SAEIMAS AIZSARDZĪBAS, IEKŠLIETU UN KORUPCIJAS NOVĒRŠANAS KOMISIJAS

IEKŠĒJĀS DROŠĪBAS APAKŠKOMISIJAS

SĒDES PROTOKOLS

**Nr. 141.1.9/6/2-2-14/23**

**2023. gada 7. martā plkst. 13.00**

**Rīgā, Jēkaba ielā 16, komisijas sēžu zālē**

**Videokonference attiecībā uz uzaicinātajiem**

**Sēdē piedalās:**

apakškomisijas locekļi:

**Edvīns Šnore** – apakškomisijas priekšsēdētājs

**Jānis Skrastiņš** – apakškomisijas sekretārs

**Igors Rajevs**

**Aleksejs Rosļikovs**

**Uģis Rotbergs**

**Andrejs Vilks**

**Edmunds Zivtiņš**

Aizsardzības, iekšlietu un korupcijas novēršanas komisijas deputāts **Ainars Latkovskis**

Uzaicinātie:

* Aizsardzības ministrijas parlamentārais sekretārs **Jānis Eglīts**
* Aizsardzības ministrijas Kiberdrošības politikas departamenta direktors **Edgars Kiukucāns**
* Valsts prezidenta padomniece informatīvās telpas un digitālās politikas jautājumos **Ieva Ilvesa**
* CERT.LV vadītāja **Baiba Kaškina**
* Vides aizsardzības un reģionālās attīstības ministrijas parlamentārā sekretāre **Agnese Geduševa**
* Vides aizsardzības un reģionālās attīstības ministrijas valsts sekretāra vietnieks **Gatis Ozols**
* Satiksmes ministrijas Drošības politiku koordinācijas nodaļas vecākais referents **Artūrs Veselis**
* Valsts policijas Kibernoziegumu apkarošanas pārvaldes priekšnieka vietnieks **Jevgeņijs Zujevs**
* MilCERT pārstāvis
* Satversmes aizsardzības biroja pārstāvis
* Latvijas Valsts radio un televīzijas centra pārstāvis
* Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas (LIKTA) eksperti **Artūrs Filatovs** un **Kirils Teniševs**
* SIA Tet valdes loceklis, Galvenais tehnoloģiju direktors **Dmitrijs Ņikitins**
* SIA Tet TD Datu aizsardzības un IT risku nodaļas vadītājs **Uldis Lībietis**
* Drošības un aizsardzības industriju federācijas (DAIF) pārstāvis **Aleksandrs Orlovs**

**Komisijas darbinieki: vecākā konsultante Ieva Barvika un konsultante Inese Silabriede**

**Sēdi vada**: E.Šnore

**Sēdi protokolē**: I.Silabriede

**Sēdes veids**: atklāta

*Izskatāmie materiāli:*

*Aizsardzības ministrijas prezentācija “Kiberdrošības aktualitātes Latvijā”, 07.03.2023.;*

**Darba kārtība:**

# Kiberdrošība: aktuālais stāvoklis un valsts gatavība.

**E.Šnore** atklāj sēdi, informē par jautājuma aktualitāti. Dod vārdu atbildīgās Aizsardzības ministrijas (turpmāk – AM) pārstāvjiem.

**J.Eglīts** demonstrē prezentāciju *(prezentācijas materiāls – protokola pielikumā)* un informē par kiberdrošības aktualitātēm AM redzējumā. J.Eglīts akcentē, ka kiberdrošības situācija valstī ir stabila; pārskatāmajā laika periodā ir notikuši vairāki kiberuzbrukumi, bet bez būtiskām sekām. Tomēr mums ir jābūt gataviem situācijai, kad kāds kiberuzbrukums var izdoties, un pēc tam būs jānovērš tā izraisītās sekas. Īsumā raksturo aktualitātes Latvijas kibertelpā, norāda uz iestāžu nepieciešamību vairāk pievērst uzmanību savas IKT sistēmas kiberdrošībai. Uzsver, ka notiek palielināta tīklu skenēšana un ievainojamības meklēšana, kā arī DDoS uzbrukumi valsts pārvaldes resursiem un privātā sektora pakalpojumu sniedzējiem. Informē par galvenajiem šī laika izaicinājumiem sniedz īsu katra izaicinājuma raksturojumu:

- sistēmu ilgtermiņa uzturēšana un attīstība – nepieciešamība pilnveidoties, lai novērstu kiberuzbrukumu izdošanos nākotnē;

- nepieciešamība pilnveidot normatīvo regulējumu – īpaši Ministru kabineta (turpmāk – MK) noteikumus Nr. 442);

- kvalificēta IKT drošības personāla trūkums;

- neregulāra un fragmentēta uzraudzība – šobrīd nevienai iestādei nav tiesības noteikt sankcijas par esošo prasību neievērošanu.

J.Eglīts informē par 2022. gadā kiberdrošības jomā paveikto:

- AM informatīvais ziņojums MK kiberdrošības sistēmas reformas uzsākšanai, kas ir pamatā pozitīvam MK lēmumam par kiberdrošības pārvaldības uzsākšanu;

- valsts informatīvo sistēmu (VIS) drošības prasību izvērtēšana pirms projektu uzsākšanas, arī AM piedalās šajā vērtēšanā. Jaunie noteikumi šobrīd atrodas izstrādes procesā;

- paplašināts CERT.LV sensoru tīkls, pēc 2022. gada 24. februāra novērojama arvien lielāka vēlme tos uzstādīt;

- veiksmīgas draudu meklēšanas operācijas sadarbībā ar starptautiskajiem partneriem;

- palielināts DDoS aizsardzības pārklājums, palielinājusies interese par šo AM bezmaksas nodrošināto bezmaksas pakalpojumu;

- nosūtītas rekomendējošas vēstules ministrijām u.c. institūcijām par nepieciešamību nodrošināt savu informācijas sistēmu drošību, nākotnē veikt to monitoringu.

Informē par 2023. gadā paveicamajiem būtiskajiem uzdevumiem kiberdrošībā:

- turpināt darbu pie normatīvā regulējuma pilnveides – NIS2 Direktīvas ieviešana, atbilstoši grozījumi MK noteikumos Nr. 442 un ar šo jautājumu saistītos citos MK noteikumos;

- Nacionālā kiberdrošības centra (turpmāk – NKDC) izveide, papildu personāla piesaiste jauno uzdevumu izpildei;

- uzraudzības sistēmas izveide, kura centrā ir jaunais NKDC, kas cieši sadarbojas ar Satversmes aizsardzības biroju (turpmāk – SAB). Turpmāk kiberdrošības uzraudzība būs SAB pārziņā;

- turpināsies plānveida draudu meklēšanas operācijas visā valsts sektorā un kritiskajā infrastruktūrā.

J.Eglīts informē par NKDC izveidi un tā plānotajām funkcijām. Šis centrs sadarbībā ar SAB plānots kā valsts kiberdrošības kodols. Centra funkcijas:

- valsts kiberdrošības politikas veidošana un uzraudzība;

- valsts IKT minimālo drošības prasību ievērošanas uzraudzība;

- NIS2 direktīvas ieviešana un strukturēta prasību uzraudzība. NIS2 direktīvas mērķis ir izveidot visām ES valstīm vienādu kiberdrošības līmeni un izstrādāt plānus šī mērķa sasniegšanai, problēmu novēršanai un sodīšanai par direktīvas neieviešanu;

- kiberdrošības incidentu risināšana;

- drošības operāciju centri valsts koplietošanas datu centros;

- Eiropas Kiberdrošības kompetenču centra (ECCC) Latvijas NKC.

Raksturo būtisko Kiberdrošības stratēģijā 2023.-2026. gadam. Nemainīgi paliek lielie virzieni:

- kiberdrošības pārvaldības pilnveidošana;

- kiberdrošības veicināšana un izturētspējas stiprināšana;

- sabiedrības izpratne (svarīgi), izglītība un pētniecība;

- starptautiskā sadarbība un tiesiskums kibertelpā;

- kibernoziedzības novēršana un apkarošana.

Kā jaunus un būtiskus stratēģijas elementus J.Eglīts atzīmē un īsumā raksturo katru no tiem:

- jauno pārvaldības modeli;

- publiskā-privātā sektora sadarbības uzlabošanu;

- vienotas kiberhigiēnas vadlīnijas;

- kiberdrošības pratības veicināšanu un izglītošanas veicināšanu;

- plašāku kiberelementu izspēli teorētiskā un praktiskās mācībās (pišinga atklāšana, piem.).

Nobeigumā J.Eglīts iezīmē jomas, kurās valstī ir vieta tālākai kiberdrošības izaugsmei:

- plašāka pentestu izmantošana;

- plašākas draudu meklēšanas operācijas (varbūt speciāla aprīkojuma iegāde);

- regulāras diskusijas MK ietveros par iespējām uzlabot sistēmu;

- jomas speciālistu piesaiste (likums ļauj speciālistiem maksāt atbilstoši);

- drošības pārvaldnieku standarts (vienots IT drošības standarts visām valsts pārvaldes iestādēm);

- SOC + plašāka telemetrijas datu apkopošana (draudu meklēšana darbinieku tīklos).

**E.Šnore** dod vārdu CERT.LV pārstāvjiem.

**B.Kaškina** īsumā raksturo situāciju kiberdrošībā pagājušajā gadā CERT.LV skatījumā. Ir būtiski palielinājies incidentu skaits kibertelpā, apm. 4 reizes. Notiek laba atbildīgo institūciju sadarbība draudu gadījumā, piekļuves lieguma nodrošināšana. Salīdzinājumā ar citām Eiropas valstīm esam labā līmenī. Iezīmē raksturīgākos Krievijas grupējumu finansētos kiberuzbrukumus gan valsts iestādēm (mēģinājumi kompromitēt informācijas piegādes ķēdes – 5 gadījumi), gan arī koordinēti uzbrukumi kritiskās infrastruktūras objektiem un komerciāli motivēti noziegumi. Pagājušo gadu raksturo kā karstāko visā CERT.LV pastāvēšanas vēsturē, kā arī atzīmē, ka iestādēm pietika kapacitātes šos apdraudējumus laicīgi novērst.

Šogad arvien vēl mēs esam interesants uzbrukumu mērķis gan Krievijas, gan Baltkrievijas noziedzīgajām kiberaktivitātēm. Palielinās arī aktivitātes no Ķīnas puses, tas var paplašināties. DDoS uzbrukumi notiek, bet bez ietekmes. Ir laba sadarbība ar starptautiskajiem partneriem no ASV un Kanādas. Valsts gatavība kopumā nav pietiekama, problēmas var atrast gandrīz visās institūcijās. Uzsver, ka atkopšanās no kiberuzbrukumiem ir ilgstošs process; tas jāņem vērā, nepieciešama operatīva rīcība. Kā pozitīvu atzīmē DDoS aizsardzību, kuru nodrošina Latvijas Valsts radio un televīzijas centrs (LVRTC) un SIA Tet.

Gada laikā ir arī dubultojies Kiberaizsardzības vienības lielums – no 100 uz 200 cilvēkiem.

**Deputātu jautājumi**

**E.Šnore** vēlas plašāku komentāru par Krievijas valsts un aktīvistu grupu sponsorētajiem kiberuzbrukumiem.

**B.Kaškina** informē par zināmajām Krievijas aktīvistu grupām saistībā ar kiberuzbrukumiem Latvijas valsts iestādēm. Latvija ir viena no uzbrucēju galvenajiem mērķiem, jo sniedz būtisku palīdzību Ukrainai. Ir arī Krievijas valsts dienestu gatavoti kiberuzbrukumi (Turla, Gamaredons u.c.).

**E.Šnore** interesējas, vai ir arī organizētas darbības kibervidē no Latvijas valsts iekšienes. Atzīmē saiti “Army.lv”.

**B.Kaškina** apliecina, ka ir tādas PC adreses, par tām tiek ziņots valsts drošības iestādēm.

**E.Šnore** interesējas par minētajām Ķīnas aktivitātēm, vēlas plašāku komentāru, kā arī aktualizē pēdējā laika TikTok kontekstu.

**B.Kaškina** raksturo dažādu kategoriju apdraudējumus saistībā ar TikTok: privātuma apdraudējums, iespēja profilēt lietotāju un pielāgot viņam saturu (saistība ar Ķīnu), iespēja piegādāt ļaunatūru, lai inficētu ierīci. Šie riski būtiski neatšķiras no citiem sociālajiem tīkliem, būtiska ir saistība ar Ķīnas valdību. Atgādina par CERT.LV brīdinājumiem iestādēm šajā sakarībā jautājumā par darbā izmantojamām ierīcēm.

**I.Ilvesa** sniedz papildu informāciju kiberdrošības jautājumā. Atzīmē, ka CERT.LV darbs tiek starptautiski augstu novērtēts, mēs esam konkurētspējīgi. Akcentē būtisko saistībā ar NKDC darbību perspektīvā, agresīva un skrupuloza informatīvā darba nepieciešamību. Atzīmē arī finansējuma jautājumu, nepieciešamību kiberdrošībā ieguldīt lielākus valsts budžeta līdzekļus. Izsaka viedokli arī par ES naudas izmantošanas jautājumiem: ES līdzekļi tiek ieguldīti kāda jauna tehnoloģiskā risinājuma izveidei, bet tas nestrādā ilgtermiņā, jo arī vēlāk ir vajadzīgs finansējums šī risinājuma uzturēšanai. Finansējums ir kritisks.

**E.Šnore** interesējas par NKDC, vai centra finansējums ietverts aizsardzības budžetā. Jautājumā par NIS2 direktīvas ieviešanu vēlas zināt, kas mums vēl šajā jomā jāpaveic.

**J.Eglīts** uzsver finansējuma jautājuma svarīgumu, piekrīt I.Ilvesas norādītajiem aspektiem. NKDC ir ietverts aizsardzības budžetā. Jautājumā par NIS2 direktīvu J.Eglīts uzsver nepieciešamību direktīvas prasības ietvert nacionālajā likumdošanā un MK noteikumos. Atzīmē arī sodu jautājumu. Šobrīd nav kritisku punktu NIS2 direktīvas prasību ieviešanā.

**B.Kaškina** papildina informāciju par NKDC, valsts budžeta aspektu centra izveidē. Jautājumā par NIS2 direktīvas ieviešanu kā būtisku norāda faktu, ka palielināsies uzraugāmo iestāžu loks, kā arī pastiprināsies kiberuzraudzības prasības, tās būs stingrākas un konkrētākas. Direktīvas ieviešanai atvēlēts laiks līdz 2024. gada oktobrim, ir sistemātiski pie tā jāstrādā.

**J.Skrastiņš** vēlas papildu informāciju par NKDC un CERT.LV korelāciju.

**B.Kaškina** informē, ka NKDC veido departaments AM, kopā ar CERT.LV, tas nodrošina visas nepieciešamās kompetences. CERT.LV paliek esošajā struktūrā Latvijas Universitātes Matemātikas un informātikas institūta sastāvā.

*Notiek diskusija par kiberdrošības aktualitātēm saistībā ar NKDC izveidi un finansējuma pietiekamību tā uzturēšanas izmaksām. Jautājumus un viedokļus izsaka* ***E.Šnore****,* ***E.Kiukucāns****,* ***B.Kaškina****,* ***I.Rajevs****,* ***I.Ilvesa****,* ***J.Eglīts****.*

**E.Šnore** apkopo uzklausīto informāciju, aicina AM un CERT.LV pārstāvjus arī turpmāk informēt komisiju par nozares aktualitātēm.

**E.Šnore** pateicas par dalību un slēdz sēdi.

Sēde pabeigta plkst. 14.00

Apakškomisijas priekšsēdētājs E. Šnore

Apakškomisijas sekretārs J. Skrastiņš

Protokolētāja I.Silabriede