



# The NREN View on Security

Marko Bonač

ARNES, Slovenia

TERENA TEC





# Why this presentation

Academic and Research Network of Slovenia

- 20 years of experience
  - *The Morris Worm* hit in 1988
- NRENs always like to share
  - We do things so others can use them also
- Cooperation is key
  - Doing things together is always more interesting





# What happened in 1988

Academic and Research Network of Slovenia

- Security = authentication
  - no packet filtering, no firewalls, ...
- Incidents seemed theoretical
  - implicit trust in the (then small) community
- Uncoordinated and isolated response
  - problem reappeared really soon



# NREN and attacks

Academic and Research Network of Slovenia

- ≡ Problems: hacked systems, viruses, DoS attacks, firewalls, spam, phishing, ...
  - NREN solution:  
establishment of a CSIRT  
(Computer Security Incidents Response Teams, CERT)
  - Internationally:  
TERENA organised TF-CSIRT and TI





# TERENA: TF-CSIRT

Academic and Research Network of Slovenia

- Forum where members of the community can exchange experiences and knowledge in a trusted environment





# TERENA: Trusted introducer

Academic and Research Network of Slovenia

- To cooperate efficiently and swiftly when security incidents occur, a certain level of mutual trust is needed between CSIRTs.
- An important pre-requisite for mutual trust is shared and accurate operational knowledge about one another.
- The TI accreditation service is meant to do just that: facilitate trust by formally accrediting CSIRTs that are ready to take that step.





# CSIRT teams

Academic and Research Network of Slovenia

- ☰ There are three different types of CSIRTs
  - local site security teams
  - co-ordinating/national CSIRTs
  - vendor security teams





# CSIRT functions

Academic and Research Network of Slovenia

## Announcements and Information Dissemination

- proactive services
- distribute information about good security practice
- usually done by co-ordinating CSIRTs at a national/network level







# CSIRT functions

Academic and Research Network of Slovenia

## ☰ Incident Detection and Analysis

- reactive service
- normally done by local security teams  
with co-ordinating CSIRTs providing support





# CSIRT functions

Academic and Research Network of Slovenia

## ☰ Incident Response on-site

- reactive service
- containment of a security incident
- normally provided by local security teams





# CSIRT functions

Academic and Research Network of Slovenia

## ➤ Incident Response Co-ordination

- reactive service
- co-ordination of incidents that may involve multiple sites
- inform others who may have been affected
- normally provided by coordinated CSIRTs at national level





# CSIRT function

Academic and Research Network of Slovenia

## ☰ Vulnerability Handling

- reactive service
- handling vulnerability in products
- done by producers/distributers of the affected products
- supported by coordinating CSIRTs





# NREN and authentication

Academic and Research Network of Slovenia

- Problem: secure web sites need certificates
  - some NRENs use commercial certificate providers, some set up their own certificate service
  - internationally: NRENs in collaboration with TERENA set up *Server Certificate Service*





# Some remarks from NREN point of view

Academic and Research Network of Slovenia

- Some sense of déjà vu
- Everyone has to work within larger context
- Rich NREN experience available
- CSIRT model proven
- No forced model
- Could existing cooperation platforms be used ?



# Sustainable infrastructures

Academic and Research Network of Slovenia

- Networking in European R&E community is organised in a hierarchical model
- One NREN per country and coordination through TERENA and NREN PC
- It seems that a similar structure is needed for sustainable grid infrastructure in Europe (NGI, EGI)





## Conclusion

Academic and Research Network of Slovenia

- ⇒ "NREN CERTs and Grid experts need to develop a close working relationship and good communication channels"

*(Terena 3rd NREN-Grids WS 2006)*

