arnes
p.p. 7, SI-1001 Ljubljana
T +386 1 479 88 77, F +386 1 479 88 78
E arnes@arnes.si, www.arnes.si

APEK
Stegne 7
p.p. 418
1001 Ljubljana

Ljubljana, 22. junij 2013

Zadeva: Predlog dopolnitev Splošnega akta o varnosti omrežij in storitev (0073-45/2013)

Spoštovani!

Pošiljam vam dopolnjeni predlog dopolnitev Splošnega akta o varnosti omrežij in storitev, ki je v javni razpravi.

Gorazd Božič
vodja SI-CERT, ARNES

Predlog dopolnitev Splošnega akta o varnosti omrežij in storitev (SI-CERT)

1. K 1. odstavku 2. člena se doda opredelitev izraza SI-CERT:

> SI-CERT je nacionalni odzivni center za omrežne incidente, ki deluje v okviru javnega zavoda Akademska in raziskovalna mreža Slovenije (ARNES).

2. Za 14. členom (obveščanje in poročanje) se doda nov člen:

15. člen
(obravnava incidenta omrežne in informacijske varnosti)

(1) Agencija operativno razreševanje incidenta omrežne in informacijske varnosti preda SI-CERT z namenom strokovne pomoči in svetovanja operaterju, usklajevanja z deležniki znotraj države, ter koordinacijo z odzivnimi CERT centri in drugimi sorodnimi službami v tujini.

(2) Po zaključeni obravnavi incidenta SI-CERT poda poročilo Agenciji o poteku obravnave in rezultatih, skupaj z morebitnimi priporočenimi ukrepi za izboljšanje varnosti omrežja in storitev.

(3) Obveščanje o incidentih omrežne in informacijske varnosti, ter poročanje o rezultatih njihove obravnave se izvaja elektronsko.

Obrazložitev predlaganih sprememb

Splošni akt o varnosti omrežij in storitev izhaja iz novega Zakona o elektronskih komunikacijah (ZEKom-1, Ur.l. RS, št. 109/2012). Ta v 2. odstavku 81. člena določa tudi, da *"Agencija o posameznih kršitvah varnosti omrežij in storitev ter o kršitvah celovitosti omrežij po potrebi in glede na stopnjo kršitve obvešča nacionalno kontaktno točko za obravnavo varnostnih incidentov (SI-CERT)"*, 216. členu pa, da *"Zaradi zagotavljanja varnosti in celovitosti omrežij lahko agencija zaprosi za strokovno sodelovanje tudi SI-CERT, ki deluje v okviru javnega zavoda Akademska in raziskovalna mreža Slovenije (ARNES), in druge organe, pristojne za varnost in celovitost omrežij."* Poleg normativne ureditve obveščanja o varnostnih incidentih je pomemben tudi primeren odziv v smislu tehnične analize konkretnega incidenta z namenom identifikacije ranljivosti, ki so do njega pripeljale in morebitnega širšega konteksta omrežnih napadov. SI-CERT obravnava *incidente omrežne ali informacijske varnosti*, tj. dogodke, ki predstavljajo kršitev varnostnih mehanizmov in pravil dopustne uporabe v informacijskih sistemih, računalniških omrežjih in javno dostopnih omrežnih storitvah, oziroma predstavljajo grožnjo za to kršitev. SI-CERT s strokovno podporo operaterju in drugim prizadetim v incidentu lahko v okviru svojih pristojnosti in zmogljivosti pomaga pri zamejitvi škodljivih vplivov incidenta, zbiranju dokazov na računalniških sistemih in v omrežju, odstranitvi škodljivih komponent in povrnitvi v prejšnje stanje. SI-CERT kot član mednarodnih združenj odzivnih CERT centrov po potrebi opravi tudi koordinacijo razreševanja incidenta skupaj s tujimi partnerji.

Ob zaključenem incidentu s podajo poročila Agenciji SI-CERT opiše ugotovljene vzroke za posamezni incident, uporabljene metode v njem in njegove posledice. Na podlagi tega se izoblikuje priporočila, ki jih lahko Agencija upošteva pri nadaljnjih dopolnitvah predpisanih ali priporočenih zaščitnih ukrepov za operaterje. Tak proces omogoča, da se ukrepi ščitenja dopolnjujejo skupaj z razvojem storitev in novimi načini zlorab in napadov na informacijske sisteme in storitve na omrežjih.

ZEKom-1 v zgoraj navedenih členih daje pravno podlago za sodelovanje med Agencijo in SI-CERT, zato je tudi primerno, da se v Splošnem aktu o varnosti omrežij in storitev to sodelovanje opiše. Tako bo akt

pripomogel tudi k odzivanju na incidente, pomoči operaterjem in dolgoročno k izboljšanju splošne ravni varnosti računalnišlih omrežij in storitev v Sloveniji.