**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) 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 veikšanu, otrkārt, Aizsardzības ministrijai (turpmāk – AIM) centralizēti organizēt iepirkumu auditiem un ielaušanās testiem. 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 arī 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 AIM veica institūciju aptauju, lai noskaidrotu, cik daudz un kādas paaugstinātas drošības sistēmas ir institūciju pārziņā vai turējumā. AIM izsūtīja vēstules 156 institūcijām, taču 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 demonstrēja 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 noziņo 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 savu mērķi un uzlabotu konkrētās sistēmas drošību, katras sistēmas audita un ielaušanās testa veikšanai būtu jāraksta sava tehniskā specifikācija. Centralizēti un pēc viena parauga šādu specifikāciju nav iespējams sagatavot.   4. nav iespējams noteikt konkrētas izmaksas. Balstoties uz iepriekš minētajiem argumentiem, kā arī faktu, ka sekmīgai mērķa sasniegšanai nav iespējams izmantot “*one-size-fits-all*” modeli, pēc kā arī provizoriski noteikt vismaz aptuvenās izmaksas, finanšu plānošana šīs funkcijas veikšanai nav reālistiska.   5. Sistēmu auditēšana un ielaušanās testi nav veicami noteiktajā laikā. Spriežot pēc Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (turpmāk – CERT.LV) darbības pieredzes, 1 sistēmas ielaušanās testa veikšanai nepieciešama apmēram 1 nedēļa (neskaitot drošības dokumentācijas auditu, atkārtotas pārbaudes, konsultācijas utt). Arī privātajā sektorā pieredze ir līdzīga. Līdz ar to 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 atklāto 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 laikā jāveic visas drošības nepilnības 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. AIM izvērtēja nepieciešamību ieviest papildus mehānismu pēc-pārbaužu un atskaitīšanās kārtības ieviešanai, taču tika secināts, ka tas radītu nesamērīgu papildus 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 veikšanas, secināms, ka esošā Ministru kabineta noteikumu redakcija nosaka neefektīvu audita un ielaušanās testu iepirkšanas un īstenošanas kārtību, kura rezultātā nav pārliecības par lietderīgu valsts budžeta līdzekļu izmantošanu, tāpēc to nepieciešams grozīt, tādēļ grozījumi paredz svītrot 34. punktu, atceļot pienākumu, pirmkārt, institūcijām nodrošināt auditu un ielaušanās testus konkrētai sistēmu grupai, otrkārt, AIM veikt centralizētu iepirkumu.  Jāuzsver, ka līdz ar 34.punkta svītrošanu institūcijām netiek atcelts pienākums pārbaudīt savu sistēmu, t.sk. paaugstinātas drošības sistēmu, kas pieejamas, izmantojot publisku datu pārraides tīklu, drošību. Pirmkārt, Informācijas tehnoloģiju drošības likuma 8.panta trešās daļas 2) apakšpunkts nosaka pienākumu “ne retāk kā reizi gadā veikt informācijas tehnoloģiju drošības pārbaudi un atbilstoši tās rezultātiem organizēt atkāto trūkumu novēršanu.” Otrkārt, noteikumu 18.punkts nosaka pienākumu institūcijai nodrošināt, ka “pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi.” Šos testus atbilstoši noteikumiem var veikt gan juridiskas personas, kuras institūcija piesaista par saviem līdzekļiem, gan institūcijas darbinieki, kuri nav piedalījušies sistēmas izstrādē. Treškārt, noteikumu 19.punkts nosaka, ka institūcijas nodrošina sistēmu drošības pārbaudi, “vismaz reizi gadā veicot drošības dokumentācijas prasību izpildes pārbaudi.” Svītrojot 34.punktu institūcijas netiek ierobežotas pasūtīt auditu un ielaušanās testu veikšanu esošā budžeta ietvaros vai pieprasot papildus valsts budžeta līdzekļus, ievērojot 35.punktā noteiktās prasības juridiskajām personām, kas veic auditu.  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 uzrauga veikto testu rezultātu ieviešanu un drošības trūkumu novēršanu. Šobrīd Aizsardzības ministrija izstrādā kārtību, kādā CERT.LV ielaušanās testu veikšanā varētu iesaistīt Zemessardzes Kiberaizsardzības vienību, tādējādi palielinot kapacitāti šīs funkcijas īstenošanai.  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, kura 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 mājas lapu apmeklēšanu. Ja mājas lapas lietotājs (apmeklētājs) vienkārši apmeklē iestādes mājas lapu, un tam nav nepieciešams reģistrēties, tad tam arī nav nepieciešams izmantot paroli.  Otrkārt, nepieciešams grozīt 15.4. apakšpunktu, kura esošā redakcija definē prasības sistēmas lietotāju parolei, 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 izmantotiem 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 IT drošības padomes š.g. 10.marta sēdē. |
| 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 AIM, jo nav nepieciešams organizēt centralizēto iepirkumu. Administratīvais slogs mazinās arī tām valsts un pašvaldību institūcijām, kurām ir kaut viena paaugstinātas drošības sistēma, kas pieejama, izmantojot publisku datu pārraides tīklu, jo tām vairs nav obligāti jānodrošina audita un ielaušanās testu veikšana. |
| 3. | Administratīvo izmaksu monetārs novērtējums | Nav. |
| 4. | Cita informācija | Nav. |

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

|  |  |  |
| --- | --- | --- |
| **IV. Tiesību akta projekta ietekme uz spēkā esošo tiesību normu sistēmu** | | |
| 1. | Nepieciešamie saistītie tiesību aktu projekti | Nav. |
| 2. | Atbildīgā institūcija | AIM. |
| 3. | Cita informācija | Nav. |

|  |  |  |
| --- | --- | --- |
| **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 | Nav. |
| 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 V sadaļa – projekts šo jomu neskar.

Aizsardzības ministrs R. Bergmanis

Vīza: Valsts sekretārs J. Garisons

1462

03.04.2017 13:56:00

E. Vīksne, 67335353

[elina.viksne@mod.gov.lv](mailto:elina.viksne@mod.gov.lv)