29.10.2024.

BIEŽĀK UZDOTIE JAUTĀJUMI

Aizsardzības ministrijas Kiberdrošības politikas departaments ir apkopojis biežāk uzdotos jautājumus par Nacionālā kiberdrošības likuma (NKDL) piemērošanu. Dokuments tiks aktualizēts pēc Ministru kabineta noteikumu Par minimālajām kiberdrošības prasībām pieņemšanas.

SUBJEKTU PAŠIDENTIFIKĀCIJAS JAUTĀJUMI

1. **Kā var pārliecināties par atbilstību NKDL statusam?**

A: Aicinām izmantot izstrādāto interaktīvo rīku - testu, kas palīdzēs noteikt, vai NKDL izpratnē esat uzskatāms par NKDL subjektu un vai uz Jūsu pārstāvēto organizāciju attiecas NKDL normas. Ja pēc testa aizpildīšanas nav iegūta pārliecība par atbilstību vai rodas papildu jautājumi, aicinām sazināties ar NIS2 kontaktpunktu: NIS2@mod.gov.lv

2. **Vai iestāde var vienlaikus būt gan būtisko, gan svarīgo pakalpojumu sniedzējs, gan IKT kritiskās infrastruktūras turētājs?**

A: Kaut arī iestāde var atbilst vairākām NKDL subjekta kategorijām, kā atbilstošo nosaka augstāko.
Gadījumā, ja attiecībā uz pakalpojuma sniedzēju vienlaicīgi izpildās būtisko pakalpojumu sniedzēja un svarīgo pakalpojumu sniedzēja pazīmes, šāds pakalpojuma sniedzējs NKDL izpratnē uzskatāms par būtisko pakalpojumu sniedzēju. Piemēram, valsts dibināta augstskola, kas vienlaikus ir atvasināta publiska persona un izglītības informācijas sistēmas uzturētājs, NKDL izpratnē uzskatāma par būtisko pakalpojumu sniedzēju, savukārt šīs augstskolas dibinātās pastarpinātās pārvaldes iestādes (piemēram, zinātniskie institūti), kā arī subjekti, kas uztur augstskolas izglītības informācijas sistēmas (piemēram, privāto tiesību juridiskā persona - izglītības informācijas sistēmas ārpakalpojuma sniedzējs), uzskatāmi par svarīgo pakalpojumu sniedzējiem.

Augstāk minētājos gadījumos NKDL subjektu uzraudzību veic Aizsardzības ministrija. Savukārt ja uzņēmums ir būtisko pakalpojumu sniedzējs, bet tā valdījumā ir IKT kritiskā infrastruktūra, tam piemēro IKT kritiskajai infrastruktūrai noteiktās prasības un tā uzraudzību veic SAB.

3. **Vai starptautiska uzņēmuma filiāle Latvijā var būt NKDL subjekts?**

A: Ja uzņēmuma tiesiskā formā ir filiāle, tā attiecīgi nav juridiska personas un uz to nav attiecināmas NKDL prasības.

4. **Kas uzraudzīs uzņēmuma kiberdrošību, ja tā valdījumā ir sistēma, kas ir IKT KI?**

A: Šādā gadījumā uzraudzību veiks Satversmes aizsardzības birojs.

5. **Vai visi vidējas saimnieciskās darbības veicēji, kuri uztur tiešsaistes tirdzniecības vietu, ir tiešsaistes tirdzniecības vietas pakalpojumu sniedzēji saskaņā ar NKDL?**

A: Nē, saskaņā ar NIS2 Direktīvu un Negodīgas komercprakses aizlieguma likumu, tiešsaistes tirdzniecības vieta ir pakalpojuma sniegšanas vieta, izmantojot programmatūru, tostarp tīmekļa vietne, tīmekļa vietnes daļa vai lietotne, ko uztur komercprakses īstenotājs vai kas tiek uzturēta komercprakses īstenotāja vārdā un kas ļauj patērētājiem slēgt distances līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai patērētājiem. Attiecīgi tiešsaistes

tirdzniecības vietas pakalpojumu sniedzējs ir tikai tādas platformas uzturētājs, kurā patērētājam ir iespēja slēgt līgumus ar citiem pārdevējiem, pakalpojumu sniedzējiem vai citiem patērētājiem, nevis ar pašu interneta vietnes uzturētāju.

SODI

6. Kā soda valsts iestādes par neatbilstībām? Vai valsts iestāžu vadītājiem neatbilstību gadījumā piespriestu naudas sodu?

A: Attiecībā uz valsts iestāžu vadītājiem neatbilstību gadījumā netiek piemērots naudas sods. Ja NKDL subjekts, kurš ir tiešās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par šo neatbilstību ziņo attiecīgajam Ministru kabineta loceklim. Šādā gadījumā Ministru kabineta loceklis izvērtē nepieciešamību ierosināt disciplinārlietu un lemj par turpmāko rīcību neatbilstības novēršanai, savukārt atbildīgais Ministru kabineta loceklis par neatbilstības novēršanas gaitu ziņo Ministru kabinetam. Ja NKDL subjekts, kurš ir pašvaldība vai pašvaldības dibināta pastarpinātās pārvaldes iestāde, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par šo neatbilstību ziņo attiecīgās pašvaldības domes priekšsēdētājam, kuri lemj par pašvaldību institūciju un amatpersonu (darbinieku) atbildību Pašvaldību likumā noteiktajā kārtībā, kā arī informē vides aizsardzības un reģionālās attīstības ministru.

Vienlaikus, ja NKDL subjekts, kurš ir iepriekš neminēta valsts vai pašvaldības institūcija, neveic visus nepieciešamos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs par konstatēto neatbilstību ziņo Ministru kabinetam un Ministru kabinets lemj par turpmāko rīcību neatbilstības novēršanai.

7. Kādi ir naudas sodi par likuma prasību neievērošanu?

A: Attiecībā uz privāto tiesību juridiskajām personām, sankcijas par prasību neizpildi ietver soda naudas piemērošanu un administratīvā akta piespiedu izpildi. Attiecībā uz būtisko pakalpojumu sniedzējiem un IKT kritisko infrastruktūru, soda naudu var piemērot līdz 10 milj. *euro* vai līdz 2% no uzņēmuma kopējā gada apgrozījuma pasaulē. Attiecībā uz svarīgo pakalpojumu sniedzējiem – līdz 7 milj. *euro* vai līdz 1,4% no kopējā gada apgrozījuma pasaulē.

Vienlaikus, Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam atbilstoši NKDL noteiktajam, veicot uz noteiktu darbību vai darbības aizliegumu vērsta lēmuma piespiedu izpildi, ir tiesības uzlikt piespiedu naudu, kas vienā reizē nepārsniedz 10 000 *euro*.

PRASĪBAS KIBERDROŠĪBAS PĀRVALDNIEKAM

8. Vai kiberdrošības pārvaldnieks var būt uzņēmuma IT departamenta pārstāvis?

A: Jā, vienlaikus pēc labās prakses atbildīgajam par kiberdrošības pārvaldību būtu jābūt tiešā uzņēmuma/iestādes vadītāja pakļautībā, lai novērstu iespējamu interešu konfliktu, kā arī pastāv interešu konflikta risks, jo pēc būtības kiberdrošības pārvaldnieks netieši novērtē/var novērtēt arī organizācijas IT uzturētāju darbu. Vienlaikus norādām, ka subjekta vadītājs atbild par kiberdrošību organizācijā un, ja attiecīgo personu ieceļ organizācijā par pārvaldnieku, tam jāsadarbojas ar uzņēmuma vadītāju nevis IT departamenta direktoru.

9. Vai kiberdrošības pārvaldnieku var nolīgt ārpakalpojumā?

A: Jā, subjekts var piesaistīt kiberdrošības pārvaldības ārpakalpojumus, nodrošinot kiberdrošības prasībām atbilstošu kontroli. Vienlaikus ir jāņem vērā, ka IKT KI turētājiem ārpakalpojumu saņemšanu jāsaskaņo ar valsts drošības iestādi.

Šobrīd strādājot pie Ministru kabineta noteikumu projekta par minimālajām kiberdrošības prasībām ir plānots noteikt cik subjektos viena fiziskā persona var vienlaicīgi būt kiberdrošības pārvaldnieks, atkarībā no tā vai subjekts ir būtisko pakalpojumu sniedzējs, svarīgo pakalpojumu sniedzējs vai IKT KI īpašnieks un tiesiskais valdītājs. Minētais MK noteikumu projekts atrodas saskaņošanas procesā starp iesaistītajām institūcijām un plānots to virzīt otrai saskaņošanas kārtai provizoriski novembra sākumā. Aicinām sekot līdzi MK noteikumu projekta virzībai Tiesību aktu portālā: šeit.

10. Kāda izglītība nepieciešama kiberdrošības pārvaldniekam? Kādi starptautiskie kursi vai sertifikāti ir nepieciešami/derīgi?

Atbilstoši Ministru kabineta noteikumu projekta par minimālajām kiberdrošības prasībām 8.3. apakšpunktam, par kiberdrošības pārvaldnieku var būt fiziska persona, kurai ir augstākā vai vidējā profesionālā izglītība kiberdrošības pārvaldības vai citā saistītā jomā, vai kura ir saņēmusi starptautiski atzītu sertifikātu, kas apliecina personas kvalifikāciju kiberdrošības pārvaldības jomā (piemēram, CISM, CISSP), vai kurai ir vismaz divu gadu darba pieredze kiberdrošības pasākumu plānošanā vai īstenošanā. Līdz ar to ir jāizpildās vismaz vienam no iepriekš uzskaitītajiem kritērijiem, lai persona varētu tikt nozīmēta par kiberdrošības pārvaldnieku subjektā.

Ir virkne starptautiski atzītu un labu sertifikātu, piemēram, *CompTIA Security+ ,Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), ISO/IEC 27001 Lead Implementer, NIST Cybersecurity Framework*. Vienlaikus norādām, ka attiecībā uz starptautiskajiem sertifikātiem, kas būtu atbilstoši kiberdrošības pārvaldniekiem, primāri uz kiberdrošības pārvaldību attiektos apgabalu *Security and Risk Management* un *Security Assessment And Testing* (*Intermediate* līmeņa un uz augšu) – CISO, CISM, CISSP. No Latvijā biežāk izplatītajiem derētu arī ISACA izdotie CISA sertifikāti vai ITIL.

11. Vai kiberdrošības pārvaldnieks var būt Latvijas nepilsonis?

A: Saskaņā ar Ministru kabineta noteikumu projekta par minimālajām kiberdrošības prasībām 9. punktā noteikto, par kiberdrošības pārvaldnieku var būt fiziska persona, kurai ir NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonība, ja tā atbilst minēto noteikumu 8.2.-8.9. apakšpunkta prasībām, un ja ir saņemts Satversmes aizsardzības biroja atzinums, ka personas noteikšana par kiberdrošības pārvaldnieku nav pretrunā ar nacionālās drošības interesēm.

APMĀCĪBAS

12. Sākotnējā minimālo kiberdrošības prasību redakcijā noteikts, ka sākotnējās apmācības (instruktāžas) jānodrošina visiem nodarbinātajiem. Attiecīgi sētnieki, apkopējas utt., kas nestrādās ar IS, tad tik un tā būs jāapgūst sākotnējā instruktāža?

A: Kiberhigiēnas apmācības organizē nodarbinātajiem, kas strādā ar konkrētā uzņēmuma/iestādes informācijas sistēmām.

13. Vai tiks organizētas apmācības valsts un pašvaldību iestādēm?

A: CERT.LV divas reizes gadā organizē apmācības kiberdrošības pārvaldniekiem. Vienlaikus vēršam uzmanību uz to, ka Valsts administrācijas skolā ir pieejams bezmaksas kurss: Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem, lai sniegtu praktiskas zināšanas par kiberhigiēnas jautājumiem publiskās pārvaldes darbiniekiem.

TEHNISKĀS PRASĪBAS

14. Vai IS darbības nodrošināšanai drīkst izmantot atvērtā koda vai bezmaksas programmnodrošinājumu, kuru ir radījusi kopiena (fizisku personu grupa), kuru valstiskā piederība precīzi nav zināma?

A: Var, bet ir jāizvērtē potenciālie riski pret ieguvumiem. Atvērtā koda būtība – liels loks ar izstrādātājiem un entuziastiem – lielā mērā izslēdz iespēju vienam izstrādātājam/programmētājam kodā ietvert ļaunatūru. Vienlaikus, lai pārliecinātos par koda drošumu, vēlams veikt tā revīziju un pārskatīt atvērtā koda programmatūras konfigurāciju pēc lielāku atjauninājumu veikšanas.

Piegādātājs vai pat lietotājs, ja viņam ir nopietns nodoms balstīt savus risinājumus uz konkrēto atvērtā koda sistēmu vai bibliotēku pats var kļūt par vienu no "entuziastiem", kas attīsta konkrēto atvērto kodu vai var veidot savu atzaru "branch", kuru attīsta un neļauj citiem "entuziastiem" tajā kaut ko pievienot.

15. Ja KI turētāja A klases informācijas sistēma, kas izvietota mākoņpakalpojuma resursos: a) vai šajā gadījumā mākoņpakalpojuma sniedzēja resursi ir uzskatāmi par kritisko infrastruktūru un b) vai mākoņpakalpojuma sniedzējam, piemēram, Microsoft, ir jānodrošina pašnovērtējuma u.c. ziņojumu sagatavošana?

A: Aicinām iepazīties ar MK noteikumu projektā par minimālajām kiberdrošības prasībām iekļauto informācijas sistēmu gradāciju, lai pārliecinātos, ka tiešām pārvaldāt A klases informācijas sistēmu jaunā regulējuma ietvarā. A klases informācijas sistēmu izvietošana mākoņpakalpojumos nebūs pieļaujama.

Vēršam uzmanību, ka saistībā ar šo tiek izstrādāti citi noteikumi "Noteikumi par informācijas sistēmu izvietošanu un datu centru drošības prasībām". Tajos tiks noteikts kādos Datu centros atļauts izvietot A kategorijas IS. Publiskajos mākoņpakalpojumos, kur fiziskos resursus dala vairākas personas, A kategorijas sistēmas nebūs atļauts izvietot

16. Vai informācijas sistēmas ar A drošības klasi var būt tikai būtisko pakalpojumu sniedzējam? Vai svarīgo pakalpojumu sniedzējiem informācijas sistēmu drošības klase pēc noklusējuma nevar būt augstāka par B drošības klasi?

A: Aicinām iepazīties ar MK noteikumu projektā par minimālajām kiberdrošības prasībām iekļauto informācijas sistēmu gradāciju, lai pārliecinātos, ka tiešām pārvaldāt A klases informācijas sistēmu jaunā regulējuma ietvarā. A klases informācijas sistēmas varēs būt tikai būtisko pakalpojumu sniedzējiem.

INFORMĀCIJAS IESNIEGŠANA NKDC

17. Kad uzņēmumam jāiesūta sākotnējā informācija, konstatējot, ka tas atbilst NKDL subjekta statusam?

A: Subjekta statusa atbilstības paziņojuma iesniegšanas termiņš ir **01.04.2025**.
Savukārt 01.10.2025. NKDL subjektiem jāiesniedz pirmais pašvērtējuma ziņojums un jāinformē par kiberdrošības pārvaldnieka iecelšanu.

18. Kā noformēt iesniedzamo informāciju? Vai ir pieejami šabloni?

A: Veidlapas iesūtīšanai būs pieejamas Ministra kabineta noteikumu projekta par minimālajām kiberdrošības prasībām pielikumā.

19. Kā nosūta informāciju NKDC?

A: Izmantojot Latvija.lv, nosūta ziņojumu un veidlapas uz Aizsardzības ministrijas Nacionālā kiberdrošības centra oficiālo e-adresi (NKDC@90000022632).

Neatradi atbildi uz interesējošo jautājumu? Raksti uz NIS2@mod.gov.lv