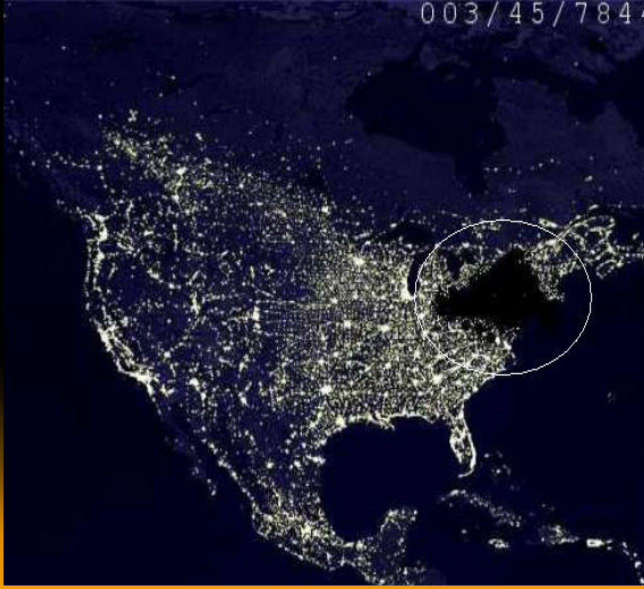

Control System Cyber-Security Workshop

Exchanging ideas on HEP security

— Discussion —

Dr. Stefan Lüders (CERN Computer Security Officer)

(CS)^2/HEP Workshop, Kobe (Japan)
October 11th 2009

Discussion Topics (1/5)

Is there *really* a risk ?

- Has your lab been under attack / Is it under attack ? Of which type ?
- Has your lab had controls-related incidents ? What was the impact ?
- How do you see the future ? More attacks ? Less ? Incidents ?

Who is the *real* threat ?

- Attackers, visitors & their laptops, or local engineers with finger trouble ?
- The local security team ?
- What about physical security ? More important ? Less ?

  Does local staff need "cyber" to break into systems ?

Discussion Topics (2/5)

How to obtain *sincere* commitment /resources/money ?

► Which approaches do work ? Top-down or bottom-up ?

► How to obtain management buy-in ? How did you /your team ?

► How to provoke a mind change of developers/experts/managers ?

How to balance/prioritize between:

Efficiency — Safety — Security

Operation/Production — Academic Freedom — Security

► What should be the ideal balance/priority ?

► Which changes might this imply to your lab ? Will this be accepted ?

Discussion Topics (3/5)

How to *harden* operating systems ?

- What is your patching strategy/cycle for control-PCs ?

  How fast did you fix CVE-2009-2692/2698 (Linux kernel vulnerability) ?
- Do you consider this to be optimal ? What should it be ? Why is it not ?
- How do you patch embedded devices (like oscilloscopes) ?

  Does the corresponding vendor support this ? Provide recommendations ?
- What are other preventive means ?

  Is firewalling working ? What about antivirus software & CPU cycles ?

How to *harden* the software applications ?

Discussion Topics (4/5)

How does your network provide *additional* security ?

- ►How to push data to the world (e.g. status information, historic data) ?
- ►What do you think of wireless networks for controls ?
- ►What is your experience with intrusion detection ?

How to deal with access control ?

- ►How do you control secured access to e.g. PLCs or field devices ?
- ►How do you deal with remote access for experts & developers ?

  Are they happy ? How to improve ?
- ►Will multi-factor authenticated be feasible/acceptable ? Why ? Why not ?

Discussion Topics (5/5)

Does security need better procedures ?

- What are your experiences with Software Development Life-Cycles ?
- …with security demands in procurement contracts ?
- What about laws and external directives ? Do you have to adhere to some ?
- Are there good standards out ?
- Is an asset inventory useful ? What about conducting risk assessment ?

What is *your* security strategy ?

- What worked ? What not ?
- *What else ?*