**Informatīvais ziņojums**

**“Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē”**

1. **Ievads**

Aizsardzības ministrija (turpmāk – AM) ir sagatavojusi informatīvo ziņojumu “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē” (turpmāk – informatīvais ziņojums).

Informatīvais ziņojums izstrādāts ar mērķi informēt par koordinētas ievainojamību atklāšanas procesa (turpmāk - KIAP), agrāk apzīmēts arī kā atbildīgas ievainojamību atklāšanas politikas ietvars, ieguvumiem, līdzšinējo KIAP ieviešanas virzību Latvijā, un piedāvāts risinājums KIAP sākotnēji ieviešot valsts pārvaldē. Ziņojumā ir ietverta informācija par Eiropas Komisijas plāniem ieviest KIAP ar priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 (COM(2020) 823 final)[[1]](#footnote-1) (turpmāk – NIS 2 direktīva).

Attīstoties informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) nozarei un pakalpojumiem kļūstot arvien vairāk digitalizētiem, palielinās arī apdraudējumi un iespējamais kaitējums, ko iespējams nodarīt, izmantojot kiberuzbrukumus. Tajā pašā laikā, lai kādi resursi tiktu ieguldīti dažādu IKT sistēmu un infrastruktūras drošībā, jāpieņem, ka tās nekad nebūs 100% drošas un iespējamība atrast ievainojamību pastāvēs vienmēr.

Līdz ar to, informācijas sistēmu un IKT infrastruktūras darbības nodrošināšana, tajās apstrādāto datu aizsardzība un sistēmu noturības veicināšana ir pastāvīgs process, kas jānodrošina visā to dzīves cikla laikā. KIAP ieviešana ir viens no veidiem, kā veicināt ievainojamību meklēšanu un atrašanu, kā arī šo kļūdu novēršanu. Tas ļauj sabiedrībai iesaistīties drošības veicināšanā (ļoti bieži attiecībā uz pakalpojumiem, kurus paši izmanto), bez lielu finanšu līdzekļu piesaistes. Tas ir īpaši nozīmīgs aspekts tādās valstīs kā Latvija, kurai objektīvu iemeslu dēļ nav pieejami lieli resursi kiberdrošībai.

Vienlaikus, NIS 2 direktīvā iekļautais satvars[[2]](#footnote-2) paredz pienākumu dalībvalstīm nacionāli noregulēt KIAP procesu. Attiecīgi arī Eiropas Savienība uz ievainojamību atklāšanas procesu sakārtošanu un koordinēšanu dalībvalstu ietvaros raugās kā uz nozīmīgu risinājumu kiberdrošības stiprināšanai.

1. **KIAP**

Mūsdienu sabiedrībā IKT ir neatņemama ikdienas sastāvdaļa. Tās tiek plaši izmantotas kā saziņā un informācijas ieguvē, tā daudzu citu funkciju īstenošanā un pakalpojumu nodrošināšanā. Valsts pārvaldē daudzas no šīm tehnoloģijām un sistēmām tiek izmantotas un ir vitāli svarīgas sabiedrības un valsts patstāvīgai funkcionēšanai. Palielinoties tehnoloģiju daudzveidībai un skaitam, to savstarpējai atkarībai, arvien grūtāk ir izsekot un novērtēt to atbilstību drošības prasībām. Tāpat digitālā vide nemitīgi attīstītās un drošības risinājumi, kas sniedza aizsardzību vēl nesenā pagātnē, šobrīd var nebūt pietiekami. Sistemātiska drošības nepilnību atklāšana ir dārgs process, kas prasa augsti kvalificētus un labi atalgotus speciālistus, taču to trūkums īpaši jūtams valsts pārvaldē.

Koordinēta ievainojamības atklāšana ir strukturēts process, kurā par ievainojamību tiek ziņots noteiktā kārtībā, dodot iespēju iestādei diagnosticēt un novērst ievainojamību, pirms informācija par ievainojamību tiek izplatīta publiski. KIAP dod iespēju informācijas tehnoloģiju drošības nepilnību atklāšanā iesaistīties ikvienam interesentam, kuram ir attiecīgas zināšanas (ētiskajam hakerim, pētniekam vai sistēmas lietotājam), nosakot iesaistīto pušu tiesības un pienākumus, veicot drošības nepilnību atklāšanu, ziņošanu, novēršanu un informācijas publiskošanu.

**2.1. KIAP citās valstīs**

KIAP ir vēsturiski pazīstams kā *Responsible Disclosure* vai, jaunākos informācijas avotos – arī kā *Coordinated Vulnerability Disclosure*. Pasaules praksē KIAP ir ieviesuši daudzi starptautiski uzņēmumi, kā, piemēram, *Google*, *Microsoft*, *Facebook* u.c., bet īpaši populārs tas ir ASV privātajā sektorā. 2016. gada martā ASV Aizsardzības departaments izziņoja programmu “Uzlauz Pentagonu”[[3]](#footnote-3), kuras ietvaros aicināja hakerus pieteikties dalībai, lai programmas ietvaros varētu pārbaudīt Pentagona kiberdrošību.

Valstiskā līmenī KIAP kopš 2013. gada veiksmīgi darbojas Nīderlandē[[4]](#footnote-4), kur labā prakse no publiskā sektora ir pārņemta arī daudzos privātā sektora uzņēmumos. Nīderlandes KIAP modelis paredz, ka par centrālo valdības resursu ievainojamībām jāziņo Nacionālajam kiberdrošības centram (turpmāk - NCSC). Savukārt, ja ievainojamība konstatēta citos valsts resursos ar vitāli svarīgu funkciju, piemēram, enerģijas un telekomunikāciju sektoros, tad vispirms jāmēģina sazināties ar šīm organizācijām. Ziņojumā NCSC ievainojamība jāapraksta pēc iespējas detalizētāk, lai to var pārbaudīt un novērst, kā arī jānorāda kontaktinformācija tālākai saziņai. Papildus tiek lūgts:

1. par ievainojamību ziņot pēc iespējas ātrāk;
2. par ievainojamību neinformēt citus, kamēr tā nav novērsta;
3. pret savām zināšanām izturēties ar atbildību un neveikt darbības, kas pārsniedz to, kas ir nepieciešams, lai pierādītu ievainojamību.

Tāpat Nīderlandes KIAP aprakstā tiek kopumā paskaidrots, ko atklājējam darīt, ko nedarīt un ko sagaidīt pēc ziņošanas. Nīderlande arī publicējusi vadlīnijas, lai sekmētu visu pušu iesaisti KIAP[[5]](#footnote-5), kas starptautiski tiek uzskatīta par labo praksi, kam seko lielākā daļa KIAP ieviesēju.

Slovākijas nacionālais CERT, sadarbībā ar Nīderlandes NCSC, ir sagatavojis vadlīnijas par KIAP un ziņošanu.[[6]](#footnote-6) Vadlīnijās tiek aicināts ziņot par ievainojamībām nacionālajam CERT, ziņojumā iekļaujot pēc iespējas detalizētāku aprakstu un, iespējams, arī potenciālo risinājumu. Slovākijas KIAP modelī tiek pieļauta iespēja, ka ziņotājs pats nosaka termiņu, kurā ievainojamība jānovērš, pirms tā tiek publiskota, taču tiek uzsvērts, ka labā prakse ir dot 30-90 dienas ievainojamības novēršanai. Vienlaikus, kaut arī Slovākijas nacionālais CERT uzņemas koordinatora lomu ievainojamības novēršanā, katrai iestādei un organizācijai tiek rekomendēts ieviest mehānismus, kā ziņojumus par ievainojamībām apstrādāt.

Savukārt ASV noteikts, ka federālajām izpildaģentūrām jāpublicē ievainojamību atklāšanas politika, kā arī pieļauj, ka nākotnē šī iniciatīva varētu tikt paplašināta nacionālā līmenī.[[7]](#footnote-7) Atšķirībā no Nīderlandes un Slovākijas modeļiem, ASV pieeja neparedz vienas nacionālās iestādes lomu ziņojumu saņemšanā, apstrādē un ievainojamību novēršanas koordinēšanā. Tā vietā, katrai iestādei, ir jāizstrādā savs KIAP saskaņā ar vispārējām vadlīnijām, un Kiberdrošības un infrastruktūras drošības aģentūra jāinformē par ievainojamībām, kas var ietekmēt citas iestādes, vai gadījumos, kad tas var palīdzēt ievainojamības novēršanā.

Par labo praksi attiecībā uz ievainojamību atklāšanas KIAP, t.sk. par izaicinājumiem un rekomendācijām, Eiropas Savienības Kiberdrošības drošības aģentūra (ENISA)[[8]](#footnote-8) jau 2016. gadā publicējusi apkopojumu. Minētajā publikācijā ENISA uzsver, ka kā viens no lielākajiem izaicinājumiem, un reizē arī rekomendācija, uzskatāma nepieciešamība pēc juridiskā ietvara, kas nodrošina, ka ziņošana par ievainojamībām netiek apdraudēta ar iepriekš neparedzētām sekām, kas izriet no civillikuma vai krimināllikuma. Vienlaikus publikācijā uzsvērta nepieciešamība pēc vienotiem un visām iesaistītajām pusēm pieņemamiem principiem, jo secināts, ka pastāv nevienprātība starp to, kā uz ievainojamību atklāšanu raugās atklājēji, kuri biežāk ir ieinteresēti informācijas publicēšanā un kā – resursa uzturētāji, kuri savukārt vēlas informācijas izplatību ierobežot finansiālu, reputācijas u.c. apsvērumu dēļ. Šī iemesla dēļ komunikācija starp abām pusēm var būt sarežģīta, taču to var uzlabot, iesaistot vidutāju, kas primāri vērtētu kopējās sabiedrības intereses. Konkrēti, šī loma ir piemērota CSIRT komandām (*Computer Security Incident Response Team* (Datordrošības incidentu reaģēšanas vienība)), kuras jau nereti aktīvi iesaistās dažādu ievainojamību identificēšanas un novēršanas procesā arī ārpus KIAP.

Tīklu un informācijas sistēmu ievainojamību ļaunprātīga izmantošana var izraisīt būtiskus traucējumus un kaitējumu. Savukārt kiberdrošības riska mazināšanā svarīgi ir šādas ievainojamības ātra apzināšana un novēršana, tāpēc plānotajā NIS 2 direktīvā paredzēts, ka dalībvalstīm jāveicina KIAP ieviešana, ieviešot atbilstošu valsts politiku. Attiecībā uz KIAP īpaši svarīga ir koordinācija starp ziņotājiem un IKT produktu ražotājiem vai pakalpojumu sniedzējiem, un būtu jāievieš nepieciešamās procedūras informācijas saņemšanai no trešajām personām. Direktīvas 6. pants paredz, ka dalībvalstīm būs jāizraugās vienu no savām CSIRT vienībām, lai tā uzņemtos “koordinatora” lomu, nepieciešamības gadījumā darbodamās kā starpnieks starp ziņotāju un IKT produktu ražotājiem vai pakalpojumu sniedzējiem. Direktīva paredz, ka CSIRT koordinatora pienākumos būtu jo īpaši jāiekļauj iesaistīto apzināšana un saziņa ar tiem, atklājēju (ziņotāju) atbalstīšana, ievainojamības atklāšanas termiņu apspriešana un vairāku organizāciju ietekmējošas ievainojamības pārvaldība (vairāku pušu ievainojamības atklāšana / koordinēšana). Ja ievainojamība ietekmē vairākus IKT produktu ražotājus vai pakalpojumu sniedzējus, kas veic darbību vairāk nekā vienā dalībvalstī, izraudzītajam CSIRT no katras skartās dalībvalsts būtu jāsadarbojas ar NIS 2 direktīvas CSIRT tīklu. Šobrīd gan nav prognozējams, kad NIS 2 direktīva tiks apstiprināta un kāda būs normas gala redakcija.

**2.2 KIAP ieviešana Latvijā**

Līdzšinējā gan iestāžu, gan Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV (turpmāk – CERT.LV) pieredze rāda, ka ziņojumi no personām par drošības nepilnībām tiek saņemti aizvien biežāk[[9]](#footnote-9) un Latvijā ir izveidojusies aktīva un kompetenta drošības pētnieku kopiena. Šie pētnieki pārsvarā strādā privātajā sektorā un par Latvijas informācijas sistēmu[[10]](#footnote-10) drošību mēdz pārliecināties gan saistībā ar darba pienākumiem, gan arī citā kontekstā. CERT.LV vairākas reizes ir pieredzējusi situāciju, kad šie pētnieki ir ziņojuši par atrastām kritiskām ievainojamībām un tālāk kopā ar iesaistīto iestādi vai ražotāju ir ticis koordinēts ievainojamību novēršanas process. Tāpat ir bijuši gadījumi, kad pēc ievainojamības novēršanas par to ir arī publicēti raksti vai runāts konferencēs. Kā viens no zināmākajiem piemēriem minama programmatūrā *eParakstītājs* atrastā ievainojamība, kura tika atrasta un novērsta, ievērojot atbildīgas ievainojamību atklāšanas principus.[[11]](#footnote-11) CERT.LV ieskatā, pētnieki, kuri ar CERT.LV sadarbojas regulāri, ir labi informēti par ievainojamības atklāšanas procesa ētisko pusi, sadarbības procesiem, un citām ar KIAP saistītām niansēm. Savukārt, pēc veiksmīgas sadarbības ievainojamības atklāšanā, CERT.LV izsniedz arī pateicības vēstuli par ieguldījumu Latvijas kibertelpas drošībā. Arī privātajā sektorā Latvijā šāda politika jau ilgstoši sekmīgi darbojas, piemēram, banku sektorā – AS “*SEB banka”[[12]](#footnote-12)* un AS “*Swedbank”*[[13]](#footnote-13). KIAP ietvars ļauj iestādēm laicīgi plānot savus resursus un reakciju uz šādiem ziņojumiem.

Skaidri definēts KIAP ietvars ir būtisks arī ievainojamības atklājējam, jo nosaka darbības, kas šai personai jāveic, t.sk., kam informācija par ievainojamību jānodod, nosaka formātu, kādā ziņojums jāstrukturē, kā arī informē par robežām, kurā brīdī labs nodoms var kļūt par likuma pārkāpumu. CERT.LV praksē ir gadījums, kad sistēmas lietotājs atklāja ievainojamības kādā valsts informācijas sistēmā. Lai šīs ievainojamības atklātu un apstiprinātu, drošības pētnieks tam bija veltījis laiku un pūles. Viņš sazinājās ar attiecīgo valsts iestādi, informēja, ka ir atradis ievainojamības un lūdza atlīdzināt (samaksāt) par ieguldīto laiku, norādot, ka informācija par ievainojamībām tiks sniegta tikai pēc atlīdzības saņemšanas. Valsts iestāde atteicās maksāt, iesniedza iesniegumu policijā, pret ievainojamību atklājēju tika ierosināta lieta par izspiešanu, notiek tiesvedība un CERT.LV procesā pieaicināts kā liecinieks. Papildus, valsts iestāde noalgoja ārēju kompāniju, kas veica ielaušanās testu, lai sameklētu potenciālās ievainojamības. Skaidri noteikts KIAP, definējot pieļaujamās darbības un nosakot, kādu pateicību iespējams iegūt, ļautu izvairīties no līdzīgām situācijām.

CERT.LV mēdz saņemt ziņojumus arī no drošības pētniekiem ārpus Latvijas. Piemēram, pieminams gadījums ir studenti no Indijas, no kuriem samērā regulāri tiek saņemti ziņojumi par drošības nepilnībām. Šo ziņotāju mērķis ir uzlabot savu vērtējumu augstskolā. CERT.LV šo pētnieku atsūtīto informāciju pārbauda, un dažos gadījumos tā netiek atzīta par ievainojamību. Visbiežāk šo studentu atklātās nepilnības nav kritiskas, tomēr tās jānovērš, lai novērstu apdraudējumus konkrētajām mājaslapām vai sistēmām. CERT.LV koordinē novēršanu ar iesaistīto iestādi, un procesa noslēgumā izsniedz pateicības vēstuli ziņotājam. Šādi piemēri norāda uz to, ka būtiski, lai informācija par konkrētās iestādes pieņemto KIAP ir pieejama arī ārvalstu pētniekiem kādā no starptautiski izmantotām valodām, piemēram, angļu valodā.

Šobrīd Informācijas tehnoloģiju drošības likuma 6.1 pants regulē rīcību informācijas tehnoloģiju drošības nepilnības (turpmāk — drošības nepilnība) konstatēšanas gadījumā valsts vai pašvaldības institūcijās, informācijas tehnoloģiju kritiskajā infrastruktūrā. Pantā ir ietverta drošības nepilnības definīcija[[14]](#footnote-14) un aprakstīta iesaistīto pušu rīcība. Pēc drošības nepilnības konstatēšanas institūcijai 90 dienu laikā jāveic visas tās novēršanai nepieciešamās darbības, kā arī par konstatēto tūlīt jāinformē kompetento informācijas tehnoloģiju drošības incidentu novēršanas institūciju. Savukārt informācijas tehnoloģiju drošības incidentu novēršanas institūcija, konstatējot drošības nepilnību, par šo faktu tūlīt informē informācijas sistēmas vai elektronisko sakaru tīkla īpašnieku vai tiesisko valdītāju.

Latvijā diskusijas par KIAP ieviešanu normatīvā regulējuma līmenī norisinās jau kopš 2015. gada, kad tā ieviešanu sākotnēji atbalstīja Nacionālā informācijas tehnoloģiju drošības padome. 2016. gadā Aizsardzības ministrija veica darbu pie Informācijas tehnoloģiju drošības likuma grozījumu izstrādes, tai skaitā, pie normu izstrādes, kas paredzētu KIAP ieviešanu Latvijā. Grozījumu mērķis bija sniegt iespēju jebkuram sabiedrības pārstāvim ar zināšanām IT jomā meklēt valsts un pašvaldības iestāžu informācijas sistēmās drošības nepilnības un atklāt tās sistēmas turētājiem, lai nepilnības varētu novērst. Informācijas tehnoloģiju drošības likuma grozījumu izstrādes procesā iebildumus pret KIAP ieviešanu uzturēja Valsts policija un Iekšlietu ministrija, kas norādīja, ka ieviešot KIAP, valsts pavērtu iespēju atsevišķām personām attaisnoti (likuma ietvaros) piekļūt informācijas sistēmai ļaunprātīgos nolūkos un Valsts policija nevarētu viņus saukt pie atbildības, ja tiktu pierādīts, ka sistēma uzlauzta KIAP ietvaros.

Ministru kabineta sēdē 2016. gada 18. oktobrī tika konceptuāli atbalstīti grozījumi Informācijas tehnoloģiju drošības likumā, ar norādi, ka likumprojektam nepieciešams papildu izvērtējums attiecībā uz KIAP pirms tālākas virzības, jo Valsts policija saglabāja iebildumus pret KIAP ieviešanu. Saskaņošanas procesā Aizsardzības ministrijai ar Valsts policiju neizdevās panākt vienošanos par KIAP. Aizsardzības ministrijas ieskatā Valsts policijas piedāvājums reģistrēties visiem, kas veiktu KIAP kārtībā paredzēto ievainojamību meklēšanu, mainītu pēc būtības KIAP pamatdomu – jebkuram ir iespēja meklēt un atklāt drošības nepilnības un par tām ziņot atbildīgajām institūcijām.

Ņemot vērā kompetento iestāžu dažādos viedokļus, Nacionālā informācijas tehnoloģiju drošības padome 2016. gada 4. novembra sēdē atbalstīja normu, par KIAP ieviešanu, izslēgšanu no Informācijas tehnoloģiju drošības likuma grozījumu projekta, ja netiktu panākts saskaņojums starp iesaistītajām iestādēm. Saskaņojums netika panākts, tādēļ Aizsardzības ministrija 2016. gada beigās iesniedza Ministru kabinetā Informācijas tehnoloģiju drošības likuma grozījumu projektu bez KIAP paredzētajiem grozījumiem.

Diskusijas par KIAP ieviešanu tika atsāktas 2018. gadā, un KIAP ieviešana tikusi iekļauta kā īstenojams uzdevums Nacionālās kiberdrošības stratēģijā 2019.–2022. gadam, atsaucoties uz Valsts aizsardzības koncepciju (uzdevums 2.1.). 2020. gadā Aizsardzības ministrija aicināja kompetentās iestādes uz diskusiju, lai vērtētu Informācijas tehnoloģiju drošības likuma grozījumus par KIAP ieviešanu. Sanāksmē būtisks progress attiecībā uz KIAP jautājumu netika panākts. Kaut arī kopumā iestādes pauda atbalstu, joprojām aktuāls ir jautājums par KIAP iesaistīto personu identificēšanu.

1. **Iespējamais KIAP modelis valsts pārvaldē**

Latvijā nav definēts KIAP, tomēr atsevišķi uzņēmumi Latvijā izmanto tā priekšrocības un ievainojamības tiek meklētas un atklātas, un par tām tiek saņemti ziņojumi. Tāpat informācija tiek saņemta par ievainojamībām valsts un pašvaldību institūcijās. KIAP definēšana ir būtiska nevis, lai dotu atļauju ”lauzt sistēmas”, bet lai veidotu vienotu izpratni un regulētu procesu. Vienlaikus ir skaidrs gan tas, ka ievainojamību meklēšanas un atklāšanas procesu nav iespējams apturēt, gan arī tas, ka nevienu IKT produktu nav iespējams izveidot par pilnīgi drošu. Turklāt, ņemot vērā Eiropas Savienības iniciatīvu šajā jautājumā, secināms, ka Latvijā KIAP ieviešana ir laika jautājums. Ievērojot NIS 2 direktīvas priekšlikumā minēto, dalībvalstīm pēc tās apstiprināšanas paredzams, ka būs jānosaka KIAP pamatprincipi, koordinators un jādefinē tā loma KIAP un komunikācijā starp iesaistītajām pusēm.

Ieviešot KIAP, tiktu stiprināta iestāžu kiberdrošība, atklājot un mazinot esošās drošības nepilnības un novēršot to ļaunprātīgu izmantošanu, tāpat KIAP stimulētu valsts un pašvaldību institūcijas pievērst uzmanību savu IKT resursu drošībai (sk. 1. tabulu). KIAP veicinātu pētnieku un augstas kvalifikācijas informācijas tehnoloģiju speciālistu iesaisti, kuri pašreiz neiesaistās KIAP, jo nevēlas piedzīvot situāciju, kad iestāde vēršas pret ziņotāju. Sākotnēji KIAP būtu regulējams valsts pārvaldē, kas varētu veicināt šī procesa plašāku ieviešanu arī Latvijas privātajā sektorā.

|  |
| --- |
| Ieguvumi valstij |
| 1. samazinās kopējās identificēto ievainojamību novēršanas pasākumu izmaksas un palielinās novēršanas pasākumu efektivitāte, īpaši, ja līdzīgas ievainojamības attiecās uz vairākām iestādēm;
2. koordinētā veidā tiek saņemta un reģistrēta informācija par nepilnībām un ievainojamībām, kas dod iespēju apkopot un analizēt datus, tādejādi: 1) iegūstot pilnīgāku informāciju par valsts infrastruktūras/sistēmu/vides ievainojamībām; 2) attīstot spēju iespējami ātri identificēt un novērst liela apjoma uzbrukumus valsts infrastruktūrai;
3. iespēja mazināt reputācijas zaudēšanas riskus;
4. iespēja demonstrēt valsts aktīvu atbalstu infrastruktūras un sistēmu drošības uzlabošanā, kas praksē notiktu, reģistrējot visus ziņojumus un pasakot katram paldies;
5. valsts netiešā veidā veicina IKT drošības ekspertu kopienas veidošanos un pašu pētnieku izaugsmi.
 |
| Ieguvumi iestādei |
| 1. CERT.LV uzņemas koordinējošo lomu un seko līdzi ievainojamību novēršanas gaitai, kā arī sniedz atbalstu ievainojamības ietekmes izvērtēšanā un novēršanas pasākumu identificēšanā un koordinēšanā ar pakalpojumu sniedzējiem;
2. iestāde saņem informāciju par identificētām nepilnībām un ievainojamībām, kas attiecas uz iestādes sistēmām un infrastruktūru;
3. iestādei nav jāapstrādā ievainojamību ziņojumus par sistēmām un infrastruktūru, kas nav tās pārziņā, tādejādi iestādei ir iespēja savus cilvēkresursus novirzīt citu būtisko jautājumu risināšanai;
4. iespēja mazināt reputācijas zaudēšanas riskus;
5. iespēja uzzināt par potenciālajām ievainojamībām no CERT.LV gadījumos, kad par tām ir ziņots citām iestādēm, kas izmanto to pašu infrastruktūru, sistēmas, pakalpojumus vai iekārtas;
6. iespēja sadarboties ar drošības pētniekiem, tādējādi, bez papildu investīcijām, uzlabojot sistēmu un vides drošību;
7. tiek nodrošināts CERT.LV atbalsts iestādes un pētnieka sadarbībai gadījumos, kad: a) nepieciešama ievainojamības detalizēta izpēte; b) pētnieks lūdz iespēju veikt detalizētākas sistēmas/infrastruktūras pārbaudes sava pētījuma vajadzībām.
 |
| Ieguvumi drošības pētniekam |
| 1. visām iestādēm vienādas prasības ievainojamības ziņošanai;
2. ir iespējams vienā paziņojumā norādīt uz vairākām iestādēm vai infrastruktūru kopumā;
3. vienkopus pieejama informācija par to, kuras iestādes piedalās KIAP un kādus resursus tiek rekomendēts testēt;
4. skaidra informācija par to, kur un kam ziņot par atrastajām nepilnībām;
5. informācija par ievainojamību novēršanas gaitu;
6. pateicība par ievainojamības atbildīgu ziņošanu (piemēram, pateicības vēstules);
7. iespēja iekļaut informāciju par atklāto ievainojamību zinātniskajā rakstā/publicēt forumos (ar iestādi saskaņotā apjomā).
 |
| Ieguvumi sabiedrībai |
| 1. valsts sektors rāda priekšzīmi privātajam sektoram un veicina arī privātā sektora atvērtību KIAP jautājumā;
2. brīvprātīga iesaiste šobrīd ļauj pakāpeniski sagatavoties NIS2 direktīvas ieviešanai, kad KIAP kļūs par obligātu;
3. skaidri definēts veids, kā ziņot par drošības nepilnībām, kas palīdz uzlabot saziņu starp ievainojamības atklājēju un valsti, nebaidoties par sodu un nepieciešamību tērēt nesamērīgi daudz laika ziņošanai.
 |

**1. tabula – Apkopojums par ieguvumiem valstij, iestādēm, drošības pētniekiem un sabiedrībai no vienoti koordinēta KIAP ieviešanas.**

CERT.LV galvenā funkcija ir informācijas tehnoloģiju drošības veicināšana Latvijā Informācijas tehnoloģiju drošības likuma ietvaros. Turklāt CERT.LV arī pašreiz ir iestāde, kurai tiek nodota informācija par konstatētajām drošības nepilnībām, vadoties no Informācijas tehnoloģiju drošības likuma 6.1 panta (Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā). Aizsardzības ministrija pauž viedokli, ka Latvijā varētu ieviest modeli, kas satur gan ASV, gan arī Nīderlandes un Slovākijas modeļu elementus, paredzot CERT.LV vidutāja un koordinatora lomu KIAP, savukārt iestāžu dalību nosakot kā brīvprātīgu.

Latvijā Informācijas tehnoloģiju drošības likuma 8. pants nosaka, ka informācijas tehnoloģiju drošības pārvaldību katrā iestādē nosaka tās vadītājs, tādēļ iestādes pārziņā ir noteikt, kā tiek veicināta tās kiberdrošība. Šajā sakarā iestādēm būtu saglabājamas izvēles tiesības iesaistīties KIAP, kā arī noteikt, kurām informācijas sistēmām un resursiem, un ar kādiem ierobežojumiem var veikt drošības nepilnību meklēšanu. Informācija par iesaistīšanos KIAP un vadlīnijas rīcībai, ja tiek atklāta ievainojamība, būtu publicējamas CERT.LV mājas lapā un iestāžu mājas lapā, tādējādi informējot sabiedrību par iesaisti KIAP. Vienlaikus, būtu nepieciešams izveidot centralizētu KIAP sistēmu, kurā CERT.LV, pildot koordinatora lomu, saņem un apstrādā saņemtos ziņojumus par atklātajām ievainojamībām, apkopo un publicē informāciju par iestādēm, kuras iesaistījušās KIAP, kā arī izstrādā mehānismu, kas ļautu iestādēm sazināties ar ievainojamības atklājēju, lai saņemtu papildu informāciju par ievainojamībām. Papildus CERT.LV varētu arī sniegt konsultācijas drošības pētniekiem par testu veikšanu un ierobežojumiem.

Iestādēm, kas iesaistītas KIAP, publicējamajā koordinētas ievainojamības atklāšanas aprakstā būtu jāiekļauj vismaz šāda informācija (paraugs 1. attēlā):

1. Kuras sistēmas un resursus tas aptver;
2. Kāda veida *testus* vai *pārbaudes* drīkst veikt (vai tieši otrādi – noteikt, ko nedrīkst). Vienlaikus, jānosaka, ka ir aizliegts trešajām pusēm atklāt sensitīvus datus, ierobežotas pieejamības informāciju;

Papildus, iestādēm nepieciešams publicēt aprakstu, kā iesniegt ziņojumu par atklāto nepilnību. Aprakstā nepieciešams iekļaut:

* 1. Kur ziņojumu sūtīt (CERT.LV e-pasts);
	2. Kādu informāciju un kā sniegt par ievainojamību, lai to varētu atkārtot un analizēt;
	3. Ziņotāja kontaktinformāciju, paredzot arī anonīmas ziņošanas iespēju.
	4. Informāciju, cik ilgā laikā ievainojamība tiks novērsta un kādās situācijās ar ziņotāju sazināsies, lai iegūtu papildinformāciju vai informētu par termiņa pagarinājumu.

 

**1. attēls – Paraugs informācijai par iestādes iesaisti KIAP un informācija ziņotājam, kā iesniegt ziņojumu par atklāto nepilnību**

Pēc informācijas par ievainojamību saņemšanas:

1. CERT.LV izvērtē saņemto ziņojumu, pārliecinās par ievainojamības esamību. Ja nepieciešams, sazinās ar ziņojuma iesniedzēju un precizē iesniegto informāciju.

2. Ja ievainojamības esamība tiek apstiprināta, CERT.LV koordinē KIAP un iestāde sadarbojas ar CERT.LV, lai nodrošinātu maksimāli efektīvu ievainojamības novēršanu informācijas tehnoloģiju drošības likuma 6.1 pantā noteiktajos termiņos.

* 1. Atkarībā no ievainojamības veida, ietekmētajiem resursiem, iesaistītajiem pakalpojumu sniedzējiem u.c. aspektiem, CERT.LV vienojas ar iestādes KIAP kontaktpersonu par ievainojamības risināšanas darbībām.
	2. CERT.LV uzrauga ievainojamības novēršanas gaitu.
	3. Iestāde, sadarbojoties ar CERT.LV, izvērtē nepieciešamību un apjomu, kādā informēt ziņojuma iesniedzēju, partnerus un klientus par identificēto ievainojamību un tās novēršanas gaitu.

3. Pēc ievainojamības novēršanas informācija par to tiek publiskota, ja tas nepieciešams, un var nest labumu sabiedrībai.

1. Pirms informācijas publiskošanas iesaistītās puses vienojās par to, kad un kādā apjomā tā ir publiskojama.
2. Specifiskos gadījumos var tikt pieņemts lēmums informāciju par ievainojamību nepubliskot. CERT šādā gadījumā informē ziņotāju par iemesliem.
3. Tiek nosūtīta pateicība ievainojamības ziņotājam.

 

**2. attēls – KIAP shematisks attēlojums[[15]](#footnote-15)**

Paredzams, ka ievainojamības joprojām tiks meklētas un atrastas iestāžu IKT infrastruktūrā, taču, ieviešot šādu brīvprātīgu KIAP modeli, iestādēm būtu iespēja demonstrēt savu gatavību pieņemt sabiedrības iesaisti ievainojamību identificēšanā un novēršanā konkrētās iestādes resursos. Turklāt, iesaistoties KIAP, būtu iespēja jau laikus nacionāli veidot NIS2 direktīvā dalībvalstīm paredzēto pienākumu satvaru.

Šādā kontekstā būtiski norādīt, ka ar KIAP netiek plānots attaisnot rīcību, kas radījusi būtisku kaitējumu vai smagas sekas, par ko paredzēta atbildība Krimināllikuma 241. pantā par patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai vai 243. pantā par automatizētas datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju.

1. **Turpmākā rīcība**

Kā jau ticis uzsvērts, ieviešot KIAP, tiktu uzlabota iestāžu kiberdrošība, savlaicīgāk atklājot un mazinot esošās drošības nepilnības un novēršot to ļaunprātīgu izmantošanu, tāpat KIAP veicinātu valsts un pašvaldību institūciju drošības pārvaldības procesu sakārtošanu un sadarbošanos ievainojamību novēršanas risinājumu identificēšanā un ieviešanā. Informatīvā ziņojuma 3. nodaļā ir aprakstīts KIAP modelis, kas ņem vērā iepriekš paustos iestāžu iebildumus, starptautisko praksi un nodrošina NIS 2 direktīvā plānoto pienākumu izpildi, veicinot sabiedrības iesaisti un iestāžu kiberdrošības uzlabošanu.

Pašreiz Informācijas tehnoloģiju drošības likuma 6.1 pants paredzrīcību drošības nepilnības konstatēšanas gadījumā, informācijas tehnoloģiju drošības incidentu novēršanas institūcijas lomu un uzdevumus šo nepilnību novēršanā. Taču, ir nepieciešams valdības lēmums, ka valsts un pašvaldību iestādes var brīvprātīgi pieņemt lēmumu par iesaistīšanos informatīvajā ziņojumā aprakstītajā KIAP modelī un noteikt resursus, uz kuriem KIAP attiecināms. Vienlaikus, Aizsardzības ministrija aicina noteikt, ka:

1. CERT.LV īsteno KIAP koordināciju Latvijā, un iestādēm ir pienākums sadarboties ar CERT.LV ievainojamību atklāšanas un novēršanas procesā (t.sk. jautājumā par informācijas par ievainojamību izplatīšanu citām iestādēm un partneriem);
2. iestādēm, kuras pieņēmušas lēmumu par iesaisti KIAP, par to ir jāinformē CERT.LV, norādot tos iestādes resursus, uz kuriem attiecināms KIAP un kontaktpersonām ar ko sazināties KIAP ietvaros, kā arī jāpublicē šī informācija un informatīvā ziņojuma 3. nodaļā iekļautais KIAP apraksts iestādes mājaslapā;
3. CERT.LV mājaslapā publicē informāciju par iestādēm, kuras informējušas par iesaisti KIAP procesā un norādes uz katras iestādes resursiem, uz kuriem attiecināms KIAP.

Ministru prezidenta biedrs,

aizsardzības ministrs Artis Pabriks

K. Kadeģis, 67335030

karlis.kadegis@mod.gov.lv

1. Pieejams: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN [↑](#footnote-ref-1)
2. Direktīvas 6. pants. [↑](#footnote-ref-2)
3. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe [↑](#footnote-ref-3)
4. https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure [↑](#footnote-ref-4)
5. https://www.enisa.europa.eu/news/member-states/WEB\_115207\_BrochureNCSC\_EN\_A4.pdf [↑](#footnote-ref-5)
6. https://www.sk-cert.sk/wp-content/uploads/2019/10/Vulnerability\_reporting.pdf [↑](#footnote-ref-6)
7. https://cyber.dhs.gov/bod/20-01/ [↑](#footnote-ref-7)
8. https://www.enisa.europa.eu/publications/vulnerability-disclosure [↑](#footnote-ref-8)
9. Informācija par saņemtajiem ziņojumiem par drošības nepilnībām pieejama CERT.LV ceturkšņu atskaitēs, 2020. gadā saņemti 20 pamatoti ziņojumi. [↑](#footnote-ref-9)
10. IP adrešu apgabalā, ko izmanto Latvijā (https://www.nic.lv/lix), vai .lv domēnu vārdu apgabalā. [↑](#footnote-ref-10)
11. https://cert.lv/lv/2016/01/aicinam-atjauninat-eparakstitajs-programmaturu [↑](#footnote-ref-11)
12. https://www.seb.lv/zinosana-par-drosibas-nepilnibam; [↑](#footnote-ref-12)
13. https://www.swedbank.lv/private/d2d/ebanking/authentication. [↑](#footnote-ref-13)
14. Informācijas tehnoloģiju drošības nepilnība ir būtiska informācijas sistēmas vai elektronisko sakaru tīkla izveides, uzturēšanas vai pārveidošanas gaitā tīši vai nejauši radīta sistēmiska vājība, kuras rezultātā var tikt apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte. [↑](#footnote-ref-14)
15. Procesa koncepcija veidota izmantojot ENISA vadlīnijas “Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, Key steps involved in the disclosure of security vulnerabilities”: https://www.enisa.europa.eu/publications/vulnerability-disclosure [↑](#footnote-ref-15)