**Ministru kabineta noteikumu projekta „Grozījumi Ministru kabineta 2015. gada 28. jūlija noteikumos Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”” sākotnējās ietekmes novērtējuma ziņojums (anotācija)**

|  |
| --- |
| **I. Tiesību akta projekta izstrādes nepieciešamība** |
| 1. | Pamatojums | Noteikumu projekts izstrādāts, pamatojoties uz Aizsardzības ministrijas iniciatīvu.  |
| 2. | Pašreizējā situācija un problēmas, kuru risināšanai tiesību akta projekts izstrādāts, tiesiskā regulējuma mērķis un būtība | Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” (turpmāk – noteikumi) 2. punkts paredz, ka noteikumi neattiecas uz kritiskās infrastruktūras informācijas sistēmām. Savukārt Ministru kabineta 2011. gada 1. februāra noteikumu Nr. 100 “Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība” 7.2. apakšpunkts paredz, ka kritiskās infrastruktūras aktuālo risku novērtēšanu un pārvaldīšanu sadarbībā ar Satversmes aizsardzības biroju un Informācijas tehnoloģiju drošības incidentu novēršanas institūciju nodrošina par kritiskās infrastruktūras drošību atbildīgā persona. Ja kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs ir Latvijā reģistrēts finanšu un kapitāla tirgus dalībnieks vai par kritisko infrastruktūru ir noteikta valsts informācijas sistēma, vai uz attiecīgo kritisko infrastruktūru attiecas citas speciālās prasības informācijas tehnoloģiju drošības jomā, drošības pasākumu dokumentus izstrādā atbilstoši attiecīgo nozari reglamentējošajām prasībām, pamatojoties uz noteikumu 7.2. apakšpunktā identificētajiem riskiem un ievērojot drošības incidentu novēršanas institūcijas un Satversmes aizsardzības biroja ieteikumus. Projektā paredzēts svītrot norādi, ka noteikumi neattiecas uz kritiskās infrastruktūras informācijas sistēmām. Izņēmums tiek svītrots, jo noteikumos noteiktās minimālās drošības prasības ir pietiekami augstas, lai tās piemērotu arī kritiskās infrastruktūras informācijas sistēmām. Grozījumi tiek izdarīti arī ar skatu uz nākotni, ieviešot Eiropas Parlamenta un Padomes direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienības kontekstā.Noteikumu 34. punkts uzliek pienākumu, pirmkārt, valsts un pašvaldību institūcijām (turpmāk – institūcijas), kurām ir kaut viena paaugstinātas drošības sistēma, kas pieejama, izmantojot publisku datu pārraides tīklu, nodrošināt ārēju drošības dokumentācijas auditu (turpmāk – audits) un ielaušanās testu, otrkārt, Aizsardzības ministrijai (turpmāk – AM) organizēt auditu un ielaušanās testu centralizētu iepirkumu. Valsts un pašvaldību institūciju pienākums ir nodrošināt šo sistēmu drošības pārbaudes vismaz reizi divos gados. Atbilstoši noteikumu 38. punktam institūcijām līdz š. g. 1. janvārim bija jāizstrādā noteikumu 8. punktā minētā dokumentācija visām savām pārziņā vai turējumā esošajām informācijas un komunikācijas tehnoloģiju sistēmām (turpmāk – sistēmām), tādējādi iedalot katru sistēmu kādā no divām kategorijām (pamata vai paaugstinātas drošības), reizē arī nosakot, vai tā ir pieejama, izmantojot publisku datu pārraides tīklu. Šī gada sākumā AM veica institūciju aptauju, lai noskaidrotu, cik daudz un kādas paaugstinātas drošības sistēmas ir institūciju pārziņā vai turējumā. AM izsūtīja vēstules 156 institūcijām un saņēma atbildes no 116. Atbildējušās institūcijas kopumā identificējušas 501 paaugstinās drošības sistēmas. No tām dokumentācija atbilstoši noteikumu prasībām pilnībā ir izstrādāta 345 sistēmām. Izmantojot publisku datu pārraides tīklu, ir pieejamas 242 sistēmas, un šīm sistēmām atbilstoši noteikumu 34. punktam ir jāveic auditi un ielaušanās testi. Institūciju atsūtītā informācija atklāja ļoti plašu sistēmu daudzveidību un skaitu. Balstoties uz šo informāciju, tika veikta analīze un secināts, ka:* 1. centralizēta iepirkuma procedūras uzsākšana nav iespējama, jo:
	2. nav iespējams apzināt reāli auditējamo sistēmu skaitu. Informācija par paaugstinātas drošības sistēmām norāda uz ļoti lielo sistēmu dažādību, un no iesniegtajām atbildēm var secināt, ka ievērojami atšķiras tas, kādas sistēmas savas institūcijas dēvē par paaugstinātas drošības sistēmām. Piemēram, ir institūcijas, kuras paziņo par vienu paaugstinātas drošības sistēmu, taču realitātē šī viena sistēma satur vairākus desmitus vai simtus apakšsistēmu (moduļus), kurus arī attiecīgajā gadījumā būtu nepieciešams pārbaudīt, auditēt un testēt. Informācija par sistēmām un to īpatnībām ir tikai iestāžu kompetencē;
	3. nav iespējams definēt iepirkuma specifikāciju. Lai noteikumos ierakstītā norma sasniegtu mērķi un uzlabotu konkrētās sistēmas drošību, katras sistēmas auditam un ielaušanās testam būtu jāveido sava tehniskā specifikācija. Centralizēti un pēc viena parauga šādu specifikāciju nav iespējams sagatavot;
	4. nav iespējams noteikt konkrētas izmaksas. Balstoties uz minētajiem argumentiem, kā arī faktu, ka sekmīgai mērķa sasniegšanai nav iespējams izmantot *one-size-fits-all* modeli, pēc kura provizoriski noteikt vismaz aptuvenās izmaksas, finanšu plānošana šīs funkcijas veikšanai nav reāla.
	5. Sistēmu auditēšana un ielaušanās testi centralizētā veidā nav veicami noteiktajā laikā. Spriežot pēc Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (turpmāk – CERT.LV) darbības pieredzes, vienas sistēmas ielaušanās testa veikšanai nepieciešama apmēram viena nedēļa (neskaitot drošības dokumentācijas auditu, atkārtotas pārbaudes, konsultācijas utt.). Arī privātajā sektorā pieredze ir līdzīga. Tādējādi esošais modelis, kā arī apzinātais sistēmu skaits un daudzveidība fiziski neatļauj plānotajā laikā (reizi 2 gados) veikt nepieciešamās pārbaudes visām sistēmām.
	6. Nav mehānisma, kas nodrošinātu audita un ielaušanās testu efektivitāti. Esošā noteikumu redakcija nenosaka atskaitīšanās kārtību, lai nodrošinātu, ka institūcijas novērš auditā un ielaušanās testos atklātos trūkumus. Noteikumi atsaucas uz Informācijas tehnoloģiju drošības likuma normām, kas uzliek pienākumu institūcijām novērst atklātos trūkumus (piemēram, 6.1 pants par rīcību informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā nosaka, ka institūcijai 90 dienu laikā jāveic visas drošības nepilnību novēršanai nepieciešamās darbības), taču, ņemot vērā resursus, kas tiktu ieguldīti audita un ielaušanās testa veikšanā, bez konkrēta atskaitīšanās mehānisma nav iespējams garantēt pārbaužu lietderību un efektivitāti. Aizsardzības ministrija izvērtēja nepieciešamību ieviest papildu mehānismu atskaitīšanās kārtības ieviešanai pēc pārbaudēm, taču tika secināts, ka tas radītu nesamērīgu papildu birokrātisko slogu.
	7. Lai arī precīzu finansējuma apmēru nav iespējams noteikt, funkcijas īstenošanai tas ir nepieciešams. Aizsardzības nozarei atvēlētais finansējums jau ir saplānots līdz 2019. gadam, un tā prioritāte ir sabiedroto klātbūtnes Latvijā nodrošināšana. Turklāt, ņemot vērā valstī ierobežotos finanšu resursus, Ministru kabinets ir uzdevis ministrijām izvērtēt normatīvajos aktos paredzētās funkcijas, apzinot, kuras no tām būtu īstenojamas efektīvāk un ekonomiskāk.

Pēc padziļināta izvērtējuma secināms, ka esošā Ministru kabineta noteikumu redakcija nosaka neefektīvu audita un ielaušanās testu iepirkšanas un īstenošanas kārtību, pēc kuras nav pārliecības par lietderīgu valsts budžeta līdzekļu izmantojumu, tāpēc to nepieciešams grozīt. Grozījumi paredz svītrot 34. punkta otro teikumu, atceļot pienākumu Aizsardzības ministrijai veikt centralizētu iepirkumu. Jānorāda, ka CERT.LV jau šobrīd veic ielaušanās testus institūciju sistēmās atbilstoši iestāžu pieprasījumiem. Taču ielaušanās testi tiek veikti tām sistēmām, kuras CERT.LV vērtējumā ir prioritāras. Tāpat ielaušanās testi tiek veikti CERT.LV pieejamo resursu ietvaros. CERT.LV arī uzrauga testu rezultātu ieviešanu un drošības trūkumu novēršanu. Kopš noteikumu stāšanās spēkā esošajā redakcijā ir konstatētas dažas nepilnības, kuras nepieciešams precizēt, lai novērstu pārpratumus vai neskaidrības, kas rodas noteikumu piemērošanas procesā, konkrēti – izstrādājot sistēmas drošības politiku (noteikumu 15. punkts). Pirmkārt, nepieciešams papildināt 15.3. apakšpunktu, jo esošā redakcija nosaka pienākumu sistēmas lietotājiem obligāti lietot paroles, ja sistēmā netiek izmantota daudzfaktoru autentifikācija, tas ir, viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts. Šajā punktā nepieciešams iekļaut norādi, ka prasība attiecināma uz reģistrētiem sistēmas lietotājiem, lai novērstu neskaidrības saistībā ar iestāžu mājaslapu apmeklēšanu. Ja mājaslapas lietotājs (apmeklētājs) vienkārši apmeklē iestādes mājaslapu un tam nav nepieciešams reģistrēties, tad viņam nav nepieciešams izmantot arī paroli. Tāpat arī 14. punkts un 15.2. apakšpunkts attieksies tikai uz reģistrētiem sistēmas lietotājiem.Otrkārt, nepieciešams izdarīt grozījumu 15.4. apakšpunktā, jo esošā redakcija definē sistēmas lietotāju paroles prasības, nosakot, ka tās garums nav mazāks par deviņiem simboliem un tā satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu. Taču, ņemot vērā situācijas, kad ar valsts un pašvaldību informācijas sistēmās plaši izmantotajiem tehniskajiem līdzekļiem (piemēram, *Microsoft Active Directory*) nav iespējams īstenot noteikumu prasības, nepieciešams noteikt prasību, ka parole satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu vai speciālo simbolu.  |
| 3. | Projekta izstrādē iesaistītās institūcijas | Informācija par tiesību akta projektu un tā mērķi izklāstīta Nacionālās informācijas tehnoloģiju drošības padomes š. g. 10. marta sēdē.Noteikumu 2. punkta grozījumu izstrādē tika iesaistīts Satversmes aizsardzības birojs un CERT.LV. |
| 4. | Cita informācija | Nav. |
|   |

|  |
| --- |
| **II. Tiesību akta projekta ietekme uz sabiedrību, tautsaimniecības attīstību un administratīvo slogu** |
| 1. | Sabiedrības mērķgrupas, kuras tiesiskais regulējums ietekmē vai varētu ietekmēt | Visas valsts un pašvaldību institūcijas.  |
| 2. | Tiesiskā regulējuma ietekme uz tautsaimniecību un administratīvo slogu | Veicot attiecīgos grozījumus, administratīvais slogs tiek mazināts Aizsardzības ministrijai, jo nav nepieciešams organizēt centralizēto iepirkumu.  |
| 3. | Administratīvo izmaksu monetārs novērtējums | Projekts šo jomu neskar. |
| 4. | Cita informācija | Nav. |

|  |
| --- |
| **III. Tiesību akta projekta ietekme uz valsts budžetu un pašvaldību budžetiem** |
| Tiesību akta projekts atceļ nepieciešamību pieprasīt papildu valsts budžeta finansējumu. Lai arī finansējuma aprēķinu nav iespējams noteikt, kā pierāda izvērtējums, provizoriskais nepieciešamais finansējums ir mērāms vairākos miljonos *euro*.  |
|  |
|  |
|  |

|  |
| --- |
| **VI. Sabiedrības līdzdalība un komunikācijas aktivitātes** |
| 1. | Plānotās sabiedrības līdzdalības un komunikācijas aktivitātes saistībā ar projektu | Projekts sabiedriskajai apspriešanai publicēts Aizsardzības ministrijas mājaslapas sadaļā “Sabiedrības līdzdalība”.  |
| 2. | Sabiedrības līdzdalība projekta izstrādē | Projekts šo jomu neskar. |
| 3. | Sabiedrības līdzdalības rezultāti | Projekts konceptuāli atbalstīts.  |
| 4. | Cita informācija | Nav. |

|  |
| --- |
| **VII. Tiesību akta projekta izpildes nodrošināšana un tās ietekme uz institūcijām** |
| 1. | Projekta izpildē iesaistītās institūcijas | Visas valsts un pašvaldību iestādes, kurām ir vismaz viena paaugstinātas drošības sistēma.  |
| 2. | Projekta izpildes ietekme uz pārvaldes funkcijām un institucionālo struktūru. Jaunu institūciju izveide, esošu institūciju likvidācija vai reorganizācija, to ietekme uz institūcijas cilvēkresursiem | Jaunu institūciju izveide nav nepieciešama.  |
| 3. | Cita informācija | Nav. |

Anotācijas IV, V sadaļa – projekts šo jomu neskar.

Aizsardzības ministrs R. Bergmanis

Valsts sekretārs J. Garisons

1462

25.10.2017 14:38:00

D. Baumanis, 67335352

Davis.Baumanis@mod.gov.lv

S. Žogota, 67335353

Sanita.Zogota@mod.gov.lv