



circa Computer Incident Response Coordination Austria

vienna university
computer center

Wilfried Wöber: ACOnet-CERT
for TF-CSIRT, 13th Meeting – Malta, MT
September 23, 2004



What is it?

- A public - private partnership project
 - ISPA: Internet Service Providers Austria
 - coordinating the private sector
 - BKA: Bundeskanzleramt (Federal Chancellor's Head Office)
 - coordinating the public sector
- A name and an umbrella for various activities
 - deal with worms, viruses, DDoS, attacks on core
 - tools, policies, framework for crisis management
 - human networking and information exchange



The components or building blocks

- Constituency (organisations), membership (individuals), steering committee
- Well-defined policy for participation
- Secretariat, run by the ISP Association
- A platform for secure communications
- A framework for detecting and declaring, responding to, and managing emergencies:
 - "Krisenstab"



Building Block: Constituency

- Organisations which operate large-scale internet services, with national impact
 - (Big) Commercial ISPs (& ASPs in the future?)
 - NREN
 - Government agencies and IT administration
 - Large companies (industry, banking)
- Membership is offered to key individuals, representing an organisation (~25 / 15 now)
 - non-disclosure agreement signed
 - approval by management of organisation



Building Block: Policy

- only core operations and/or security staff which can act "immediately" in case of incidents
 - not: sales, helpdesk, PR or non-tech management
- personal signature on documents required, countersigned by employer, ISPA membership
 - non-disclosure, code of conduct
 - information not to be used for competitive advantage
 - responsibility to report changes in function or employment



Building Block: Secretariat

- Technical project support
 - Provisioning of certificates
 - Signing of PGP Keys
- Administrative project support
 - Membership management
 - Event coordination
 - Repository of documentation
 - Web site and mailing list/archive responsibility



B-Block: Secure communications

- 2 Mailing List Hubs
 - 1 for the private sector, 1 for the public sector, secure operational environment
 - Manual forwarding of relevant information
- Based on "Sympa" Mailer
 - Verification of sender's signature *and* encryption
 - X.509 *and* (eventually!) PGP support, interworking
 - Archive
 - Subscription approval (for non-pub) by secretariat



Building Block: "Krisenstab"

- Emergency/Crisis Management Team
 - Contact details (confidential)
 - Individuals from different environments
- Procedures to follow for
 - Detecting and declaring an emergency
 - Coordination of press releases and contacts
 - Physical meeting if necessary
- Out of Band emergency server (patches,...)



Lessons learned: problems

- Acquisition and management of X.500 certificates is a major pain
 - local, reliable source vs. ease of use in end systems, cost of certificate vs. expiration
 - installing certificates into different (versions of) applications can be nontrivial
- Become a CA in its own right?
- Move to PGP/GnuPG?
- Find a stable, reliable and trustworthy vendor?



Lessons learned: problems (cont...)

- Everything takes 3.1415962 times as long as expected to get set up reliably :-)
- Provisioning of emergency management components requires a "real" commitment!
- Sandbox and mental exercises are OK, but you need regular fire-alarm training!
- Admission procedures for participation need on-going review, who decides/manages trust?
- We didn't have a real emergency yet - hmmm...



Lessons learned: the good stuff

- X.509 and PGP inter-working on the lists
- Exchange of information
 - On the lists (help, discuss, info, warning, alert)
 - During meetings (Round Table Events)
- Marketing advantage for the participants
- Improved communication between private and public sector
- General increase of security awareness





Questions

