

Kopsavilkums un noderīga informācija

Rīga, 2016.gada 18.februāris

Semināra programma

Laiks	Norise	Lektors
13:00 -13.30	Dalībnieku reģistrācija	
13:30-13:55	„Kopsavilkums un noderīga informācija” MK noteikumu prasību ietvars; Atbildīgās personas pienākumi un tiesības; CERT.LV paraugu gatavošanas metodoloģija; Pārejas periods.	Baiba Kaškina, CERT.LV Edgars Tauriņš, CERT.LV
13:55-14:20	“Aktuālās MK noteikumu prasības” Prasības iepirkumiem; Prasības ārpakalpojumu sniedzējiem; Drošības pārbaudes un auditi.	Baiba Kaškina, CERT.LV
14:20-14:50	Kafijas pauze	
14:50-15:20	“Pamata vai paaugstinātas drošības sistēma?”	Egils Stūrmanis, CERT.LV
15:20-16:30	“Dokumentācijas sakārtošana un prasību ievērošana” Vispārējās prasības dokumentācijai - izstrāde, pārskatīšana, atjaunošana, integrēšana esošajā regulējumā.	Egils Stūrmanis, CERT.LV Edgars Tauriņš, CERT.LV
16:30	Semināra noslēgums	

Šodienas tēma

(MK NOTEIKUMI)

Ministru kabineta noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”

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

Paldies

**Visiem, kas palīdzējuši ar idejām, labojumiem,
komentāriem un jautājumiem:**

- **Sergejam Kanterukam**
- **Kristapam Miļevskim**
- **Kirilam Solovjovam**

... citiem

Izmaiņu nepieciešamība

- Mērķis - nodrošināt minimālo drošības prasību izpildi visās valsts un pašvaldību institūcijās
- Pirms šiem MK noteikumiem drošības regulējums neattiecās uz lielu daļu no valsts un pašvaldību informācijas sistēmām
- Pirms šiem MK noteikumiem nekur nebija noteiktas konkrētas tehniskās drošības prasības
- Informācijas drošības riski netika pietiekami apzināti
- Drošības prasības netika pietiekami iekļautas iepirkumu prasībās

Saistītie normatīvie akti

- Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības
- Valsts informācijas sistēmu vispārējās tehniskās prasības
- Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības
- Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu
- Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi
- ...

MK noteikumu ietvars

**Valsts un pašvaldību institūciju pārziņā vai turējumā
esošās informācijas un komunikācijas tehnoloģiju
sistēmas**

**Valsts informācijas
sistēmas**

**Kritiskās
infrastrukturās
informācijas sistēmas**

**Sistēmas, kurās tiek veikta valsts
noslēpuma, Ziemeļatlantijas līguma
organizācijas, Eiropas Savienības un
ārvalstu institūciju klasificētās
informācijas vai informācijas dienesta
vajadzībām apstrāde**

Likums un noteikumi

Reglamentēti informācijas tehnoloģiju drošības noteikumi

Pamata
informācijas
sistēmas

Paaugstinātas drošības informācijas
sistēmas

IT apraksti un shēmas

Personu pienākumi

IT drošības
incidentu vadības plāns

IT risku pārvaldības plāns

Sistēmas drošības politika

Sistēmas drošības
politika

Sistēmas drošības
noteikumi

Sistēmas
lietošanas
noteikumi

Sistēmas
darbības
atjaunoša
nas plāns

Sistēmas drošības risku pārvaldības
plāns

Darba plāns

- Atbildīgās personas noteikšana/identificēšana
- Esošo/plānoto sistēmu inventarizācija
- Pieejamības, integritātes un konfidencialitātes klases (A,B,C) noteikšana
- Drošības kategorijas (pamata vai paaugstināta) noteikšana
- Esošās dokumentācijas pārskatīšana/papildināšana
- Jaunu dokumentu sagatavošana
- Noteikumu prasību izpildes kontrole

Informācijas un komunikācijas tehnoloģiju sistēma

CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

No Valsts informācijas sistēmu likuma

- Informācijas un komunikācijas tehnoloģiju sistēma (Sistēma) - strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta iestādes funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana

Lietošanai, lai izstrādātu CERT.LV noteikumu paraugus

- Informācijas un komunikācijas tehnoloģiju sistēma (Sistēma) ir Iekārtu (HW) un Programmatūras (SW) un datu kopums, kas organizēts tādā veidā, lai nodrošinātu iestādes funkciju un/vai pakalpojumu nodrošināšanu

Sistēmas MK noteikumu izpratnē

- Valsts informācijas sistēmas
- Iestādes mājas lapas/tīmekļa vietnes
- Iestādes iekšējās sistēmas:
 - Personālvadība
 - Grāmatvedība
 - Videonovērošanas sistēma
- IKT resursi
 - E-pasts
 - Iekšējā DNS sistēma
 - IP telefonijas sistēma
 - IDS/IPS ...

Atbildīgā persona (sistēmas drošības pārvaldnieks)

- Iestādes vadītāja pilnvarota ar nepieciešamajiem līdzekļiem/resursiem funkciju veikšanai
- Nosaka sistēmas drošības kategoriju
- Nodrošina nepieciešamo Sistēmas drošības dokumentu uzturēšanu un īstenošanu
- Atbild par risku analīzes veikšanu
- Veic noteikto drošības prasību ievērošanas uzraudzību un drošības incidentu izmeklēšanu
- Nodrošina darbinieku apmācību informācijas drošības jomā

Atbildīgā persona (piemēri)

- Pakļauts tieši iestādes vadītājam
- Pakļauts IT vadītājam
- Procesu pārvaldības nodaļā
- Ārpakalpojums

Dokumentācija

- **Pamata drošības sistēmām - 14 tehniskas prasības**
 - sistēmas drošības politika
- **Paaugstinātas drošības sistēmām - 25 tehniskas prasības**
 - sistēmas drošības politika
 - sistēmas drošības iekšējie noteikumi
 - sistēmas lietošanas noteikumi
 - sistēmas drošības riska pārvaldības plāns
 - sistēmas darbības atjaunošanas plāns

Kāpēc nepieciešama dokumentācija

- Rūpes par organizācijas un sadarbības partneru sistēmu drošību
- Rīcības plāns drošības incidentu gadījumā
- Atbilstība normatīvajiem aktiem

Dokumentu pārvaldība

- Visus dokumentus apstiprina institūcijas vadītājs (praktiski «maka turētājs»)
- Izstrādā un aktualizē atbildīgā persona
- Pārskata vismaz reizi gadā, ja nepieciešams, atjauno
- Var būt vienoti visām/vairākām sistēmām, atsevišķi izdalot specifiskās prasības
- Iekšējais normatīvais akts
- Pieļaujams izstrādāt dokumentus padotības/pakļautības iestādēm

CERT.LV paraugi

- Vispārīgi ar ieteikumiem, kas būtu jāievēro
- Pielāgoti iedomātai virtuālajai iestādei
- Iespējami īsi un vienkāršoti
- Publicēti mājas lapā
- Brīvi izmantojami
- Pielāgojami iestādes vajadzībām
- Jautājumu un atbilžu sadaļa

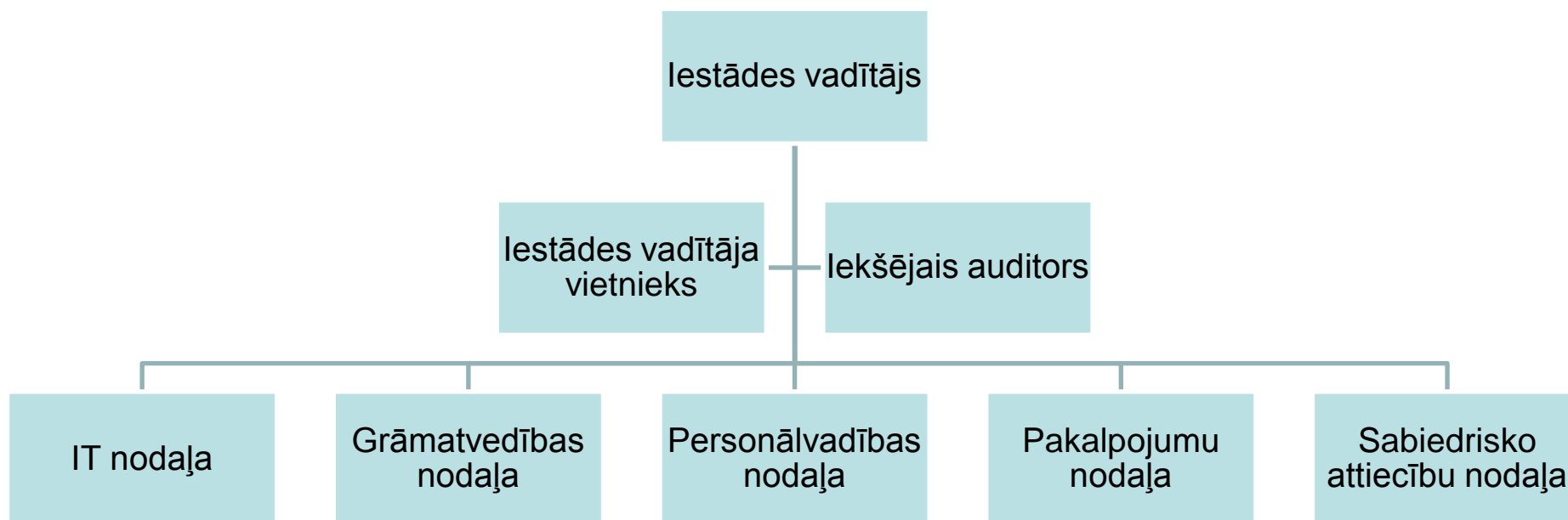
Par dokumentu paraugiem

- Maksimāli ievērota MK noteikumu struktūra un terminoloģija (sarkanā krāsā)
- Precīzie formulējumi tehniskajām prasībām atrodami MK noteikumos
- Paraugos iekļautie formulējumi un skaidrojumi nav juridiski saistoši
- Paraugos iekļauts CERT.LV viedoklis/priekšlikumi
- Paraugos apzināti iekļauta informācijas pārklāšanās

Virtuālā iestāde

- Pagaidām nav IT drošības dokumentācijas
- Identificētas 5 informācijas sistēmas:
 - Ievieš jaunu personālvadības sistēmu PERSONĀLS
- Nosaukums – IESTĀDE
- Funkcijas – PAKALPOJUMA nodrošināšana iedzīvotājiem

Virtuālā iestāde - struktūra



Citās valstīs

- Igaunija (ISKE)
 - Trīs drošības līmeņi
 - 1000 tehniskās prasības
 - Vairākas versijas sākot no 2003.gada
- ASV (NIST 800 ...)
 - Trīs drošības līmeņi
 - Vairāk kā 200 kontroles
 - 4.versija

Paldies!