DDIRV.LV
Datoru drošības incidentu reaģēšanas vienība

Aktuālā informācija par datoru drošības incidentiem un riskiem

Egils Stūrmanis
LR Satiksmes ministrija
Nacionālā datoru drošības incidentu reaģēšanas vienība
2010.gada 30.septembris

Tēmas

- Plānotās izmaiņas tiesību aktos
- Nacionālās datoru drošības incidentu reaģēšanas vienības (DDIRV) darbības principi
- Kā atpazīt incidentu
- Kā rīkoties incidenta gadījumā
- Kopsavilkums

Plānotās izmaiņas tiesību aktos

- Likumprojekts “Informācijas tehnoloģiju drošības likums”
- Grozījumi Elektronisko sakaru likumā
- Grozījumi Valsts informācijas sistēmu likumā
- Plānots stiprināt nacionālo datoru drošības incidentu reaģēšanas vienību (kā Informācijas tehnoloģiju drošības incidentu novēršanas institūciju)
- Plānots izveidot kritiskās infrastruktūras sistēmu
- Plānots noteikt pamatprasības valsts un pašvaldību IT, kā arī sadarbību ar minēto institūciju

DDIRV darbības principi

- Sadarbība balstoties uz brīvprātību un uzticību
- Palīdzība incidentu gadījumos ir bez maksas, bez līguma
- Labā prakse – katra incidenta gadījumā, ja ir iespēja sniedz informāciju, kā risināt problēmas
- Incidentu pieteikšana – ieguldījums kopējā datorsistēmu un tīklu drošībā
- Ikviens incidents ir neizpaužams
- Pamatprincips – palīdzēt, bet ne “sodīt”

Kā atpazīt datoru drošības incidentu

Incidents ir jebkāds kaitīgs notikums vai nodarījums, kura rezultātā tiek vai var tikt ietekmēta datoru vai datoru tīklu drošība.

- Pakalpojuma atteice
- Neautorizētas resursa satura izmaiņas
- Aizdomīga / netipiska aktivitāte tīklā
- Masveida kaitīgu programmu izplatība tīklā
- Jūtīgas informācijas izpaušana

Kā rīkoties incidenta gadījumā

- Paziņot tiešajam vadītājam
- Paziņot DDIRV, ja nepieciešams policijai
- Saglabāt pierādījumus
- Atjaunot sistēmas darbību
- Sagatavot paziņojumu organizācijas iekšienē
- Sagatavot priekšlikumus ārējai komunikācijai

Kopsavilkums

- DDIRV darbības pamatprincipi
- Incidentu atpazīšana un rīcība krīzes situācijā
- Līdzsvars starp izveidoto drošību un pašu atbildību
- Sadarbības nepieciešamība
- Informācijas apmaiņa

Paldies par uzmanību!

Nacionālā datoru drošības incidentu reaģēšanas vienība

- telefons: 67028040, 67028041
- tīmekļa vietne: www.ddirv.lv , www.sam.gov.lv
- e-pasts incidentu pieteikšanai: ddi@ddirv.lv
- e-pasts informācijai: info@ddirv.lv
- incidenta pieteikšana tīmekļa vietnē: www.ddirv.lv
- Reģistrēšanās par dalībnieku: www.ddirv.lv

DDIRV.LV
Datoru drošības incidentu reaģēšanas vienība