Valsts un pašvaldību vietņu ievainojamību ziņošana

Sanita Vītola, CERT.LV

«Esi drošs» seminārs

24.03.2022

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Kiberdrošības stiprināšana

2021. gada 14. decembrī pieņemts Informatīvais ziņojums "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē"

- Piedāvā iespējamo KIAP modeli 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) (NIS2 direktīva).

AIM informatīvais ziņojums "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

NIS2 direktīva
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

Koordinētas ievainojamību atklāšanas process

Coordinated vulnerability disclosure

Responsible disclosure

Collaborative disclosure

Pilnīga izpaušana

Neizpaušana

Ieguvumi

Ieviešot KIAP

- tiktu uzlabota iestāžu kiberdrošība, **savlaicīgāk atklājot** un **mazinot** esošās drošības nepilnības un **novēršot** to ļaunprātīgu izmantošanu
- veicinātu valsts un pašvaldību institūciju **drošības pārvaldības procesu sakārtošanu** un **sadarbošanos** ievainojamību novēršanas risinājumu identificēšanā un ieviešanā.

AIM informatīvais ziņojums "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Kā uzzināt par ievainojamības esamību?

- Iestādes darbinieki, pakalpojuma sniedzēji atrod ievainojamību
- CERT.LV atsūta informāciju par informācijas tehnoloģiju drošības pārvaldību atbildīgajai personai
- Sistēmas/resursa lietotājs paziņo par ievainojamību, izmantojot iestādes publiski pieejamo kontaktinformāciju vai CERT.LV
- Atbildīgie par drošību iegūst informāciju profesionālajos forumos un ievainojamību reģistros

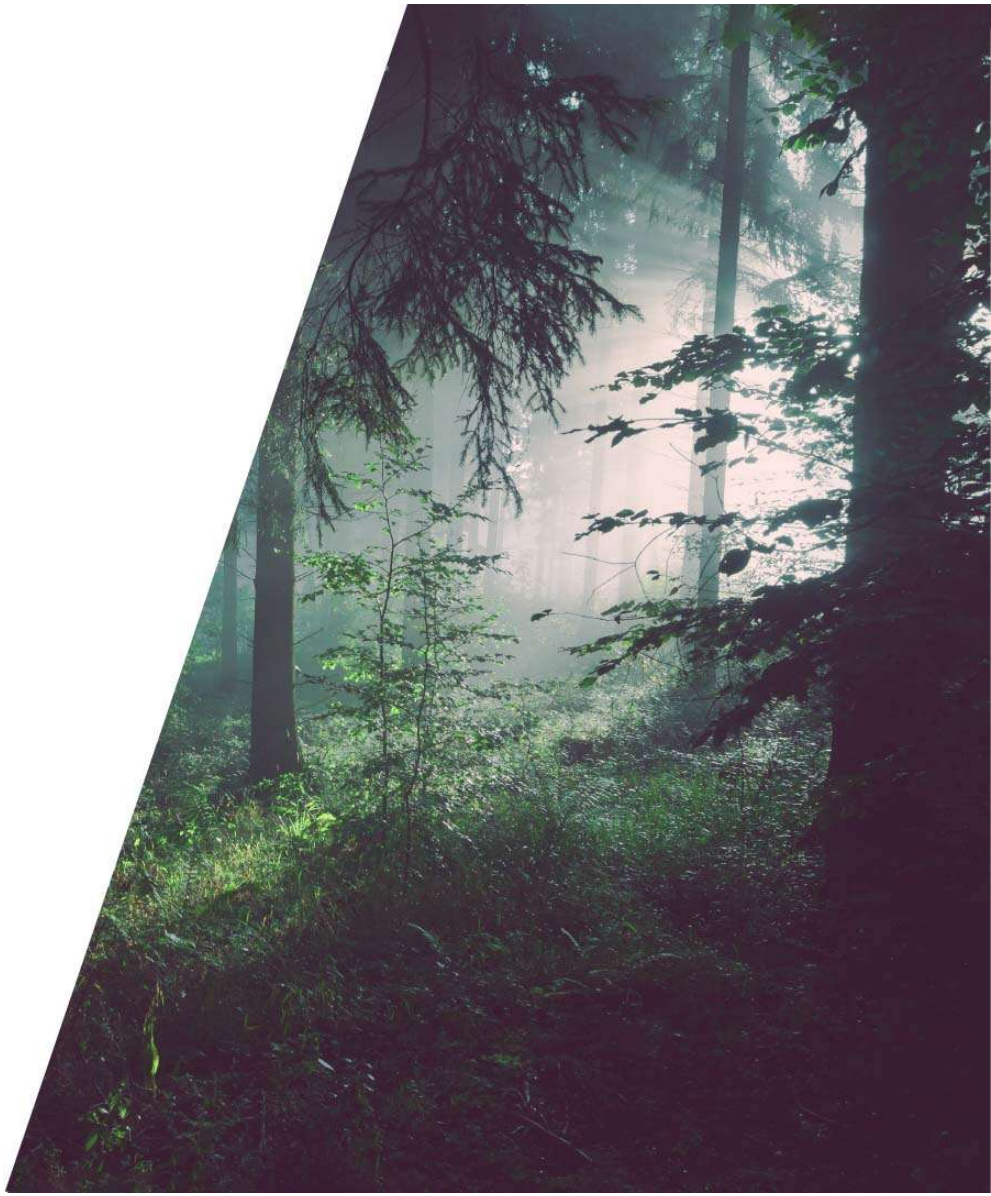
---

- Informācija par ievainojamību parādās sociālajos mēdijos, presē, ziņu portālos u.c.
- Analizējot/izmeklējot incidentu (nepieejamas sistēmas, zaudēti dati, sabojāta reputācija u.c.)

- Būt atvērtiem informācijas saņemšanai. Mazinot gadījumu skaitu, kad ievainojamība ir zināma pētniekiem, tomēr resursa turētājam par to neziņo, lai neradītu sev liekas problēmas

CERT.LV

Identificēta ievainojamība – ko tālāk?



Definīcija

LV **ievainojamība**, EN **vulnerability**

Datu apstrādes sistēmas trūkumi, kas var pazemināt tās drošību draudu gadījumā.

https://termini.gov.lv/atrast/vulnerability/en

Definīcija

‘vulnerability’

means a weakness, susceptibility or flaw of an ~~*asset, system, process or control*~~ ***ICT products or ICT services*** that can be exploited by a cyber threat”

(NIS2 piedāvājums Article 4 (8), tiek precizēta saskaņošanas laikā).

*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 (*NIS2 direktīva) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

Definīcija

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 (ITDL 6.[1])

ITDL - https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums

Novēršana - prasības

(2) Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, konstatējis drošības nepilnību,
90 dienu laikā veic visas tās novēršanai nepieciešamās darbības, kā arī
par konstatēto tūlīt informē kompetento Drošības incidentu novēršanas institūciju. (ITDL 6.[1])

(3) Kompetentā Drošības incidentu novēršanas institūcija,
konstatējusi drošības nepilnību, par šo faktu tūlīt informē informācijas sistēmas vai elektronisko sakaru tīkla īpašnieku vai tiesisko valdītāju.
Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kompetentās Drošības incidentu novēršanas institūcijas noteiktajā termiņā, bet ne vēlāk kā 90 dienu laikā kopš informēšanas brīža veic visas drošības nepilnības novēršanai nepieciešamās darbības. (ITDL 6.[1])

ITDL - https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums

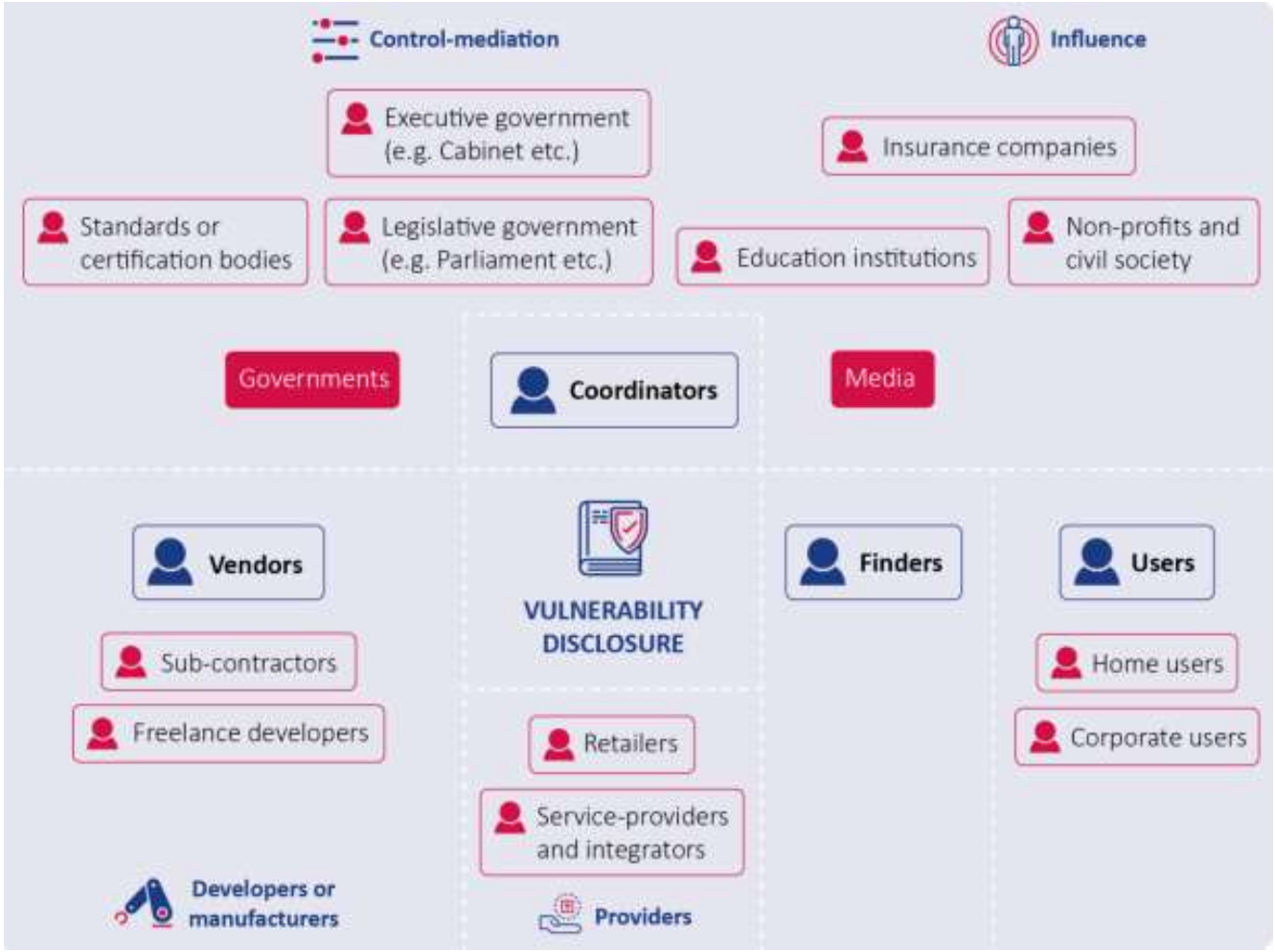
Izaicinājumi

- Atšķirīga izpratne par ievainojamību identificēšanas un ziņošanas procesu
- Atšķirīgas intereses attiecībā uz informācijas publicēšanu
- Atšķirīga izpratne par ievainojamības ietekmi un riskiem

- Izmaksu novērtēšana - novēršanas izmaksas, incidenta izmaksas
- Nevar novērst - nav pieejami nepieciešamie tehnoloģiskie risinājumi, personāls
- Trešā puse nav ieinteresēta iesaistīties ievainojamības novēršanā

- Komunikācija starp iesaistītajām pusēm var būt sarežģīta un radīt konfliktsituācijas

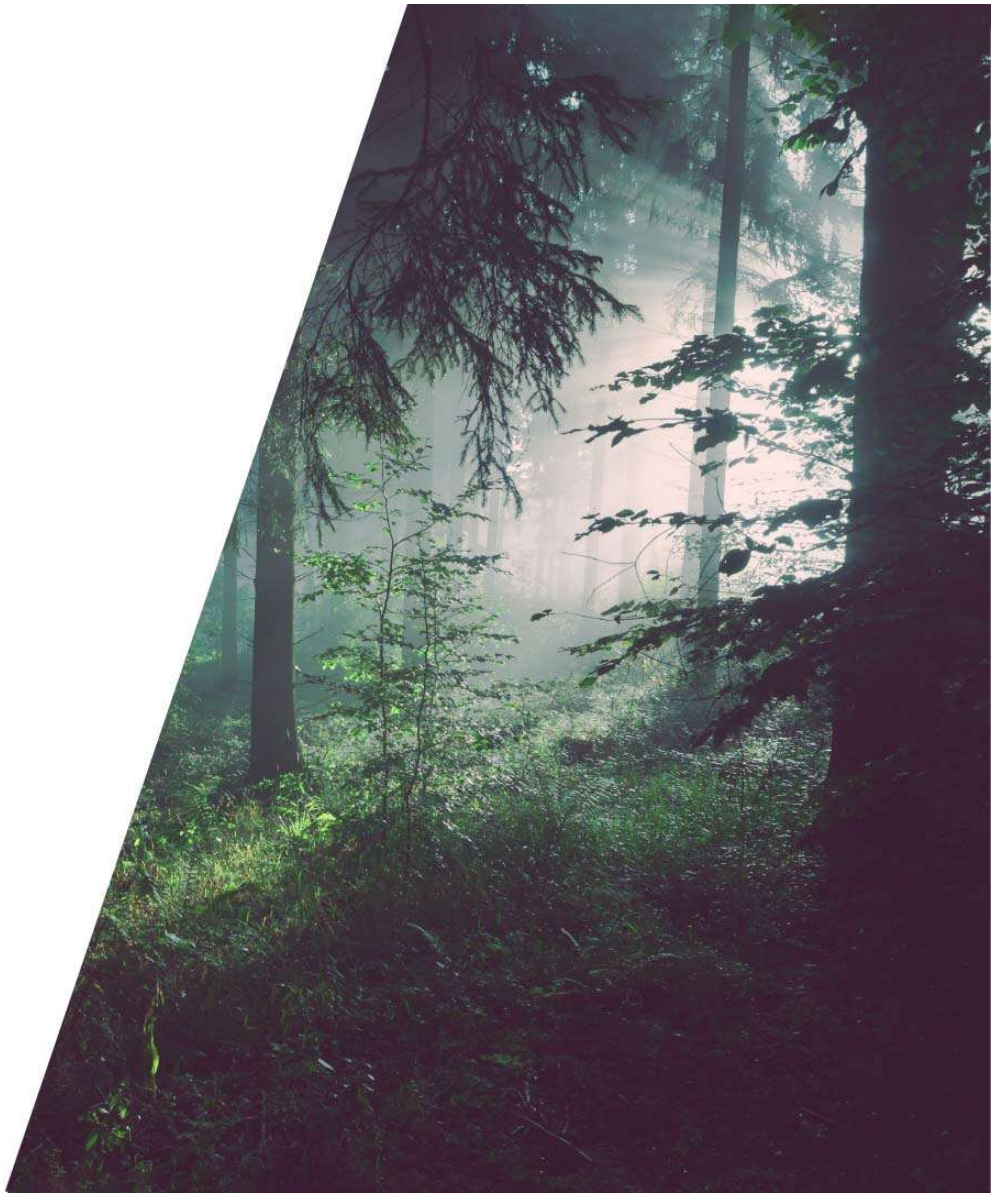
ENISA - ievainojamības atklāšanā iesaistītās puses



Economics of vulnerability disclosure, ENISA
https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

CERT.LV

KIAP ieviešana valsts pārvaldē

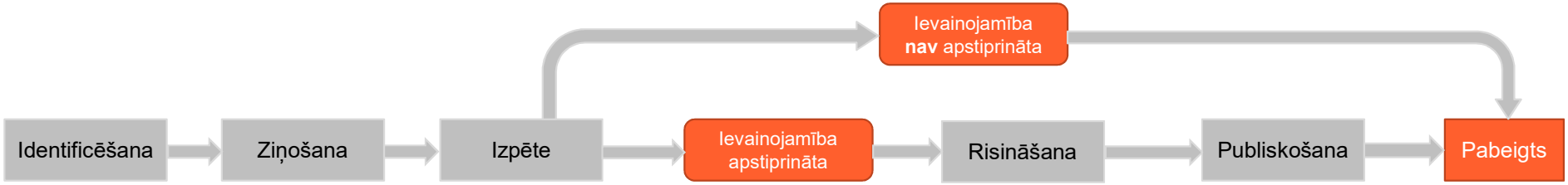


CERT.LV uzdevumi

- CERT.LV īsteno informatīvajā ziņojumā aprakstītajā KIAP koordināciju Latvijā un nodrošina atklātās informācijas par ievainojamību nodošanu konkrētās sistēmas pārzinim.
- CERT.LV mājaslapā publicē informāciju par iestādēm, kuras informējušas par iesaisti KIAP un saites uz katras iestādes resursiem, uz kuriem attiecināms KIAP, kā arī vadlīnijas valsts un pašvaldības iestādēm, kā noteikt resursus, uz kuriem KIAP attiecināms.

AIM informatīvais ziņojums “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Koordinētas ievainojamības ziņošana valsts pārvaldē



Ievainojamības atklājējs saglabā iespējami daudz pierādījumu par identificēto sistēmas darbības/pakalpojumu infrastruktūras neatbilstību/ ievainojamību.

Ievainojamības atklājējs vai viņa pārstāvis informē iestādi un/vai CERT par identificēto ievainojamību, nosūtot ievainojamības ziņojumu uz mājaslapā norādīto KIAP kontaktadresi.

CERT.LV vienas dienas laikā nosūta apstiprinājumu par ziņojuma saņemšanu.

CERT.LV pārliecinās, vai Iestāde ir saņēmusi ziņojumu.

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

CERT.LV koordinē KIAP un Iestādes sadarbojas ar CERT, lai nodrošinātu maksimāli efektīvu ievainojamības novēršanu.

Atkarībā no ievainojamības veida, ietekmētajiem resursiem, iesaistītajiem pakalpojumu sniedzējiem u.c. aspektiem, CERT.LV vienojas ar Iestādes KIAP kontaktpersonu par ievainojamības risināšanas darbībām.

CERT.LV uzrauga ievainojamības novēršanas gaitu.

Iestāde, sadarbojoties ar CERT.LV, izvērtē nepieciešamību un apjomu, kādā informēt partnerus un klientus par identificēto ievainojamību un tās novēršanas gaitu.

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

Tiek nosūtīta pateicība ievainojamības ziņotājam.

Pirms informācijas publiskošanas iesaistītās puses vienojās par to, kad un kādā apjomā tā ir publiskojama.
Specifiskos gadījumos var tikt pieņemts lēmums informāciju par ievainojamību nepubliskot.
CERT.LV šādā gadījumā informē ziņotāju par iemesliem.

AIM informatīvais ziņojums “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Brīvprātīga iesaistīšanās KIAP

Valsts un pašvaldību iestādes var

- brīvprātīgi pieņemt lēmumu par iesaistīšanos KIAP
- noteikt resursus, uz kuriem KIAP attiecināms
- noteikt KIAP prasības katram resursam – kas ir/kas nav atļauts
- jebkurā brīdī apturēt atļauju testēt savus resursus
- lemt, vai nepieciešams iesaistīt CERT.LV un noteikt kāda palīdzība ir nepieciešama, sadarbojoties ar citām iesaistītajām pusēm
- noteikt prasības informācijas publiskošanai

AIM informatīvais ziņojums "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Brīvprātīga iesaistīšanās KIAP

Pirms iesaistīties KIAP:

- apzināt iekšējo kapacitāti apstrādāt ziņojumus
- izvērtēt, kurus resursus iekļaut KIAP, piem., Iestādes vietņu ievainojamību ziņošanu
- pārliecināties, ka KIAP resursam nodrošināta atbilstība drošības prasībām (MK442), ir pietiekams tehnoloģiskā personāla atbalsts, un tiek veiks notikumu monitorings un veidoti auditācijas pieraksti (notikumu izmeklēšanas vajadzībām)

AIM informatīvais ziņojums “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Pienākumi

Iestādēm, kuras pieņēmušas lēmumu iesaistīties KIAP

- jāinformē CERT.LV, norādot
    - iestādes resursus, uz kuriem attiecināms KIAP
    - kontaktpersonas, ar ko sazināties KIAP ietvaros
- iestādes mājaslapā jāievieto informācija par iesaisti KIAP, tai skaitā iekļaujot nosacījumus drošības pētniekiem
- ir pienākums sadarboties ar CERT.LV ievainojamību atklāšanas un novēršanas procesā

AIM informatīvais ziņojums “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Ziņojumu apstrādes vide

KIAP platforma

- Atbalsta efektīvu, pārskatāmu ziņojumu apstrādi un iesaistīto pušu sadarbību
- Pieejama tiešsaistē 24/7
- Izstrādāšana, ieviešana, uzturēšana: CERT.LV
- Lietotāju atbalsts: CERT.LV

- Nākotnē:
  - iespēja izmantot NIS2 iekļautajiem uzņēmumiem
  - datu apmaiņa ar Eiropas Savienības reģistriem, sadarbības partneriem
  - ...

CERT.LV piedāvātā dokumentācija

- KIAP apraksts iestādēm.
- KIAP shēma iestādēm
- KIAP vadlīnijas iestādēm
- KIAP vadlīnijas ziņotājam (LV, EN)
- KIAP platformas/portāla lietošanas instrukcija

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, tādējādi 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.

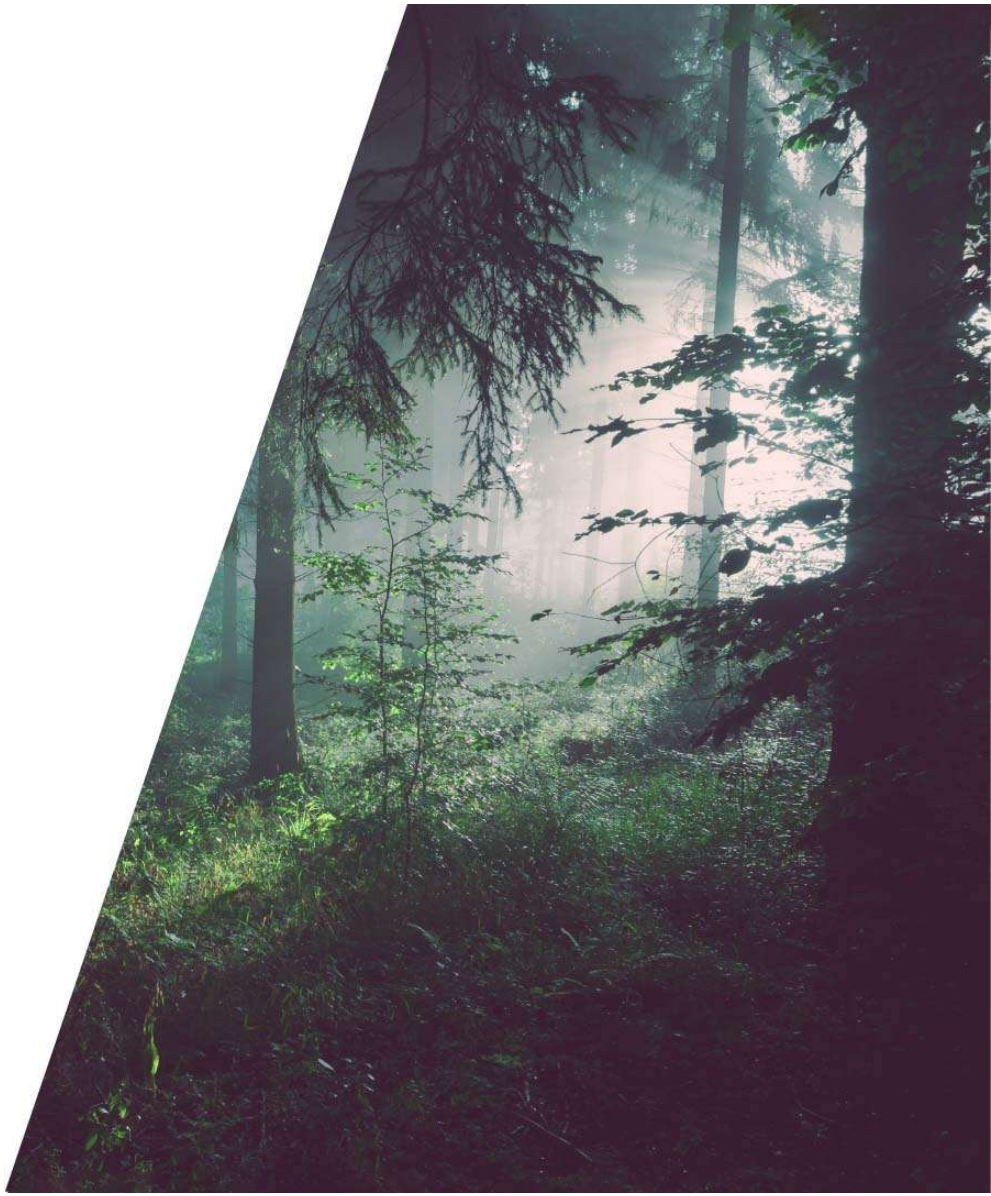
AIM informatīvais ziņojums “Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē
https://tapportals.mk.gov.lv/legal_acts/b7ee2e30-a7bd-4433-9592-57e6c884b0f7

Nākamie soļi

- dokumentācijas izstrāde - CERT.LV - procesā, Q2
- platformas izstrāde - CERT.LV – procesā, Q2/Q3
- pirmie dalībnieki/testētāji - iestādes un pētnieki - Q2

CERT.LV

Vai piedalīsies?



CERT.LV

Paldies!

cert@cert.lv
sanita.vitola@cert.lv

certlv

certlv