Serbian Open eXchange

CERT
DA LI NAM I ZAŠTO TREBA?

Dr Nenad Krajnović
Serbian Open Exchange
E-mail: krajko@sox.rs

Šta je CERT?

- ***C**omputer **E**mergency **R**esponse **T**eam*
- ***C**omputer **E**mergency **R**eadiness **T**eam*
- ***C**omputer **S**ecurity **I**ncident **R**esponse **T**eam*

- CERT predstavlja grupu eksperata iz oblasti *cyber* bezbednosti koji se bave pitanjima informacionih incidenata i informacione bezbednosti.

Da li je ovo CERT?

Više je nešto slično ovome...

... ili malo formalnije

Šta može da se desi?!?!

- U doba opšte informatizacije društva, *cyber* napadi mogu da budu destruktivniji od klasičnog vojnog napada.
- Samo neki mogući scenariji:
  - Totalno gašenje elektro-energetske mreže.
  - "Obaranje" telekomunikacione infrastrukture (telefoni, prenos podataka, TV,...)
  - Blokada i prekid rada Interneta u zemlji

Kako je počelo?

- 2003. SAD objavljuju dokument "*National Strategy to Secure Cyberspace*".
- 2005. Nemačka usvaja "Nacionalni plan za zaštitu informacione infrastrukture".
- 2006. Švedska: "Strategije za poboljšanje bezbednosti na Internet mreži u Švedksoj".
- 2007. Estonija posle sigurnosnog incidenta objavljuje opšti dokument strategije informacione bezbednosti.
- ...

Kako CERT može da pomogne?

- Kada vas neko opljačka zovete policiju, a koga zovete kada neko napadne vaš informacioni sistem?
- Za odbranu i zaštitu informacione bezbednosti potrebna je značajna koncentracija znanja iz oblasti IKT tehnologija.
- Nije isplativo i nije izvodljivo da svaka kompanija formira svoj ekspertski tim za oblast informacione bezbednosti.
- Potrebni su nam ekspertski timovi (CERT) na nivou grupe kompanija.

Vrste CERT-ova

- Kompanijski CERT
- "Esnafski" CERT
- Posebni CERT
- Nacionalni CERT

https://www.enisa.europa.eu/topics/national-csirt-network/csirt-inventory/certs-by-country-interactive-map

Zakonska regulativa

- Evropska unija je jula 2016. godina objavila dokument "*Network and Information Security Directive*" poznatiji kao NIS direktiva.
- Ova direktiva propisuje mere sa ciljem postizanja visokog zajedničkog stepena bezbednosti mreža i informacionih sistema unutar zemalja članica EU.

NIS direktiva

- Propisuje obavezu za sve zemlje članice da usvoje nacionalnu strategiju o bezbednosti mreža i informacionih sistema.
- Uspostavlja Grupu za međunarodnu saradnju kako bi se omogućila i olakšala strateška saradnja i razmena informacija među zemljama članicama EU, i izgradilo međusobno poverenje.
- Uspostavlja mrežu CERT organizacija, sa ciljem da doprinese razvoju poverenja i efikasne operativne saradnje među ovim organizacijama.
- Postavlja zahteve za bezbednošću i deljenje informacija sa operatorima ključne infrastrukture i servisa, i operatorima digitalnih servisa.
- Propisuje obvezu za sve zemlje članice da definišu nadležne organe, jedinstvene tačke kontakta, i CERT organizacije čiji će zadatak biti očuvanje bezbednosti mreža i informacionih sistema.

Ma šta će to nama...

- Tipičan odgovor je da mi nemamo takvih problema.
- Informacije o sigurnosnim incidentima iz oblast informacione bezbednosti se ne objavljuju.
- Kako da znamo da li smo ugroženi?
- Kako da znamo da li je uopšte bilo sigurnosnih incidenata?
- Hakeri vole da se hvale...

Ukupan broj hakovanih *web* stranica u .RS domenskom prostoru

izvor: www.zone-h.org

Ovo je samo jedan izvor informacija!!!

Mesec i godina	Broj hakovanih *web* stranica
01.2016.	115
02.2016.	73
03.2016.	95
04.2016.	39
05.2016.	43
06.2016.	105
07.2016.	50
08.2016.	106
09.2016.	36

Šta se dešava u Srbiji?

- 28.01.2016. objavljen je Zakon o informacionoj bezbednosti.
- Pojam „informaciona bezbednost“ definisan je kao skup mera koje omogućavaju da podaci kojima se rukuje korišćenjem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

Šta piše u Zakonu?

- Član 14. Zakona odredio formiranje Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima – Nacionalni CERT.
- RATEL dobio zadatak da formira Nacionalni CERT.

Uloga Nacionalnog CERT-a (prema Zakonu)

- Prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema.
- Prikuplja i razmenjuje informacije o događajima koji ugrožavaju bezbednost IKT sistema.
- Obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji.
- Zakon predviđa i dodatni skup zadataka za Nacionalni CERT.

Dodatni skup zadataka nacionalnog CERT-a

- Prati stanje o incidentima na nacionalnom nivou.
- Pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima.
- Reaguje po prijavljenim ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja.
- Kontinuirano izrađuje analize rizika i incidenata.
- Podiže svest kod građana, privrednih subjekata i organa javne vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti.
- Vodi evidenciju posebnih CERT-ova.

Najvažniji zadatak Nacionalnog CERT-a

Konstantna edukacija svih o načinima zaštite prilikom korišćenja informacionih sistema.

(prevencija)

Gde smo sada?

- RATEL intenzivno radi na formiranju Nacionalnog CERT-a.
- Vlada Republike Srbije treba uskoro da donese podzakonska akta koja prate Zakon.
- Vojska i MUP su već formirali posebne CERT-ove.
- Narodna banka Srbije ima svoj CERT kao i većina banaka.
- Ostali operatori kritičnih IKT sistema su već formirali ili su u procesu formiranja CERT-a.

Serbian Open eXchange

CERT
DA LI NAM I ZAŠTO TREBA?

Dr Nenad Krajnović

Serbian Open Exchange

E-mail: krajko@sox.rs