Aizsardzības ministrija

IT drošības likuma grozījumi

drošāka vide un papildus prasības

Kirils Solovjovs, Rīgā, 2015. gada 29. aprīlī.

Aizsardzības ministrija

IT drošības vēsture Latvijā

Aizsardzības ministrija

IT drošības vēsture Latvijā līdz 2012. gadam

- 2009.-2010. no VID informācijas sistēmas tiek iegūti apmēram 120GiB datu
- 18.02.2010. tiek uzsākta datu publicēšana
- 05.05.2010. Saeimas NDK sagatavo un iesniedz izskatīšanai "Informācijas tehnoloģiju drošības pārvaldības likumu", nodots AIKNK
- 28.10.2010. Saeima pabeidz izskatīt un pieņem "Informācijas tehnoloģiju drošības likumu"
- 01.02.2011. Likums stājas spēkā, tiek izveidots CERT.LV

Aizsardzības ministrija

IT drošības vēsture Latvijā kopš 2013. gada

- 01.01.2013. CERT.LV darbības nodrošināšana nodota AM
- 01.01.2014. NITDP darbības nodrošināšana nodota AM
- 22.10.2014. Saeimas AIKNK sagatavo un iesniedz izskatīšanai grozījumus "Informācijas tehnoloģiju drošības likumā"
- 05.02.2015. Saeima pabeidz izskatīt un pieņem grozījumus grozījumus "Informācijas tehnoloģiju drošības likumā"
- 04.03.2015. Grozījumi stājas spēkā

Aizsardzības ministrija

Informācijas tehnoloģiju drošības likuma grozījumi

Aizsardzības ministrija

6.[1] pants. Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā

(1) Informācijas tehnoloģiju drošības nepilnība ir

- būtiska
- informācijas sistēmas vai elektronisko sakaru tīkla
- izveides, uzturēšanas vai pārveidošanas gaitā
- tīši vai nejauši radīta
- sistēmiska vājība,
- kuras rezultātā var tikt apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

Aizsardzības ministrija

6.[1] pants. Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā

(2) Institūcija, konstatējusi drošības nepilnību,

- 90 dienu laikā veic visas tās novēršanai nepieciešamās darbības,
- kā arī par konstatēto tūlīt informē CERT.LV.

Aizsardzības ministrija

6.[1] pants. Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā

(3) CERT.LV, konstatējusi drošības nepilnību, par šo faktu tūlīt informē institūciju.

Institūcija CERT.LV noteiktajā termiņā veic visas drošības nepilnības novēršanai nepieciešamās darbības.

Termiņš nav ilgāks par 90 dienām kopš informēšanas brīža.

Aizsardzības ministrija

Biežāk uzdotie jautājumi (1)

- **Uz ko attiecas** 6.[1] pants?
  - **Valsts** institūcijām
  - **Pašvaldības** institūcijām
  - Informācijas tehnoloģiju **kritiskās infrastruktūras** īpašniekiem vai tiesiskajiem valdītājiem

Aizsardzības ministrija

Biežāk uzdotie jautājumi (2)

.**Vai drīkstu neziņot** par nepilnībām, ja mana sistēma

a) nav pieejama no Interneta

b) ir paredzēta tikai iekšējai iestādes lietošanai

c) satur valsts noslēpumu

d) ir valsts informācijas sistēma

e) nav valsts informācijas sistēma

.**Nē**, prasība attiecas uz visām informācijas sistēmām

Aizsardzības ministrija

Biežāk uzdotie jautājumi (3)

- Vai **jāziņo par katru** nepilnību?
  - **Nē**, jāizvērtē tās atbilstība definīcijai
- **Kāda informācija jāiesniedz** ziņojot par nepilnību?
  - Vismaz **ievainojamības apraksts** un **ietekmētās sistēmas nosaukums** vai ietekmētās infrastruktūras uzskaitījums
- **Kur** var **iesniegt** informāciju?
  - **cert@cert.lv**
  - ja nepieciešams, jāizmanto PGP šifrēšana
  - atkarībā no informācijas klasifikācijas, **jānodrošina atbilstoša** informācijas **aizsardzība**

Aizsardzības ministrija

Pirmās daļas beigas (vieglākais ir aiz muguras)

Aizsardzības ministrija

Otrā daļa – VSS-343

Aizsardzības ministrija

VSS-343

Kārtība, kādā valsts un pašvaldību institūcijas nodrošina informācijas un komunikācijas tehnoloģiju sistēmu, tajā skaitā valsts informācijas sistēmu, atbilstību minimālajām drošības prasībām[1]

[1] projekts[2]

[2] plānots, ka stāsies spēkā[3] 2015. gada pirmajā pusē

[3] paredzēts saprātīgs pārejas periods

Aizsardzības ministrija

Noteikumu mērķis un tvērums

- Vismaz minimālais drošības līmenis **visur**.
- Attiecas uz
  - **valsts un pašvaldību** institūciju IKT sistēmām,
  - **valsts informācijas sistēmām**.
- Bet neattiecas uz
  - klasificēto informāciju, t.sk. DV,
  - kritisko infrastruktūru.

Aizsardzības ministrija

Pieeja

- Ļoti plaša diapazona sistēmas un speciālisti
- Sistēmu kategorijas – pamata un paaugstinātas drošības sistēmas
- **Pamata** – viens dokuments, 14 tehniskas prasības
- **Paaugstinātas** – pieci dokumenti, 26 tehniskas prasības

Aizsardzības ministrija

Pamata vai paaugstināta drošība? Pieejamība

.Pieejamība

.**A** 4h-

.**B** 4 - 24h

.**C** 24h +

Aizsardzības ministrija

Pamata vai paaugstināta drošība? Integritāte

.Integritāte

.**A** daļa datu rada risku valstij vai visi dati rada risku pamatfunkcijām

.**B** daļa datu rada risku pamatfunkcijām

.**C** nav riska pamatfunkcijām

Aizsardzības ministrija

Pamata vai paaugstināta drošība? Konfidencialitāte

- Konfidencialitāte
- **A** sensitīvi personas dati, smagas sekas
- **B** personas dati, reputācijas kaitējums
- **C** publiski dati, nav riska

Aizsardzības ministrija

Pamata vai paaugstināta drošība?

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

- Prasības, kas attiecas tikai uz paaugstinātas drošības sistēmām, tālāk atzīmētas ar '*'

Aizsardzības ministrija

Kādas ir prasības? (1)

- Katrai sistēmai jāizstrādā
  - sistēmas **drošības politika**;
  - *sistēmas **drošības** iekšējie **noteikumi**;
  - *sistēmas **lietošanas noteikumi**;
  - *sistēmas **drošības riska pārvaldības** plāns;
  - *sistēmas **darbības atjaunošanas** plāns.
- Būs pieejami paraugi

Aizsardzības ministrija

Kādas ir prasības? (2)

- Pirms **jaunas sistēmas** pieņemšanas ekspluatācijā, tai ir veikti ielaušanās testi
- Institūcija nodrošina sistēmas drošības pārbaudi, veicot drošības **dokumentācijas prasību īstenošanas** pārbaudi (1x gadā)
- *Ja sistēma pieejama, izmantojot publisku datu pārraides tīklu, institūcija pasūta **ārēju drošības dokumentācijas auditu** un **ielaušanās testu** veikšanu (1x 2 gados)
- *Auditu veic NATO, ES, EEZ jur. persona

Aizsardzības ministrija

Kādas ir prasības? (3)

- Ārpakalpojumu līgumā norāda **precīzas** un **izmērāmas** prasības
- *Ārpakalpojumu līgumu atļauts slēgt ar NATO, ES, EEZ personu
- Sistēmas izstrādes iepirkuma specifikācijā paredz atbilstošas drošības **tehniskās** prasības
  - 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]
  - aizliegumu ierobežot **pasūtītāja tiesības veikt nepieciešamās izmaiņas** programmatūras pirmkodā

[1] tikai jaunām sistēmām

Aizsardzības ministrija

Par ārpaklpojumiem
Precīzas un izmērāmas prasības

- Līgumā iekļauj
  - 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

Aizsardzības ministrija

Tehniskās prasības

(Atļauts paredzēt arī stingrākas prasības)

Aizsardzības ministrija

Tehniskās prasības
Konti

- Atsevišķi **administratoru** konti
- Lietotāja konts piesaistīts **fiziskai personai**
- *Konts **tiek bloķēts** pēc pieciem neveiksmīgiem pieteikšanās mēģinājumiem
- *Administrators ārpus iestādes pieslēdzas tikai ar **daudzfaktoru autentifikāciju**

Aizsardzības ministrija

Tehniskās prasības
Paroles

- Katram lietotājam ir jābūt **parolei**
  Izņēmums – daudzfaktoru autentifikācija
- Paroles garums un sarežģītība !234s67B9
- Paroli vienmēr **šifrē** un nekad **neattēlo** lietotājam
  Izņēmums – **vienreizējā** parole derīga **72h**
- Sistēma **nedrīkst** piedāvāt "**atcerēties**" paroles
- Nedrīkst izmantot noklusējuma paroles
- *__Parole jāmaina__ ik pēc 90 dienām, bet ne biežāk kā 2x 24h
- *Parole **nedrīkst sakrist** ar 5 iepriekšējām

Aizsardzības ministrija

Tehniskās prasības
Auditācijas pieraksti

- Tiek veidoti **auditācijas pieraksti**, kas tiek glabāti 6 mēnešus
  *18 mēnešus
- Katra piekļuve sistēmai ir izsekojama līdz **lietotāja kontam** vai **IP adresei**
- *Auditācijas pieraksti (vai kopijas) tiek glabāti **atsevišķi no sistēmas**
- *NTP
- *Auditācijas pierakstu **plānveida** analīze

Aizsardzības ministrija

Tehniskās prasības
Pārējā sistēmas funkcionalitāte

- Gala lietotāju iekārtas satur **pretvīrusu** funkcionalitāti
- Sistēma darbojas ar **minimāli iespējamām tiesībām**
- *Lietotājam redzamie **kļūdu paziņojumi** satur tikai **minimālu** informāciju

Aizsardzības ministrija

Tehniskās prasības
Datortīkls un fiziskā drošība

.*__Ugunsmūris__ katrai sistēmai

.*Nevajadzīgie *Network Services* ir **atslēgti**

.*Tiek kontrolēta **fiziskā piekļuve** iekārtām

Aizsardzības ministrija

Tehniskās prasības
Pārējās prasības

.Sistēmai jābūt uzliktiem visiem pieejamiem **nepieciešamajiem** programmatūras atjauninājumiem

.*Sistēmas izstrāde un testēšana tiek veikta, nodrošinot, ka **netiek sabojāta** sistēmā glabātā **informācija**

.*Sistēmu atļauts izvietot pie tāda ārpakalpojumu sniedzēja, kas ir ES, EEZ jur. persona

Aizsardzības ministrija

Paredzamais pārejas periods

- 01.01.2017. Dokumenti apstiprināti
- 01.01.2018. paaugstinātas drošības sistēmām stājas spēkā tehniskās prasības
- 01.07.2018. paaugstinātas drošības sistēmas, kas neatbilst prasībām, tiek likvidētas
- 01.01.2021. pamata drošības sistēmām stājas spēkā tehniskās prasības
- 01.07.2021. paaugstinātas drošības sistēmas, kas neatbilst prasībām, tiek likvidētas

Aizsardzības ministrija

Papildus informācija pieejama, sazinoties ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu

kirils.solovjovs@mod.gov.lv