



UiO-CERT



UiO CERT at a glance

- Constituency: the University of Oslo and cooperating partners/groups
- 10 members representing different aspects of the organization
- The team has professionals handling press, information and legal matters too



Integration with the organization

- Close integration will ensure that all team members are at all times up to date with their technology
- We can pull on other than our own members in special cases
- We can help the organization think security with this close integration
- BUT! We may be considered time stealers



The road to here

- Security was an integral part of operations
- Works often well, however
 - does not ensure consistent incident handling
 - No statistics of incidents
 - Accidental destruction of evidence
- As malware and incident density increased, the need for organized incident handling becomes apparent



So where are we?

- Vulnerability watch and handling
- Intrusion detection and log analyzers (netflow, syslog, AD etc)
- Incident handling and coordination
- Artifacts handling and analysis

- Information, information, information
 - Talks, articles, campaigns, conferences



Challenges

- The line between operations and UiO CERT
 - A lot of the security is done elsewhere in the organization
 - The understanding of responsibilities need to be complete, and there must be no possessiveness of incidents
- The incident handling has to be done with proper respect towards those who must take a step back
- We must not be too paranoid (is that possible?) to be taken seriously
- Containing the information flow is part of any incident handling but more of a challenge if there are outside parties involved



UiO CERT and other teams

- Cooperation and flow of information has been crucial from day one.
- We seek to share information, if sharing is appropriate.
- Uninett is the ISP of the University of Oslo and the University delivers services to Norwegian higher ed, so naturally we have a close cooperation with Uninett CERT.
- UiO CERT normally contacts security groups directly but will include Uninett CERT or NorCERT or other groups if the case is relevant to them.



The road ahead

- Tune the existing machinery
 - More information (lecture series and books)
 - Malware analysis - more and more systematic
- Involvement in international projects and efforts
- Applying for FIRST-membership
- GRID-cooperation



Contact address

- cert@uio.no
- <http://cert.uio.no/>