Sistemci i službe za računalnu sigurnost, udružene snage

Računalno sigurnosni incidenti učestala su pojava u računalnom svijetu, a ni Hrvatska nije izuzetak po tom pitanju. Provale na računala i računalne mreže, širenje malicioznih programa, skeniranje portova...samo su neki primjeri povreda računalne sigurnosti što ima za posljedicu narušavanje normalnog funkcioniranja računala odnosno računalnih mreža.
Hrvatska akademska i istraživačka mreža CARNet ima brzu i razvijenu mrežu i ona je kao takva zanimljiva meta potencijalnim napadačima, no isto tako često predstavlja i izvor napada i stoga je vrlo bitno zajedničko djelovanje CARNet-a i sistem inženjera na ustanovama članicama u suzbijanju nedopuštenih aktivnosti.

CARNet CERT i Abuse služba obraćaju se CARNet sistem inženjerima ukoliko zaprime prijave o nedozvoljenim aktivnostima koje imaju izvor u ustanovi članici. Najčešće prijave odnose se na pokušaje neovlaštenih pristupa drugim sustavima, slanje neželjene pošte i kršenje autorskih prava. Od sistem inženjera očekuje se poduzimanje konkretnih aktivnosti vezanih uz incidente koji imaju izvor u mreži njihove ustanove, odnosno upozoravanje te sankcioniranje korisnika kao i slanje povratne informacije Abuse odnosno CERT službi.

Sigurnosna politika pojedine ustanove članice temelj je za poduzimanje aktivnosti i sankcioniranje korisnika ustanova, jer su na taj način definirani prihvatljivi i neprihvatljivi načini ponašanja, jasna raspodjela zadataka i odgovornosti te sankcije u slučaju nepridržavanja. Onim ustanovama koje još nisu definirale svoju sigurnosnu politiku, preporučamo što skorije donošenje iste, jer se na taj način jasno definiraju pravila korištenja te se sistem inženjerima olakšava poduzimanje konkretnih aktivnosti prema svim korisnicima njihove ustanove. Prijedlog sigurnosne politike možete pogledati na adresi: http://sistemac.carnet.hr/system/files/sigurnosna_politika_ustanove.pdf

Ukoliko sistemac ne reagira na zahtjev CERT odnosno Abuse službe ni nakon nekoliko upozorenja, a radi se o teškom incidentu ili učestalom ponavljanju incidenata, poduzimaju se oštrije mjere poput privremenog isključivanja ustanove s CARNetove mreže kako bi se otklonila mogućnost ugrožavanja ostalih korisnika.

Dosadašnja iskustva vezana za suradnju CERT i Abuse službi s CARNet sistem inženjerima uglavnom su pozitivna, pa se nadamo da ćemo i u budućnosti zajedničkim djelovanjem utjecati na povećanje razine sigurnosti cjelokupne mreže.

pet, 2007-03-09 09:55 - Uredništvo**Kategorije:** Informacijska sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/108

Links
[1] https://sysportal.carnet.hr/taxonomy/term/32