

The logo for SWITCH, featuring the word "SWITCH" in a bold, sans-serif font. The letter "S" is blue, "W" is yellow, "I" is blue, "T" is blue, "C" is blue, and "H" is blue. The letters are closely spaced and have a slight shadow effect.

The Swiss Education & Research Network

# **The (NREN-)CERT view on ownership and responsibility**

**Who owns the grid, or assumes ownership?**

**What are the assets and their criticality?**

**What level of security is needed?**

**To what risks are those assets exposed to?**

**To whom are responsibilities assigned to?**

**The CERT view on it:**

- This stuff should be clarified
- It helps the CERTs in their work, if they know about it as well

## Who is responsible for the operation of the grid?

- Includes knowing the customers and how to reach them
- Includes assessing and reacting to incident notifications

## Who is responsible for the software running on the grid?

- Liaison with those responsible for package components
- Responsible for packaging
- Secure coding practices
- Secure configurations
- Includes assessing and reacting to vulnerability alerts

## The NREN-CERT view:

- NREN-CERTs feel responsible to identify and mitigate risks to their NREN and their customers (on application level, NOCs care about IP)
- NREN-CERTs won't assume the responsibilities above, but will support those assuming the responsibility

## What do all those cases have in common?

- Flowerpot falls over and takes down a grid machine
- DoS against a grid machine
- Root compromise due to old versions of SSH or GridFTP
- Strange stuff happening with a presumably stolen grid identity
- Authentication bypass identified in grid software

## The CERT view on it:

- Those cases should all be regarded as grid incidents by the responsible as per previous slide
- They need be assessed by grid specialists
- CERTs can help in the clean-up
- CERTs should do that in a defined way



SWITCH

The Swiss Education & Research Network