Dionici i razmjena informacija u informacijskoj sigurnosti

MIPRO ISS, 29. 5. 2014., OPATIJA

STJEPAN GROŠ I TONIMIR KIŠASONDI

VERZIJA 20140523

Pregled prezentacije

Uvod

Problemi s kojima se susrećemo

Posljedice problema

Kako promijeniti situaciju

Dugoročni i kratkoročni ciljevi

Neki primjeri suradnje u svijetu

Pregled događanja na skupu

Prije početka…

Svi imamo zajednički cilj

- Obavljati svoj posao profesionalno

I radi to cilja smo se okupili

- Da se upoznamo,
- Vidimo tko što radi,
- Saznamo koje probleme imaju drugi,
- Saznamo što bi od drugih mogli dobiti,
- Raspravimo o mogućnostima bolje suradnje.

Međutim,

- **Prilagodimo očekivanja!** Promjene su mukotrpne i spore, za dobre rezultate treba vremena.
- Treba imati cilj i biti uporan!

Problemi s kojima se susrećemo

Informacijska sigurnost obuhvaća svaki dio informacijskih i komunikacijskih sustava

- Izuzetno veliko područje
- Ogromna količina informacija
- Velika složenost sustava

Vrlo dinamično područje

- Konstantan razvoj novih tehnologija
- Razvoj novih metoda napada

Napadač mora pronaći barem jedan propust

- Oni koji se brane moraju zatvoriti sve propuste
  - Gotovo nemoguća misija
- Napredna ustrajna prijetnja (engl. *Advanced Persistant Threat*)

Još problema…

Svako okruženje specifično je i drugačije od ostalih

- Hrvatska je specifična okolina
- Tvrtka u kojoj radimo je specifična

Niz dionika koji sudjeluju i s kojima se susrećemo (ili ne):

- Znanstvenici, razne državne institucije, razne privatne tvrtke, hakeri, …

Ograničeni resursi na raspolaganju

- Rijetko kada neka okolina alocira dovoljno resursa za pokrivanje sigurnosti
  - Često se radi u situaciji u kojoj je potrebno pokriti veliko područje
- Hrvatska je mala zemlja s ograničenim brojem ljudi

Do sada smo bili relativno izolirani

- Jezik nam je specifičan, valuta specifična, pravila specifična
- Ulaskom u EU i sve jačom integracijom to se brzo mijenja

Posljedice problema

Jedan čovjek, ili čak i grupa ljudi, nema dovoljno znanja i resursa da pokrije sve

- Treba pratiti što se sve dešava u okolini i obavljati evaluaciju
  - Evaluacije, ako se žele napraviti dobro, su duge i složene
- Dovoljno brzo to obavljati kako bi informacije bile raspoložive na vrijeme

Poslovi se ne obavljaju dobro

- Prisutna velika količina nesigurnosti
- Neke stvari se čak rade i krivo (procjena rizika!)

Zaključak

- Ostvarivanje sigurnosti: Nemoguća misija

Kako promijeniti situaciju

Trebali bi težiti suradnji

- Malo nas je i strategija mora biti što veća suradnja
- Tako da posao koji obavljamo bude kvalitetniji
- Da sustavi za koje brinemo budu sigurniji

Kako bi suradnja bila bolja moramo se **dobro poznavati**

- Koji su sve dionici u sigurnosti
- Što su zadaće svakog dionika
- Što se od drugih dionika može dobiti
- Što se drugim dionicima može pružiti

Kratkorični cilj

Upoznati se međusobno

Saznati tko što radi

Vidjeti što se može koristiti od drugih i ponuditi drugima

Pokušati dogovoriti neke konkretne korake

Dugoročni cilj

Regionalno okupljanje svih stručnjaka za sigurnost

Neovisno o pojedinoj tvrtci

- Sveučilište u Zagrebu i MIPRO jamci neovisnosti

Kontrola kvalitete kao na znanstvenim konferencijama

- Za svako predavanje minimalno dva pozitivna mišljenja recenzenata

Dionici u sigurnosti

Državne institucije

- Ured Vijeća za nacionalnu sigurnost
- MUP
- Zavod za sigurnost informacijskih sustava

Tvrtke

- Financijske institucije
- Telekomi

Ljudi

- Voditelji sigurnosti
- Znanstvenici
- Hakeri

Primjeri suradnje – NIST

Izdavanje preporuke

- Javno objavljeno te se komentari prikupljaju od svih zainteresiranih u svijetu
- Aktivno traže ljude da komentiraju

Preporuke se koriste u državnoj administraciji SAD-a

- Ali i niz privatnih tvrtki koristi te preporuke

Primjer suradnje – razvoj CVSSv2 mjere

Skala od 1 do 10 za mjerenje ozbiljnosti neke ranjivosti

- Naočigled, vrlo jednostavno, postoji formula uz pomoć koje se to izračunava
- Međutim, razvoj nije bio jednostavan, niti brz

Neki citati iz dokumenta o povijesti razvoja CVSSv2 mjere*

- The initial CVSS v1 design **was not subjected to mass peer review** across multiple organizations or industries. After production use, feedback from CVSS-SIG and others **indicated there were significant issues with the initial draft of CVSS**.
- Razvoj tekao u niz iteracija
- Konačni izraz opet ima problema i radi se na razvoju CVSSv3 (iako već prilično dugo)

Zaključak: Razvoj na prvi pogled jednostavne mjere je vrlo složen proces!

(*) http://www.first.org/cvss/history