Aizsardzības ministrija

Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām

Kirils Solovjovs, Rīgā, 2015. gada 28. jūlijā.

Aizsardzības ministrija

Prezentācijas saturs

- Kārtības mērķis, tvērums un ieviešana
- Drošības kategorijas
- Prasības
- Tehniskās prasības
- Ārpakalpojumu izmantošana
- Spēkā stāšanās

Aizsardzības ministrija

Kārtības juridiskais spēks

Kārtība pieņemta 2015. gada 28. jūlijā ar Ministru kabineta lēmumu.

Tā stājas spēkā nākamajā dienā pēc publicēšanas oficiālajā izdevumā «Latvijas Vēstnesis».

Reizē spēku zaudē Ministru kabineta 2005. gada 11. oktobra noteikumi Nr. 765 „Valsts informācijas sistēmu vispārējās drošības prasības”.

Aizsardzības ministrija

Kārtības mērķis un tvērums

- Vismaz minimālais drošības līmenis **visur**.
- Attiecas uz
  - **valsts un pašvaldību** institūciju IKT sistēmām,
  - **valsts informācijas sistēmām**.
- Neattiecas uz
  - sistēmām, kas apstrādā klasificēto informāciju un informāciju dienesta vajadzībām,
  - kritisko infrastruktūru.

Aizsardzības ministrija

Kārtības ieviešana

- Kārtību rekomendēts ieviest četros soļos:

1. identificēt visas iestādes pārziņā vai turējumā esošās IKTS[1]
2. atbilstoši metodoloģijai (7. punkts) noteikt katras sistēmas drošības kategoriju
3. sagatavot un apstiprināt nepieciešamos dokumentus (8. un 9. punkts) vai pārskatīt, ja tādi jau ir
4. pārliecināties, ka dokumenti tiek īstenoti praksē (19. punkts)

[1] IKTS – informācijas un komunikācijas tehnoloģiju sistēma

Aizsardzības ministrija

Drošības kategorijas

Pamata un paaugstinātas drošības sistēmas (6. pants)

- **Pamata** – viens dokuments, 14 tehniskas prasības (15. punkts), nav jāīsteno III nodaļā minētais
- **Paaugstinātas** – pieci dokumenti, 26 tehniskas prasības (15. un 24. punkts)

Aizsardzības ministrija

Drošības kategorijas noteikšanas principi

Lai noteiktu katras sistēmas drošības kategoriju, analizē sistēmas:

1) **pieejamības** prasības;
2) **integritātes** prasības;
3) **konfidencialitātes** prasības.

Aizsardzības ministrija

PIEEJAMĪBA

Jāizvērtē maksimāli pieļaujamais sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā (atbilstoši dokumentācijai) viena kalendārā mēneša laikā (summāri)

A pieļaujams ne garāks par 4 stundām

B pieļaujams robežās no 4 – 24 stundām

C pieļaujams ilgāks par 24 stundām

Aizsardzības ministrija

INTEGRITĀTE

Jāizvērtē, vai integritātes apdraudējums

A datiem rada risku valstij

A jebkuriem datiem rada risku pamatfunkcijām

B kādai daļai datu rada risku pamatfunkcijām

C nerada risku pamatfunkcijām

Aizsardzības ministrija

KONFIDENCIALITĀTE

Sistēma satur

A sensitīvus personas datus

B ierobežotas pieejamības informāciju

C publiskus datus

Datu noplūde var radīt

A Smagas sekas

B Reputācijas kaitējums

C Nav riska

Aizsardzības ministrija

Drošības kategorijas noteikšana

Ja no iepriekš minētajiem A,B,C burtiem

- vismaz **viens A** → paaugstināta
- **trīs B** → paaugstināta
- pārējos gadījumos → pamata

Turpmāk prezentācijā:

Prasības, kas attiecas tikai uz paaugstinātas drošības sistēmām

Pamata prasības, kas attiecas uz abām drošības kategorijām

Aizsardzības ministrija

Kādas ir prasības? (1)

- Katrai sistēmai jāizstrādā [8.,9.]:
  - sistēmas drošības politika;
  - sistēmas drošības iekšējie noteikumi;
  - sistēmas lietošanas noteikumi;
  - sistēmas drošības riska pārvaldības plāns;
  - sistēmas darbības atjaunošanas plāns.
- CERT.LV sagatavos paraugus
- Pārskata vismaz reizi gadā [10.]
- Var veidot vienu drošības politiku (lietošanas noteikumus utt.) vairākām sistēmām [11.]
- Iestādes drīkst apstiprināt šos dokumentus savām pakļautības iestādēm

Aizsardzības ministrija

Kādas ir prasības? (2)

- Pirms **jaunas sistēmas** pieņemšanas ekspluatācijā, tai ir veikti ielaušanās testi [18.]
- Institūcija nodrošina sistēmas drošības pārbaudi, veicot drošības **dokumentācijas prasību īstenošanas** pārbaudi (1 reizi gadā) [19.]

- Ja sistēma pieejama, izmantojot publisku datu pārraides tīklu, institūcija pasūta **ārēju drošības dokumentācijas auditu** un **ielaušanās testu** veikšanu (1 reizi 2 gados) [34.]
- Auditu veic NATO, ES, EEZ juridiska persona [35.]

Aizsardzības ministrija

Kādas ir prasības? (3)

- Ārpakalpojumu līgumā norāda precīzas un izmērāmas prasības
- Sistēmas izstrādes gaitā tiek ievērota drošības politika [17.]

- Ārpakalpojumu līgumu atļauts slēgt ar NATO, ES, EEZ personu [36.]

Aizsardzības ministrija

Kādas ir prasības? (4)

Sistēmas izstrādes iepirkuma specifikācijā iekļauj **drošības prasības** un paredz atbilstošas drošības **tehniskās** prasības [21., 22.]:

- noteiktu sistēmas **uzturēšanas** un **atbalsta** nodrošināšanas **laika periodu**[1]
- sistēmas datorprogrammu **pirmkoda** un tā izmantošanas tiesību **nodošanu institūcijai**[1]
- iespēju turpināt sistēmas **ekspluatēšanu ar jaunākām programmnodrošinājuma versijām**[1]
- [23.]aizliegumu ierobežot **pasūtītāja tiesības veikt nepieciešamās izmaiņas** programmatūras pirmkodā

[1] tikai no jauna veidojamām sistēmām

Aizsardzības ministrija

Par ārpakalpojumiem
Precīzas un izmērāmas prasības

- Līgumā iekļauj [20.]
  - pakalpojuma aprakstu
  - precīzas prasības attiecībā uz apjomu un kvalitāti
  - pušu tiesības un pienākumus, t.i.
    - institūcijas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti
    - institūcijas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus
    - institūcijas tiesības iesniegt ārpakalpojuma sniedzējam motivētu rakstveida pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu

Tehniskās prasības

(Atļauts paredzēt arī stingrākas prasības)

Prasības pilnībā aprakstītas 15. un 24. punktā.

Aizsardzības ministrija

Tehniskās prasības
Konti

- Atsevišķi administratoru konti [15.1.]
- Lietotāja konts piesaistīts fiziskai personai [15.2.]

- Konts **tiek bloķēts** pēc pieciem neveiksmīgiem pieteikšanās mēģinājumiem [24.3.]
- Administrators ārpus iestādes pieslēdzas tikai ar **daudzfaktoru autentifikāciju** [24.4.]

Aizsardzības ministrija

Tehniskās prasības
Paroles

- Katram lietotājam ir jābūt parolei [15.3.]
  - ✓ *Izņēmums – daudzfaktoru autentifikācija*
- Paroles garums un sarežģītība *!234s67B9* [15.4.]
- Paroli vienmēr šifrē un ievadot neattēlo lietotājam [15.5., 15.6.]
  - ✓ *Izņēmums – vienreizējā parole derīga 72h [15.7.]*
- Sistēma nedrīkst piedāvāt "atcerēties" paroles [15.8.]
  - ✓ *HTML: autcomplete=«off»*
- Nedrīkst izmantot noklusējuma paroles [15.9.]

- Parole jāmaina ik pēc 90 dienām, bet ne biežāk kā 2x 24h [24.1.]
- Parole nedrīkst sakrist ar 5 iepriekšējām [24.2.]

Aizsardzības ministrija

Tehniskās prasības
Auditācijas pieraksti

- Tiek veidoti auditācijas pieraksti, kas tiek glabāti

✓ *6 mēnešus [15.10.]*

✓ *18 mēnešus [24.6.]*

- Tie satur informāciju par katru darbību un attiecīgo lietotāja kontu vai IP adresi [15.11.]
- Auditācijas pieraksti (vai kopijas) tiek glabāti atsevišķi no sistēmas [24.6.]
- Auditācijas pieraksti tiek veikti norādot pareizu (sinhronizētu) pulksteņa laiku [24.7.]
- Auditācijas pierakstu plānveida analīze [24.8.]

Aizsardzības ministrija

Tehniskās prasības
Pārējā sistēmas funkcionalitāte

- Gala lietotāju iekārtas satur pretvīrusu funkcionalitāti [15.13.]
- Sistēma darbojas ar minimāli iespējamām tiesībām [15.14.]

- Lietotājam redzamie **kļūdu paziņojumi** satur tikai **minimālo** informāciju, kas nepieciešama, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu [24.9.]

Aizsardzības ministrija

Tehniskās prasības

Datortīkls un fiziskā drošība

- Tiek kontrolēta fiziskā piekļuve iekārtām [24.5.]
- Ugunsmūris katrai sistēmai [24.10.]
- Nevajadzīgie *Network Services* ir atslēgti [24.11.]

Aizsardzības ministrija

Tehniskās prasības
Pārējās prasības

- Sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību [15.12.]
- Sistēmas izstrāde un testēšana tiek veikta, nodrošinot, ka **netiek apdraudēta** sistēmā glabātā **informācija** [24.12.]
- Sistēmu atļauts izvietot pie tāda ārpakalpojumu sniedzēja, kas ir ES, EEZ jur. persona; informācija tiek glabāta ES, EEZ. [24.13.]

Aizsardzības ministrija

Spēkā stāšanās
Bez pārejas perioda

Nekavējoties stājas spēkā prasības attiecībā uz

- uzturēšanas ārpakalpojumiem,
- pieņemšanu ekspluatācijā,
- iepirkumiem
- un drošības pārbaudēm

(17., 18., 20., 21., 22., 23., 34., 35., 36. pants)

Aizsardzības ministrija

Spēkā stāšanās Pārejas periods[1]

[1] attiecīgā gada 1. janvāris

2017
- apstiprināta visa nepieciešamā dokumentācija

2018
- paaugstinātas drošības sistēmām stājas spēkā tehniskās prasības (15. un 24. punkts)

2019
- paaugstinātas drošības sistēmas, kas neatbilst prasībām, tiek likvidētas

2021
- pamata drošības sistēmām stājas spēkā tehniskās prasības (15. punkts)

2022
- pamata drošības sistēmas, kas neatbilst prasībām, tiek likvidētas

Aizsardzības ministrija

Informatīvais materiāls. Iekļautie formulējumi un skaidrojumi nav juridiski saistoši. Precīzie formulējumi atrodami Ministru kabineta noteikumos.

Papildus informācija pieejama, sazinoties ar Informācijas tehnoloģiju drošības incidentu novēršanas institūciju CERT.LV

cert@cert.lv