Pol34 CERT

current work

Tomasz Adam Nowocien

Poznan Supercomputing and Networking Centre
POL34 - CERT team

address: ul. Noskowskiego 10
61-704 Poznan, POLAND

phone: (+48 61) 8582108

e-mail: nowocien@man.poznan.pl
Current work

Distributed Incident Handling System (DIHS)
Purposes of creation DIHS

- simplify the collection of incident reports
- formalise the collection of incident handling
- simplify the incident handling process
- give additional features to net administrators
The working schema of DIHS

- Report collector
- Incident
- Incident handler
- Functional analyser
- Presentation analyser
- Incident database
Report Collector

• collects reports from users
• informs users about incident handling status
Report Qualifier

- verifies reports
- qualifies reports
Incident Handler

- distributed
- documents all incident handling actions
- gives insight view into incident handling history
Functional Analyser

- Analyses database
- Finds correlation between incidents
- Helps to discover attack paths
Data stored in database

- reporter(s) personal data
- incident type
- offenders address (addresses)
- victims address (addresses)
- attack date and time (including timezone)
Implementation

• is now being implemented
• is to be finished and put into practise till the end of 2002
• in springtime 2003 we would like to share the experience