Seminārs Interneta pakalpojumu sniedzējiem 13.10.2011. - programma

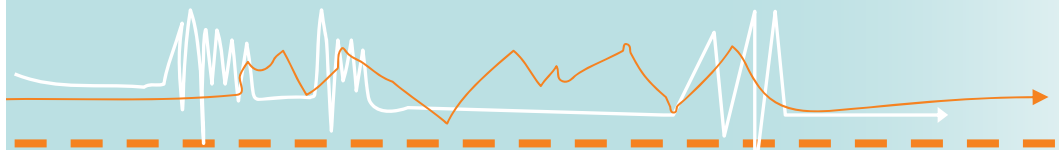
1. „Īsi par CERT.LV” - Baiba Kaškina, CERT.LV vadītāja, 20 minūtes
2. „IT drošības likuma un MK noteikumu prasības attiecībā uz IPS” - Baiba Kaškina, CERT.LV vadītāja, 45 minūtes
3. „Personas datu aizsardzības pārkāpuma paziņošana” - Mārtiņš Indāns, Datu valsts inspekcija, 15 minūtes
4. „Botnetu un datorvīrusu apkarošana sadarbībā ar CERT.LV” - Gints Mālkalnietis, CERT.LV tehniskais speciālists, 30 minūtes

IT drošības likuma un MK noteikumu prasības attiecībā uz IPS

Seminārs Interneta pakalpojumu sniedzējiem

13.10.2011., Rīga

Baiba Kaškina, CERT.LV



CERT.LV

IT drošības likums

IT drošības likums

- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājās spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Paredz MK noteikumu izstrādi par
  - Kritiskās infrastruktūras drošības pasākumu plānošanu (spēkā no 2011.gada 1.februāra)
  - Elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam (no 2011.gada 1.maija)
- Nosaka Nacionālās informācijas tehnoloģiju drošības padomes izveidi

Elektronisko sakaru komersantu pienākumi

- Nodrošināt maksimāli iespējamo pakalpojumu sniegšanas nepārtrauktību un sastādīt rīcības plānu nepārtrauktas darbības nodrošināšanai
- Informēt CERT.LV būtisku incidentu gadījumā
- Sniegt CERT.LV pieprasīto informāciju saistībā ar incidentiem
- Pēc CERT.LV pieprasījuma, ja ir būtiski drošības vai integritātes pārkāpumi, organizēt auditu
- Pēc CERT.LV pieprasījuma slēgt galalietotājam piekļuvi elektronisko sakaru tīklam

MK noteikumi nr.327 “Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam”

MK noteikumi

- Stājušies spēkā 2011.gada 1.maijā
- Rīcības plāns jāizstrādā 6 mēnešu laikā – līdz 31.oktobrim

Atsauce uz direktīvu

Noteikumos iekļautas tiesību normas, kas izriet no Eiropas Parlamenta un Padomes 2009.gada 25.novembra Direktīvas 2009/140/EK, ar ko izdara grozījumus direktīvā 2002/21/EK par **kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem**, direktīvā 2002/19/EK par **piekļuvi elektronisko komunikāciju tīkliem un ar tiem saistītām iekārtām un to savstarpēju savienojumu** un direktīvā 2002/20/EK par **elektronisko komunikāciju tīklu un pakalpojumu atļaušanu**.

Rīcības plāna saturs

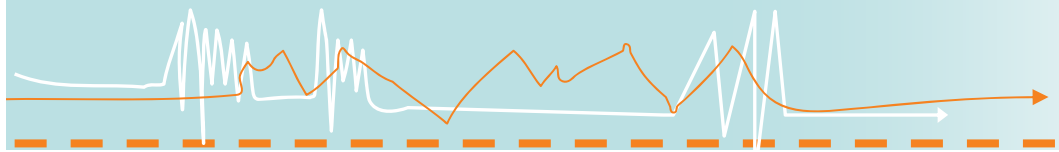
1. Vispārīgas ziņas par komersantu, juridiskā adrese, elektroniskā pasta adreses
2. Persona vai struktūrvienība, kas nodrošina drošības pasākumu īstenošanu (tālruņa numurs, fakss, e-pasts)
3. Elektronisko sakaru tīkla uzbūves vispārīgs apraksts un shēma
4. Elektronisko sakaru tīkla risku analīze
5. Reaģēšanas kārtība uz drošības incidentiem
6. Tīkla darbības atjaunošanas pasākumu apraksts

Svarīgi no MK noteikumiem

- Izņēmumi attiecībā uz Kritisko infrastruktūru.
- Ja ir izmaiņas – plāns jāaktualizē
- Mēneša laikā par izmaiņām jāinformē CERT.LV
- Jānorāda, ja informācija ir ierobežotas pieejamības
- CERT.LV izvērtē plānu un var lūgt izdarīt labojumus
- CERT.LV izmanto informāciju, īstenojot IT drošības likumā noteiktos uzdevumus un tiesības

Galalietotāju īslaicīga atslēgšana

- CERT.LV var pieprasīt atslēgt galalietotāju uz laiku līdz 24h
- Pieprasījums tiek nosūtīts elektroniski
- CERT.LV informē arī telefoniski gan IPS, gan VP
- Jāatslēdz stundas laikā
- Atslēgšana – lai darbība skartu pēc iespējams mazāku skaitu citu galalietotāju



CERT.LV

Rīcības plāns

Vispārīgas ziņas par komersantu, juridiskā adrese, elektroniskā pasta adreses

- Nosaukums.
- Reģistrācijas numurs.
- Juridiskā adrese.
- Uzņēmuma e-pasta adrese.

Persona vai struktūrvienība, kas nodrošina drošības pasākumu īstenošanu

- Kas ir atbildīgs par drošību?
  - Persona vai struktūrvienība?
- Jānorāda:
  - Vārds, uzvārds vai nosaukums.
  - Telefona numuri, fakss.
  - Elektroniskā pasta adrese.
- Vēlams norādīt:
  - Adrese (ja atšķiras no juridiskās).
  - Darba režīms (24x7?)

Elektronisko sakaru tīkla uzbūves vispārīgs apraksts un shēma

- Ģeogrāfiskā izplatība.
- Centrālie mezgli.
- Izmantotās tehnoloģijas.
- Shēma vai shēmas.

- Iespējams iesniegt gan jau esošus un apstiprinātus dokumentus, gan arī izveidot kopsavilkumu MK noteikumu izpildei.

Elektronisko sakaru tīkla risku analīze

- Būtiskākie apdraudējumi.
- Risku pārvaldība
  - Risku novērtēšana.
  - Risku ierobežošana.

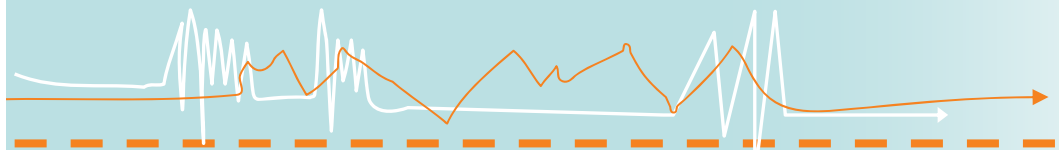
Reaģēšanas kārtība uz drošības incidentiem

- Kā tiek saņemta informācija par drošības incidentiem?
  - Monitorings
  - No CERT.LV
  - Klientu sūdzības
  - No citiem avotiem, piem. *abuse* ziņojumi
- Incidentu klasifikācija, svarīgums, reakcija
- Kā tiek apziņoti klienti?
  - Palīdzība datora “ārstēšanā”?
- Kā tiek reaģēts uz incidentiem savā infrastruktūrā?
  - Incidenta identificēšana, cēloņi, seku novēršana
- Kā notiek sadarbība ar CERT.LV?

Tīkla darbības atjaunošanas pasākumu apraksts

- Kādi ir pienākumi pret klientiem
  - Cik ilgi pārtraukumi ir pieļaujami
- Darbības fizisku bojājumu gadījumā
- Darbības loģisku bojājumu gadījumā
- Ko darīt DDoS gadījumā?

- “Nepārtrauktības plāns”



CERT.LV

Risku analīze

Metodoloģija

- Risk Management Guide for Information Technology Systems
- http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- Izmantoti Ilzes Murānes prezentāciju materiāli

Risku pārvaldības process

- Lomas
- Riska novērtēšana
  - Sistēmas raksturošana
  - Apdraudējumu identificēšana
  - Ievainojamību identificēšana
  - Vadīklu (*controls*) analīze
  - Iespējamību noteikšana
  - Ietekmju analīze
  - Risku noteikšana
  - Vadīklu (*controls*) ieteikšana
  - Rezultātu dokumentēšana
- Riska ierobežošana

Lomas

- Augstākā vadība
- Atbildīgais par informāciju
- Resursu turētāji
- Iestādes procesu pārzinātāji
- IT drošības speciālisti
- Atbildīgais par IT drošības apmācību

Sistēmas raksturošana

- Aparatūra, programmatūra, dati, uzturēšanas process, sistēmas misija, kritiskums
- Funkcionālās prasības, lietotāji, drošības arhitektūra, tīkla shēma, informācijas plūsmas, pārvaldības procedūras, fiziskā aizsardzība
- Informācijas iegūšanas tehnikas
  - Aptaujas anketas
  - Intervijas
  - Dokumentu analīze
  - Automātiski rīki
- Rezultāts: IT sistēmas raksturojums, laba izpratne par vidi un sistēmas robežām

Apdraudējumu identificēšana

- Apdraudējumu avoti
  - Daba (plūdi, zemestrīce)
  - Cilvēki (nejaušas kļūdas, ļaunprātīga rīcība, iekšēji/ārēji uzbrukumi)
  - Vide (elektrības piegādes traucējumi, uguns, tehnikas problēmas)
- Ļaunprātības motivācija: hakeri, noziedznieki, spiegi, neapmierināti darbinieki
- Rezultāts: avotu saraksts, kas varētu izmantot sistēmas ievainojamības

Ievainojamību identificēšana

- Ievainojamību un apdraudējumu avotu pāri.
- Ievainojamību datu avoti:
  - Iepriekšējas risku analīzes
  - Audita ziņojumi
  - Dati no pētījumiem/ražotājiem
  - u.c.
- Sistēmas testi.
- Drošības prasību kontrollapa.
- Rezultāts: Sistēmas ievainojamību saraksts.

Iespējamību noteikšana

- **Augsta** – apdraudējuma avots ir augsti motivēts, ar pietiekamiem resursiem, vadīklas neefektīvas.
- **Vidēja** – apdraudējuma avots ir motivēts, ar resursiem, vadīklas ir, bet daļējas.
- **Zema** – apdraudējuma avotam trūkst motivācijas un/vai resursu, vadīklas ir labas.
- **Rezultāts**: Iespējamības novērtējums.

Ietekmju analīze

- Jāatkārto sistēmas misija, kritiskums u.tml.
- Integritātes, pieejamības, konfidencialitātes zudums:
  - **Augsta** – lielas izmaksas, būtiski ietekmē organizācijas misiju vai reputāciju, cilvēku dzīvības apdraudējums
  - **Vidēja** – nozīmīgas izmaksas, ietekmē organizācijas misiju vai reputāciju, cilvēku veselības apdraudējums
  - **Zema** – nelielas izmaksas, nedaudz ietekmē organizācijas misiju vai reputāciju.
- Rezultāts: ietekmes lielums.

Risku noteikšana

- Iespējamība X Ietekme

- **Augsts** – steidzami jāveido un jāīsteno riska ierobežošanas plāns.
- **Vidējs** – papildus riska ierobežošanu veic saprātīgā termiņā.
- **Zems** – visbiežāk risks ir pieņemamā līmenī.
- **Rezultāts**: riska līmenis, risku novērtējuma tabula.

Risku pārvaldība – ierobežošanas stratēģijas

- Riska pieļaušana (To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level)
- Izvairīšanās no riska (To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified))
- Riska samazināšana (To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls))
- Riska plānošana (To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls)
- Riska nodošana (To transfer the risk by using other options to compensate for the loss, such as purchasing insurance)

Dokumentu paraugi www.cert.lv

- Piemērs: IT drošības pārvaldības shēma
- Pašvaldību un valsts iestāžu IT drošības noteikumu vadlīnijas
- Ieteicamās prasības izmaiņu pārvaldībai
- Piemērs: Virtuālas iestādes apraksts
- Piemērs: Resursu klasifikācija, Risku analīze un pārvaldība

Paldies par uzmanību!

http://ww.cert.lv/
cert@cert.lv
baiba.kaskina@cert.lv

Seminārs Interneta pakalpojumu sniedzējiem 13.10.2011. - programma

1. „Īsi par CERT.LV” - Baiba Kaškina, CERT.LV vadītāja, 20 minūtes
2. „IT drošības likuma un MK noteikumu prasības attiecībā uz IPS” - Baiba Kaškina, CERT.LV vadītāja, 45 minūtes
3. „Personas datu aizsardzības pārkāpuma paziņošana” - Mārtiņš Indāns, Datu valsts inspekcija, 15 minūtes
4. „Botnetu un datorvīrusu apkarošana sadarbībā ar CERT.LV” - Gints Mālkalnietis, CERT.LV tehniskais speciālists, 30 minūtes