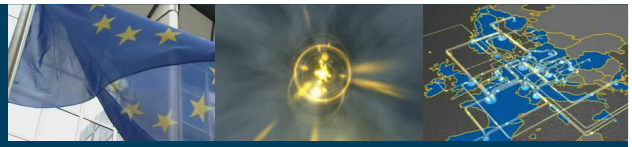
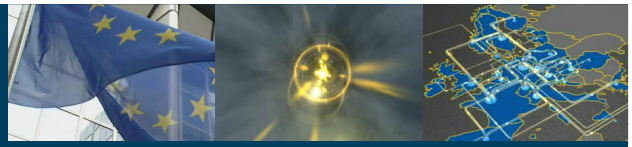


Connect. Communicate. Collaborate

Sigurnost GÉANT2 mreže
JRA2: Security

Nino Jogun
voditelj CARNet CERT-a
Odjel za računalnu sigurnost
Hrvatska akademska i istraživačka mreža – CARNet

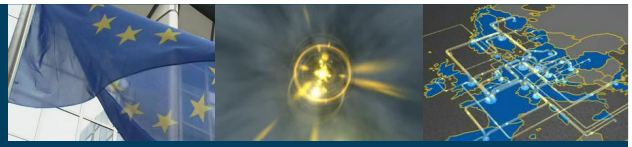
CUC 2007, Rijeka, 21.11.2007.



Connect. Communicate. Collaborate

Sadržaj

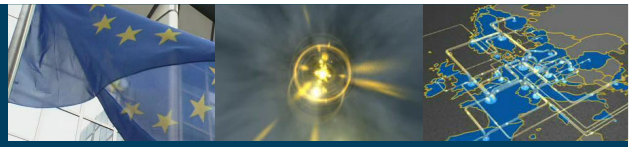
- Općenito o projektu GÉANT2
- GÉANT2 i sigurnost – JRA2: Security
- Pregled aktivnosti unutar JRA2
- JRA2 i CARNet



Općenito o GÉANT2

Connect. Communicate. Collaborate

- Sedma generacija paneuropske istraživačke i obrazovne mreže koja je nasljednik dosadašnje 10 Gbps mreže GÉANT
- Projekt započet 1. rujna 2004. s trajanjem od četiri godine
- Projekt financiraju europske akademske i istraživačke mreže (**NREN**) i Europska komisija kroz 6. okvirni program EU
- Mreža GÉANT2 povezuje 34 zemlje, 30 milijuna korisnika i više od 3.500 akademskih ustanova
- Veličina mreže iznosi preko 50.000 kilometara, od čega čak 12.000 kilometara *dark fibre* optike



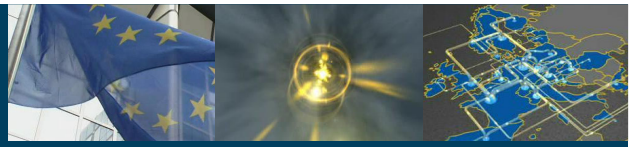
Connect. Communicate. Collaborate

Potreba

- Cyberkriminal po profitu dostiže trgovinu drogom
- Industrija informacijske sigurnosti *teška* 100 milijardi dolara
- U RH na snagu stupa Zakon o informacijskoj sigurnosti

→ Sigurnost je postala sastavni dio *online* zajednice!

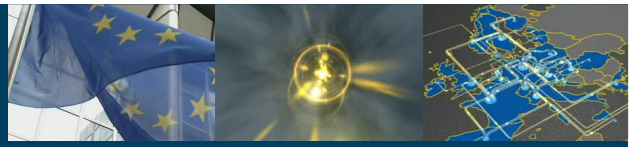
- Mreža GÉANT2 nije izuzetak
- Sigurnost prestaje biti *dodatna oprema* i postaje preduvjet za izgradnju mreže
- Paralelno s izgradnjom mreže, implementira se sigurnost – *design-time* odluka za *built-in* funkcionalnost



Connect. Communicate. Collaborate

JRA2: Security

- JRA2 pokrenut sa sljedećim ciljevima:
  - Ojačati mrežne sigurnosne mehanizme uzimajući u obzir velike brzine i nove uzorke mrežnog prometa
  - Poboljšati suradnju i koordinaciju oko sigurnosnih incidenata zasnovanu na definiranom skupu usluga
  - Osigurati mrežne elemente, računalne sustave i usluge mreže GÉANT2
  - Definirati zajednički pristup sigurnosti svih partnera koji vodi ka raspoloživosti *end-to-end* usluga



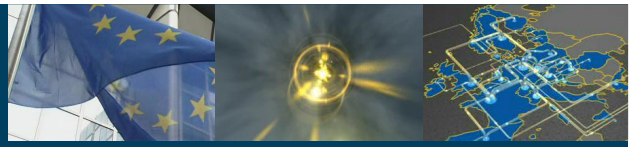
Connect. Communicate. Collaborate

JRA2 Work Items

- (WI0: Management)
- WI1: Securing GN2 network elements and services
- WI2: Building of security services
- WI3: Infrastructure for coordinated incident handling
- WI4: Relationship with TF-CSIRT
- WI5: Establishment of advisory panel

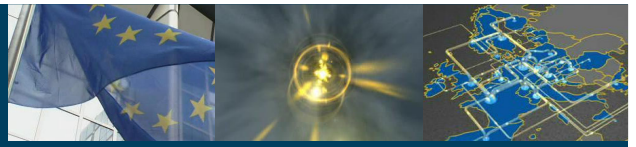
Work Item 1

Sigurnost mrežnih elemenata i usluga u GN2



Connect. Communicate. Collaborate

- Izrada preporuka i smjernica za GÉANT2 i priključene NREN-ove → Sigurnosna politika za GÉANT2 mrežu
- Implementacija na pristupnim linkovima i okosnici mreže
- Po slojevima:
  - Layer 3 – IP, Multicast, QoS
  - Layer 2 – VLAN
  - Layer 1 – SDH, WDM, PtP Eth.

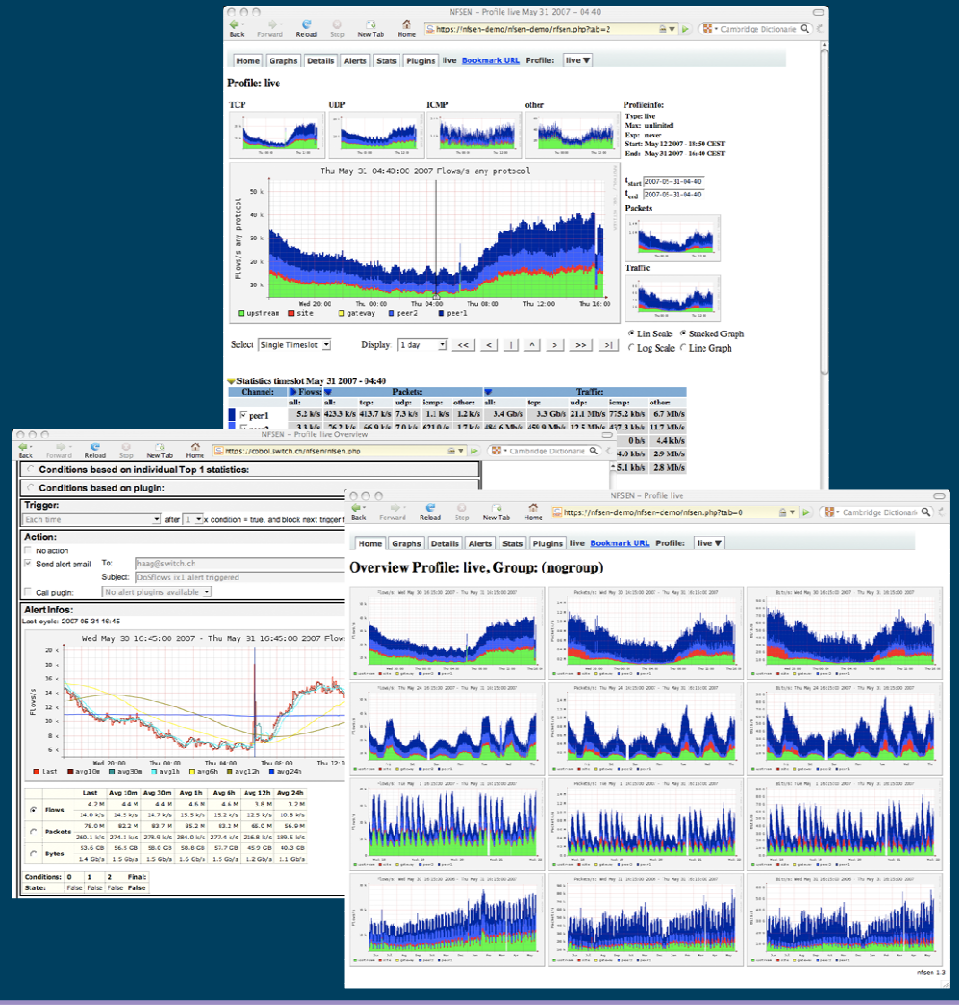


Connect. Communicate. Collaborate

Work Item 2

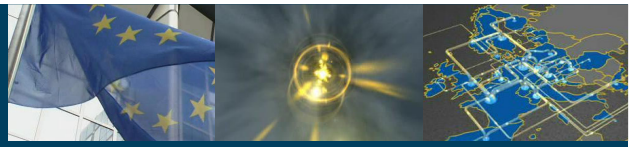
Izgradnja sigurnosnih alata i servisa

- Skup alata za analizu mrežnog prometa
- Karakteristike:
  - Otkrivanje anomalija
  - Daljna istraga anomalije
  - Odgovor na anomaliju
- Zahtjevi:
  - Primjena otvorenih standarda
  - Nikakva inspekcija podataka
  - Upotreba otvorenog kôda
- “Toolset”:
  - NERD
  - NFsen
  - Stager
  - Flowd
  - NetFlow Monitor
  - FTAS
- Netflow v9 *exporter* za brzine > 1Gbps



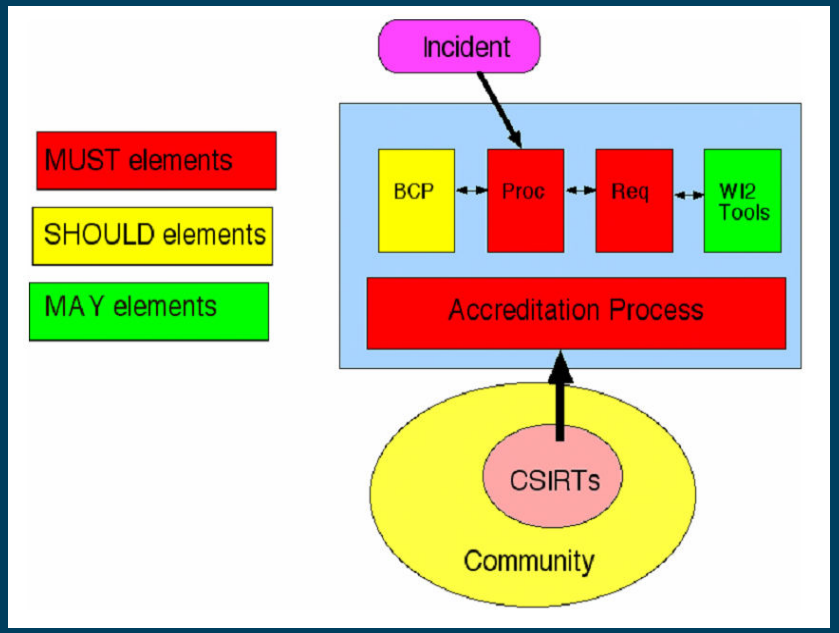
Work Item 3

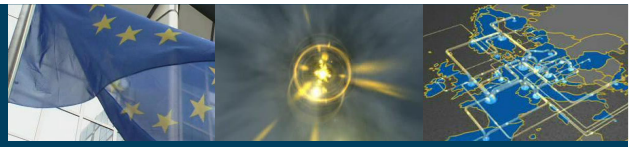
Definiranje i uspostava infrastrukture za koordinirano rješavanje računalno-sigurnosnih incidenata



Connect. Communicate. Collaborate

- Korištenje proizvoda iz WI2 i pružanje kvalitetne povratne informacije
- Izrada pravila i procedura kao okvira za suradnju između sigurnosnih timova (klasifikacije, vremenski rokovi, dokumentiranje, upotreba alata...)
- Uspostava utvrđenih komunikacijskih kanala unutar i izvan GÉANT2





Connect. Communicate. Collaborate

Work Item 4

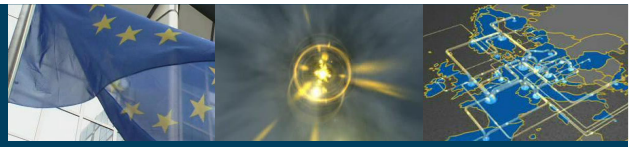
Suradnja s radnom skupinom TF-CSIRT*

- Postoji preklapanje u članstvu i interesima
- Osnivanje ekspertnih ad-hoc grupa sastavljenih od članova TF-CSIRT-a za rješavanje specifičnih pitanja iz područja rada ostalih JRA aktivnosti, a tiču se računalne sigurnosti (npr. programiranje)
- Kroz suradnju s TF-CSIRT-om JRA2 dobiva otprije akumulirano iskustvo i ekspertizu na području računalne sigurnosti

* *TF-CSIRT je radna skupina pod okriljem TERENA-e koja okuplja europske CERT/CSIRT timove i promovira njihovu suradnju od 2000. godine*

Work Item 5

Uspostava savjetodavnog vijeća



Connect. Communicate. Collaborate

- Savjetodavno vijeće čine pretežno etablirani stručnjaci iz redova radne skupine TF-CSIRT
- Diskusija i oblikovanje strategije / smjera daljnjeg razvoja JRA2
- Trendovi:
  - prijelaz od vandalizma ka organiziranom kriminalu
  - sigurnost mrežnih usluga dobiva na značaju
  - konvergencija govornog i podatkovnog prometa
  - izrada i implementacija *cyber* legislative
  - virtualizacija

3 Conclusions

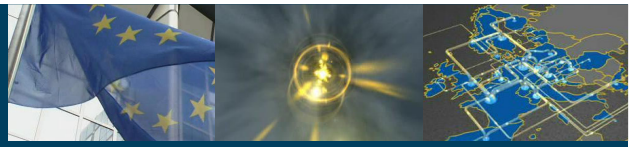
The panel is convinced that the work carried out by JRA2 is relevant to the GÉANT community and also beyond, to the private sector and particularly to ISPs.

Concrete recommendations on the activity plan of JRA2 were devised on the following topics:

- Promoting the establishment of CSIRTs
- Defining the security service portfolio
- Preparing for rare events
- Becoming more proactive

The following main trends relevant to JRA2 were identified, their relevance discussed and recommendations devised for future phases of JRA2:

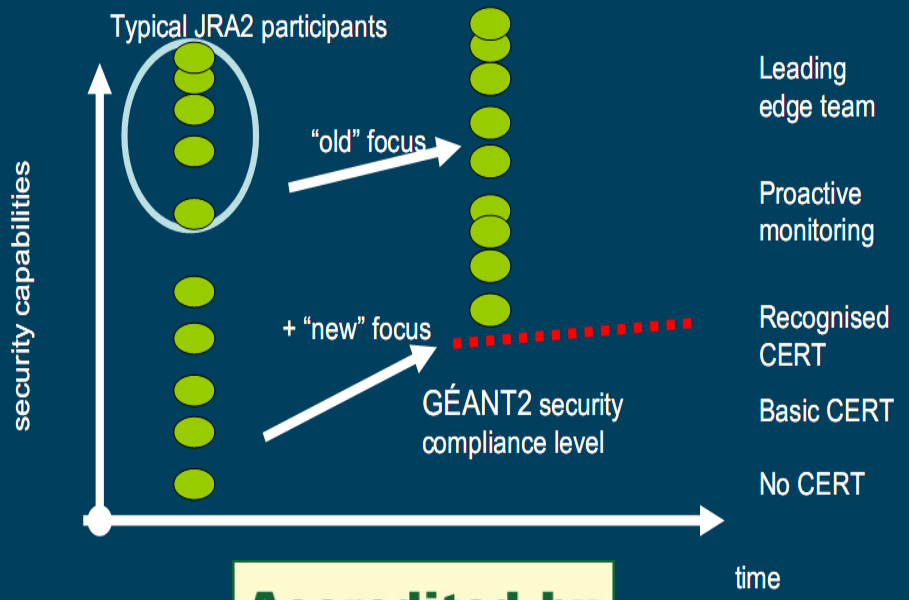
- The shift from vandalism to financially motivated abuse
- Security implications of overlay networks, such as bandwidth-on-demand links
- The availability and integrity of network-based services is becoming increasingly crucial
- Increasing enforcement of relevant laws and security practices to the "virtual" world
- Convergence of voice and data
- Virtualisation



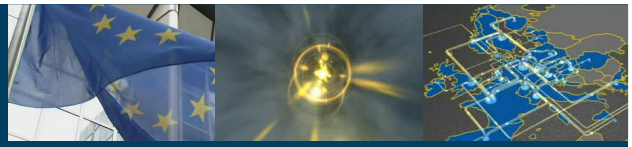
CARNet i JRA2 (1)

Connect. Communicate. Collaborate

- Jedan od 12 partnera u aktivnosti JRA2
- CARNet je “iznad crte” s operativnim sigurnosnim timom koji zadovoljava postavljene kriterije na razinu postojeće mrežne sigurnosti te postupke i procedure u skladu sa specifikacijom
- Angažman u WI2

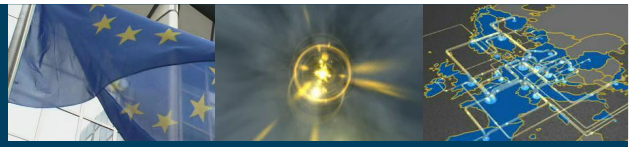


Accredited by TRUSTED Introducer The European CSIRT Directory



CARNet i JRA2 (2)

- Konkretno:
  - Testiranje sonde za generiranje i *export* Netflow v9 podataka “Flowmon”
  - Testiranje platforme za detekciju anomalija u mrežnom prometu “NetReflex”
  - Evaluacija skupine računalno-sigurnosnih alata za definiciju “Toolseta”



Connect. Communicate. Collaborate

Hvala na pažnji!

Pitanja?

Nino Jogun
Nino.Jogun @ CARNet.hr
http://www.cert.hr