Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2023
C4

Publiskais pārskats par CERT.LV uzdevumu izpildi

2023. gada 4. ceturksnis (01.10.2023. – 31.12.2023.)

Kopsavilkums

Situācija Latvijas kibertelpā 2023. gada 4. ceturksnī bija intensīva, bet stabila. Apdraudēto unikālo IP adrešu apjoms līdzīgs iepriekšējam ceturksnim un šim pašam periodam pagājušajā gadā. Izteikti krasas svārstības apdraudēto IP adrešu apjomā nav novērotas, kas liecina par to, ka Latvijas kibertelpas aizsardzības pasākumi ir efektīvi un atbilstoši.

Statistika par unikālo IP adrešu apdraudējuma veidiem 4. ceturksnī rāda, ka **konfigurācijas nepilnības joprojām ir visbiežāk sastopamais drauds**, bet to daļa ir nedaudz samazinājusies salīdzinājumā ar iepriekšējo ceturksni un ar to pašu laika posmu pirms gada. Otrajā vietā ir ļaundabīgs kods, turklāt pārsteidzot ar palielinājumu par 62% salīdzinājumā ar 3. ceturksni. Trešajā vietā ir ielaušanās mēģinājumi, un arī to skaits palielinājies par 19% salīdzinājumā ar iepriekšējo ceturksni un par 65% vairāk salīdzinājumā ar to pašu laika posmu pirms gada.

2023. gada 4. ceturksnī CERT.LV tika reģistrētas 335 143 apdraudētas unikālas IP adreses. Tas ir par 0,32% mazāk nekā iepriekšējā ceturksnī un par 7% mazāk nekā pirms gada. Aktīvās aizsardzības DNS ugunsmūris, ko nodrošina CERT.LV un NIC.LV (augstākā līmeņa domēna .LV reģistra uzturētājs), sasniedzis jaunu rekordu – tā lietotāji (unikālie) tika pasargāti no kaitīgām saitēm, vīrusiem un ļaunprātīgi veidotu tīmekļa vietņu apmeklēšanas 467 888 reizes. Tas ir par 1 046% vairāk nekā 3. ceturksnī un par 521% vairāk nekā pirms gada attiecīgajā laika periodā. DNS ugunsmūris apstrādāja aptuveni 1,5 miljonus DNS pieprasījumu katru mēnesi.

Veicot datu analīzi, secināts, ka **aktuālie uzbrukumi joprojām saistās ar ļaunatūras izmantošanu**, lai iegūtu piekļuvi valsts un privātajā sektorā strādājošu darbinieku iekārtām un sistēmām, tostarp aktīvi izmantojot e-pastus ar attālinātās piekļuves failiem kā pielikumiem. Tīklu kompromitēšanas gadījumu skaits publiskajā un privātajā sektorā pieaudzis, izplatot šifrējošos izspiedējvīrusus, kas nošifrē upura iekārtas datus un pieprasa izpirkuma maksu to atgūšanai.

Ņemot vērā pašreizējo ģeopolitisko spriedzi un hibrīdkara draudus, var pieņemt, ka **ielaušanās mēģinājumu būtiskais pieaugums kibertelpā** ir skaidrojams ar politiski motivētiem Krievijas hakeru uzbrukumiem un mērķiem, it īpaši tiem, kas saistīti ar acīmredzamiem centieniem kompromitēt NATO un ES dalībvalstu kritiskās infrastruktūras drošību.

2023. gada nogalē, it īpaši pirmssvētku periodā, pret Latvijas iedzīvotājiem tika vērsts **liels skaits komerciāli motivētu krāpniecības kampaņu**. Ļaundari izmantoja īsziņas, krāpnieciskus telefona zvanus vai uzdevās par valsts iestāžu un citu organizāciju darbiniekiem, turklāt sūtījuši arī fotogrāfiju ar viltotu policijas darbinieka dienesta apliecību, lai tādējādi it kā apliecinātu identitāti un radītu uzticamību, un izgūtu iedzīvotāju personas vai internetbankas piekļuves datus. Kā ierasts, gada nogalē pastiprināta krāpnieku uzmanība tika pievērsta arī uzņēmumu un organizāciju grāmatvežiem, nosūtot paziņojumus par it kā laikus neapmaksātu rēķinu. Organizēto noziedzīgo grupu dalībnieki plaši izmanto mākslīgā intelekta (MI) risinājumus ziņojumu sagatavošanai un nosūtīšanai, kā arī īsteno krāpniecības ar viltotiem zvanītāju identifikatoriem (ID) – vairāki cilvēki neatpazina krāpnieku shēmas, un, piemēram, uzstādot savās iekārtās krāpniecisku programmatūru vai apstiprinot krāpnieku ierosinātās darbības, zaudēja savus finanšu līdzekļus.

Periodiski tika novēroti aktīvi Krievijas agresīvo režīmu atbalstošo haktīvistu grupējumu veikti pakalpojumu atteices (DDoS) uzbrukumi pret valsts un pašvaldību iestādēm un kapitālsabiedrībām, kā arī uzņēmumiem finanšu, transporta, enerģētikas, pasta un telekomunikāciju nozarēs. Tomēr mērķu infrastruktūras bija gatavas uzbrukumus atvairīt, un tie neradīja ietekmi uz attiecīgo pakalpojumu vai resursu pieejamību.

Krievija joprojām ir galvenais kiberapdraudējuma avots, kas izmanto politisko situāciju, uzbrukumam mērķi izvēloties atbilstoši politiskajām aktualitātēm, piemēram, aktivizējoties pilsonības un uzturēšanās atļauju jautājumiem. Bet, ja iepriekš politiski motivēti uzbrukumi bija vērsti uz sistēmu darbības traucēšanu, tad 4. ceturksnī tika novērota

taktikas maiņa uz kiberspiegošanu un Kremļa ietekmes operācijām.

CERT.LV turpina stiprināt savu lomu kā līdere draudu medību operāciju organizēšanā un vadīšanā Eiropas Savienībā – attīstot un stiprinot stratēģisko sadarbību ne tikai nacionālajā, bet arī starptautiskajā līmenī, sniedzot savu ieguldījumu NATO kolektīvajā Eiropas aizsardzībā, izstrādājot un pilnveidojot draudu medību metodiku, kā arī organizējot pieredzes apmaiņas pasākumus ar sabiedroto valstu partnerorganizācijām.

CERT.LV uzsver, ka kiberhigiēna ir būtiska valsts un uzņēmumu līmenī, lai pasargātu Latvijas un sabiedroto kibertelpu no dažādiem kiberuzbrukumiem. Lai sasniegtu šo mērķi, ir svarīgi stiprināt kritiskās infrastruktūras noturību pret kiberdraudiem un spēju pēc iespējas ātrāk atjaunot pakalpojumus pēc incidentiem, tostarp hibrīdkara apstākļos. CERT.LV iesaka sekot līdzi iespējām un draudiem, ko paver mākslīgā intelekta attīstība.

Pildot savu misiju, CERT.LV turpina veicināt kiberdrošību un būt par uzticamu viedokļa līderi Latvijas kibertelpā.

CERT.LV turpina aktīvi informēt Latvijas sabiedrību par kiberdrošības riskiem un kiberhigiēnas labajām praksēm. Pārskata periodā **CERT.LV eksperti piedalījās 55 izglītojošos pasākumos, izglītojot 16 144 dalībniekus par IT drošību, kas ir gandrīz 8 reizes vairāk nekā iepriekšējā ceturksnī**. Konference “Kiberšahs 2023” bija veiksmīga, pulcējot klātienē 670 dalībniekus no 26 valstīm un piesaistot ap 6 000 tiešraides skatījumus no 38 valstīm. Ar 376 publikācijām plašsaziņas līdzekļos, kas ir par 47% vairāk nekā iepriekšējā ceturksnī, iegūti 16,5 miljoni skatījumu.

Pārskatā iekļauta vispārpieejama informācija par CERT.LV aktivitātēm un darbības rezultātiem, neietverot ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Satura rādītājs

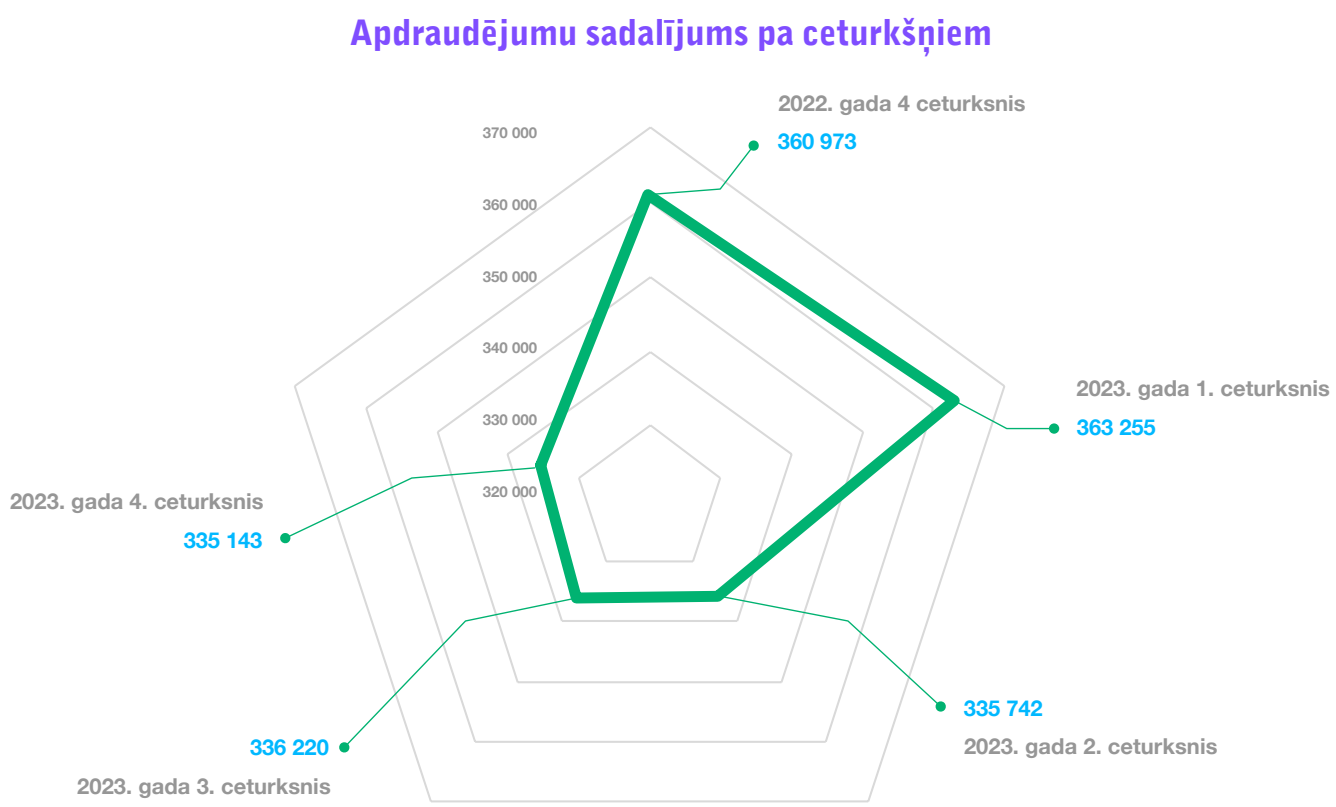
1. Kibertelpas drošības apdraudējumi: statistika un tendences

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju. Pārskata periodā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos apdraudējumu veidos (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī ļaunatūru un konfigurācijas nepilnību tipos.

Taksonomija – formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju.

2023. gada 4. ceturksnī CERT.LV tika reģistrētas 335 143 apdraudētas unikālas IP adreses, kas ir par 0,32% mazāk nekā 3. ceturksnī un par 7% mazāk nekā pagājušā gada attiecīgajā ceturksnī.

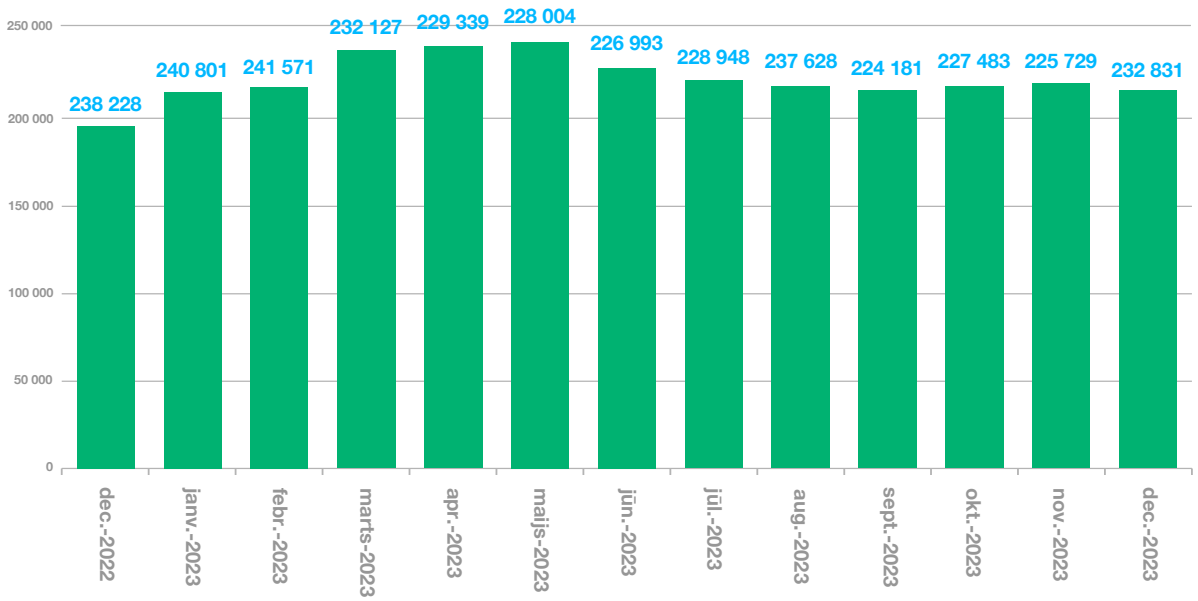
Kopumā 4. ceturksnis bija intensīvs, bet stabils. Kopējais apdraudējumu un incidentu skaits ir maz mainījies 2023. gada pēdējo trīs ceturkšņu laikā. Kā jau gaidīts, stāsts par apdraudējumu motīviem saglabājas tas pats – izaicinājumi mūsu kibertelpas drošībai ir gan ģeopolitiskās un digitālās pārmaiņas, gan karadarbība Ukrainā un Krieviju atbalstošu haktīvistu, tostarp valsts sponsorētu grupējumu darbības, gan arī tādi sezonālie faktori kā "melnās piektdienas" iepirkšanās drudzis un gada nogales pirmssvētku periods, kam raksturīgi viltus veikali un loterijas un kad pastiprināti jāuzmanās no dažādām pikšķerēšanas kampaņām un krāpnieciskām e-pasta vēstulēm, kurās tiek aicināts apmaksāt nepiegādātus sūtījumus vai segt atmuitošanas izdevumus.



1. attēls. Apdraudētās unikālās IP adreses pa ceturkšņiem

Pārskata periodā apdraudējumu līmenis bija stabils, un izteikti krasas svārstības apdraudēto IP adrešu apjomā nav novērotas. Tas signalizē par to, ka uzbrukumu biežums un ietekmes amplitūda salīdzinājumā ar iepriekšējā gada ceturksni ir mazinājušies.

Apdraudējumu sadalījums 12 mēnešu griezumā



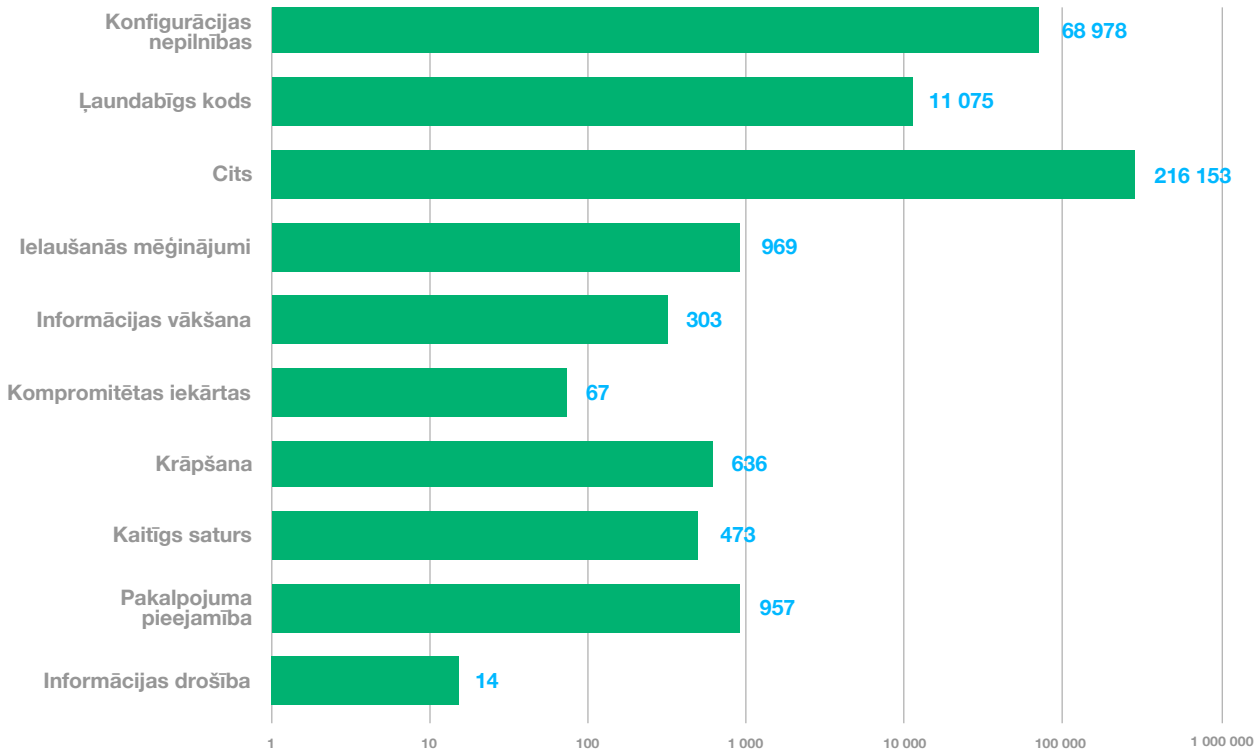
2. attēls. Apdraudētās unikālās IP adreses 12 mēnešu griezumā

2023. gada 4. ceturksnī izplatītākais apdraudējuma veids bija **konfigurācijas nepilnības** (68978 unikālas IP adreses) ar kritumu par 3% salīdzinājumā ar 3. ceturksni un par 25% mazāk nekā šajā pašā periodā pirms gada.

2. vietā ierindojas **Ļaundabīgs kods** (11075 unikālas IP adreses), pārsteidzot ar palielinājumu par 62% salīdzinājumā ar 3. ceturksni, toties par 2% mazāk nekā šajā pašā periodā pirms gada.

Savukārt 3. vietu saglabā **ielaušanās mēģinājumi** (969 unikālas IP adreses) ar palielinājumu par 19% salīdzinājumā ar 3. ceturksni un par 65% vairāk nekā šajā pašā periodā pirms gada.

Apdraudējumu sadalījums pēc apdraudējuma veida



3. attēls. Apdraudēto unikālo IP adrešu skaits 4. ceturksnī pēc apdraudējuma veida

Salīdzinot ar šo pašu periodu pirms gada, 2023. gada 4. ceturksnī reģistrēto apdraudēto unikālo IP adrešu skaitā bija vērojams būtisks pieaugums četros apdraudējuma veidos: ielaušanās mēģinājumi, krāpšana, kaitīgs saturs un informācijas drošība. Toties kritiens bija vērojams sešos apdraudējuma veidos: konfigurācijas nepilnības, ļaundabīgs kods, informācijas vākšana, kompromitētas iekārtas, pakalpojuma pieejamība, kā arī kategorijā – cits.

Pašreizējā ģeopolitiskajā situācijā un hibrīdkara apstākļos var pieņemt, ka ielaušanās mēģinājumu būtiskais pieaugums kibertelpā ir skaidrojams ar politiski motivētiem Krievijas hakeru uzbrukumiem un uzbrukumu mēģinājumiem, īpaši kas saistīti ar acīmredzamiem centieniem kompromitēt NATO un ES dalībvalstu kritisko infrastruktūru.

Tāpat 4. ceturksnī pret Latvijas iedzīvotājiem tika vērsts liels apjoms komerciāli motivētu krāpniecisku aktivitāšu, kurās uzbrucēji, izmantojot īsziņas, krāpnieciskus telefona zvanus un uzdodoties par valsts iestāžu, tostarp Valsts policijas, tiesas, VID, CERT.LV un citu organizāciju, kā piemēram, VAS "Latvijas Pasts", AS "Citadele banka", "Google" darbiniekiem, centās izgūt internetbankas piekļuves datus. Vairāki iedzīvotāji krāpniecības neatpazina, un, instalējot attālinātās piekļuves programmatūru savos datoros, zaudēja ievērojamus finanšu līdzekļus.

Kā varēja paredzēt, apdraudējumu skaits gada nogalē ir salīdzinoši vairāk audzis decembrī, kad tika fiksētas vairākas krāpnieciskas kampaņas. Pirmssvētku periodā tika novērots skaita pieaugums krāpnieciskiem interneta veikaliem, kas cenšas pievilināt lētticīgus pircējus ar neticami zemām cenām plaši pazīstamiem zīmolu produktiem, kā arī sociālajos tīklos tika izplatītas viltus reklāmas, kurās it kā sabiedrībā atpazīstami uzņēmumi piedāvā iedzīvotājiem par nelielu samaksu iegādāties atpakaļ atgrieztus pasta sūtījumus vai lidostā pamestus bagāžas koferus, tādējādi izkrāpjot iedzīvotāju maksājumu karšu datus. Kā ierasts, gada nogalē pastiprināta krāpnieku uzmanība tika pievērsta arī uzņēmumu un organizāciju grāmatvežiem, kuriem šis laiks ir īpaši noslogots. Krāpnieki sūtīja paziņojumus par it kā laikus neapmaksātu rēķinu vai arī vadītāja vārdā pieprasīja steidzamu maksājumu, cerot uz to, ka steigā netiks pamanītas saņemtās e-pasta vēstules viltojuma pazīmes.

Gada pēdējie mēneši bija nozīmīgām ievainojamībām piesātināti. Operatīva atjauninājumu uzstādīšana ievainojamību novēršanai bija nepieciešama gan dažādiem uzņēmumos izmantotiem aizsardzības rīkiem, gan e-pasta serveriem, gan

CERT.LV ekspertu komentārs

Pārskata periodā lielākajā daļā gadījumu kiberapdraudējuma avots ir bijusi Krievija, mērķi izvēloties atbilstoši politiskajām aktualitātēm, piemēram, aktivizējoties pilsonības un uzturēšanās atļauju jautājumiem. Tomēr, ja sākotnēji politiski motivēti uzbrukumi tika veikti, lai traucētu sistēmu darbību, tad 4. ceturksnī bija vērojama taktikas maiņa uz kiberspiegošanu un Kremļa ietekmes operācijām. Tā, piemēram, spridzināšanas draudu e-pasta vēstuļu kampaņa, izsūtīta Latvijas skolām, bērnudārziem, tiesām un pašvaldībām, visticamāk, bija Krievijas organizēta ietekmes operācija pret Latvijas sabiedrību.

Periodiski tika novēroti aktīvi Krievijas agresīvo režīmu atbalstošo haktīvistu grupējumu veikti pakalpojumu atteices (DDoS) uzbrukumi, kas bija vērsti galvenokārt pret valsts un pašvaldību iestādēm un kapitālsabiedrībām, kā arī finanšu, transporta, enerģētikas, pasta un telekomunikāciju nozares uzņēmumiem, taču mērķu infrastruktūras bija gatavas uzbrukumus atvairīt, un tie neradīja ietekmi uz attiecīgo pakalpojumu vai resursu pieejamību.

Labā ziņa ir tā, ka sekmīgi uzbrukumi ar būtisku ietekmi valsts un kritiskās infrastruktūras sektorā līdz šim nav konstatēti. CERT.LV komanda, sniedzot savu ieguldījumu NATO kolektīvajā Eiropas aizsardzībā, kā pārliecinoša līdere draudu medību operāciju vadīšanā Eiropas kibertelpā pārskata periodā sekmīgi identificējusi un no mērķa infrastruktūras neitralizējusi gan politiski (Krievijas, Baltkrievijas, Ķīnas), gan komerciāli motivētus uzbrucējus.

Sliktā ziņa ir tā, ka Krievija joprojām ir galvenais drauds Latvijai un NATO, turklāt ir viens no aktīvākajiem kiberagresoriem, kas izmanto dažādas metodes, lai ietekmētu citu valstu politiku, ekonomiku un sabiedrisko domu. Sagaidāms, ka pašreizējā ģeopolitiskā situācija arvien vairos kiberdrošības riskus visur pasaulē. Saglabājas bažas, ka kiberuzbrukumu intensitāte palielināsies, īpaši valstīs, kurās ieviestas sankcijas pret Krieviju. Turklāt Rietumvalstīm ir jātiek galā ar diviem nopietniem izaicinājumiem, jo bez Krievijas kara Ukrainā bažas rada arī Izraēlas karš ar teroristisko organizāciju "Hamās", kas varētu pāraugt plašākā reģionālā konfliktā.

arī mobilajiem telefoniem. Uzbrucēji nekavējās ar centieniem izmantot šīs ievainojamības, lai inficētu neatjauninātās iekārtas un pārņemtu tās savā kontrolē.

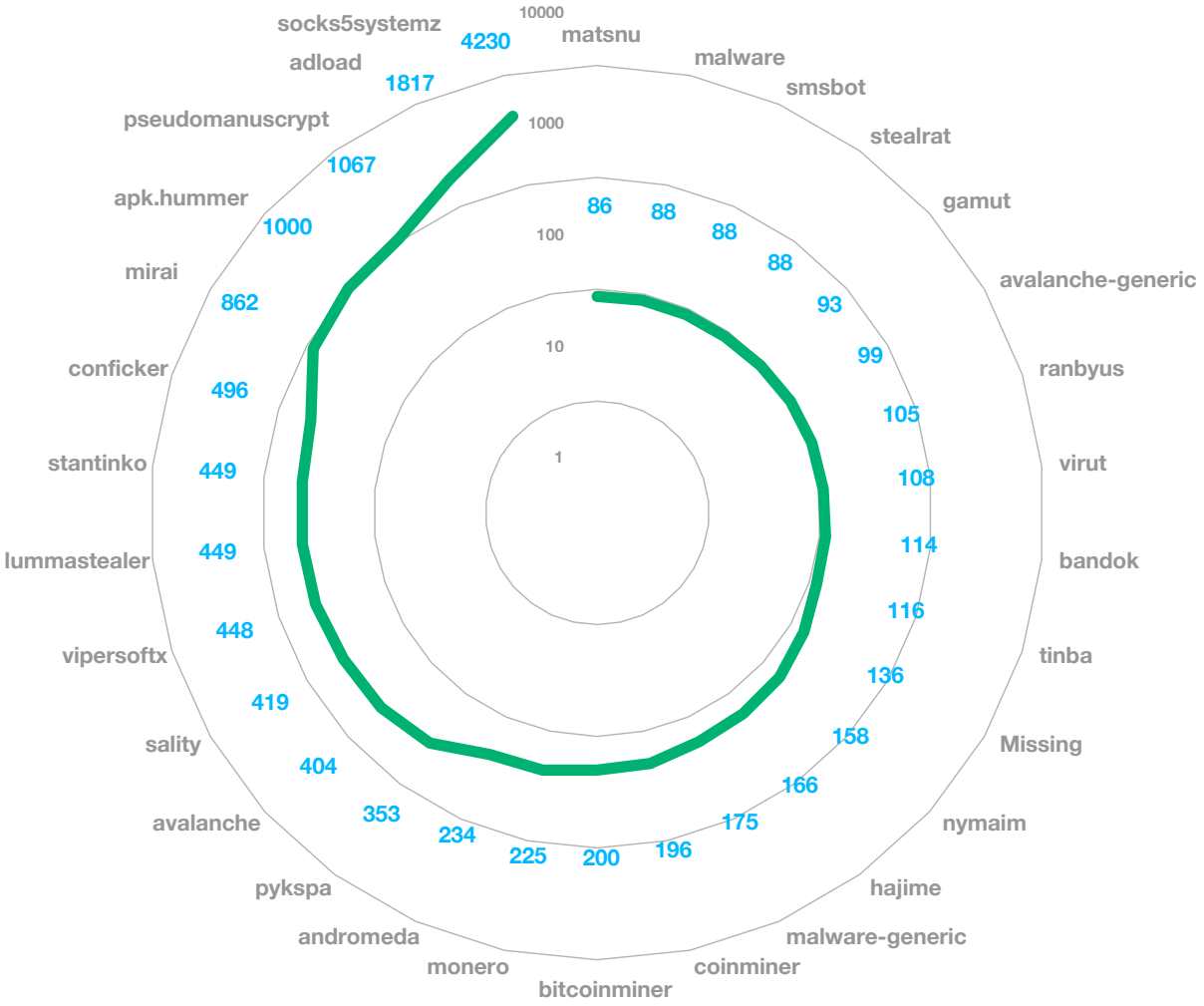
Lai pasargātu Latvijas kibertelpu un sabiedrotos no kiberuzbrukumiem, pārskata periodā CERT.LV akcentēja efektīvas kiberhigiēnas nozīmi valsts un uzņēmumu līmenī, kritiskās infrastruktūras kiberdrošības noturību un spēju atjaunot pakalpojumu sniegšanu pēc incidentiem, tostarp hibrīdkara apstākļos, kā arī iespējas un draudus, ko paver mākslīgā intelekta attīstība.

Ļaundabīgu kodu jeb ļaunatūru TOP30

2023. gada 4. ceturksnī ļaunatūru topā **1. vietu** ieņem jaunpienācēja – ļaunatūra ***Socks5systemz***, kas inficē iekārtas un pārvērš tās par pāradresācijas ***proxy*** jeb starpniekserveriem, savukārt ļaundari tos varētu izmantot, lai padarītu grūtāku viņu nelegālo un kaitīgo darbu izsekošanu. Tādējādi ar ***Socks5systemz*** inficēta ierīce tiek neautorizēti pārņemta no trešo personu puses un ar lielu varbūtību tiek iesaistīta nelegālo darbību atbalstīšanā.

2. vietā ir ierindojusies ļaunatūra ***Adload***, kas zog upuru pārlūkmeklētāju datus un ievieto viltus/krāpnieciskas reklāmas upura interneta pārlūkā. Ja MAC ierīcei ir konstatēta ***Adload*** ļaunatūra, nepieciešams veikt pilnu datora pārbaudi ar atjauninātu antivīrusu programmu.

3. vietā – ļaunatūra *Pseudomanuscrypt*, kas ir spiegošanas *trojāns*, kurš spēj neautorizēti piekļūt un eksfiltrēt datus no inficētās ierīces, tai skaitā datus par nospiestiem klaviatūras taustiņiem, datus no *clickbord*, lietotņu autentifikācijas datus, kā arī spēj veikt inficētās sistēmas ekrānšāviņus, skaņas ierakstīšanu ar mikrofonu un citas darbības.



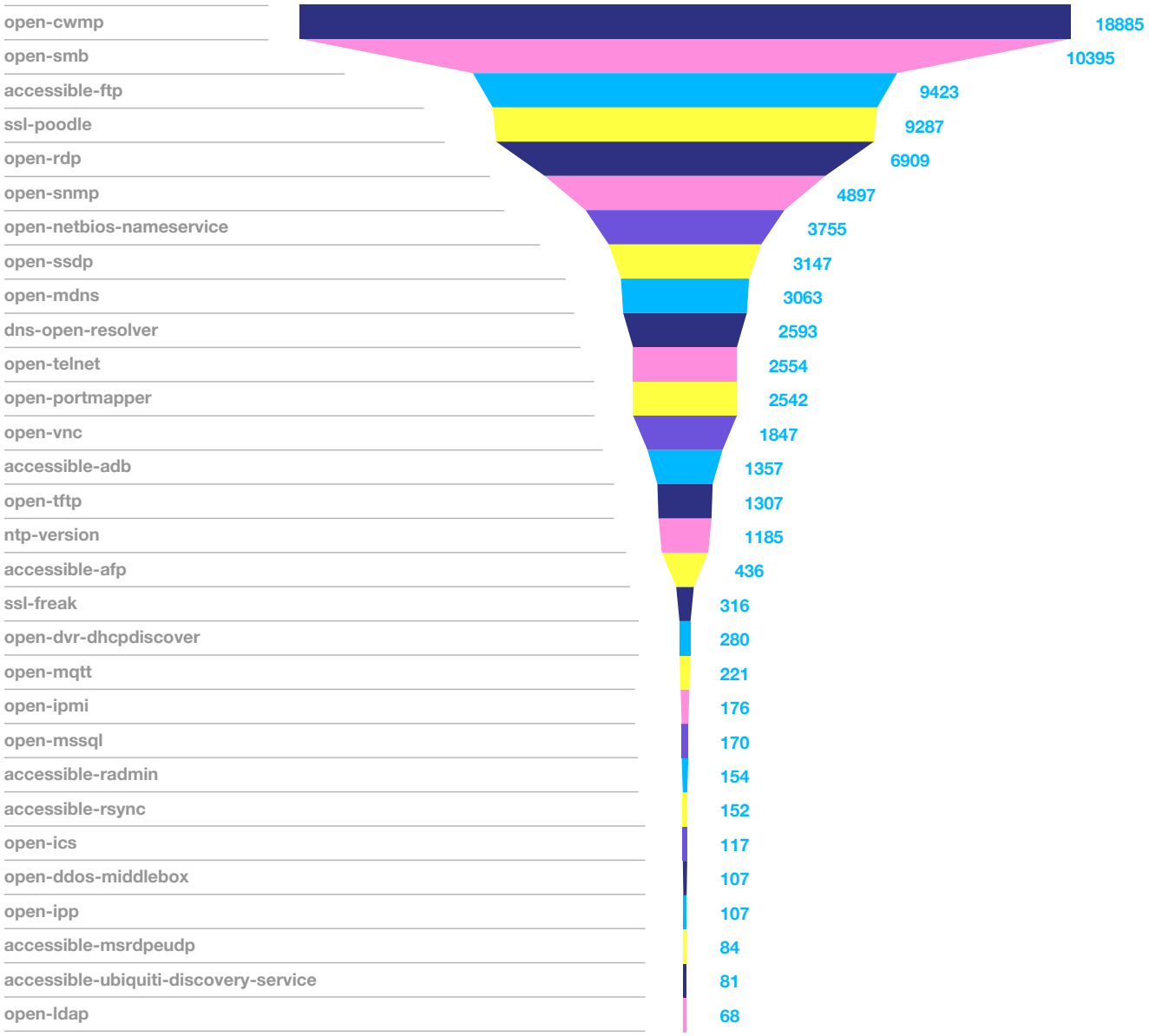
4. attēls. Apdraudēto unikālo IP adrešu skaits 4. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods

Konfigurācijas nepilnību TOP 30

2023. gada 4. ceturksnī konfigurācijas nepilnību topa **1. vietu** notur *Open-cwmp* – pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla. Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, piemēram, izmantojot VPN.

2. vietā nemainīgi ir *Open-smb*. Ievainojamība norāda, ka konkrētajām iekārtām uz publisko internetu ir atvērts ports, kuru izmanto SMB protokols, kas paredzēts, lai piekļūtu datnēm un iekārtām iekšējā tīklā. Kompromitējot SMB protokolu, uzbrucēji iegūtu iespēju piekļūt iekšējā tīkla iekārtām un inficēt tās, piemēram, ar izspiedējvīrusu.

3. vietā ierindojas *Accessible-ftp*. FTP datu pārraides protokols nenodrošina pārraidāmo datu šifrēšanu, ja vien netiek izmatota papildu aizsardzība TLS vai SSL protokola formā (attiecīgi FTPS). Šī konfigurācijas nepilnība pakļauj noplūdes riskam sensitīvu informāciju un piekļuves datus.



5. attēls. Apdraudēto unikālo IP adrešu skaits 4. ceturksnī – konfigurācijas nepilnība

Pārskata periodā apdraudēto unikālo IP adrešu sadalījums matricā

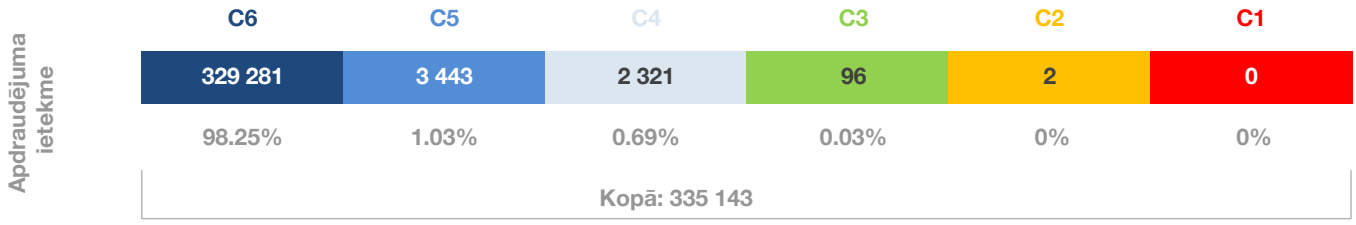
Pilnvērtīgākam kiberdrošības situācijas ikmēneša novērtējumam CERT.LV lieto Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidoto apdraudējumu matricu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde/uzņēmums, cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs.

Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

C1	Nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte.
C2	Augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra.
C3	Nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C4	Būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C5	Mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C6	Ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

6. attēls. Apdraudējumu matricas sadalījums kategorijās

Pārskata periodā nacionāla līmeņa apdraudējumi (C1) nav reģistrēti. Lielākais īpatsvars jeb 98% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā (C6) un ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm.



7. attēls. Apdraudēto unikālo IP adrešu sadalījums kategorijās pēc apdraudējuma ietekmes 4. ceturksnī

Augstas nozīmes apdraudējumu (C2) kategorijā reģistrētas divas IP adreses, kas saistītas ar vienu incidentu 2023. gada 31. oktobrī. Incidents saistīts ar ***Barracuda*** ievainojamību (CVE-2023-2868), kas noveda pie kompromitētas iekārtas kādā valsts iestādē. Pārbaužu rezultātā tika noskaidrots, ka kompromitētā iekārta atradās izolētā vidē un liela apjoma datu izgūšana no uzbrucēja puses netika veikta un netika ietekmētas citas iekšējās iekārtas.

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,03% jeb 96 apdraudētas unikālas IP adreses/gadījumus no visiem kategorizētajiem apdraudējumiem, kas ir par 62 apdraudētām unikālām IP adresēm vairāk nekā iepriekšējā ceturksnī. Visvairāk jeb gandrīz 80% šo apdraudējumu veido ļaundabīgs kods vairākās pašvaldību, veselības aprūpes un izglītības iestāžu un elektronisko sakaru komersantu iekšējās iekārtās un sistēmās.

Apdraudējuma ietekme						
5	0	0	0	0	0	0
4	28	5	0	0	14	2
3	10 313	243	56	67	54	28
2	127 744	7 524	929	506	1 013	735
1	176 033	6 551	1 088	372	738	1 100
	1	2	3	4	5	6

Skarto iedzīvotāju, institūciju vai uzņēmumu skaits un / vai nozīmība

8. attēls. Apdraudēto unikālo IP adrešu izvietojums matricā 4. ceturksnī

Būtiski apdraudējumi ar vidēju ietekmi (C4) veido 0,69% (2321 apdraudētas unikālas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Lielākā daļa C4 līmeņa apdraudējumu bija konfigurācijas nepilnības (***Accessible-ftp, Ntp-version, Dns-open-resolver*** u.c.), tāpat tika novēroti arī ielaušanās mēģinājumi, krāpšanas incidenti, ļaundabīgs kods augstas un vidēji augstas prioritātes iestādēs (vairākās pašvaldībās un valsts iestādēs, augstskolās un citās organizācijās).

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

Lai veicinātu IT drošību Latvijā un stiprinātu noturību pret kibernoziegumiem, 2023. gada 4. ceturksnī tika turpināta CERT.LV aktīva sadarbība ar valsts un pašvaldību institūcijām, bankām, elektronisko sakaru komersantiem un citām organizācijām un kiberdrošības ekosistēmas partneriem dažādas bīstamības incidentu risināšanā.

Kiberuzbrukumi pret valsts iestādēm, organizācijām un kritiskās infrastruktūras pakalpojumu sniedzējiem ir nopietni draudi, kas varētu negatīvi ietekmēt iedzīvotāju, iestāžu un uzņēmumu drošību, kā arī radīt apdraudējumus pamatpakalpojumu un digitālo pakalpojumu sniedzējiem, tādējādi ietekmējot valsts drošību, finanšu stabilitāti un pat vājinot tautsaimniecības izaugsmi.

Ziņošana par incidentiem, sadarbība un informācijas apmaiņa joprojām ir būtiski efektīvas kiberdrošības priekšnoteikumi. CERT.LV turpina regulāri informēt valdības pārstāvjus, valsts institūciju vadītājus un kiberdrošības speciālistus par notikumiem Latvijas kibertelpā. Tāpat CERT.LV turpina nodrošināt ikmēneša notikumu apkopošanu un analīzi, sniedzot lēmumu pieņēmējiem informāciju, kas nepieciešama, lai savlaicīgi prognozētu un novērstu valsts iekšējo un ārējo apdraudējumu, kā arī uzlabotu valsts kritiskās infrastruktūras aizsardzību un noturību.

CERT.LV ir valstī lielākais kiberapdraudējumu datu un informācijas apkopotājs, kas automatizēti apstrādā un analizē vairākus miljonus ienākošo signālu mēnesī.
Būtiskākie kiberincidenti un apdraudējumi, kas izgaismo 4. ceturksnī novērotās tendences, aplūkoti turpinājumā – 2.1. līdz 2.6. apakšnodaļās.

CERT.LV komandas atbalsts incidentu izmeklēšanā		
15-20 manuāli risināti incidenti katru dienu	Vairāk nekā 6,5 miljoni kiberdrošības telemetrijas signālu mēnesī	Atbalsts ikvienam, bet prioritāri: pamatpakalpojumu un digitālo pakalpojumu sniedzējiem, kritiskās infrastruktūras turētājiem un valsts iestādēm

2.1. Krāpšana

Krāpniecības kampaņu skaits joprojām liels un turpina pieaugt

2023. gada 4. ceturksnī novērots nemainīgi liels krāpnieciska rakstura īsziņu, e-pasta vēstuļu un zvanu skaits, krāpniekiem uzdodoties par dažādu valsts iestāžu, organizāciju un uzņēmumu pārstāvjiem. CERT.LV saņemtie iedzīvotāju iesniegumi liecina, ka pieaug metožu skaits un dažādība – tehnikas kļūst arvien noslīpētākas, un latviešu valoda arī vairs nav šķērslis krāpniekiem. Galvenais krāpnieku mērķis – piekļūt sociālo tīklu kontiem (“Facebook”, “Google”, “Instagram”) vai izgūt personas datus un piekļuvi internetbankai, pieprasot upuri apstiprināt krāpniecisku darījumu autorizējoties.

4. ceturksnī bija izplatīti smikšķerēšanas gadījumi, kad iedzīvotājiem tika nosūtīta viltus īsziņa it kā no tiesas vai policijas ar pievienotu krāpniecisku saiti. Nolūkā iegūt iedzīvotāju uzticību, viltvārži saziņas lietotnēs sūtījuši arī fotogrāfiju ar viltotu policijas darbinieka dienesta apliecību, lai tādējādi it kā apliecinātu identitāti.

Oktobrī daudz iesniegumu tika saņemts no iedzīvotājiem, kuri meklē darbu un ar kuriem ir sazinājušies krāpnieki, uzdodoties par kāda uzņēmuma personāla daļas darbiniekiem. Pēc garākas saziņas tika noskaidrots, ka šo krāpnieku mērķis ir bijis izvilināt upura bankas kontu datus, un vairākos gadījumos tas ir arī sekmīgi izdevies.

Kā varēja paredzēt, krāpšanas gadījumu, tostarp krāpniecisku interneta veikalu, skaits gada nogalē ir audzis, jo īpaši novembrī, un vēl vairāk – decembrī. Tāpat decembra sākumā tika fiksētas vairākas krāpnieciskas kampaņas, kurās uzbrucēji uzdevās par pasta pakalpojumu sniedzējiem, policijas, Valsts ieņēmumu dienesta, "Google" un citu uzņēmumu pārstāvjiem, lai pārliecinātu iedzīvotājus atklāt savus internetbankas piekļuves datus. Pastiprināta krāpnieku uzmanība tika pievērsta arī uzņēmumu un organizāciju grāmatvežiem.

Kā papildu pārbaudījums iedzīvotāju modrībai bija kiberuzbrucēju inovatīvā pieeja krāpnieciskajiem telefona zvaniem, īstenojot tos ar viltotiem zvanītāju identifikatoriem (ID) – izliekoties par banku un izvilinot iedzīvotāju internetbankas piekļuves datus. Autorizējot krāpnieka darbību internetbankā, krāpniekam ir iespēja izraisīt ievērojamus naudas zaudējumus upurim, pat ja viņam tādi līdzekļi nav kontā. Krāpnieks var pieprasīt vairākus kredītus un attiecīgi izkrāpt naudu, kas upurim faktiski nemaz nav.

Pārskata periodā izplatītākās TOP 5 krāpšanas shēmas

Viltvārži, kas imitē tiesībsargājošās iestādes: krāpnieki, uzdodoties par Valsts policijas darbiniekiem, informē par it kā pretlikumīgām darbībām bankas kontā vai vēlmi nelegāli noformēt kredītu uz zvana saņēmēja vārda. Lai viestu uzticību, krāpnieki bieži darbojas komandā un telefonsarunas laikā iesaista sarunā savu "kolēģi", tādējādi palielinot uzticību un nostiprinot domu, ka situācija tiešām ir īsta.

Uzdošanās par bankas darbiniekiem: viena no populārākajām krāpnieku darba metodēm. Krāpnieki informē savu upuri, ka ar kontu notiek krāpnieciskas darbības un steidzami nepieciešams novērst situāciju, aicinot personu atklāt pieejas datus. Piemēram, viena no tendencēm: krāpnieki, uzdodoties par kādas bankas darba devēju, aicināja atvērt bankas kontu un tad dalīties ar datiem. Tas tika darīts, izmantojot gan telefonsarunas, gan īsziņas, gan veidojot viltus vietnes un interneta reklāmas, kas vizuāli līdzīgas bankas izmantotajiem komunikācijas materiāliem. CERT.LV ir zināms gadījums, kad krāpnieks faktiski veidoja bankas kontu upurim tai pašā laikā, kad upuris, ejot cauri konta izveides procesam un domājot, ka apstiprina pats savas darbības, faktiski apstiprināja krāpnieka darbības un izveidoja bankas kontu savā vārdā, bet pats tam nevarēja piekļūt, jo piekļuve bija **nodota** krāpniekam.

Viltus finanšu uzraugi: pārskata periodā ir fiksēti gadījumi, kad krāpnieki uzdodas par Datu valsts inspekcijas, VID vai finanšu regulatora pārstāvjiem. Lai izvilinātu personas datus un piekļuvi bankas kontam, krāpnieki ziņo par it kā atvērtu kriptovalūtu kontu, kurā ziņas saņēmēja vārdā it kā notiekot nelegāli darījumi.

Viltvārži, kas uzdodas par "Google", "Netflix", "booking.com": krāpnieki bieži uzdevās par vietējo un starptautisko uzņēmumu darbiniekiem, piemēram, izmantojot "Google" zīmolu, lai ziņotu par aizdomīgām darbībām jeb pieslēgumiem "Google" kontam. Krāpnieki mēģināja pārliecināt upurus lejupielādēt attālinātās pārvaldības programmatūru, piemēram, AnyDesk vai TeamViewer, lai iegūtu piekļuvi viņu naudai.

Krāpnieki, kas uzdodas par VAS "Latvijas Pasts", "DPD" un "Omniva": VAS "Latvijas Pasts" atdarināšana oktobrī fiksēta sociālajā vietnē "Facebook", kur krāpnieki izveidoja lapu ar nosaukumu "Latvijas Pasts Express", piedāvājot iegādāties it kā neizsniegtus sūtījumus. VAS "Latvijas Pasts" vārds tika izmantots arī krāpnieciskās īsziņās un e-pasta vēstulēs, cenšoties maldināt iedzīvotājus par papildu informācijas sniegšanu piegādes vajadzībām

CERT.LV ekspertu komentārs

Krāpnieki būtiski uzlabojuši psiholoģiskā uzbrukuma jeb sociālās inženierijas metodes. Visbūtiskākās izmaiņas novērojamas ziņojumu nosūtīšanas metodēs, kas kļūst aizvien efektīvākas, izmantojot mākslīgo intelektu (MI) ziņojumu sagatavošanai un nosūtīšanai. MI attīstība rada gan iespējas, gan draudus, līdz ar to var prognozēt, ka arī turpmāk kiberkrāpniecību skaits un intensitāte pieaugs. Kiberkrāpšanā organizēto noziedzīgo grupu dalībnieki visbiežāk strādā lielās grupās, plaši izmanto inovācijas un jaunus risinājumus informācijas tehnoloģiju jomā, lai kaitētu cilvēkiem. Sliktā ziņa ir tā, ka ar MI palīdzību tiek radītas viltotas tīmekļa vietnes, attēli un audio faili, kas maldina cilvēkus, tādējādi tiek izvilināti upura internetbankas dati, sociālo tīklu profilu pieejas dati vai cita informācija. Diezgan daudz cilvēku iekrīt uz šīm krāpšanas kampaņām, jo tās ir ticamas, kā arī tīmekļa vietnes, kas izveidotas, lai izvilinātu piekļuves datus, ir ļoti labi izstrādātas un atdarina oriģinālās vietnes, turklāt tiek izmantota latviešu valoda. Neskatoties uz to, labā ziņa ir tā, ka pārdomātas investīcijas MI var rezultēties arī labākas aizsardzības spējās un labākos instrumentos, lai cīnītos pret apdraudējumu.

vai muitas nodokļa apmaksu. Iecienīta krāpnieku shēma bija uzdoties arī par privātā sektora kurjerpakalpojumu sniedzējiem – "DPD" un "Omniva". Izveidojot viltus mājaslapas, kas vizuāli ļoti līdzīgas šo uzņēmumu interneta vietnēm, no iedzīvotājiem tika izvilināti bankas karšu dati un izkrāpta nauda.

REKOMENDĀCIJAS UN IETEIKUMI DROŠĪBAI

Lai pasargātu sevi no pikšķerēšanas uzbrukumiem, CERT.LV aicina iedzīvotājus būt vērīgiem un, saņemot īsziņas vai e-pasta vēstules, neievadīt bankas vai personīgos datus saitēs, ko ir atsūtījis kāds svešinieks, pirms neesat pārbaudījis to patiesumu. Kā arī pievērst īpašu uzmanību:

- **sūtītāja kontaktinformācijai (piemēram, e-pasta adresei From: laukā);**
- **tekstā ievietotajām saitēm - vai tās ved uz atbilstošo vietni;**
- **e-pasta vēstulei pievienotajiem failiem un to paplašinājumiem – kādi burti redzami faila nosaukuma labajā pusē aiz pēdējā punkta. Ja pēdējie burti ir .iso, .exe, .img, .rar vai .zip, pielikumu vaļā labāk nevērt.**

2.2. Pakalpojuma pieejamība (DDoS)

Pārskata periodā periodiski tika novēroti aktīvi Krievijas agresīvo režīmu atbalstošo haktīvistu grupējumu veikti pakalpojumu atteices (DDoS) uzbrukumi, kas bija vērsti galvenokārt pret valsts un pašvaldību iestādēm un valsts kapitālsabiedrībām, kā arī finanšu, transporta, enerģētikas, pasta un telekomunikāciju nozaru uzņēmumiem, taču mērķu infrastruktūras bija gatavas uzbrukumus atvairīt, un tie neradīja ietekmi uz attiecīgo pakalpojumu vai resursu pieejamību.

Lai gan kopumā situācija vērtējama kā stabila, viens no agresīvākajiem kiberuzbrukumiem notika 14. novembrī un vēlreiz 22. novembrī, kad haktīvistu grupējums "Killnet" izplatīja informāciju platformā "Telegram", aicinot veikt pakalpojumatteices uzbrukumus dažādiem mērķiem Baltijas reģionā – tajā skaitā aizsardzības sektoru un valsts drošības iestādēm. CERT.LV apkopotā informācija liecina, ka notikušo uzbrukumu ietekme Latvijā vērtējama kā nebūtiska, proti, ietekmes nav bijis vai arī tā bijusi īslaicīga.

CERT.LV sniedza rekomendācijas aktīvās aizsardzības risinājumu un procedūru uzlabošanai.

REKOMENDĀCIJAS UN IETEIKUMI DROŠĪBAI

CERT.LV ir apkopojusi sagatavošanās darbus, kas jāizpilda, gaidot DDoS uzbrukumu, lai mazinātu vai novērstu šāda uzbrukuma ietekmi. Katrai iestādei, uzņēmumam un organizācijai jāizvērtē uzskaitīto punktu prioritāte un jāveic ieviešana, ņemot vērā savas infrastruktūras specifiku.

Vairāk informācijas: https://cert.lv/lv/2022/08/ieteikumi-ddos-ietekmes-mazinasanai

2.3. Ievainojamības un konfigurācijas nepilnības

CERT.LV turpina informēt publiskā un privātā sektora organizācijas par jaunatklātām kritiskām ievainojamībām un veicamajām darbībām iestādes iekārtu un tīklu pasargāšanai.

Veicot apdraudēto iekārtu apzināšanu Latvijas kibertelpā, tika konstatēts, ka valsts sektorā un pašvaldībās novērots manāmi zemāks kompromitēto iekārtu skaits, salīdzinot ar iepriekšējo gadu, iespējams, pateicoties diezgan ātrai un aktīvai komunikācijai no CERT.LV puses par potenciālajiem apdraudējumiem.

Vienlaikus 4. ceturksnī bija daudz jaunatklātu kritisku ievainojamību. CERT.LV apziņoja ievainojamo sistēmu turētājus, kā arī sniedza atbalstu incidentu analīzē un novēršanā. CERT.LV brīdināja par ievainojamībām un atjauninājumiem, sniedzot koordinētus norādījumus un rekomendācijas.

CERT.LV ekspertu komentārs

Kritiskās ievainojamības sniedz uzbrucējiem iespēju veikt attālinātu koda izpildi (RCE), iegūstot piekļuvi ievainojamajai sistēmai.

Pie kritiskām ievainojamībām pieskaitāmas arī tādas, kas ļauj neautentificētam vai neautorizētam lietotājam piekļūt sistēmai. Tāds lietotājs var nesankcionēti nolasīt sistēmā glabāto informāciju un pēc tam, iespējams, meklēt arī iespējas RCE izpildei. CERT.LV aicina sekot līdzi izstrādātāju ieteikumiem un nekavējoties atjaunot programmatūru uz jaunāko pieejamo versiju.

Ievainojamību TOP 6 pārskata periodā

***Exim* ievainojamības:** 2. oktobrī CERT.LV brīdināja *Exim* e-pasta serveru uzturētājus par vairākām ievainojamībām, tostarp CVE-2023-42115, kas saistīta ar attālināto pievienošanos (*external authorization*) un sniedz iespēju uzbrucējiem veikt attālināto koda izpildi (RCE). Visiem *Exim* lietotājiem tika ieteikts sekot līdzi izstrādātāju ieteikumiem un atjaunot programmatūru uz jaunāko pieejamo versiju.

Plašāk: https://cert.lv/lv/2023/10/exim-ievainojamibas

Kritiska *WinRAR* ievainojamība: 20. oktobrī CERT.LV brīdināja par *WinRAR* programmatūras kritisku ievainojamību CVE-2023-38831, ko aktīvi izmanto APT (*advanced persistent threat*) grupējumi ar nolūku kompromitēt ierīces un tīklus. Skartas visas programmatūras versijas līdz 6.23. *WinRAR* ievainojamība sniedz uzbrucējiem iespēju veikt patvaļīgu koda izpildi, ja lietotājs mēģina apskatīt nekaitīgu datni ZIP arhīvā, turklāt ir jāizpildās vairākiem citiem nosacījumiem. CERT.LV aicināja operatīvi veikt programmatūras atjaunināšanu uz 6.24. versiju visas infrastruktūras mērogā.

Plašāk: https://cert.lv/lv/2023/10/kritiska-winrar-ievainojamiba-cve-2023-38831

Kritiska ievainojamība vairākos *QNAP* produktos: 6. novembrī CERT.LV izplatīja brīdinājumu par kritisku ievainojamību vairākos *QNAP* produktos. Ievainojamība CVE-2023-23368, kas paver uzbrucējiem iespēju veikt attālinātu koda izpildi un ir ietekmējusi vairākus *QNAP* (*QTS, QuTS hero* un *QuTScloud*) produktus, ir ļoti nopietna un CVSS skalā (1-10) novērtēta ar 9.8. Dažu pēdējo gadu laikā ir novērotas kritiskās ievainojamības vairākiem *QNAP* produktiem, un tās tika ļaunprātīgi izmantotas izspiedējvīrusu uzbrukumos iestāžu un uzņēmumu resursiem Latvijā. CERT.LV aicināja nekavēties ar *QNAP* produktu atjauninājumu uzstādīšanu.

Plašāk: https://cert.lv/lv/2023/11/kritiska-ievainojamiba-vairakos-qnap-produktos

Kritiska *OwnCloud* ievainojamība (CVE-2023-49103): 30. novembrī CERT.LV izplatīja brīdinājumu par *OwnCloud* ievainojamību – tā risinājuma komponentei *graphapi* no 0.2.0 līdz 0.3.0 versijai tika konstatēta kritiska ievainojamība CVE-2023-49103, kurai piešķirts CVSS vērtējums 10.0 skalā no 1 līdz 10. Ievainojamība ļauj neautentificētam lietotājam piekļūt *phpinfo* konfigurācijas informācijai un nolasīt sistēmas mainīgo (*environment variables*) vērtības,

piemēram, administratora paroli, licenču atslēgas, e-pasta servera piekļuves datus un citu sensitīvu informāciju. CERT.LV informēja par nepieciešamajām darbībām, kā arī aicināja pievērst uzmanību citām būtiskām *OwnCloud* ievainojamībām.

Plašāk: https://cert.lv/lv/2023/11/kritiska-owncloud-ievainojamiba-cve-2023-49103

Kritiskas ievainojamības *Zyxel NAS* ierīcēs: 1. decembrī CERT.LV brīdināja par vairākām ievainojamībām *Zyxel NAS* (*network-attached storage)* ierīcēs, tostarp trim kritiskām ievainojamībām, kuras ļauj neautentificētam uzbrucējam izpildīt sistēmas komandas operētājsistēmas līmenī. Šīs ievainojamības skar NAS326 un NAS542 ierīces, un ievainojamību izmantošana var radīt neautorizētu piekļuvi, sensitīvu sistēmas informācijas noplūdi vai ļaut uzbrucējam pilnībā pārņemt ietekmētās *Zyxel NAS* ierīces. CERT.LV informēja par nepieciešamajiem atjauninājumiem un aicināja nekavēties ar to uzstādīšanu.

Plašāk: https://cert.lv/lv/2023/12/kritiskas-ievainojamibas-zyxel-nas-ierices

Kritiska *SSH* protokola ievainojamība: decembra izskaņā CERT.LV konstatēja vairāk nekā 10 000 unikālas iekārtas, kuras ir eksponētas publiskajā tīklā un pakļautas kritiskai ievainojamībai CVE-2023-48795. Tā ir *SSH* protokola ievainojamība, kura skar *OpenSSH* paplašinājumu funkcijas. Šīs ievainojamības izmantošana ļauj uzbrucējam pazemināt drošības līmeni lietotāja iekārtā vai arī to pilnībā atslēgt. Šo ievainojamību var izmantot *Terrapin* uzbrukumā (*prefix truncation attack*), un tā skar dažādus produktus, kā piemēram, *OpenSSH* versijas, kas vecākas par 9.6, *Dropbear* versijas pirms 2022.83 un daudzus citus produktus, kuri uztur *SSH* servera funkcionalitāti.

CERT.LV aicina pārskatīt visas iekārtas, kuras uztur internetā pieejamu *SSH* servisu, atslēgt neizmantotos *SSH* servisus un atjaunināt nepieciešamo iekārtu programmatūru atjauninājumu uzstādīšanu.

Plašāk: https://cert.lv/lv/2024/01/kritiska-ssh-protokola-ievainojamiba-cve-2023-48795

Par ievērojamākajām ievainojamībām un rekomendācijām to novēršanai CERT.LV ar elektronisko sakaru komersantu starpniecību regulāri informē interneta lietotājus. Plašāka informācija par apdraudējumiem pieejama tīmekļa vietnē: https://www.esidross.lv/informacija-par-apdraudejumiem/

2.4. Ļaundabīgs kods

Ļaunatūras arī 2023. gada 4. ceturksnī tika izplatītas galvenokārt diviem mērķiem – lai izvilinātu datus vai gūtu peļņu. Informācijas izgūšanai banku, iestāžu un uzņēmumu vārdā kampaņveidīgi tika izplatītas e-pasta vēstules ar kaitīgiem pielikumiem. Atverot pielikumu, iekārta tika inficēta ar ļaunatūru, kas ievāc lietotājvārdus, paroles, kriptovalūtu maciņu un to piekļuves informāciju u.tml., lai nosūtītu to uz uzbrucēja kontrolētu serveri.

Novērojot 2023. gada tendences, kopumā attiecībā uz ļaunatūras aktivitāti un informācijas tehnoloģiju drošības incidentiem, var secināt, ka sistēmu uzlaušanas un inficēšanas notika, pielietojot šādas metodes:

- pikšķerēšana;
- publiski zināmu ievainojamību ļaunprātīga izmantošana – versiju ievainojamības un "nulles dienas" (*zero-day*) ievainojamības;
- nekorektas konfigurācijas rezultātā tīmeklī eksponēto servisu ļaunprātīga izmantošana – noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi *(brute-force)*, versiju ievainojamības;
- inficēti datu nesēji – USB zibatmiņas;
- pirātiskas programmatūras uzstādīšana;

- nopludinātas un viegli uzminamas lietotāju paroles;
- automatizētie uzbrukumi.

Galvenie ļaunatūras tipi pārskata periodā

- Lietotāju datu zadzēji;
- *Bot-net* jeb zombēti datori;
- Izspiedējvīrusi;
- Attālinātās kontroles *trojāni,* mērķēti uz datu izgūšanu vai tālāko infrastruktūras kompromitēšanu.

Ir konstatēts, ka visbiežāk sastaptā lietotāju datu zadzēju ļaunatūra ir mērķēta 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.

Tāpat pārskata periodā tika konstatēts pieaugums gadījumiem, kad ar viltus reklāmu maldināti lietotāji ir paši instalējuši viltus mākslīgā intelekta spraudņus tīmekļa pārlūkā. Piemēram, tika fiksēti gadījumi, kad tika instalēti *AiGoogle* ļaundabīgo spraudņu paveidi, kuri veidoti "Facebook" kontu piekļuves datu zādzībai.

Peļņas gūšanas nolūkā tika izplatīti šifrējošie izspiedējvīrusi, kuru uzbrukuma rezultātā dati upura iekārtā tika nošifrēti, un datu atgūšanai tika pieprasīta izpirkuma maksa. Šifrējošo vīrusu uzbrukumi tika piedzīvoti gan privātajā , gan publiskajā sektorā.

Papildus tam nereti kompromitēti e-pasti vai lietotņu konti tiek izmantoti, lai tālāk izplatītu ļaunatūru. Piemēram, tika konstatēti vairāki gadījumi, kad no kompromitētiem e-pastiem izplatīja *Agent Tesla* ļaunatūru, izsūtot viltus rēķinus.

Tāpat tika novēroti arī gadījumi, kad pēc e-pasta kontu uzlaušanas uzbrucēji izveidoja e-pasta filtrus, lai pārtvertu un pārvirzītu sev interesējošo saraksti. Minētās darbības tika veiktas krāpšanas nolūkā, piemēram, pārtverot uzlauzta uzņēmuma klientu e-pastus, klientiem tika nosūtīti rēķini ar nomainītiem bankas rekvizītiem.

Starp Latvijas IP adrešu apgabalā novēroto ļaunatūru aktivitātēm līderību ieņem tādi banku trojāni kā *Ranbyus*, *Corebot*, *Tinba*. Joprojām salīdzinoši aktīva ir *RaspberryRobin* ļaunatūra, kas pārsvarā tiek izplatīta no iekārtas uz iekārtu ar inficētām USB zibatmiņām, piemēram, pārskata periodā vairāku valsts iestāžu tīklos tika konstatēta *RaspberryRobin* ļaunatūras klātbūtne.

Tāpat ir atklāti gadījumi, kad ļaunatūra nepamanīti funkcionējusi infrastruktūrā vairākus gadus. Piemēram, tika identificēti *Windows* serveri, kuri kompromitēti jau 2021. gada sākumā, izmantojot uz to brīdi jaunu CVE-2021-26855 ievainojamību, un inficēti ar attālinātās kontroles ļaunatūru *SparrowDoor*.

2023. gadā, tostarp arī pārskata periodā, Latvijā bija izteikti vērojama robotu tīklu aktivitāte. Konstatēts, ka daļa *brute-force* (izmantojot paroļu minēšanu) un DDoS uzbrukumos iesaistītās ierīces, kas atrodas Latvijas IP apgabalā, bija inficētas un iekļautas *Mirai* un *Gamut* ļaunatūru robotu tīklos. Vērojama arī *socks5systemz* un *SystemBc botnet* aktīva izplatīšanās. Vēl vairāk – 4. ceturksnī ļaunatūru TOP30 sarakstā *socks5systemz* ierindojās 1. vietā.

CERT.LV ekspertu komentārs

Svarīgi atzīmēt, ka pārskata periodā visbiežāk pie nošifrētām sistēmām noveda nevis jaunatklātu ievainojamību izmantošana, bet gan nepietiekama resursu aizsardzība. Vājas paroles un novecojis programmnodrošinājums ar vairākus gadus publiski zināmām ievainojamībām, kuras bija iespējams novērst, savlaicīgi veicot programmatūras atjaunināšanu, bija galvenie sākotnējās inficēšanās vektori. Atsevišķos gadījumos papildu veicinošais faktors vīrusa izplatībā bija nepārdomāts IT infrastruktūras plānojums.

2.5. Ielaušanās mēģinājumi

Informācija par ielaušanās mēģinājumiem tika saņemta visa 4. ceturkšņa garumā ievērojamā intensitātē. Šie uzbrukumi veikti, lielākajā daļā gadījumu izmantojot paroļu minēšanu (*brute-force*) pret dažādiem elektronisko sakaru komersantiem, valsts un pašvaldību iestādēm, kā arī privāto sektoru. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

Lielākā uzbrucēju interese bija par attālinātajam darbam izmantotajām tehnoloģijām, tādām kā RDP (*Remote Desktop Protocol*), VPN (*Virtual Private Network*) un tiešsaistes sanāksmju un tērzēšanas platformām. Kibernoziedznieki, pielietojot dažāda veida uzbrukumus, tajā skaitā jaunatklātas ievainojamības, uzstājīgi meklēja iespējas iekļūt uzņēmumu un organizāciju iekšējos tīklos, lai nesankcionēti piekļūtu sensitīvai informācijai vai nošifrētu iekārtas un pieprasītu maksu par datu atgūšanu. Uzbrucēji ķērās arī pie sen zināmām konfigurācijas nepilnībām plaši lietotos produktos.

REKOMENDĀCIJAS UN IETEIKUMI DROŠĪBAI

CERT.LV norāda, ka efektīvai kiberhigiēnai jebkuras organizācijas ietvaros ir būtiska loma cīņā gan pret komerciāli motivētiem, gan pret politiski motivētiem, tostarp Krievijas, kiberuzbrukumiem Latvijas kibertelpā. Kā primāro risinājumu cīņai ar ielaušanās mēģinājumiem un uzbrukumiem, kuros tiek izmantotas e-pasta vēstules ar kaitīgiem pielikumiem, kā piemēram, pievienotu RDP pieslēguma inicializācijas failu, CERT.LV uzsver nepieciešamību konfigurēt drošu e-pasta vēstuļu izsūtīšanu un saņemšanu, kā arī rekomendē veikt iekārtu konfigurāciju atbilstoši labajai praksei, tāpat arī svarīgi turpināt veicināt lietotāju izglītošanu, kā arī veikt sistēmu ievainojamību novēršanu, sekojot līdzi atjauninājumiem.

Vairāk informācijas un rekomendācijas pieejamas tīmekļa vietnē:
https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-ienakoso-e-pastu-viltosanu
https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-izejoso-e-pastu-viltosanu

2.6. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā iekārtu kompromitēšanas gadījumi skāra gan iedzīvotājus un uzņēmumus, gan arī valsts un pašvaldību iestādes. Uzbrukumu veikšanai tika izmantotas gan e-pasta vēstules ar ļaundabīgiem pielikumiem no jau kompromitētiem kolēģu vai sadarbības partneru kontiem, gan trūkumi dažādu IKT resursu aizsardzībā, kas izpaudās kā vājas paroles un novecojis programmnodrošinājums ar vairākus gadus publiski zināmām ievainojamībām. Kompromitēti ir arī maršrutētāji nelielos uzņēmumos vai individuālās mājsaimniecībās.

Kiberuzbrukumu mērķis – izgūt datus, manipulēt ar maksājumu informāciju, panākot maksājumu veikšanu uz uzbrucēju bankas kontiem, vai nošifrēt iekārtas, lai pieprasītu izpirkuma maksu par datu atgūšanu un, iespējams, nenopludināšanu.

Fiksēti gadījumi, kad datora paroles tika glabātas nešifrētā veidā, lokāli uz inficēta datora, līdz ar to ierīces inficēšanas gadījumā uzbrucēji guva pieeju pie vairākiem lietotāju kontiem, kuriem nebija aktivizēta divfaktoru autentifikācija. Fiksēti arī gadījumi, kad inficētais dators tika izmantots kā koplietošanas darbstacija, līdz ar to, inficējot vienu ierīci, uzbrucēju rīcībā nonāca vairāku personu autentifikācijas dati.

TOP incidenti pārskata periodā

Vairāki Latvijas uzņēmumi cieta no iejaukšanās biznesa sarakstē, kurā uzbrucēji piekļuva uzņēmuma vai sadarbības partnera e-pasta kontam, lai pusēm izsūtītu viltotus rēķinus ar mainītiem bankas rekvizītiem. CERT.LV aicināja uzņēmumus vienmēr, kad tiek veiktas izmaiņas finanšu datos, sazināties ar biznesa partneri, izmantojot citus komunikācijas kanālus, piemēram, piezvanot un pārliecinoties par informācijas patiesumu.
Tika fiksētas ar *Ngrok* programmatūras lietošanu saistītu aktivitāšu pazīmes augstas un vidēji augstas prioritātes

iestādēs. Attiecīgā programmatūra tiek izmantota, lai nodrošinātu attālinātu piekļuvi infrastruktūrai. Lai arī leģitīma, šī programmatūra ir populāra kiberuzbrucēju vidū, jo sniedz iespējas piekļūt infrastruktūrai, apejot aizsardzības pasākumus. Visos gadījumos CERT.LV veica incidentu izmeklēšanu.

Pārskata periodā CERT.LV reģistrēts liels skaits iesniegumu no privātpersonām un uzņēmumiem par uzlauztiem kontiem "Facebook" platformā. Uzlaužot "Facebook" kontu, krāpnieki nomaina ne tikai paroles, bet arī atgūšanās e-pasta adreses, lai apgrūtinātu īpašniekiem kontu atgūšanu. CERT.LV rekomendēja cietušajiem par notikušo operatīvi ziņot "Facebook" atbalsta dienestam, lai uzsāktu konta atgūšanas procesu.

Novembrī tika saņemta informācija par šifrējošā izspiedējvīrusa uzbrukumu kādai auto un moto tirdzniecības nozares uzņēmumu grupai. Uzbrukuma rezultātā ar izspiedējvīrusu tika nošifrēti uzņēmuma serveri un datubāzes, kā arī datu rezerves kopijas. Datu šifrēšana tika veikta ar mērķi izspiest naudu – par datu atbloķēšanu kibernoziedznieki pieprasīja veikt izpirkuma maksu kriptovalūtā.

CERT.LV sniedza uzņēmumam nepieciešamo atbalstu, veicinot incidenta ietekmes pārvarēšanu.

CERT.LV ekspertu komentārs

Apkopojot informāciju par kompromitētām tīmekļa vietnēm, novērojams, ka visbiežāk neautorizēta piekļuve tīmekļa serverim un tā failu neautorizēta modifikācija notiek, izmantojot ievainojamības CMS un to spraudņus. Papildus iezīmējās tendence, ka biežāk par citām tiek kompromitētas tīmekļa vietnes, kas veidotas uz "WordPress" bāzes. Tomēr šī tendence ir skaidrojama ar to, ka "WordPress" ir visbiežāk izmantotais CMS. Piemēram, tika konstatētas *SocGholish* un *Balada Injector* ļaundabīgās *JavaScript* injekcijas – kas nozīmē, ka tīmekļa serveros bija ievietoti šo ļaunatūru faili, līdz ar to tīmekļa vietnes papildus savam leģitīmam kodam izpildīja arī uzbrucēju kodu.

Novērots, ka uzbrucēji, kompromitējot tīmekļa serveri, veic pikšķerēšanas satura izvietošanu vai arī izmanto tīmekļa serveri kā prettiesiski iegūto datu kolektoru jeb pikšķerēšanas kampaņas kontroles serveri. Praktiski katrā gadījumā, kad uzbrucējiem ir iespēja veikt neautorizētu tīmekļa servera modifikāciju serverī, tiek ievietoti vairāki *webshell* jeb ļaundabīgi čaulas skripti, ar kuru palīdzību uzbrucējiem ir iespējas kontrolēt kompromitētus tīmekļu serverus un caur tiem attālināti izpildīt komandas.

Nereti uzbrucēji ar ievainojama tīmekļa servera starpniecību piekļūst arī citiem resursiem, piemēram, izgūst datubāzes, kuras satur personu datus. Dažos gadījumos uzbrucēji, tai skaitā politiski motivēti, veica tīmekļa vietnes izķēmošanu.

Šifrējošais vīruss ir ļaunatūra, kas sašifrē failus un sistēmas, un, lai tos atgūtu, tiek pieprasīta izpirkuma maksa *(ransomware).*

REKOMENDĀCIJAS UN IETEIKUMI DROŠĪBAI

Lai pasargātu organizāciju no izspiedējvīrusiem, ir svarīgi veikt drošības pasākumus – veidot drošas datu rezerves kopijas, izmantot pretvīrusu programmas, pārskatīt attālinātās piekļuves tiesības, nodrošināt visu ārējā perimetrā eksponēto resursu uzturēšanu atbilstošā drošības līmenī un izvairīties no aizdomīgu e-pasta vēstuļu vai saišu atvēršanas. Kiberdrošības eksperti nekādā gadījumā neiesaka maksāt izpirkuma maksu, jo tas negarantē pozitīvu iznākumu. Kā svarīgu iekārtu un kontu aizsardzības mehānismu CERT.LV aicina izmantot vairāku faktoru autentifikāciju visur, kur vien tas iespējams. Kritiski svarīga ir preventīva kiberdrošības ievērošana, piesardzības pasākumi un gatavība pret uzbrukumiem, izstrādājot pārdomātus un saprātīgus aizsardzības plānus.

3. Kiberapdraudējumu prevencija

3.1. DNS ugunsmūris: aktīvā aizsardzība

Lai sekmētu kopējo drošību valstī un efektīvi novērstu kiberapdraudējumus, turpinās darbs pie CERT.LV un NIC.LV izstrādātā aktīvās aizsardzības pakalpojuma DNS ugunsmūra attīstīšanas un popularizēšanas.

DNS ugunsmūris ik dienu tiek papildināts ar kaitīgiem domēniem, kuru krāpnieciskās saites iesūtījuši Latvijas iedzīvotāji un identificējusi CERT.LV komanda, tādējādi pasargājot DNS ugunsmūra lietotājus no kiberapdraudējumiem. Šis aktīvās aizsardzības risinājums bez maksas ir pieejams ikvienam Latvijas iedzīvotājam, uzņēmumam un organizācijai.

Pārskata periodā CERT.LV turpināja efektīvu sadarbību ar elektronisko sakaru komersantiem un uzņēmumiem, kā, piemēram, SIA "LMT", SIA "Tet". Sadarbības rezultātā sadarbības partneri saņem no CERT.LV kaitīgo domēnu sarakstu, izmantojot CERT.LV DNS RPZ zonu transfēru.

DNS ugunsmūris

CERT.LV aktīvās aizsardzības pakalpojums DNS ugunsmūris efektīvi un bez maksas pasargā ikvienu interneta lietotāju Latvijā, aizsargājot to ierīces no krāpnieciskās kampaņās izmantotām ļaundabīgām saitēm, krāpnieciskām vietnēm, kaitīga satura un dažādiem vīrusiem, kā arī nodrošinot valstī vienotu ierobežojamo domēnu zonu apstrādi un izplatīšanu.

Plašāk: https://dnsmuris.lv/

Nozīmīgākās aktīvas aizsardzības epizodes pārskata periodā:

- bloķētas viltus lapas, kuras lietotāji saņēma īsziņu (SMS) veidā – **751 reizi;**
- bloķēta lietotāja pārvirze uz kaitīgām lapām – **5 067 reizes;**
- viltus bankas lapu bloķētie pieprasījumi datu izkrāpšanai – **343 reizes.**

Gada nogalē piesātinātajā informācijas plūsmā, kad internetveikali īsteno dažādas atlaižu akcijas novembra "melnās piektdienas" ietvaros vai pirmssvētku periodā, to mēģina izmantot krāpnieki, radot internetveikalu vietņu viltus kopijas, lai šādi iegūtu no iedzīvotājiem sensitīvu informāciju – vārdu, adresi, paroli, maksājumu karšu datus u.c. datus. Statistika par DNS ugunsmūra datiem norāda, ka arī 2023. gada 4. ceturksnī ik mēnesi tika ģenerēts liels skaits viltus internetveikala un vīrusus izplatošu vietņu.

CERT.LV ekspertu komentārs

Pārskatā periodā DNS ugunsmūra darbības ietvaros ir bijuši daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot lietotājus no ļaundabīga satura un iekārtas no inficēšanas – no vairāku viltus lapu apmeklējumiem, maksājumu karšu datu zādzībām, no viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī liedzot inficētām iekārtām sazināties ar vīrusu kontroles serveriem. Šāda veida uzbrukumu skaits un intensitāte nākotnē pieaugs līdz ar tehnoloģiju, digitālās vides un kriptovalūtu attīstību, kā arī ar mākslīgā intelekta (MI) pavērto iespēju izmantošanu.

2023. gada 4. ceturksnī no kiberapdraudējumiem DNS ugunsmūra lietotāji (unikālie) tika pasargāti 467 888 reizes, kas ir par 1046% vairāk nekā 2023. gada 3. ceturksnī un par 521% vairāk nekā šajā pašā periodā pirms gada. DNS ugunsmūris apstrādāja aptuveni 1,5 miljonus DNS pieprasījumu katru mēnesi.

REKOMENDĀCIJAS UN IETEIKUMI DROŠĪBAI

CERT.LV aicina ikvienu būt uzmanīgam un stingri rekomendē vienmēr pārliecināties par saites vai sūtītāja patiesumu un atpazīstamību: kritiski vērtēt sūtītāja kontaktus, tīmekļa vietnes, kā arī atpazīt neuzticamus pielikumus e-pastos un citās saziņas platformās, savukārt par incidentiem nekavējoties informēt CERT.LV un Valsts policiju.

Vairāk informācijas par svarīgākajām drošības priekšrocībām un ieguvumiem, ko sniedz DNS ugunsmūra aktivizēšana, kā arī ērti lietojamas instrukcijas tā aktivizēšanai, pieejamas CERT.LV tīmekļa vietnē: https://dnsmuris.lv/.

3.2. Sensoru tīkls

ABS jeb sensoru tīkla izveides mērķis ir nodrošināt iestāžu atbildīgajiem iespējas laicīgi identificēt esošos apdraudējumus iestādēm. Tas tiek nodrošināts, analizējot iestādes tīkla plūsmas kopiju, izmantojot speciāli izveidotos notikumu noteikumus (*signature*).

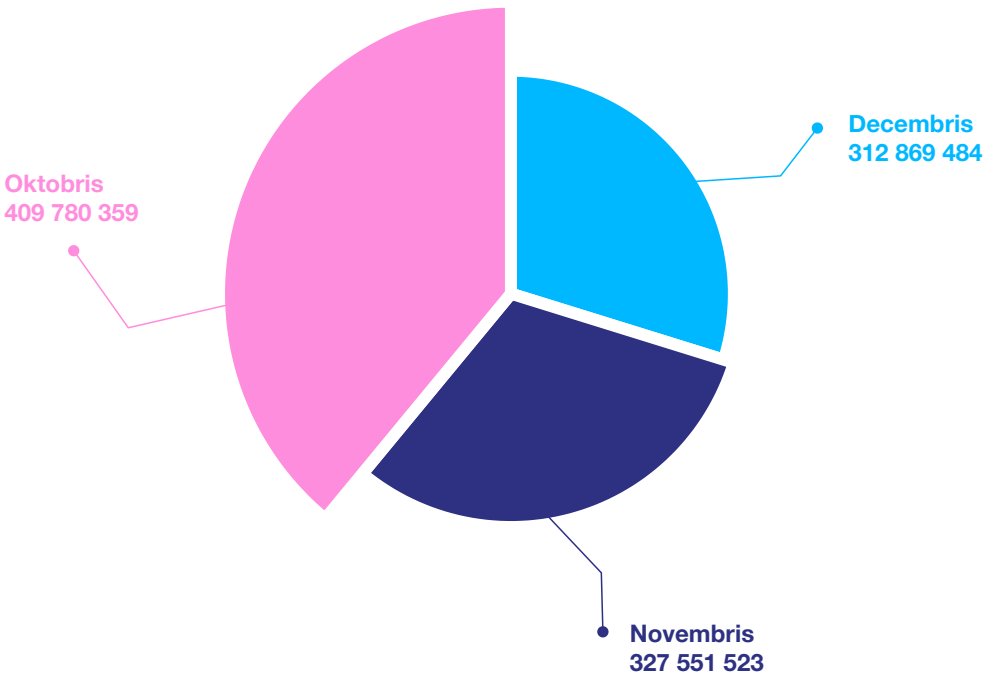
ABS ik mēnesi fiksē vidēji 6 000 augstas prioritātes (ar augstu bīstamības potenciālu) incidentus valsts, pašvaldību un kritiskās infrastruktūras (KI) iestādēs.

Pārskata periodā CERT.LV turpināja ABS sistēmas uzturēšanu un paplašināšanu.

Sensoru tīkls

Agrās brīdināšanas sistēma (ABS) jeb sensoru tīkls iestādēm, kurās tas ir uzstādīts, ļauj laicīgi pamanīt un atpazīt radušos apdraudējumus, kā arī savlaicīgi reaģēt uz tiem, papildus nodrošinot daudzpusīgāku priekšstatu par apdraudējumu spektru valsts un pašvaldību iestādēs.

Pārskata periodā kopējais brīdinājumu skaits, ko ģenerēja ABS



9. attēls. ABS ģenerēto brīdinājumu skaits 4. ceturksnī (ar vienu incidentu var būt saistīti vairāki brīdinājumi, kā arī daļa brīdinājumu nav saistīti ar incidentiem).

Pārskata periodā ABS visvairāk identificētie apdraudējumi

Apdraudējumi	Oktobris	Novembris	Decembris
Dažādas aizdomīgas darbības	7 306	5 392	2 733
Dažādi brīdinājumi par APT indikatoriem	1 277	1 869	1 560
Ar ļaunprātīgu programmatūru saistīti brīdinājumi	213	177	135
Ar pikšķerēšanu saistīti brīdinājumi	2 991	3 033	2 341
Ar ļaunprātīgu programmatūru saistītu robottīklu brīdinājumi	99 597	96 192	10 0541
Brīdinājumi no publiskiem agregatoriem par kompromitēšanas pazīmēm	9 171	4 094	3 93
Krāpnieciskas darbības	217	519	1 526

3.3. Pasākumi incidentu novēršanai

Pārskata periodā valsts un pašvaldību iestāžu atbildīgajiem par IT drošību, kā arī pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem un kritiskās infrastruktūras pārstāvjiem tika izsūtīti brīdinājumi par *WinRAR* ievainojamībām un brīdinājumi par viltus e-pasta vēstulēm, kas tika izplatītas Valsts drošības dienesta vārdā. Brīdinājumā tika iekļauti kaitīgo e-pastu indikatori, un iestādes tika aicinātas ierobežot piekļuvi kaitīgajiem resursiem. CERT.LV aicināja arī ziņot, ja iestāžu darbinieki ir saņēmuši viltotās e-pasta vēstules.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu "X" (@certlv) un "Facebook" (@cert.lv) kontos.

3.4. Koordinēta ievainojamību atklāšana (CVD)

CERT.LV turpināja mērķtiecīgu darbu pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas cvd.cert.lv (CVD) attīstības un popularizēšanas, pildot koordinētas ievainojamību atklāšanas procesa koordinētāja un vidutāja, kā arī platformas izstrādātāja, uzturētāja un pārziņa lomu.

CVD platformas darbība tika uzsākta 2023. gada martā. Tajā ir publicēta informācija par iestādēm, kuras brīvprātīgi iesaistījušās koordinētas ievainojamību atklāšanas procesā un noteikušas resursus, uz kuriem ievainojamību ziņošana attiecināma. 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, tā efektīvāk organizējot pasākumus Latvijas kibertelpas drošības aizsardzībai.

CVD.CERT.LV

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

Plašāk: https://cvd.cert.lv/

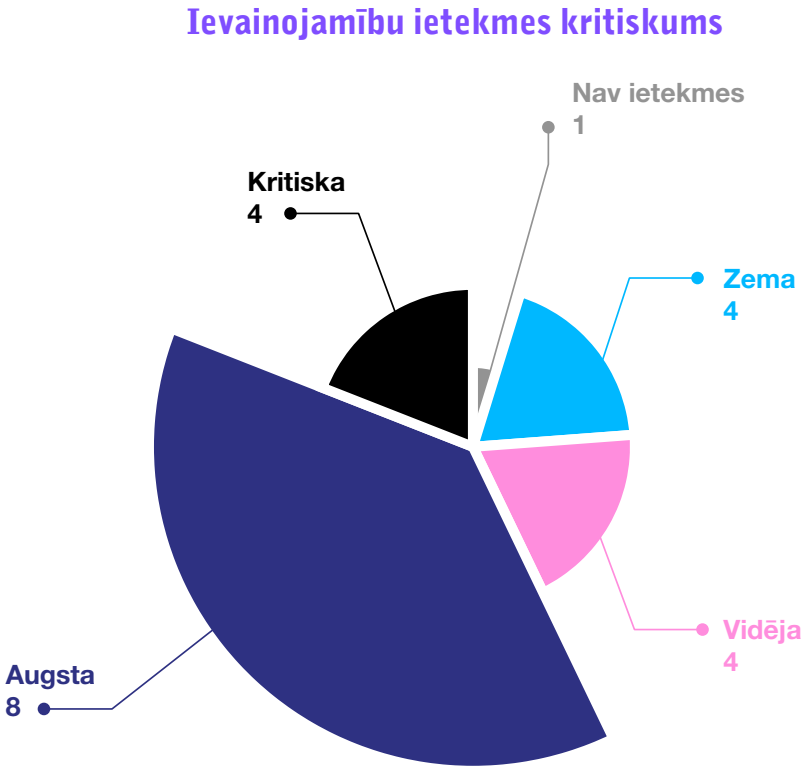
Uz pārskata perioda beigām platformā cvd.cert.lv bija reģistrēti:

- drošības pētnieki – 37;
- aktīvas programmas – 4;
- iestāžu/uzņēmumu atbildīgie pārstāvji – 28.

Uz pārskata perioda beigām kopskaitā saņemts 21 ievainojamību ziņojums, tostarp:

- CERT.LV klientūras ievainojamības – 13;
- uz konkrētām programmām reģistrētās ievainojamības – 8.

Veicinot koordinētas un atbildīgas IT drošības nepilnību atklāšanas labo praksi, pārskata periodā CERT.LV speciālisti vairākos informatīvos pasākumus un "Esi drošs" seminārā turpināja popularizēt CVD platformu, uzrunājot mērķauditoriju, kā arī aicinot drošības pētniekus ziņot par ievainojamībām CERT.LV domēnā esošajos servisos. Arī 2024. gadā CERT.LV turpinās aicināt valsts pārvaldes iestādes publicēt iestāžu programmas platformā un drošības pētniekus ziņot par atklātām ievainojamībām.



10. attēls. Ievainojamību ietekmes kritiskums 4. ceturksnī

CVD platforma tika izstrādāta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas sagatavoto informatīvo ziņojumu "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē", paredzot iespēju iestādēm brīvprātīgi iesaistīties koordinētas ievainojamību atklāšanas procesa ieviešanā valsts pārvaldē.

4. Komunikācija ar sabiedrību

4.1. Apmācības un izglītojošie pasākumi

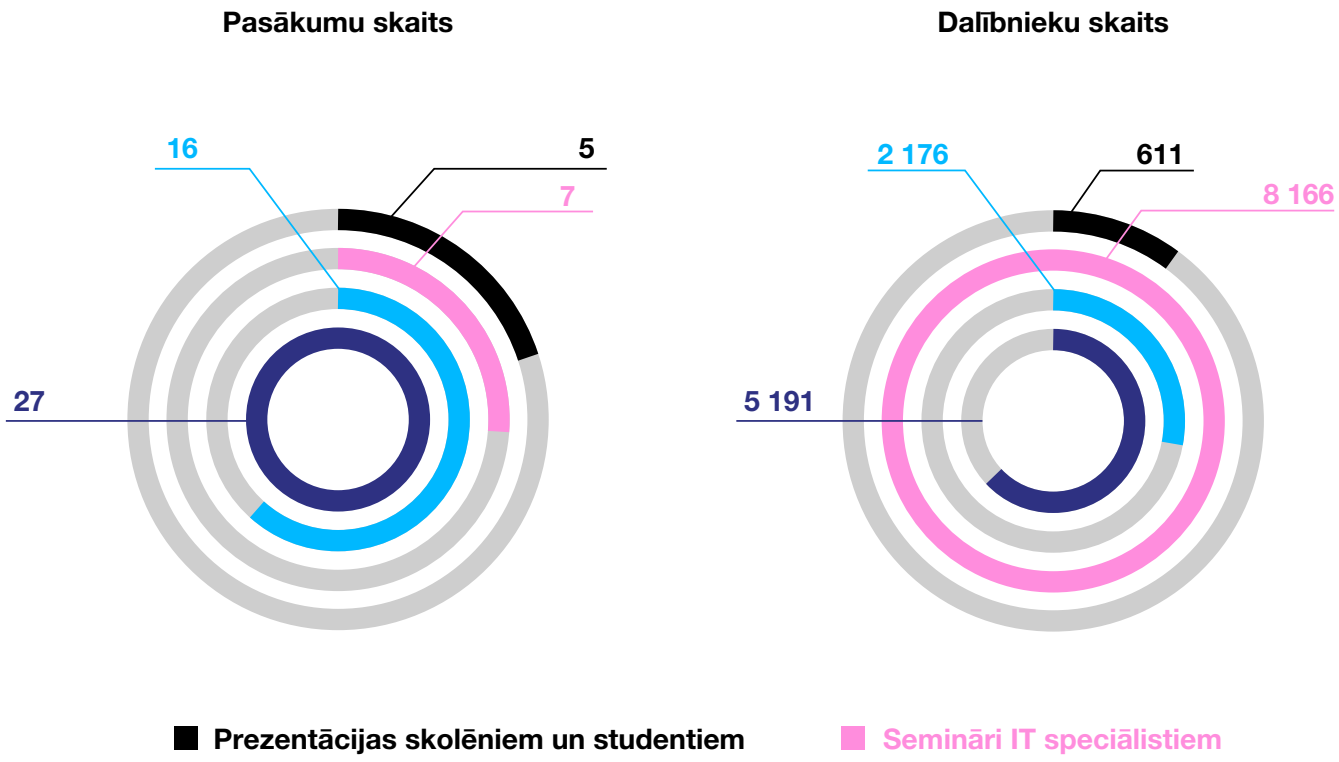
CERT.LV komanda veica aktīvu darbu sabiedrības izglītošanai, gan organizējot, gan piedaloties dažādos tematiskos semināros un informējot par aktualitātēm kiberdrošības jomā, kā arī veicinot kiberhigiēnas labo praksi. Papildus ierastajiem darbinieku izglītošanas semināriem par kiberdrošību tika novadītas vairākas lekcijas un apmācības iestāžu un kritiskās infrastruktūras uzņēmumu darbiniekiem par specifiskām, iestāžu un uzņēmumu izvēlētām tēmām.

2023. gada 4. ceturksnī, iesaistoties 55 izglītojošos pasākumos, CERT.LV par IT drošību izglītoja 16 144 dalībniekus, kas ir gandrīz 8 reizes vairāk nekā iepriekšējā ceturksnī.

CERT.LV organizētie izglītojošie pasākumi IT drošības speciālistiem

4. un 5. oktobrī, Eiropas Kiberdrošības mēneša laikā, Rīgā jau desmito reizi notika **starptautiskā kiberdrošības konference *CyberChess 2023* (“Kiberšahs 2023”)**. Pasākuma dalībniekiem tika sniegta iespēja vienuviet dzirdēt pasaules un Baltijas līmeņa kiberdrošības profesionāļus, kā arī neformālā gaisotnē savstarpēji mijiedarboties, lai papildinātu savu zināšanu bagāžu, radot jaunas un kopīgas ieceres

Izglītojošo pasākumu un apmācīto cilvēku skaits



11. attēls. Izglītojošo pasākumu un apmācīto cilvēku skaits 4. ceturksnī


CyberChess
2023
Cybersecurity Conference
October 4 - 5
Riga, Latvia


through public-private cooperation
Questions: menti.com
Code: 4622 9931
MR. RICHARD BROWNE
MR. INGMĀRS PŪKIS
MR. FLORIAN


2023

kiberdrošības jomā. Konference šogad klātienē pulcēja 670 dalībniekus un ekspertus no 26 valstīm, savukārt tiešraide piesaistīja ap 6000 skatījumu no 38 valstīm. Programmā bija vairāk nekā 60 vietējo un ārvalstu ekspertu uzrunas un diskusijas trīs sesijās – stratēģiski politiskajā, tehniskajā un domēna vārdiem veltītajā. Konferences ieraksts pieejams tīmekļa vietnē: www.cyberchess.lv.

Jau ceturto gadu paralēli konferencei "Kiberšahs 2023" norisinājās **arī tiešsaistes kiberdrošības sacensības *Capture The Flag* (CTF)**, kas ļāva spēles dalībniekiem stāties pretī dažādiem kiberdrošības izaicinājumiem tādās kategorijās kā, piemēram, kriptogrāfija, tīkla analīze, kriminālistika, binārais kods un citas. Dienā 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.

Galda izspēles mācības par kiberdrošības incidentu izmeklēšanu: pārskata periodā pirms ikgadējās konferences "Kiberšahs 2023" CERT.LV speciālisti organizēja vairākas darbnīcas. Vienā no tām CERT.LV vadībā tika izspēlēta kiberdrošības incidentu izmeklēšanas spēle (*Cybersecurity Breach Investigation Tabletop Exercise*), kuras dalībnieki interaktīvā veidā pēta un analizē uzbrukuma gaitu, kādi indikatori liecina par uzbrukumu un kā nokļūt līdz vaininiekam. Spēli sagatavojusi Eiropas Savienības Kiberdrošības aģentūra ENISA, lai veicinātu izpratni par kiberdrošību jomas nespeciālistiem, savukārt latviešu valodā to tulkojusi un pielāgojusi CERT.LV komanda. Tāpat šī spēle tika izspēlēta arī Ventspils Digitālā centra rīkotajā pasākumā, kā arī Rīgas tehniskās universitātes koledžas organizētajā tālmācības apmācībā skolotājiem.

12. decembrī CERT.LV organizēja **IT drošības semināru "Esi drošs"** valsts un pašvaldību iestāžu atbildīgajiem darbiniekiem par IT drošību, pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem, kā arī citiem interesentiem, kuri darbojas IT drošības jomā. Šajā seminārā tika aplūkotas tādas tēmas kā kiberdrošības aktualitātes gada griezumā, CERT.LV nodrošinātie pakalpojumi, SOC (*Security Operations Center*) izveide, izmantojot *open source* rīkus, tehnoloģiskie risinājumi kiberdrošības apmācībām, mākslīgā intelekta droša izmantošana u.c. tēmas. Semināra norisei tiešsaistē sekoja vairāk nekā 450 dalībnieku. (Ieraksts: https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decembri)

CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai

Nozīmīgākie pasākumi 4. ceturkšņa griezumā:

26. oktobrī UNESCO Pasaules medijpratības un informācijpratības nedēļas ietvaros Baltijas Mediju izcilības centrs rīkoja pasākumu **"Medijpratības diena: kāpēc mācīt un mācīties?".** Šis pasākums tika organizēts, lai veicinātu diskusijas, sarunas un dialogu par medijpratības mācīšanas nozīmību jauniešiem un piedāvātu skolotājiem un citiem darbiniekiem praktiskas metodes medijpratības mācīšanai. CERT.LV piedalījās diskusijā par medijpratības nepieciešamību, uzsverot to, ka medijpratība ir būtiska katra indivīda kiberdrošības sastāvdaļa.

27. oktobrī Eiropas Kiberdrošības mēneša ietvaros Latvijas tehnoloģiju uzņēmuma "Tet" organizētā foruma ***CyberShield 2023*** diskusijā par karjeru kiberdrošības jomā piedalījās un runāja CERT.LV vadītāja Baiba Kaškina. Forums pulcēja vietējos un starptautiskos kiberdrošības ekspertus un nozares profesionāļus, sniedzot izsmeļošu apskatu par jaunākajām tendencēm kibernoziedzībā, kiberdrošības izaicinājumiem un tehnoloģijām.

1. novembrī norisinājās Valsts ieņēmumu dienesta (VID) pastāvēšanas 30. gadadienai veltīta starptautiska konference **"VID 30. Transformācija un ilgtspēja"**, kurā CERT.LV eksperts piedalījās diskusijā par aktuālajiem drošības izaicinājumiem.

3. novembrī Latvijas Universitātes Datorikas fakultātes studentu pašpārvalde rīkoja CTF sacensības. To mērķis bija iepazīstināt pirmo kursu studentus no dažādām augstākās izglītības iestādēm, kā arī citus interesentus ar CTF un pievērst uzmanību kiberdrošības nozarei un tās aktualitātei izglītojoši izklaidējošu sacensību formātā. Pirms sacensību norises CERT.LV pārstāvis sniedza studentiem ieskatu kiberdrošībā un iepazīstināja ar aktuālo situāciju Latvijas kibertelpā, kā arī stāstīja par *Red Team/Blue Team* darbības principiem un pārrunāja CTF norises aspektus.

23. novembrī CERT.LV pārstāves piedalījās **Ventspils Digitālā centra organizētajā seminārā uzņēmējiem un viņu darbiniekiem**, kurā iepazīstināja klausītājus ar ieteikumiem, kā atpazīt kiberuzbrukumus un pasargāt gan savu uzņēmumu, gan domēna vārdu digitālajā vidē.

4.2. Sabiedrības informēšana un kiberhigiēnas veicināšana

CERT.LV turpināja informēt sabiedrību par kiberdrošības riskiem, kiberhigiēnas veicināšanu un labajām praksēm, kā arī citām aktualitātēm Latvijas kibertelpā. Ar 376 publikācijām plašsaziņas līdzekļos, kas ir par 47% vairāk nekā iepriekšējā ceturksnī, iegūti 16,5 miljoni skatījumu.

Pārskata periodā lielāko mediju interesi izraisīja aktuālā situācija Latvijas kibertelpā, jo īpaši gada nogalē, skolām izsūtītās draudu vēstules un droša mobilo lietotņu izmantošana.

CERT.LV turpina arī tulkot un portālā www.esidross.lv publicēt OUCH! ikmēneša izdevumus (informācijas drošības biļetens, ko sagatavo SANS institūts).

Pārskata periodā portālā esidross.lv publicētie raksti:

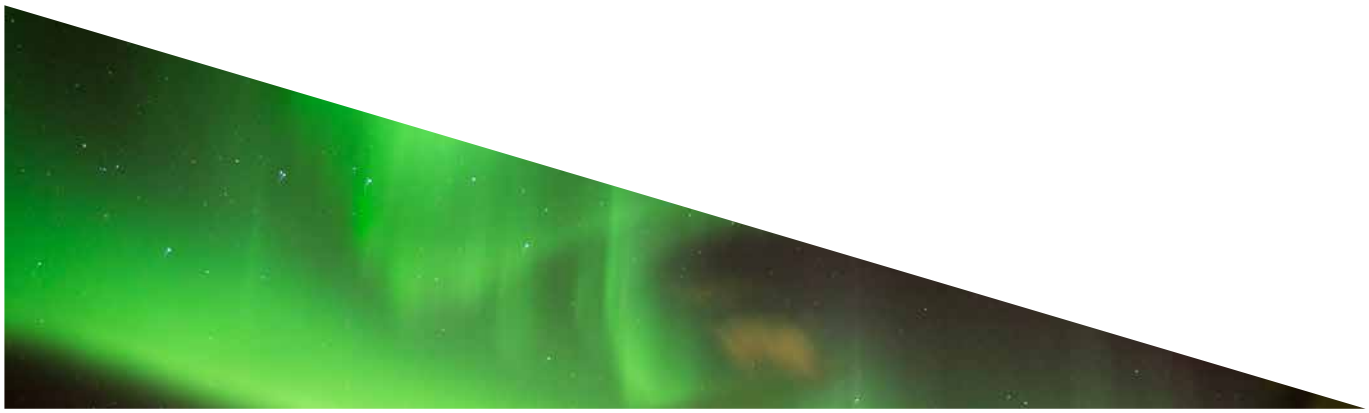
- Paroļu frāžu izmantošana OUCH! 12/2023;
- Droša un gudra iepirkšanās internetā: kā izvairīties no krāpnieku slazdiem?
- "Melns uz balta" – vienota platforma ziņošanai par dezinformācijas gadījumiem;
- Mana iekārta ir uzlauzta. Ko darīt? OUCH! 11/2023;
- Kāpēc ir svarīgi veikt atjauninājumus? OUCH! 10/2023.

Tāpat CERT.LV katra mēneša beigās turpināja apkopot informāciju par būtiskākajiem kiberincidentiem, izstrādājot un publicējot pārskatu "Kiberlaikapstākļi" tīmekļa vietnes www.cert.lv sadaļā "Ziņas".

Pārskats "Kiberlaikapstākļi"

CERT.LV piedāvā ikmēneša pārskatu kiberlaikapstākļu vērotājiem par aizvadītā mēneša spilgtākajiem notikumiem kibertelpā TOP 5 kategorijās –krāpšana, ļaunatūras un ievainojamības, piekļuves atteices uzbrukumi, ielaušanās un datu noplūde, kā arī lietu internets.

Oktobris: https://cert.lv/lv/2023/11/kiberlaikapstakli-oktobris
Novembris: https://cert.lv/lv/2023/12/kiberlaikapstakli-novembris
Decembris: https://www.cert.lv/lv/2024/01/kiberlaikapstakli-decembris



5. Stratēģiskā sadarbība Latvijā

Pārskata periodā CERT.LV pārstāvji aktīvi piedalījās **Nacionālās informācijas tehnoloģiju drošības padomes darbā**, kuras mērķis ir koordinēt ar informācijas tehnoloģiju drošību saistīto uzdevumu un pasākumu plānošanu un veikšanu Latvijā.

CERT.LV speciālisti cieši sadarbojās ar Latvijas Republikas **Zemessardzes Kiberaizsardzības vienību**, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV varētu sniegt atbalstu valstij un privātajam sektoram. Pārskata periodā svarīgākā sadarbība notika, piedaloties kiberdrošības mācību "Locked Shields" plānošanā un Latvijas komandas sagatavošanā mācībām.

CERT.LV turpināja organizēt arī **Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas (DEG) sanāksmes**, kas notiek katra mēneša otrajā ceturtdienā. DEG ir brīvprātīga Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupa ar mērķi veicināt IT/IS drošību, sekmēt drošības apziņas kultūru Latvijas Republikā un sniegt atbalstu CERT.LV. Sanāksmēs tiek apspriestas gan kiberdrošības aktualitātes, gan sekmēta grupas dalībnieku zināšanu un pieredzes apmaiņa.

CERT.LV cieši sadarbojās ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu un savas kompetences ietvaros aktīvi piedalījās Nacionālās kiberdrošības stratēģijas īstenošanā.

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

5.1. Kibernoziedzības novēršana un apkarošana

Sadarbība ar kritiskās infrastruktūras (KI) turētājiem

Turpinās sadarbība ar KI turētājiem, gan uzraugot situāciju kibertelpā, gan sniedzot konsultācijas un atbalstu KI kibernoturības stiprināšanai un dažādu sektoru sadarbības pilnveidošanai. CERT.LV aktīvi koordinē sensoru un DNS RPZ uzstādīšanu iestādēs un uzņēmumos, lai veicinātu ātrāku KI apdraudējumu identificēšanu un efektīvāku to novēršanu.

Atbalsts Latvijas valsts tiesībsargājošajām iestādēm

Pārskata periodā CERT.LV sniedza atbalstu Latvijas valsts tiesībsargājošajām iestādēm kibernoziedzības incidentu izmeklēšanā, sagatavojot atbildes Valsts policijai par vairākiem incidentiem.

Oktobrī, kad simtiem Latvijas skolu un bērnudārzu savos e-pastos saņēma draudu vēstules par iespējamiem drošības riskiem, kā arī identiska satura draudu e-pasta vēstules tika izplatītas tiesām un pašvaldībām, CERT.LV sadabojās ar Valsts policiju, lai veiktu koordinētu izmeklēšanu, un kopā ar

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, pilnveidojot arī iesaistīto institūciju sadarbību un atbildīgo institūciju reaģēšanas ātrumu.

tiesībsargājošajām iestādēm analizēja, kādas e-pasta un IP adreses un kāda veida infrastruktūra tika izmantota draudu e-pasta vēstuļu izsūtīšanai.

Vēl papildus tika sniegti komentāri par IP un e-pasta adresēm, kas potenciāli saistītas ar noziedzīgiem nodarījumiem, par interneta resursu izmantošanas iespējām, par iespējamu nesankcionētu piekļuvi e-pastam un rēķina viltošanu, kā arī veikta pikšķerēšanas vietnes analīze.

Drošības testi un izvērtējumi

2023. gada 4. ceturksnī kopskaitā tika veikti 7 drošības testi, tajā skaitā serverim kādā valsts akciju sabiedrībā, pieciem dažādiem resursiem kādā iestādē, kā arī kādas institūcijas tīmekļa vietnei.

Resursu turētājiem tika iesniegti pārskati par testu rezultātiem un sniegtas rekomendācijas nepilnību novēršanai.

Tāpat pārskata periodā tika saņemti 8 (4 sākotnējie un 4 atkārtotie) Valsts informācijas sistēmu (VIS) izvērtēšanas pieteikumi, no kuriem trīs tika saskaņoti un pieciem sniegtas rekomendācijas pirms atkārtotas iesniegšanas.

Draudu medības

Pārskata periodā ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību, tika turpinātas draudu medību operācijas. Tāpat CERT.LV speciālisti turpina ieguldīt darbu, izstrādājot un pilnveidojot draudu medību metodiskos materiālus un organizējot pieredzes apmaiņas pasākumus.

CERT.LV komanda ir līdere draudu medību operāciju organizēšanā un vadīšanā Eiropas Savienībā, sniedzot savu ieguldījumu NATO kolektīvajā Eiropas aizsardzībā, veicinot starptautisko normu piemērošanu kibertelpā un veidojot uzticamu sabiedroto loku, kas spēj gan sniegt savstarpēju atbalstu kiberdraudu izvērtējumā, gan ātri apmainīties ar informāciju un labajām praksēm.

Sadarbības tikšanās, sanāksmes un konsultācijas kiberdrošības jomā

- Aktīva iesaiste Centrālās vēlēšanu komisijas (CVK) Vēlēšanu darba grupā, sniedzot rekomendācijas drošai vēlēšanu sistēmu izstrādei un uzturēšanai. CERT.LV eksperti regulāri piedalījās Vēlēšanu IT darba grupas sanāksmēs, sniedzot rekomendācijas saistībā ar sistēmu drošības aspektiem un testēšanu. CERT.LV arī sniedza savu redzējumu par IT riskiem CVK saistībā ar Eiropas Parlamenta 2024. gada vēlēšanu nodrošināšanu.
- Iesaiste Nacionālā koordinācijas centra vadītajā Starpinstitucionālās darba grupas darbā, kuras mērķis – veicināt informācijas apmaiņu starp valsts pārvaldes iestādēm un organizācijām par aktivitātēm un pasākumiem dažādās kiberdrošības jomās, lai veicinātu efektivitāti un sadarbību.
- Pārskata periodā tika veikta likumprojektu/iniciatīvu izskatīšana, tostarp 9 reizes izskatīti Eiropas Savienības līmeņa un 8 reizes Latvijas līmeņa likumprojekti, kā arī organizētas sanāksmes ar Latvijas līmeņa likumprojektu virzītājiem atsevišķu problēmjautājumu vai komentāru pārrunāšanai.

5.2. CERT.LV atbalsts DDUK sekretariāta darbā

CERT.LV aktīvi piedalās Digitālās drošības uzraudzības komitejas (DDUK) darbā, tās ietvaros ik dienas sniedzot atbalstu kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzībā.

5.3. Izglītība un jauniešu kiberprasmju uzlabošana

CERT.LV piedalās Saldus tehnikuma administrācijas organizētajā darba grupā kvalifikācijas “Kiberdrošības tehniķis” standarta izstrādei, daloties ar savu pieredzi un sniedzot redzējumu par speciālistiem nepieciešamajām zināšanām, iemaņām un prasmēm, lai nodrošinātu, ka kvalifikācijas ieguvēji ir pieprasīti un augstu novērtēti speciālisti darba tirgū.

Aizsardzības ministrijas Eiropas Savienības kiberdrošības jautājumu nodaļa organizē Eiropas mēroga kiberdrošības sacensību jauniešiem “Eiropas kiberdrošības izaicinājums 2024” (ECSC) Latvijas nacionālo atlasi. Lai nodrošinātu sekmīgu Latvijas komandas dalību ECSC sacensībās, būtisks ir kiberdrošības kompetenču kopienas dalībnieku, īpaši augstskolu un privātā sektora uzņēmumu, iesaiste nacionālās atlases praktiskajā organizēšanā un atbalsta sniegšanā.

CERT.LV sniedz atbalstu ECSC nacionālās atlases tīmekļa vietnes izveidošanā, kā arī nacionālās atlases nodrošināšanai nepieciešamās infrastruktūras un uzdevumu kopas sagatavošanas darbos.

6. Starptautiskā sadarbība

Pārskata periodā CERT.LV turpināja pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberdrošības incidentu novēršanas vienībām un starptautiskām organizācijām. Tāpat CERT.LV darbinieki sniedza savu redzējumu un ieguldījumu dažādās darba grupās, daloties ar pieredzi un labo praksi, sniedzot konsultācijas un atbalstu, kā arī uzstājās ar prezentācijām starptautiskās konferencēs un semināros. Turpinājās arī darbinieku jaunu prasmju apgūšana un kvalifikācijas celšana, piedaloties starptautiskās mācībās.

Sadarbība ar CSIRTs tīklu, ENISA, Eiropas Savienības institūcijām un NATO

CERT.LV regulāri piedalās NIS (Tīklu un informācijas drošības) direktīvas CSIRTs Network (CSIRT tīkls) sadarbības tīkla sanāksmēs. CSIRTs Network darbu koordinē ENISA – Eiropas Savienības Kiberdrošības aģentūra, kas sniedz ieguldījumu ES politikā kiberdrošības jomā.

Pārskata periodā CERT.LV piedalījās *CSIRTs Network* darba grupā *Maturity*, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.

Tāpat CERT.LV speciālisti turpināja aktīvi līdzdarboties ENISA organizētās darba grupās:

- ***Coordinated Vulnerability Disclosure (CVD) Task Force*** – norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas;
- ***EU Cybersecurity Index*** – tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai. Pārskata periodā pēc sākotnējā prototipa testēšanas darba grupa turpināja attīstīt *EU Cybersecurity Index* platformu;
- ***CSIRT Services Framework*** – turpināja darbu, izstrādājot vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā tika veikta CERT komandu tipu noteikšanas metodoloģijas izstrāde, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.

CSIRTs Network (CSIRT tīkls)

Eiropas Savienības dalībvalstu kiberdrošības incidentu novēršanas institūciju tīkls nodrošina sadarbību starp kiberdrošības incidentu novēršanas vienībām Eiropas Savienībā. Tīkla sanāksmes notiek 3 reizes gadā, un tās organizē konkrētajā brīdī Eiropas Savienības Padomes prezidējošā valsts sadarbībā ar ENISA. Reizi gadā sanāksmē notiek arī apvienotās sesijas kopā ar NIS direktīvas Sadarbības grupu *CyCLONe.*

Plašāk:
https://csirtsnetwork.eu/
https://www.enisa.europa.eu/topics/incident-response/cyclone

***CSIRT Network Situation Update* sanāksmes:** pārskata periodā turpinājās regulāra dalība sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo kibertelpā starp CSIRT tīkla biedriem.

Eiropas Komisijas EHDS (*European Health Data Space*) regulas darba grupa: CERT.LV speciālisti sniedza savu ieguldījumu darba grupā, kuras mērķis ir veicināt 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 GDPR.

Regulāra CERT.LV ekspertu dalība Eiropas Kiberdrošības produktu sertifikācijas grupas ECCG *(European Cybersecurity Certification Group)* sanāksmēs, tostarp no 20. līdz 23. novembrim notikušajā ES sertifikācijas nedēļā Malagā, Spānijā, pārstāvot Latvijas intereses un sniedzot savu redzējumu par topošo ES mākoņpakalpojumu sertificēšanas shēmas projektu, kā arī par citiem IKT produktu kiberdrošības sertifikācijas ieviešanas jautājumiem ES valstīs.

ENISA organizētās mācības *CYBER EUROPE 2024:* CERT.LV eksperti piedalījās mācību noslēguma plānošanas konferencē, kas pārskata periodā norisinājās no 13. līdz 15. novembrim Atēnās, Grieķijā. Noslēguma konferencē dalībvalstis vienojās ne tikai par tehniskā un operacionālā līmeņa incidentiem, bet arī nolēma pārbaudīt starptautisko sadarbību *CSIRT Network* un *CyCLONe (European Cyber Crisis Liaison Organisation Network)* ietvaros.

NATO mācības CYBER COALITION: laika posmā no 2023. gada 27. novembra līdz 1. decembrim CERT.LV eksperti piedalījās NATO mācībās CYBER COALITION 2023, kas norisinājās tiešsaistē, un kurās tika vingrināti gan tehniskie, gan proceduārie jautājumi. 2023. gada mācību galvenie uzdevumi bija veicināt sabiedroto noturību pret kiberuzbrukumiem un spēju kopīgi veikt atbildes operācijas kibertelpā.

NATO CYBER COALITION

Lielākās NATO organizētās ikgadējās kolektīvās kiberdrošības mācības, kas ir vienas no lielākajām pasaulē. To mērķis ir uzlabot sadarbību un koordināciju kiberdrošības jomā sabiedroto vidū.

Sadarbība FIRST ietvaros

Turpinājās regulāra dalība *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa izmantošanu.

CERT.LV vadītāja Baiba Kaškina, kas turpina pildīt *FIRST Membership Committee* priekšsēdētājas pienākumus, piedalījās jauno biedru pieteikumu izskatīšanā, kā arī veicināja biedru uzņemšanas procesa pilnveidošanu.

FIRST

Kiberdrošības organizācija, kas apvieno CERT, CSIRT, PSIRT, SOC komandas un citus kiberdrošības profesionāļus no visas pasaules. 2024. gada sākumā FIRST biedri ir no 106 valstīm.

Sadarbība TF-CSIRT ietvaros

CERT.LV ir sertificēta *Trusted Introducer* komanda no 2016. gada 1. septembra.

Pārskata periodā CERT.LV ir viena no 47 Eiropas TF-CSIRT/*Trusted Introducer* sertificētām komandām (kopienā ir 495 komandas), kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.

Sertifikācijas uzturēšanai ik pēc trīs gadiem jāveic re-sertifikācijas process. 2022. gada 28. oktobrī, TF-CSIRT sanāksmē Viļņā, Lietuvā, tika paziņots, ka CERT.LV ir veiksmīgi re-sertificēta uz nākamajiem 3 gadiem (attiecīgi nākamais re-sertifikācijas process plānots 2025. gadā).

Sertifikācijas pamatā ir SIM3: *Security Incident Management Maturity Model* pieeja, kas vērtē organizācijas briedumu, skatoties uz organizatoriskiem, cilvēkresursu, izmantoto tehnisko rīku un procesu parametriem un to pielietojumu kvalitatīvai organizācijas darbības nodrošināšanai, primāri vērtējot incidentu risināšanas procesa briedumu.

Pārskata periodā CERT.LV turpināja darbu vairākās TF-CSIRT darba grupās.

TF-CSIRT/Trusted Introducer

TF-CSIRT ir Eiropas reģiona CERTu organizācija, kas apvieno incidentu reaģēšanas komandas no visiem sektoriem. Trusted Introducer serviss uztur uzticamu CERT vienību reģistru un veic vienību akreditāciju un sertifikāciju atbilstoši komandas demonstrētajam brieduma līmenim.

Projekta Joint Threat Analysis Network īstenošana

CERT.LV komanda turpināja darbu pie projekta *Joint Threat Analysis Network* (turpmāk – JTAN projekts) īstenošanas.

Projekta vadošais partneris ir Informācijas tehnoloģiju drošības incidentu novēršanas institūcija Polijā CERT.PL, kas darbojas institūta *Naukowa i Akademicka Sieć Komputerowa* (NASK) struktūrā. JTAN projektā piedalās arī partneri no Austrijas, Francijas, Igaunijas, Luksemburgas, Rumānijas un Slovākijas.

Joint Threat Analysis Network īstenošana

Kopējais projekta mērķis ir izveidot vienotu apdraudējumu analīzes tīklu. Tīkls būtu atvērts Eiropas CSIRT sadarbības grupai, kuras galvenā uzmanība pievērsta tehnisko, operatīvo un stratēģisko draudu izlūkošanas informācijas apmaiņai un analīzei.

2023. gada 4. ceturksnī CERT.LV tupināja *Graphoscope* risinājuma izstrādes darbus atbilstoši plānam. Pārskata periodā CERT.LV novirzīja papildu resursus projekta īstenošanai, piedalījās ikmēneša attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informē par individuāliem projekta uzdevumiem un rezultātiem.

Galvenās *Graphoscope* iezīmes:

- atbalsts daudziem datu avotiem un vienkārša sistēmas uzstādīšana;
- tīmeklī bāzēta saskarne, kas nav atkarīga no iepriekš instalētām datubāzēm;
- saskarne nodrošina elastīgus filtrus, atvieglojot liela apjoma datu analīzi.

Graphoscope

Rīks, kas paredzēts, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā.

Atbilstoši līgumam ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165, kas tika apstiprināts un uzsākts 2021. gada 1. jūlijā *2020 CEF Telecom Call – Cybersecurity* uzsaukumā, JTAN projekta īstenošana turpināsies līdz 2024. gada 30. jūnijam.

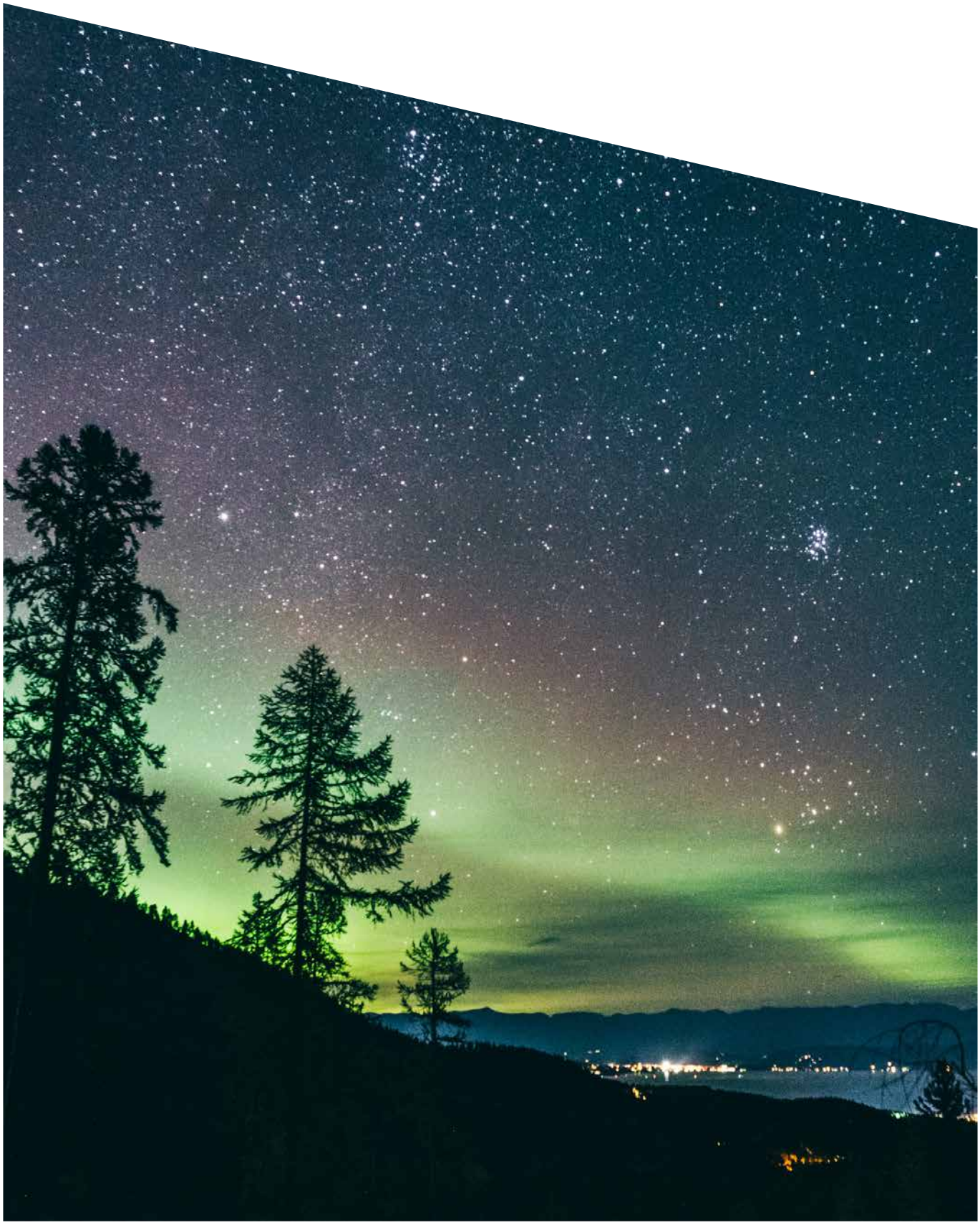
Citas starptautiskās aktivitātes

Pārskata periodā CERT.LV pārstāvji piedalījās vairākās starptautiska mēroga konferencēs un semināros, kā arī uzņēma vairākas ārvalstu delegācijas un piedalījās sanāksmēs ar ārvalstu delegāciju pārstāvjiem Latvijā.
Būtiskākās aktivitātes:

- **5. oktobrī** Eiropas kiberdrošības mēneša ietvaros Rīgā norisinājās Eiropas Kiberdrošības kompetenču centra (ECCC) nacionālo koordinācijas centru (NCC) neformālā sanāksme, kurā tās vadītāji un eksperti no sešām Eiropas Savienības dalībvalstīm – Latvijas, Igaunijas, Lietuvas, Luksemburgas, Somijas un Zviedrijas – dalījās pieredzē par kiberdrošības projektu īstenošanu saistītiem jautājumiem. Plānots, ka šādas sanāksmes notiks arī turpmāk – gan Latvijā, gan citās Eiropas Savienības dalībvalstīs. Latvijas Nacionālā koordinācijas centra (NCC-LV) funkcijas īsteno Aizsardzības ministrija sadarbībā ar CERT.LV un Centrālo finanšu un līgumu aģentūru.
- **No 28. oktobra līdz 4. novembrim** CERT.LV pārstāvis piedalījās *RISE South Korea* konferencē ar prezentāciju Heated Cyberspace in Latvia 2022-2023, kā arī apmeklēja vizītē Dienvidkorejas nacionālo CERTu KrCERT/CC. Konferencē piedalījās ap 120 dalībnieki.
- **No 8. novembra līdz 10. novembrim** Rīgā viesojās Kosovas un Maķedonijas kiberdrošības organizāciju pārstāvji. Tikšanās laikā CERT.LV komanda kopā ar kolēģiem no Aizsardzības ministrijas un Zemessardzes Kiberaizsardzības vienību iepazīstināja dalībniekus ar Latvijas kiberdrošības ekosistēmu, CERT.LV darbību, kā arī dalījās pieredzē un labajā praksē par nacionālās kiberdrošības stiprināšanu. Vizīti organizēja DCAF (*Geneva Centre for Security Sector Governance*).
- No 12. novembra līdz 22. novembrim CERT.LV pārstāvis piedalījās divos starptautiskos semināros, lai veicinātu kiberdrošības kapacitātes veidošanu dažādos reģionos. Viens no tiem bija *CSIRT Technical and Operational Development in Latin America and the Caribbean*, kas notika Dominikānas Republikā. Seminārā CERT.LV pārstāvis stāstīja gan par koordinētas ievainojamību ziņošanas aspektiem, CERT.LV praksi un pieeju šajā jomā, gan arī par situāciju Latvijas kibertelpā kopainā. Otrs seminārs, *Workshop on the International Legal Framework for Cybersecurity and EU Cybersecurity Law*, notika Montenegro, kur CERT.LV pārstāvis piedalījās diskusijās gan par labas pārvaldības principu ieviešanu, gan par privātā un publiskā sektora efektīvas sadarbības iespējām kiberdrošības jomā.

Regulāra CERT.LV ekspertu piedalīšanās *EU CyberNet* projekta ikmēneša sanāksmēs. Projekta mērķis – stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniedz iespēju CERT.LV ekspertiem iesaistīties dažādos projektos, stiprināt savas zināšanas un kapacitāti.

Regulāra CERT.LV darbinieku dalība Ziemeļvalstu un Baltijas valstu drošības operāciju centra (Nordic-Baltic SOC) izveides koordinācijas darbā.



7. LIA Drošāka interneta centra ziņojumu pārskats

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2023. līdz 31.12.2023. ir saņēmusi un izvērtējusi 487 ziņojumus. No tiem 195 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 8 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 35 ziņojumos konstatēta personas goda un cieņas aizskaršana, 11 ziņojumi saņemti par naida runu un 4 ziņojumos konstatēti vardarbīgi materiāli.

Par finanšu krāpšanas mēģinājumiem internetā saņemti 124 ziņojumi, 54 ziņojumu saturs nav bijis pretlikumīgs, 56 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 80 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 120 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 uzturētā 71 ziņojuma par bērnu seksuālu izmantošanu saturošiem materiāliem 70 ziņojumi ir dzēsti no publiskas aprites un 1 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un elektronisko sakaru komersantiem.

8. Nākamajā ceturksnī plānotie pasākumi

CERT.LV komanda turpinās efektīvu situācijas uzraudzīšanu kibertelpā, incidentu koordinēšanu un risināšanu, kā arī sabiedrības informēšanu un izglītošanu, attīstot un stiprinot stratēģisko sadarbību ne tikai nacionālajā, bet arī starptautiskajā līmenī.

Uzturot aktīvu sadarbību ar valsts un pašvaldību institūcijām, elektronisko sakaru komersantiem un citām organizācijām un partneriem, CERT.LV turpinās darbu dažādas bīstamības incidentu risināšanā un atbalsta sniegšanā. Tāpat tiks organizētas sanāksmes, konsultācijas un prezentācijas, sniedzot profesionālu atbalstu valsts un pašvaldību institūcijām valsts kiberdrošības sargāšanā.

Izvirzot CERT.LV 2024. gada prioritāros darbības virzienus, 1. ceturksnī plānoti šādi galvenie pasākumi un aktivitātes:

Pakalpojumu attīstīšana un popularizēšana

CERT.LV turpinās mērķtiecīgu darbu, attīstot un popularizējot aktīvās aizsardzības pakalpojumu – DNS ugunsmūris, izstrādājot jaunus aktīvās aizsardzības pakalpojumus, kā arī pilnveidojot un attīstot Sensoru tīkla pakalpojumus vienota un sektorāla apdraudējuma līmeņa noteikšanai, sniedzot maksimālu labumu valsts drošībai no apstrādātās informācijas.

Tāpat 1. ceturksnī tiks uzsāktas mērķtiecīgas aktivitātes drošības operāciju centru jeb CERT.LV operacionālo šūnu (SOC) veidošanai un attīstīšanai, kas būs daļa no visaptveroša, centralizēta kiberdrošības stiprināšanas modeļa valstī.

Lai veicinātu ievainojamību identificēšanu Latvijas valsts un pašvaldību iestāžu IKT resursos un to ziņošanu ievainojamību ziņošanas platformā (cvd.cert.lv.), plānots uzrunāt platformā reģistrēto iestāžu pārstāvjus un rosināt reģistrēt iestāžu programmas ar testējamajiem resursiem, kā arī izveidot drošības pētnieku reitinga tabulu.

Draudu medību operāciju turpināšana

CERT.LV turpinās stiprināt savu lomu kā līdere draudu medību operāciju organizēšanā un vadīšanā Eiropas Savienībā. Attīstot un stiprinot stratēģisko sadarbību ne tikai nacionālajā, bet arī starptautiskajā līmenī, sniedzot savu ieguldījumu NATO kolektīvajā Eiropas aizsardzībā, izstrādājot un pilnveidot draudu medību metodiku, kā arī organizējot pieredzes apmaiņas pasākumus ar sabiedroto valstu partnerorganizācijām.

CERT.LV tehniskās autoritātes atpazīstamības un reputācijas veicināšana

CERT.LV eksperti turpinās regulāri informēt lēmumu pieņēmējus par notikumiem Latvijas kibertelpā. Nodrošinot informāciju sabiedrībai un sniedzot iespēju atskatīties uz būtiskākajiem notikumiem kibertelpā TOP 5 kategorijās, CERT.LV tīmekļa vietnē publicēs ikmēneša pārskatu “Kiberlaikapstākļi”

CERT.LV speciālisti turpinās popularizēt un organizēt “Kiberdrošības galda mācības”. 1. ceturksnī plānotas izspēles ar uzņēmumiem un organizācijām finanšu, veselības, izglītības un sabiedrisko pakalpojumu sektorā. Tāpat CERT.LV speciālisti piedāvās veidot arī individuāli pielāgotus vingrinājumus, kuros pēc klienta vajadzībām tiek pārrunāti aktuālākie jautājumi, kiberuzbrukumu piemēri, procedūras vai atbildības jomas, pēc tam sniedzot kopsavilkumu un rekomendācijas.

Plānota CERT.LV ekspertu dalība kiberdrošības kopienas pasākumos, kā arī regulāra un efektīva ziņapmaiņa ar kiberdrošības kopienu, lai veicinātu sabiedrības izpratni par kiberdrošības un kiberhigiēnas aspektiem.

- Martā CERT.LV plāno organizēt ikgadējo IT drošības semināru “Esi drošs” valsts un pašvaldību iestāžu atbildīgajiem par IT drošību, kā arī citiem interesentiem.
- CERT.LV ir asociētais partneris Aizsardzības ministrijas (AM) īstenotajā projektā *NCC-LV*. CERT.LV īstenos projekta ietvarā uzticētos uzdevumus (piemēram, Kiberdrošības izaicinājums, konference “Kiberšahs

2024”), aktīvi iesaistīsies *NCC-LV* izveidotajā Latvijas kiberdrošības kopienas darbā un sniegs atbalstu AM projekta aktivitāšu īstenošanā.

Starptautiskās sadarbības veidošana un veicināšana

CERT.LV eksperti turpinās pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberdrošības incidentu novēršanas vienībām un starptautiskām organizācijām, sniedzot konsultācijas un atbalstu, uzstājoties ar prezentācijām konferencēs un daloties pieredzē.

No 16. līdz 17. janvārim Briselē, Beļģijā norisināsies NIS direktīvas *22. CSIRTs Network* sanāksme, kurā CERT.LV eksperti dalīsies ar savu ekspertīzi un pieredzi, nodrošinot efektīvu informācijas apmaiņu un sadarbību ar CSIRT kopienu.

No 26. februāra līdz 1. martam Spānijā konferencē *Open Cyber Security Conference* uzstāsies CERT.LV kiberdrošības speciālisti ar prezentācijām *Prototyping a Network Intrusion Detection System: A Deep Dive into CERT.LV's IACS Lab for Safeguarding Critical Infrastructures* un *Defending From the Beast in the East – Multinational Threat Hunting Operations*.

NIS2 direktīvas ieviešana Latvijā

Sekmējot Kiberdrošības pārvaldes reformas mērķu sasniegšanu, tiks ieguldīts darbs pie jauno normatīvo aktu skaidrošanas un vadlīniju sagatavošanas, lai atbalstītu CERT.LV klientūru jauno prasību ieviešanā.

2024. gada 15. janvārī

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:

www.twitter.com/certlv

www.facebook.com/certlv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija