli notika **4** organizācijās. Kopskaitā no visām organizācijām spēlē piedalījās **249 dalībnieki, kas ir 7 reizes vairāk nekā 3. ceturksnī**. Praktisko mācību ietvarā dalībniekiem bija iespēja noklausīties CERT.LV lekciju "Kiberdrošības aktualitātes – draudi un risinājumi".

Kiberdrošības incidentu izmeklēšanas spēli sagatavojusi Eiropas Savienības Kiberdrošības aģentūra ENISA, lai veicinātu izpratni par kiberdrošību jomas nespeciālistiem, savukārt latviešu valodā to tulkojuši un pielāgojuši CERT.LV eksperti.

Veiksmīgi īstenota informatīvā kampaņa par DNS ugunsmūra jauno mobilo lietotni

Lai veicinātu DNS ugunsmūra pakalpojuma lietošanu un padarītu to iedzīvotājiem viegli un ērti izmantojamu, pārskata periodā CERT.LV ieviesa DNS ugunsmūra lietotni, kas ir ērti lejupielādējama un aktivizējama mobilajās iekārtās Android un iOS lietotājiem.

DNS ugunsmūra un mobilās lietotnes popularizēšanas kampaņas "Liec mūri pret krāpnieka dūri!" laikā, jaunā lietotne tika lejupielādēta vairāk nekā **30 000** reižu.

Dalība Baltijas kiberdrošības inovāciju foruma "CyberBazaar 2024" konferencē

5. decembrī Rīgā tika atklātā pirmā Baltijas kiberdrošības inovāciju foruma "CyberBazaar 2024" tehnoloģiju un biznesa konference. Tās ietvaros no 3. līdz 4. decembrim norisinājās kiberhakatons, vairāk nekā 300 studentiem no Baltijas valstīm paverot iespēju radīt jaunus tehnoloģiskus risinājumus kiberdrošības pārvaldībā, inovācijās un izpratnes veicināšanā. Hakatona laikā dalībniekiem atbalstu sniedza mentori, tajā skaitā CERT.LV pārstāvji Dana Ludviga un Bernhards Blumbergs, savukārt Sanita Vītola piedalījās žūrijas komisijā.

Konferences dalībniekiem bija pieejama arī konferences EXPO zona, kurā CERT.LV pārstāvji interesentus iepazīstināja ar DNS ugunsmūra mobilās lietotnes priekšrocībām.

Atbalsts Aizsardzības ministrijas reģionālo kiberdrošības semināru organizēšanā

CERT.LV sniedza atbalstu informatīvo semināru organizēšanā par visaptverošu valsts aizsardzību. Pārskata perioda semināri tika organizēti pārstāvjiem no Zemgales reģiona.

CERT.LV ekspertu uzstāšanās citos nozīmīgos pasākumos

9. oktobrī "SEB CFO Forum 2024" uzņēmumu vadītāju un finanšu direktoru foruma ietvaros paneļdiskusijā pieredzē dalījās Baiba Kaškina.
17. oktobrī "EPALE kopienas konferencē 2024" Dana Ludviga piedalījās ar prezentāciju – "Kiberdrošības Kods: Latvijas kibertelpas draudi, ekspertu izaicinājumi un mans ceļš".
18. oktobrī konferencē "Mākslīgais intelekts un drošība digitalizācijā" paneļdiskusijā ar zināšanām dalījās Gints Mālkalnietis.
18. oktobrī Dekšāru iedzīvotājiem latgaliešu valodā par kiberdrošību stāstīja Armīns Palms.

21. oktobrī konferencē "Izglītības tehnoloģiju diena" Jānis Džeriņš tehnoloģiju skolotājiem sniedza prezentāciju "MI drošības aspekti", apskatot ģeneratīvā MI aspektus un izaicinājumus.
30. oktobrī tehnoloģiju un inovāciju forumā "5G Techritory" Kristians Teters runāja par kiberdrošības ekosistēmu – publiskā un privātā sektora partnerības lomu kiberdrošības jomā.
7. novembrī LTRK seminārā uzņēmējiem prezentācijā "No klikšķa līdz krīzei: kā Kiberhigiēna var palīdzēt?" ar praktiskiem ieteikumiem dalījās Mārtiņš Vecstaudžs.
21. novembrī konferencē "Digitālā transformācija: no domas līdz veiksmes stāstam" Dana Ludviga stāstīja par kiberdrošību Latvijā: apdraudējumi, izaicinājumi un noturības stiprināšana.
28. novembrī "Mākslīga intelekta impulss" rudens konferencē augstāka līmeņa vadītājiem ar prezentāciju "Drošības dimensijas, izmantojot MI valsts iestādē" uzstājās Baiba Kaškina.
9. decembrī Rīgas Tehniskajā universitātē "Google" kiberdrošības apmācību programmas atklāšanas pasākumā paneļdiskusijā runāja Varis Teivāns.
11. decembrī LPKS LATRAPS kopsapulcē ar ievadlekciju par kiberdrošības konceptu un veidiem, kā varam sevi pasargāt pret ārējiem draudiem, stāstīja Baiba Kaškina.

- Organizācijas "Sievietes drošībai" līderības un mentoru programmā mentora statusā piedalījās Baiba Kaškina, sniedzot atbalstu jaunajām profesionālēm izaugsmes ceļā

4.2. Sabiedrības informēšana un kiberhigiēnas veicināšana

Pārskata periodā CERT.LV turpināja informēt sabiedrību par kiberdrošības riskiem, kiberhigiēnas labo praksi un dažādām aktualitātēm Latvijas kibertelpā.

Tīmekļa vietnē www.cert.lv publicētas kopskaitā 25 ziņas gan par aktuāliem kiberapdraudējumiem un ievainojamībām, gan par citiem būtiskiem notikumiem Latvijas kibertelpā.

CERT.LV uzturētajā portālā www.esidross.lv publicēti 6 raksti no ikmēneša izdevuma OUCH! (informācijas drošības biļetens, ko veido SANS institūta).

- **Lejupielādes briesmas: kā pārspēt ļaunprātīgas mobilās lietotnes.**10/ 2024
- **Neļaujiet kibernoziedzniekiem izkrāpt jūsu uzkrājumus: pasargājiet savus kontus!** 11/2024
- **Interneta lietotajiem bez maksas pieejama lietotne kiberkrāpnieku atvairīšanai.** 11/2024
- **Padomi, lai pasargātu sevi no finanšu krāpniekiem.** 11/2024
- **Atklājot ēnu pasauli: kā kibernoziedznieki nozog jūsu paroles.** 12/2024
- **Kā nekļūt par viltus internetveikalu upuri?** 12/2024

CERT.LV turpina apkopot ikmēneša apskatu "KiberLaikapstākļi" par spilgtākajiem notikumiem Latvijas kibertelpā TOP 5 kategorijās – krāpšana, ļaunatūras, ievainojamības, pakalpojuma pieejamība, ielaušanās / datu noplūde, kā arī lietu internets. Apskati pieejami tīmekļvietnes cert.lv sadaļā "Ziņas":

- **Oktobris:** https://cert.lv/lv/2024/11/kiberlaikapstakli-2024-oktobris
- **Novembris:** https://cert.lv/lv/2024/12/kiberlaikapstakli-2024-novembris
- **Decembris:** https://cert.lv/lv/2025/01/kiberlaikapstakli-2024-decembris

5. Stratēģiskā sadarbība Latvijā

Sadarbība ar kompetentajām institūcijām

CERT.LV speciālisti savas kompetences ietvaros piedalās Nacionālās kiberdrošības stratēģijas uzdevumu īstenošanā un normatīvo dokumentu izstrādes procesā, cieši sadarbojoties ar LR Aizsardzības ministrijas Kiberdrošības politikas departamentu, kā arī savstarpēji apmainās ar informāciju par kiberincidentu jomas aktualitātēm.

CERT.LV piedalās Nacionālās kiberdrošības padomes darbā, kuras mērķis ir koordinēt ar kiberdrošību saistītās politikas izstrādi, uzdevumu un pasākumu plānošanu un īstenošanu.

Turpinās cieša sadarbība ar LR Zemessardzes Kiberaizsardzības vienību, kas informācijas tehnoloģiju krīzes vai kiberapdraudējuma situācijā sadarbībā ar CERT.LV sniedz atbalstu valsts un privātajam sektoram.

CERT.LV turpina organizēt DEG sanāksmes ar mērķi veicināt un sekmēt kiberdrošības kultūru Latvijā un sniegt atbalstu CERT.LV.

CERT.LV atbalsts DDUK sekretariāta darbā

Turpinās sadarbība ar Digitālās drošības uzraudzības komiteju (DDUK) – jautājumos, kas skar elektroniskās identifikācijas pakalpojumu sniedzējus un to sniegtos pakalpojumus, uzticamus sertifikācijas pakalpojumu sniedzējus un to sniegtos pakalpojumus, parakstu vākšanas tiešsaistes sistēmas, būtisko pakalpojumu un svarīgo pakalpojumu sniedzējus. CERT.LV veic arī Latvijas uzticamības saraksta (LV TSL – LV trust list) uzturēšanu.

Turpinās CERT.LV ekspertu iesaiste topošās eIDAS 2.0 regulas projekta izskatīšanā, kā arī tā ietekmes uz DDUK plānotajiem darbiem novērtēšanā, tostarp iesaistoties digitāla maka ieviešanas darba grupas sanāksmēs. Pārskata periodā tika veikta uz eiDAS 2.0 bāzes izstrādājamo īstenošanas aktu 1. un 2. pakotnes izskatīšana no DDUK un CERT.LV kompetences viedokļa, kā arī komentāru sniegšana un ISO standartu izpēte, kas tiešā mērā attiecināmi uz IKT produktu drošības sertifikācijas jautājumiem, lai stiprinātu DDUK kompetenci darbam pie digitāla maka nacionālas sertifikācijas shēmas.

Ieguldījums kiberdrošības rīcībpolitikas attīstībā

Pārskata periodā turpinājās darbs pie CERT.LV iekšējās un ārējās dokumentācijas pielāgošanas atbilstoši Nacionālās kiberdrošības likuma (NKDL) prasībām.

CERT.LV eksperti turpina sniegt ieguldījumu nozares politikas pamatnoteikumu sagatavošanā. Pārskata periodā tika sniegti komentāri uzlabojumiem topošajos ar kiberdrošības tēmām saistītajos MK noteikumos, tajā skaitā gan par noteikumiem minimālajām kiberdrošības prasībām, gan par datu centra noteikumiem. Tika veikti vairāki auditi, kas saistīti ar kiberdrošību. Turpinās darbs

Lepojamies!

2024. gada 11. novembrī Aizsardzības ministrs Andris Sprūds pasniedza Pateicības rakstus par veiksmīgu sadarbību un ieguldījumu Latvijas kibertelpas drošības un valsts aizsardzības spēju stiprināšanā CERT.LV darbiniekiem – Kristiānai Muzei-Feldbergai un Artūram Daņiļēvičam. Pateicības raksts piešķirts arī Dainai Ozoliņai.

2024. gada 18. novembrī visai CERT.LV komandai tika piešķirts Nacionālo bruņoto spēku (NBS) Goda raksts par būtisku ieguldījumu NBS kiberdrošības jomas attīstībā un valsts aizsardzības stiprināšanā.

pie jauno normatīvo aktu skaidrošanas un vadlīniju sagatavošanas, lai atbalstītu NKDL subjektus jauno prasību ieviešanā.

Pārskata periodā tika veikta tiesību aktu projektu/iniciatīvu izskatīšana, tostarp 8 ES un 5 Latvijas līmeņa tiesību aktu projekti, kā arī organizētas sanāksmes ar Latvijas līmeņa likumprojektu virzītājiem atsevišķu problēmjautājumu vai komentāru pārrunāšanai. CERT.LV pārstāvji ļoti aktīvi iesaistījās MK noteikumu izstrādē par nosakāmajām drošības prasībām datu centriem.

Turpinās regulāra dalība Valsts kancelejas izveidotās Valsts informatīvās telpas drošības darba grupas sanāksmēs.

Turpinās aktīva iesaiste Nacionālā koordinācijas centra vadītajā Starpinstitucionālajā darba grupā, veicinot efektīvu informācijas apmaiņu starp valsts pārvaldes iestādēm un organizācijām par aktivitātēm un pasākumiem dažādās kiberdrošības jomās.

Turpinās sadarbība ar Latvijas Interneta asociāciju (LIA), kas izglīto sabiedrību par iespējamajiem riskiem un draudiem interneta vidē. LIA Drošāka interneta centra ziņojumu pārskatu detalizētāk skatīt 7. nodaļā.

5.1. Atbalsts kibernoziegumu atklāšanā un novēršanā

5.1.1. Sadarbība ar IKT kritiskās infrastruktūras turētājiem

Turpinās sadarbība ar IKT kritiskās infrastruktūras turētājiem, gan uzraugot situāciju kibertelpā, nodrošinot operacionālo atbalstu un centralizētu aizsardzību pret kiberuzbrukumiem, gan sniedzot atbalstu kibernoturības stiprināšanai un dažādu sektoru sadarbības pilnveidošanai.

NKDL subjektiem CERT.LV nodrošina plašu un profesionālu pakalpojumu klāstu – Drošības operāciju centra (SOC) pakalpojumus, Agrās brīdināšanas sistēmas, DNS ugunsmūri, kiberdrošības draudu medības, kiberapdraudējumu simulācijas, drošības testus, industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums u.c.

CERT.LV ir izveidojusi SOC, kas nodrošina kvalitatīvu un savlaicīgu kiberapdraudējumu un kompromitētu sistēmu atpazīšanu. Pārskata periodā būtisks uzsvars tika likts uz SOC kapacitātes un jaudas attīstīšanu, turpinot nodrošināt CERT.LV klientus ar pasaules līmeņa aizsardzības risinājumiem, kas sniedz reālus ieguvumus.

Aktuālais operacionālo tehnoloģiju (OT) iekārtu drošības veicināšanā

Lai veicinātu industriālās automatizācijas un kontroles sistēmu drošību, CERT.LV nodrošina laboratorijas pakalpojumus, kas paredzēti operacionālo tehnoloģiju (OT) iekārtu, programmatūras un komunikācijas protokolu drošības testēšanai.

CERT.LV piedāvā dažādu sektoru infrastruktūras turētājiem (enerģētika, transports, ūdens u.c.) veikt industriālās automatizācijas un vadības komponenšu drošības testēšanu. Pārskata periodā uzsākta aktīva sadarbība ar vairākiem šo sektoru pārstāvjiem, kā arī turpinājās sadarbība ar Latvijas enerģētikas sektora uzņēmumiem.

2025. gada februārī Latvija spers nozīmīgu soli energoneatkarības virzienā – Baltijas valstis pilnībā atslēgsies no Krievijas kontrolētā BRELL elektrotīkla un pievienosies kontinentālās Eiropas energosistēmai. Lai Latvija šim notikumam būtu gatava no kiberdrošības aspektiem – 2025. gada sākumā plānota CERT.LV iesaiste, koncentrējoties uz BRELL atslēgšanas procesa drošību un kibernoturības stiprināšanu.

IKT kritiskās infrastruktūras turētājiem ieteicams izmantot CERT.LV pakalpojumus, lai nodrošinātu plašāku redzamību pār OT sistēmām, to tīkliem, lietotajām iekārtām, to komunikāciju protokoliem, kā arī agrīnu reaģēšanu uz kiberincidentiem un kompromitētu sistēmu atpazīšanu. Ieteicami drošības testi un draudu medību operācijas kā efektīvi instrumenti ievainojamību konstatēšanai, uzbrucēju atklāšanai un to darbības efektīvai apturēšanai.

5.1.2. Atbalsts Latvijas valsts tiesībsargājošajām iestādēm

CERT.LV turpina sniegt atbalstu Latvijas valsts tiesībsargājošajām iestādēm – jautājumos, kas skar noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu, nodrošinot ātru un efektīvu reaģēšanu uz dažādiem kibericidentiem, veicot padziļinātas izpētes un sniedzot Valsts Policijai savā rīcībā esošo informāciju par kiberincidentiem, kiberapdraudējumiem vai ievainojamībām.

Pārskata periodā CERT.LV savas kompetences ietvaros būtisku atbalstu Valsts policijai sniedza izmeklēšanas darbā saistībā ar informācijas drošības incidentu, par ko paziņoja IT sistēmas izstrādātājs "ZZ Dats", kad tehniskas kļūmes dēļ no Vienotās pašvaldību informācijas sistēmas noplūda ievērojams datu apjoms. Incidenta izmeklēšana turpinās, Valsts policijā uzsākts kriminālprocess par notikušo. CERT.LV veica arī izvērtējumu par incidenta juridisko pusi savas kompetences ietvaros, sniedzot savu redzējumu Valsts policijai.

Tāpat pārskata periodā CERT.LV sniedza komentārus Valsts policijai par dažādos incidentos iesaistītajām IP adresēm un ar tām saistītajiem potenciālajiem kiberapdraudējumiem. Tika veikta kiberdrošības incidentos iesaistīto iekārtu analīze un sniegti atzinumi pēc programmatūru izvērtējuma.

CERT.LV akcentē nepieciešamību turpināt Latvijas sabiedrības izpratnes vecināšanu par kibertelpu un kibernoziegumu riskiem tajā, lai stiprinātu sabiedrības noturību pret kiberzubrukumiem, mazinātu to ietekmi un sekmētu to novēršanu.

Īpaša uzmanība ir jāpievērš preventīvām metodēm un iniciatīvām, kas ļautu bloķēt ar noziedzīgu mērķi radītas vai noziedzīgām darbībām izmantotas interneta vietnes, šo iniciatīvu atzīšanu un iedzīvināšanu, turpinot pilnveidot arī iesaistīto institūciju sadarbību un atbildīgo institūciju reaģēšanas ātrumu.

Lepojamies!

2024. gada 15. novembrī CERT.LV vadītāja Baiba Kaškina un CERT.LV vadītājas vietnieks Varis Teivāns saņēma godpilno 3. pakāpes kriminālpolicijas Goda zīmi par nozīmīgu ieguldījumu cīņā ar noziedzību un sakarā ar Valsts policijas 106. gadadienu. Šī Goda zīme ir augstākais kriminālpolicijas apbalvojums.

5.1.3. IT sistēmu drošības testi un izvērtējumi

2024. gada 4. ceturksnī CERT.LV speciālisti veica **4 drošības testus** un **7 pikšķerēšanas** uzbrukumu simulācijas IKT kritiskās infrastruktūras un pakalpojumu nodrošināšanas organizācijās.

To laikā tika konstatētas un novērstas vairākas ievainojamības, tostarp kopskaitā **2** kritiskas, **5** augsta riska, **9** vidēja riska un **8** zema riska ievainojamības, kā arī tika trenētas šo organizāciju darbinieku kiberhigiēnas prasmes.

IT sistēmu drošības testi

Drošības testi identificēt potenciālas ievainojamības, drošības adrošības apdraudējumus un sistēmas nepilnības, lai novērstu iespējamos kiberuzbrukumus un datu noplūdes.

Pikšķerēšanas uzbrukumu simulācijas

Ar CERT.LV pakalpojuma palīdzību organizācijas var simulēt pielāgotus un reālus pikšķerēšanas uzbrukumus, lai apmācītu un veicinātu personāla spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Tas palīdz stiprināt organizāciju aizsardzību pret sociālās inženierijas uzbrukumiem, tādā veidā mazinot cilvēciskā faktora riskus.

CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi saņemt pakalpojumu.

5.1.4. Kiberdrošības draudu medību operācijas

Līdz pārskata beigām kiberdrošības draudu medību operācijās analīze veikta **150 000 gala iekārtās** dažādās publiskā sektora iestādēs un IKT kritiskās infrastruktūras uzņēmumos.

Veicot pārbaudes, aptuveni **20% gadījumu infrastruktūrā tika konstatēta citu valstu atbalstītu uzbrucēju klātbūtne**. Šie uzbrucēji veic plaša spektra kiberoperācijas, sadarbojoties arī ar finansiāli motivētiem uzbrucējiem, no kuriem mēdz pārpirkt vai citādi iegūt sākotnējo piekļuvi. Novērota gan ar Krieviju, gan ar Ķīnu potenciāli saistītu grupējumu aktivitāte.

Vairākos gadījumos konstatēta ar Krieviju un Ķīnu saistāmo kiberoperāciju pārklāšanās, ļaujot spekulēt par grupējumu savstarpēju sadarbību. Abās pusēs konstatēta uzvedības, rīku, valodas un taktikas izmantošana, kas raksturīga otras valsts uzbrucējiem, lai, iespējams, maldinātu analītiķus atribūcijas jautājumos.

CERT.LV ir līdere Eiropā apjomīgu kiberdrošības draudu medību jomā

Lai stiprinātu Latvijas kibertelpu, CERT.LV kopā ar stratēģiskajiem partneriem turpina veikt draudu medību operācijas.

Laika posmā no 2022. gada līdz 2024. gada decembrim tika pārbaudītas vairāk nekā 150 000 iekārtas 35 organizācijās ar mērķi identificēt kiberapdraudējumu klātbūtni Latvijai svarīgās IKT infrastruktūras sistēmās.

CERT.LV gan atsevišķi, gan kopā ar sadarbības partneru apvienoto komandu darbojas iepriekš izvēlētā informācijas sistēmu tīklā (mērķa iestādes izvēle tiek izvērtēta sadarbībā ar valsts drošības iestādēm), lai identificētu uzbrucēja klātbūtni, atklātu, uzraudzītu un analizētu ļaunprātīgas darbības, kā arī lai analizētu uzbrukumu taktiku, paņēmienus un procedūras. Draudu medību atskaitē, kuru pēc katras no operācijām saņem mērķa iestādes vadība, tiek iekļauta informācija par visiem atradumiem, kā arī tiek sniegti ieteikumi notikušu uzbrukumu seku mazināšanai un kibernoturības stiprināšanai.

Citas aktualitātes pārskata periodā

Neraugoties uz augsto kiberapdraudējumu intensitāti, Latvija ne tikai stāv pretī šiem izaicinājumiem, bet ir kļuvusi par piemēru citām valstīm. CERT.LV sadarbībā ar Kanādas bruņotajiem spēkiem ir izveidojusi Draudu medību rokasgrāmatu, kurā iekļautas rekomendācijas draudu medību veikšanai, kā arī tika novadīts pirmais seminārs starptautiskajiem partneriem, daloties ar līdzšinējo pieredzi. Semināru plānots turpināt arī 2025. gadā.

- Pārskata periodā no 27. novembra līdz 13. decembrim noritēja kopīgas paaugstinātas aktivitātes draudu medības ar Polijas un Kanādas Bruņoto spēku kiberpavēlniecībām.
- Oktobrī tika aizvadīts starptautiskais draudu medību operāciju seminārs Threat Hunting Workshop, kas tika īstenots sadarbībā ar Kanādas bruņoto spēku kiberpavēlniecību un NATO CCDCOE.
- Papildus notiek darbi, lai īstenotu nākamo iterāciju uzlabotam draudu medību seminaram, kas risināsies 2025. gadā no 4. līdz 6. februārim.

Lai efektīvi pasargātu un gūtu reālo ieskatu savā IKT infrastruktūrā, NKDL subjektiem ieteicams izmantot kiberdrošības draudu medību operācijas.

Par vēlmi saņemt CERT.LV pakalpojumu rakstīt uz cert@cert.lv.

5.2. Izglītība un jauniešu kiberprasmju uzlabošana

Turpinās sadarbība un atbalsts Saldus tehnikumam, piedaloties darba grupā, kas veido profesionālās kvalifikācijas standartam "Kiberdrošības tehniķis" atbilstošas apmācību programmas piedāvājumu.

Latvijas komanda pirmo reizi startē Eiropas kiberdrošības sacensībās jauniešiem

2024. gadā Latvijas komanda pirmo reizi piedalījās "Eiropas kiberdrošības izaicinājums 2024" (ECSC) sacensībās jauniešiem 37 komandu konkurencē, kas norisinājās 2024. gadā no 8. līdz 11. oktobrim Turīnā, Itālijā. CERT.LV aktīvi iesaistās jauniešu kiberdrošības prasmju veicināšanā, gan atbalstot Nacionālā kiberdrošības izaicinājuma sacensību sagatavošanu, gan piedaloties Latvijas komandas sagatavošanā dalībai ECSC sacensībās. CERT.LV eksperts Rihards Kauliņš piedalījās Latvijas komandā kā dalībnieks, un CERT.LV eksperts Mārtiņš Vecstaudžs atbalstīja komandu gan sagatavošanas darbos, gan sacensību laikā, piedaloties sacensību komiteju darbā.

ECSC mērķis ir sekmēt jaunas kiberdrošības ekspertu paaudzes attīstību, stiprinot formālo un neformālo kiberdrošības izglītību un apmācību, veicinot jauniešu līdzdalību un aktīvu iesaisti ar kiberdrošību saistītajās aktivitātēs, kā arī sekmējot sadarbību starp Eiropas Savienības dalībvalstīm kiberdrošības jomā.

Eiropas kiberdrošības izaicinājums (ECSC)

Ikgadējās starptautiskās kiberdrošības sacensības, kuras organizē ES Kiberdrošības aģentūra (ENISA) sadarbībā ar dalībvalstīm un citiem partneriem.

Plašāk: https://kibiz.lv/#about

Lai gan Latvijas komandai, piedaloties pirmo reizi, 2024. gadā vēl neizdevās izcīnīt godalgotas vietas, jauniešiem tā bija nenovērtējama pieredze, kuras gaitā komanda apliecināja sevi kā neatlaidīgus, enerģiskus un augsti motivētus sacensību dalībniekus.

Sacensību uzdevumi veidoti tā, lai maksimāli atspoguļotu kiberdrošības problēmas, ar kurām reālajā dzīvē saskaras publiskais un privātais sektors, aptverot tādas jomas kā tīkla analīze, kriptogrāfija, ielaušanās testi, publiski pieejamo informācijas avotu izpēte (OSINT) u.c.

Aizsardzības ministrijas ES kiberdrošības jautājumu nodaļa organizē ECSC Latvijas nacionālo atlasi. Aktivitāte notiek Aizsardzības ministrijas NCC-LV koordinētā projekta ietvarā. CERT.LV piedalās ECSC nacionālās atlases tīmekļa vietnes izveidošanā, kā arī nacionālās atlases nodrošināšanai nepieciešamās infrastruktūras un uzdevumu kopas sagatavošanas darbos.

Latvijas jaunieši gūst jaunas prasmes un pieredzi kibersacensībās #KiberPlēsis

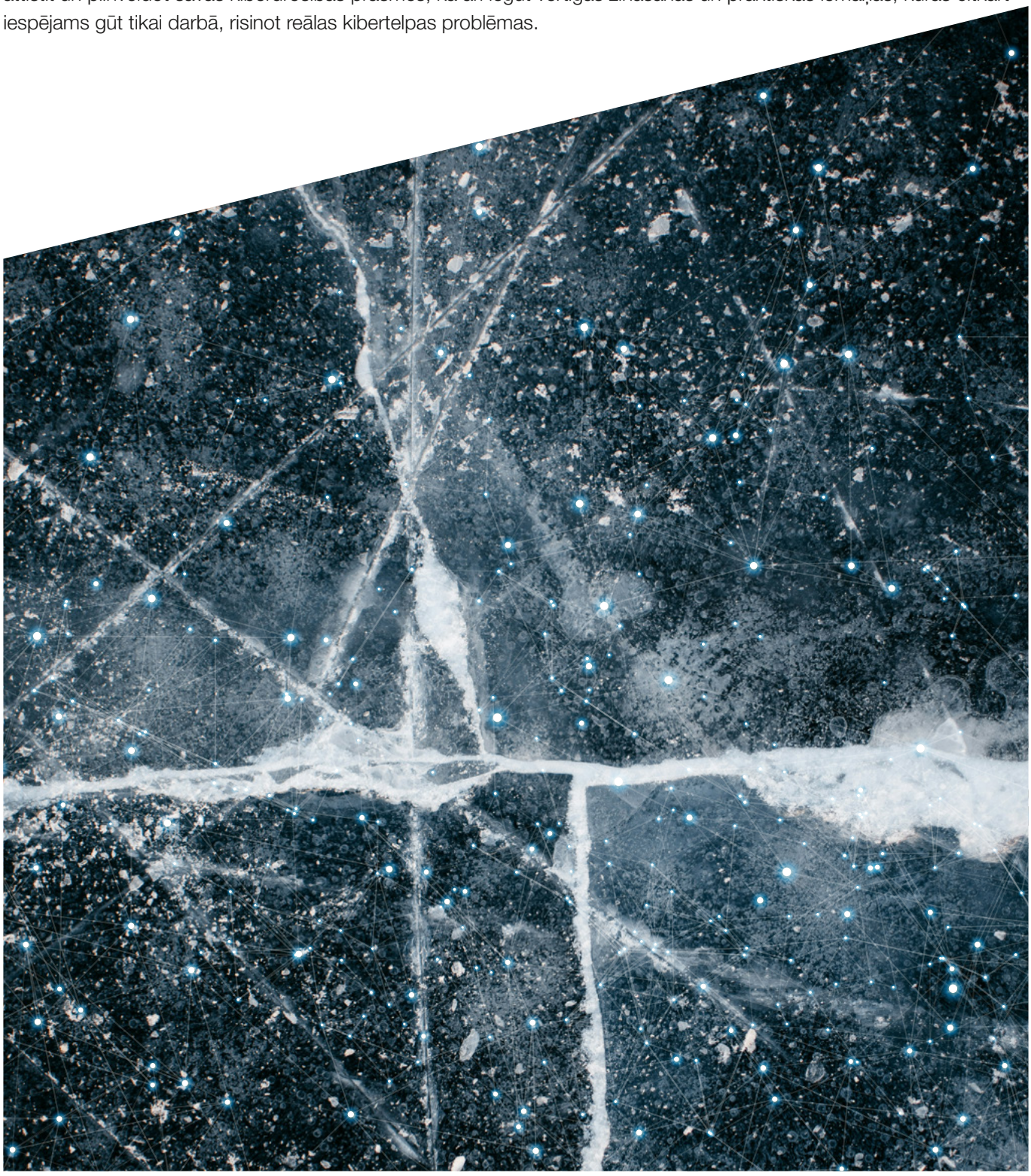
Trešo gadu pēc kārtas Latvijas jaunieši vecumā no 16 līdz 24 gadiem varēja pieteikties un piedalīties kiberdrošības sacensībās #KiberPlēsis, kas notika 2024. gada 11. novembrī. Dalībniekiem bija iespēja izaicināt savas IT prasmes,

kļūstot par kibertelpas varoņiem, risinot uzdevumus "Capture the Flag" (CTF) formātā. Sacensību mērķis ir rosināt jauniešu interesi un iedrošināt viņus izvēlēties kiberdrošību kā savu nākotnes profesiju.

Sacensības rīko drošības tehnoloģiju uzņēmums CYBER CIRCLE, savukārt CERT.LV pasākumu atbalstīja informatīvi.

> "Jauniešu iegūtās prasmes un pieredze šādās sacensībās var nākotnē kļūt par vērtīgu resursu, kas stiprina mūsu sabiedrības un valsts kibertelpas drošību un aizsardzību. "
>
> CERT.LV vadītāja Baiba Kaškina

CERT.LV vadītāja Baiba Kaškina vērsa uzmanību uz to, ka piedaloties #KiberPlēsis sacensībās, jaunieši var daudzpusīgi attīstīt un pilnveidot savas kiberdrošības prasmes, kā arī iegūt vērtīgas zināšanas un praktiskas iemaņas, kuras citkārt iespējams gūt tikai darbā, risinot reālas kibertelpas problēmas.



6. Starptautiskā sadarbība

Pārstāvot Latvijas intereses un stiprinot sadarbību ar starptautiskām kiberdrošības vienībām un organizācijām, CERT.LV veicina savstarpēju paraugprakses un pieredzes apmaiņu, sniedz konsultācijas un atbalstu, uzstājas starptautiskās konferencēs un semināros. CERT.LV darbinieki turpina apgūt jaunas prasmes un celt kvalifikāciju, piedaloties starptautiskās mācībās.

Sadarbība ar CSIRTs tīklu, ENISA, ES institūcijām un NATO

CERT.LV regulāri piedalās NIS2 (Tīklu un informācijas drošības) direktīvas CSIRTs Network (CSIRT tīkls) sadarbības tīkla sanāksmēs, ko koordinē ENISA – ES Kiberdrošības aģentūra.

Pārskata periodā CERT.LV turpināja dalību CSIRTs Network darba grupā "Maturity", kas paaugstina ES dalībvalstu CSIRT komandu brieduma līmeni.

CERT.LV dalība ENISA organizētajās darba grupās:

- Coordinated Vulnerability Disclosure Task Force – turpinās darbs pie ES līmeņa koordinētas ievainojamību atklāšanas pieredzes un prakšu apkopošanas;
- EU Cybersecurity Index – turpinās darbs pie platformas attīstīšanas.

CSIRT Network Maturity Peer-review: CERT.LV vadītāja Baiba Kaškina piedalījās CSIRT.SK procesu peer review, kas liecina par augstu profesionālo kompetenci un uzticību starptautiskai sadarbībai kiberdrošības jomā.

CSIRTs Network – ES dalībvalstu kiberdrošības incidentu novēršanas institūciju tīkls, kas nodrošina sadarbību starp institūcijām. Sanāksmes notiek 3 reizes gadā. Reizi gadā notiek apvienotās sesijas ar NIS2 direktīvas sadarbības grupu un CyCLONe.

"Šāda sadarbība sniedz vērtīgu pieredzes apmaiņu un starptautiskos kontaktus, kas kopumā veicina kiberdrošību gan Latvijā, gan starptautiski."

CERT.LV vadītāja Baiba Kaškina

Eiropas Komisijas EHDS (European Health Data Space) regulas darba grupa: CERT.LV speciālisti sniedza savu ieguldījumu, veicinot pacientu elektronisko datu pieejamību un iesaistīto pušu sadarbību Eiropas līmenī. Pārskata periodā darba grupa izvērtēja regulas saikni ar Mākslīgā intelekta aktu, Datu pārvaldības aktu un Vispārīgo datu aizsardzības regulu.

Dalība Eiropas Kiberdrošības produktu sertifikācijas grupas (European Cybersecurity Certification Group) sanāksmēs, tostarp pārstāvot Latvijas intereses un sniedzot savu redzējumu par problemātiskiem jautājumiem, kas skar ES mākoņpakalpojumu sertificēšanas shēmas (EUCS) tālāku virzību ES valstīs un par citiem IKT produktu kiberdrošības sertifikācijas ieviešanas jautājumiem ES valstīs.

ENISA organizētās mācības "Cyber Europe 2024"un "Cyber Europe 2026"

No 25. -26. novembrim CERT.LV eksperti piedalījās mācību "Cyber Europe 2024" noslēguma sanāksmē, kurā dalībvalstis vienojās par mācību noslēguma ziņojumu saturu un publicēšanas kārtību, dalījās pieredzē par mācību iepriekšējā cikla organizāciju, kā arī piedalījās "Cyber Europe 2026" sākotnējā plānošanas sanāksmē.

Mācības "Cyber Europe 2026" tiek plānotas 2026. gada maijā. Kā potenciālie mācību scenāriji tiek izvērtēti valsts pārvalde un iestādes, kas nodrošina vēlēšanu norisi, vai arī transporta nozare – dzelzceļš un ostas. Šo lēmumu

pieņems dalībvalstis, attiecīgi balsojot par scenārijiem. Mācībās, tāpat kā iepriekšējos gados, būs gan tehniskie, gan krīzes vadības un komunikācijas uzdevumi. To izstrādē un testēšanā ENISAi būs nepieciešams lielāks dalībvalstu atbalsts, īpaši tehnisko uzdevumu un mediju incidentu sagatavošanā, kā arī vērtēšanas kritēriju izstrādē.

NATO CCD COE organizētās mācības "Crossed Swords 2024"

4. ceturksnī CERT.LV piedalījās mācību "Crossed Swords 24" testa izspēlē (12.-14. oktobris) un galvenajā izspēlē (11.-14. decembris), sniedzot atbalstu organizatoriem (White Team) informācijas operāciju spēles scenārija incidentu sagatavošanā un izspēlē, stratēģiskās komunikācijas dokumentu sagatavošanā un informācijas apritē, simulējot Apvienotā Štāba Stratēģiskās komunikācijas departamenta saziņu ar Kiberpavēlniecību.

Stratēģiskās komunikācijas izspēle mācībās "Crossed Swords" notika pirmo reizi. Kiberpavēlniecības pārstāvji to atzina par noderīgu situācijas apzināšanai, auditorijas analīzei un komunikācijas plānošanai. CCD COE plāno turpināt attīstīt šo virzienu arī turpmāk.

NATO organizētās mācības "Cyber Coalition"

No 2. līdz 6. decembrim CERT.LV komanda piedalījās mācību "Cyber Coaltion" izspēlē kā mācību auditorija, risinot incidentus, kas saistīti ar civilo kritisko infrastruktūru – veselības sektoru – nodrošinot incidentu analīzi, ziņošanu MISP platformā un saziņu ar starptautiskajiem kolēģiem. Tāpat incidentu risinātāji sniedza atbalstu militārās kritiskās infrastruktūras – militārās slimnīcas – kiberuzbrukumu analīzē.

Mācību mērķis ir gan sniegt iespēju risināt tehniskos incidentus, gan uzlabot sadarbību ar NATO sabiedrotajiem, vingrināt procedūras, ziņojumu rakstīšanu, lēmumu pieņemšanu dažādos līmeņos. Mācības uzlabo arī civilo un militāro sadarbību gan Latvijā, gan starptautiskā līmenī.

Sadarbība FIRST ietvaros

Turpinājās regulāra dalība Jauno biedru uzņemšanas komitejas (FIRST Membership Committee) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, biedru kategorijas, kā arī SIM3 modeļa pielietošanu komandu sertifikācijas procesā.

FIRST ir kiberdrošības organizācija, kas apvieno CERT, CSIRT, PSIRT, SOC komandas un citus kiberdrošības profesionāļus no visas pasaules.
FIRST biedri ir no 107 valstīm.

CERT.LV vadītāja Baiba Kaškina turpina pildīt FIRST Membership Committee priekšsēdētājas pienākumus, piedaloties gan jauno biedru pieteikumu izskatīšanā, gan veicinot biedru uzņemšanas procesa uzlabošanu.

Sadarbība TF-CSIRT ietvaros

CERT.LV ir viena no 42 Eiropas TF-CSIRT/TI sertificētām komandām. Turklāt CERT.LV ir augtākā līmeņa Trusted Introducer sertificēta kiberdrošības incidentu novēršanas komanda, apliecinot CERT.LV augsto brieduma un sagatavotības līmeni. Pārskata perioda beigās kopienā ir 526 komandas.

TF-CSIRT/Trusted Introducer (TI) ir Eiropas CERTu organizācija, kas apvieno incidentu reaģēšanas komandas no visiem sektoriem. TI serviss uztur uzticamu CERT vienību reģistru un veic to akreditāciju un sertifikāciju. CERT.LV ir sertificēta TI komanda kopš 2016. gada.

Sertifikācija notiek, izmantojot SIM3 standartu un TI/TF-CSIRT noteiktos parametru līmeņus. SIM3 tiek izmantots arī NIS2 direktīvas CERTu tīklā Self-Assessment un Peer Review, atbilstoši ENISA metodoloģijai.
Sertifikācija vērtē organizācijas briedumu, skatoties uz organizatoriskiem, cilvēkresursu, tehnisko rīku un procesu parametriem, primāri vērtējot incidentu risināšanas procesa briedumu. Veiksmīga sertifikācija apliecina komandas profesionalitāti un procesu sakārtotību. Sertifikāts tiek izsniegts uz 3 gadiem, pēc tam jāveic atkārtots audits.
Pārskata periodā CERT.LV turpināja darbu vairākās TF-CSIRT darba grupās.

Latvija un Kanāda rada unikālu mācību kursu kiberspēju attīstīšanai un stiprināšanai

Sadarbojoties CERT.LV, Latvijas Aizsardzības ministrijai un Kanādas Bruņoto spēku kibervienībai ir tapis unikāls mācību kurss, kas apvieno starptautisku pieredzi un zināšanas efektīvu draudu medību īstenošanā. Pārskata periodā Rīgā norisinājās divi secīgi kiberspēju attīstīšanai un stiprināšanai veltīti semināri:

- No 21. oktobra līdz 23. oktobrim notika pirmais starptautiskais CERT.LV un Kanādas bruņoto spēku kiberpavēlniecības organizētais Draudu medību seminārs: Threat Hunt Workshop.
- No 24. oktobra līdz 25. oktobrim notika ASV Eiropas Kiberpavēlniecības EUCOM organizēts seminārs par kiberdraudu izlūkošanu: Cyber Threat Intelligenge.

Uzsverot kiberdraudu medību mācību kursa nozīmīgumu, mācības atklāja Kanādas vēstnieks Latvijā Braiens Svorks (Brian Szwarc), Aizsardzības ministrijas Kiberdrošības politikas departamenta direktors Edgars Kiukucāns, CERT.LV vadītājas vietnieks Varis Teivāns un Valsts Policijas koledžas direktora vietniece Anita Fišere.

"Unikālais mācību kurss ir Latvijas un Kanādas kiberdrošības komandu daudzu stundu sadarbības rezultāts. Kopā mēs esam izveidojuši kaut ko unikālu, kas ne tikai stiprinās mūsu pašu spējas, bet arī kalpos par paraugu sadarbībai citiem."

CERT.LV vadītājas vietnieks Varis Teivāns

Mācību pilotprojekta kursā piedalījās 20 eksperti no dažādām NATO dalībvalstu par kiberdrošību atbildīgajām institūcijām, kursu pasniedza lektori no Latvijas un Kanādas.

CERT.LV dalās pieredzē un zināšanās

12. decembrī CERT.LV vizītē Latvijā uzņēma Moldovas Kiberdrošības aģentūras un citu iestāžu kolēģus. Vizītes mērķis bija pārrunāt sadarbības iespējas, kā arī dalīties informācijā par NIS2 direktīvas ieviešanu Latvijā, aktuālo situāciju un tendencēm kibertelpā un pastāstīt par CERT. LV pakalpojumiem.

Uzstāšanās citos nozīmīgos starptautiskos pasākumos

10. oktobrī Briselē, Beļģijā CERT.EU konferencē "Tales From the Real World" CERT.LV eksperts Kārlis Svilans uzstājās ar prezentāciju "Defending From the Beast in the East - CERT.LVs Approach to Multinational Threat Hunting".

No 15. līdz 16. oktobrim Tirānā, Albānijā, un no 24. līdz 25. oktobrim Belgradā, Serbijā, ES atbalstītā "Cyber Balkans" projekta ietvaros notika divu dienu semināri kiberdrošības profesionāļiem. Tajos CERT.LV kiberdrošības eksperts un Incidentu risināšanas nodaļas vadītājs Armīns Palms dalījās pieredzē ar CERT.LV praksi kiberdrošības incidentu risināšanā.

No 15. līdz 18. oktobrim Tokijā, Japānā "CEATEC 2024 – Toward Society 5.0" konferences ietvaros tematiskajā panelī "AI for All" ar virzienu par kiberdrošības savstarpējo mijiedarbību ar AI/ML runāja CERT.LV kiberdrošības profesionālis Dr. Bernhards Blumbergs. CEATEC ir pasaulē lielākā elektronikas un tehnoloģiju izstāde ar ļoti lielu starptautisko uzmanību un redzamību (https://www.ceatec.com/en/).

7. Pārskats par LIA Drošāka interneta centra ziņojumu līnijas darbību

Latvijas Interneta asociācijas (LIA) Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2024. līdz 31.12.2024. ir saņēmusi un izvērtējusi **288** ziņojumus. No tiem **89** ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, **6** gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, **30** ziņojumos konstatēta personas goda un cieņas aizskaršana, **13** ziņojumi saņemti par naida runu un **4** ziņojumos konstatēti vardarbīgi materiāli.

Par finanšu krāpšanas mēģinājumiem internetā saņemti **73** ziņojumi, **33** ziņojumu saturs nav bijis pretlikumīgs, **40** gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīts **68** ziņojums par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. **17** ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datubāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem **72** ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem **71** ziņojuma saturs ir dzēsts no publiskas aprites internetā, un **1** ziņojums atrodas dzēšanas procesā sadarbībā ar INHOPE un Valsts policiju.

Pārskats par saņemtajiem ziņojumiem no 01.10.2024. līdz 31.12.2024.

Ziņojumi	Okt-24	Nov-24	Dec-24	Q3
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	3	0	3	**6**
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	55	19	15	**89**
Vardarbīga rakstura materiāli	0	2	2	**4**
Cieņas/ goda aizskaršana	10	13	7	**30**
Naida kurināšana/ rasisms	3	4	6	**13**
Finanšu krāpniecība	26	22	25	**73**
Konsultācijas/ padomi	16	11	13	**40**
Citi	7	14	12	**33**
KOPĀ:	**120**	**85**	**83**	**288**

Ziņojumi nosūtīti Valsts policijai	45	18	5	**68**
Ziņojumi nosūtīti INHOPE asociācijai	4	3	10	**17**
KOPĀ NOSŪTĪTI IZSKATĪŠANAI	**49**	**21**	**15**	**85**

8. Nākamajā ceturksnī plānotie pasākumi

Svarīgākie virzieni un pasākumi 2025. gada 1. ceturksnī

NKDL un NIS2 ieviešana

Atbilstoši Nacionālās kiberdrošības likumam (NDKL) turpinās darbs pārskatīto ES Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasību ieviešanā. CERT.LV turpinās sniegt atbalstu pie NKDL saistīto noteikumu izstrādē. Būtiska CERT.LV iesaiste paredzama, izglītojot un atbalstot jaunos NKDL subjektus likuma un saistīto noteikumu prasību ieviešanā, kā arī kiberdrošības pārvaldības procesu izvērtēšanā un pilnveidošanā.

Stiprinot kiberdrošību Latvijā, CERT.LV aktīvi uzrauga kibertelpu, risina un koordinē incidentus, nodrošina plašu pakalpojumu klāstu, informē un izglīto sabiedrību, kā arī veicina stratēģisku sadarbību valsts un starptautiskā mērogā.

Pakalpojumu attīstība

CERT.LV turpinās pilnveidot savu pakalpojumu klāstu, vienlaikus stiprinot savu kapacitāti kā galvenā operacionālā kiberdrošības organizācija Latvijā. Ar popularizēšanas aktivitātēm un informatīvām komunikācijas kampaņām tiks veicināta CERT.LV nodrošināto bezmaksas pakalpojumu izmantošana valsts sektorā, primāri koncentrējoties uz valsts un pašvaldību iestādēm, IKT kritiskās infrastruktūras uzturētājiem, kā arī būtisko un svarīgo pakalpojumu sniedzējiem.

Liels uzsvars ir likts uz Drošības operāciju centra (SOC) pakalpojumu jaudas attīstīšanu, lai nodrošinātu efektīvākos aizsardzības risinājumus, sniedzot būtiskus ieguvumus SOC klientiem.

Draudu medību operācijas

CERT.LV un NATO sabiedrotie turpina veicināt informācijas apmaiņu par Krievijas un Ķīnas atbalstīto kiberoperāciju radītajiem kiberriskiem un gatavību reaģēt uz tiem.

Lai padarītu Latviju par neparocīgu mērķi kiberuzbrucējiem, CERT.LV stiprina savu līderību kiberdrošības draudu medību operācijās, izmantojot jaunākās metodes un rīkus.

Draudu medību operācijas turpināsies gan saviem spēkiem, gan sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību, stiprinot Latvijas IKT sistēmu noturību un sniedzot ieguldījumu NATO kolektīvajā aizsardzībā.

No 4. līdz 7. februārim Rīgā norisināsies starptautiskais CERT.LV un Kanādas Bruņoto spēku kiberpavēlniecības organizētais Draudu medību mācību kurss, kas apvieno starptautisku pieredzi un zināšanas efektīvu draudu medību īstenošanā. Pieteikšanās kursam ir izsludināta gan NATO partneriem, gan CSIRT kopienā.

Kiberdrošības mācības

2025. gada janvārī CERT.LV piedalīsies NATO Apvienotā kiberaizsardzības izcilības centra organizēto mācību “Locked Shields” galvenajā plānošanas konferencē, White Team (mācību organizācija) un Green Team (mācību infrastruktūra) komandās, kā arī veiks tālākos uzdevumus mācību informācijas vides un tehniskās vides sagatavošanai.

Pasākumi kiberdrošības jomā

- **Dalība Nacionālā kiberdrošības centra reģionālo kiberdrošības semināru organizēšanā:** Pašvaldību un to padotības iestāžu vadītāji, kiberdrošības pārvaldnieki, kā arī būtisko un svarīgo pakalpojumu sniedzēji tiek aicināti pieteikt savu dalību reģionālajos kiberdrošības semināros, kas **2025. gada sākumā norisināsies Liepājā – 10. janvārī, Rēzeknē – 23. janvārī, Jelgavā – 6. februārī un Valmierā - 20. februārī**.

  Semināros Aizsardzības ministrija kopā ar CERT.LV stāstīs par tādiem kiberdrošībā aktuāliem tematiem kā kiberhigiēna, aktuālā situācija Latvijas kibertelpā un CERT.LV piedāvātajiem pakalpojumiem. Tāpat semināra dalībnieki tiks informēti par izmaiņām un jaunajām kiberdrošības prasībām, kas radušās Latvijas kiberdrošības pārvaldības modelī, stājoties spēkā jaunajam NKDL.
  Vairāk informācijas: https://lnkd.in/dDRQYRBi

- **Turpinās dalība NCC-LV izveidotajā Latvijas kiberdrošības kopienas darbā.** CERT.LV eksperti sadarbībā ar Aizsardzības ministriju sniegs atbalstu "Latvijas Kiberdrošības izaicinājums" projekta īstenošanā.

- **Konference "Kiberšahs 2025"** – tiks uzsākta konferences plānošana un organizēšana.

- **"Esi drošs" semināra organizēšana: Martā notiks** IT drošības seminārs "Esi drošs", ko CERT.LV organizē organizāciju atbildīgajiem par kiberdrošību, kā arī citiem interesentiem.

Starptautiskā sadarbība

CERT.LV eksperti turpina pārstāvēt Latvijas intereses un stiprināt sadarbību ar starptautiskām kiberincidentu novēršanas organizācijām un partneriem, sniedzot konsultācijas un atbalstu, kā arī uzrunājot sabiedrību starptautiskās konferencēs un semināros.

- **No 14. janvāra līdz 16. janvārim CERT.LV pārstāvji piedalīsies FIRST un TF-CSIRT reģionālajā simpozijā Monako**, kura ietvaros CERT.LV eksperti Armīns Palmas un Dana Ludviga vadīs semināru "Building OpenShield - Personal DNS Threat Intelligence with DNS Firewall", sniedzot praktisku ieskatu un daloties ar Latvijas pieredzes stāstu par DNS ugunsmūra sistēmas izveidi. Dalība plānota arī citos simpozija semināros un darba grupās. Vairāk informācijas: https://www.first.org/events/symposium/monaco2025/

- **No 20. līdz 21. janvārim Briselē, Beļģijā** norisināsies NIS direktīvas CSIRTs Network kārtējā sanāksme, kurā piedalīsies CERT.LV vadītāja Baiba Kaškina un eksperte Agnese Kriķe. Pasākumā B. Kaškina uzstāsies ar prezentāciju par DNS ugunsmūra izveidi, attīstību, kā arī stāstīs par DNS ugunsmūra mobilās lietotnes izveidi un popularizēšanas kampaņu.

CERT.LV misija ir veicināt informācijas tehnoloģiju (IT) drošību Latvijā.

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, kā arī organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Tālrunis: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: www.cert.lv

Sekot CERT.LV aktualitātēm:

@cert.lv

CERT.LV
Kiberincidentu novēršanas institūcija