Sistēmas drošības politika paaugstinātas drošības informācijas sistēmai

1. Termini

Iesakām pēc iespējas izmantot terminus kas izmantoti normatīvajos aktos (Informācijas tehnoloģiju drošības likums[1], MK noteikumi "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"[2]). Protams, pēc nepieciešamības pielāgojot iestādes specifikai. Drošības politikā lietotos terminus izmantot arī politikai pakārtotajos drošības dokumentos

1.1.

2. Sistēmas drošības politikas mērķi un pamatnostādnes

Jānosaka, kādu mērķi vēlas sasniegt ar politikas dokumentu, kā arī jāapliecina valdības atbalsts politikas īstenošanai.

2.1.

3. Sistēmas drošības politikas uzdevumi

Politikas uzdevumu uzskaitījumā var izmantot MK noteikumu 5.nodaļā minēto pasākumu kopumu, pielāgojot to iestādes vajadzībām. Šeit var atrunāt arī citus uzdevumus, ja tas nepieciešams attiecīgajai iestādei vai sistēmai.

3.1. nodrošināt informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
3.2. nodrošināt informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);
3.3. nodrošināt informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
3.4. aizsargāt Sistēmas informācijas resursus;
3.5. aizsargāt Sistēmas tehniskos resursus;
3.6. noteikt Sistēmas drošības apdraudējumus;
3.7. novērtēt Sistēmas drošības riskus;
3.8. atklāt Sistēmas drošības incidentus;
3.9. atjaunotu Sistēmas darbību pēc sistēmas drošības incidentiem.

4. Sistēmas raksturojums un analīze drošības jomā

Šeit nepieciešams augsta līmeņa sistēmas apraksts, kādām iestādes funkcijām tā paredzēta, lietotāju raksturojums. Gadījumā, ja dokuments tiek veidots par vairākām sistēmām šeit jāapraksta visas

[1] http://likumi.lv/doc.php?id=220962

[2] http://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam

4.1. Sistēma paredzēta iestādes funkciju nodrošināšanai:
4.2. Sistēmā apstrādātie dati, to klasifikācijas līmenis:
4.3. Sistēmas lietotāji/lietotāju tipi:
4.4. Saistītās sistēmas:

5. Sistēmas drošības pārvaldības organizācijas principi

Aprakstīt, kā iestādē organizēta attiecīgās sistēmas drošības pārvaldība. Uzmanību vēlams pievērst skaidri definētam pienākumu un atbildības sadalījumam. Šeit ieteicams aprakstīt arī atbildību par politikas prasību neievērošanu.

5.1.

6. Sistēmas drošības atbilstība normatīvajiem aktiem un standartiem

Uzskaitīt normatīvos aktus un standartus, kas ir piemērojami Sistēmas drošībai. Plaši izmantots informācijas drošības pārvaldības standarts ir ISO 27001 "Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības". Šis standarts ir izmantots arī, piemēram, Ministru kabineta noteikumos "Kredītinformācijas biroju licencēšanas un uzraudzības noteikumi" un "Parakstu vākšanas tiešsaistes sistēmu drošības un tehniskās prasības". Nepieciešamības gadījumā vēlams uzskaitīt Sistēmai vai Iestādei specifiskus noteikumus vai standartus.

6.1.

7. Sistēmas drošības principi

Šajā nodaļā aprakstītas MK noteikumos iekļautās prasības, kā arī nodaļu var papildināt ar Sistēmai vai Iestādei specifiskiem drošības principiem.

7.1. Sistēmas lietotāju konti.
- 7.1.1. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – sistēmas administratora konti), kas netiek izmantoti ikdienas darbību veikšanai;
- 7.1.2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai (turpmāk – sistēmkonti), tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot sistēmkontus;
- 7.1.3. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus iestādes telpām, iespējams tikai izmantojot daudzfaktoru autentifikāciju;
- 7.1.4. sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju.

7.2. Prasības parolēm.

7.2.1. ja sistēmā netiek izmantota daudzfaktoru autentifikācija, t.i. viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts, tad sistēmas lietotājiem ir obligāti jālieto paroles;
7.2.2. sistēmas lietotāja paroļu garums nav mazāks par deviņiem simboliem un satur vismaz lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un citu simbolu;
7.2.3. katram sistēmas lietotājam parole ir obligāti jāmaina pēc ne vairāk kā 90 dienām;
7.2.4. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;
7.2.5. sistēmas lietotāja paroles aizliegts glabāt un transportēt nešifrētā veidā, t.sk. lietotāja autentifikācijas procesa ietvaros;
7.2.6. sistēmas lietotāja parole netiek pilnībā attēlota lietotājam;
7.2.7. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama;
7.2.8. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
7.2.9. iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;

7.3. Izsekojamība.

7.3.1. tiek nodrošināta sistēmas pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot pierakstus vai to kopijas atsevišķi no sistēmas;
7.3.2. sistēmas pieraksti tiek veidoti, nodrošinot, ka ierakstā norādītais laiks sakrīt ar faktiskā notikuma koordinēto universālo laiku (UTC) ar vienas sekundes precizitāti;
7.3.3. tiek nodrošināta sistēmas auditēšanas ierakstu satura plānveida uzraudzība un analīze, lai konstatētu incidentus;
7.3.4. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei.

7.4. Atjauninājumi.

7.4.1. Sistēmai jābūt uzliktiem visiem pieejamajiem nepieciešamajiem programmatūras atjauninājumiem.

8. Sistēmas aizsardzības pasākumi

Šajā nodaļā aprakstītas MK noteikumos iekļautās prasības, kā arī to var papildināt ar Sistēmai vai Iestādei specifiskiem aizsardzības pasākumiem.

8.1. visās institūcijas valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;
8.2. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu;
8.3. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām;
8.4. plūsma starp informācijas sistēmu un tās lietotājiem, kā arī starp informācijas sistēmu un citām informācijas sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri;
8.5. datortīkla pakalpojumi (network services), kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;
8.6. veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmās glabāto datu integritātei;

8.7. sistēmas izvietošana ārpakalpojumu sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojumu sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

9. Sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamais līmenis

Risku pārvaldība jāapraksta atbilstoši Noteikumu 7. punktā aprakstītajai metodikai. Ja ir noteikts konkrēts risku pieņemamais līmenis, tas jāapraksta šeit.

9.1.

10. Sistēmas drošības kritēriji

Ministru kabineta noteikumi paredz, ka lietotājiem jāpadara pieejami vismaz zemāk uzskaitītie sistēmas drošības kritēriji.

10.1. Sistēmas nepārtrauktās darbības laiks:
10.2. Sistēmas darbības atjaunošanas laiks:
10.3. Nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām:
10.3.1.

11. Noslēguma jautājumi

Šajā nodaļā aprakstītas sistēmas drošības politikas pārskatīšanas regularitāte, ja nepieciešams šeit arī norādīt pārejas periodu, kādā sistēmas politika stājas spēkā.

11.1. politiku pārskata vismaz reizi gada, ka arī šādos gadījumos:
11.1.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
11.1.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
11.1.3. ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents.
11.2. Ja, pārskatot politiku, konstatēta atbilstoša nepieciešamība, to aktualizē.