- Preface
- Who am I
- What is a Incident

- How do we prepare
  - The Policy
  - The Incident response plan
  - Creating a Computer Security Incident Response Team
  - External Forensic Partner
- Incident Response and Forensic techniques
- Responsible disclosure
- Now how does this look like in real life?
- The Good
The Bad

- The Ugly

- So ...WTF, may i rant a bit please?
  - So x.509 is death, huh?

- The desasters from 20/11
  - Sony and no end
  - The comming out of the RSA Breach
  - Commodo Diginotar, StarSSL...
Preface

- Why bother?

- The first Virus was programmed 1986 and we did not learn anything!

- You are a CIO/CSO? YOU FAILED!

- over 80% of all incidents are techniques older than 20 YEARS! APT, yeah right.

- Are you any better?
Who am I

- CIO

- Computer nerd since the mid 70's

- A Hacker

- Spearhead and founder of BerlinSides

- A nobody
What is a Incident in the InfoSec

- @indi303's maintenance window.
- A attack against your Network (or Bogk in your Network)
- A SE attempt
- A lost USB Stick
- A McAfee update
How do we prepare

The Policy
- What is a incident
- Who to report to
- What to report
- Which measurements to take

The Incident response plan
- Helpdesk
- Intrusion detection monitoring personnel
- A system administrator
- A firewall administrator
- A business partner
- A manager
- The security department or a security person.
- An outside source.
Creating a Computer Security Incident Response Team
- Step 1: Obtain management support and buy-in
- Step 2: Determine the CSIRT strategic plan
- Step 3: Gather relevant information
- Step 4: Design the CSIRT vision
- Step 5: Communicate the CSIRT vision and operational plan
- Step 6: Begin CSIRT implementation
- Step 7: Announce the operational CSIRT
- Step 8: Evaluate CSIRT effectiveness

Incident Response and Forensic techniques
- WTF is WFT (WINDOWS FORENSIC TOOLCHEST™)
- FRED (First Responder's Evidence Disk)
- Responsible disclosure
  - To the Police
  - To our staff
  - To our business Partners
  - To the Public
Now how does this look like in real life?

- You’re most likely into infosec, look for yourself
- How many of you know your company’s incident response plan?
- From those who had their hands up, are you sure all employees know the IR Policy?
- Why is that so?
The Good

- Apache
  - https://blogs.apache.org/infra/entry/apache_org_downtime_report
  - https://blogs.apache.org/infra/entry/apache_org_04_09_2010

- PHPFog

- Comodo
The Bad

- **Kernel.Org**
  - Can’t find a statement on their webpage on the first page in Google search

- **Sony**
  - Very late under pressure did some kind of incident response, info from the Company was horrible

- **Diginotar**
  - Diginotar, got into incident response, took ‘em 2 months to report
The Ugly

- RSA
  - Kept the secret over a long time

- Apple
  - Very late patching things, and if mostly never the Opensource parts of the OS

- HP
  - OMG
- So ...WTF, may i rant a bit please?
  - So x.509 is death, huh?

- The desasters from 20/11
  - Sony and no end
  - The comming out of the RSA Breach
  - Comodo Diginotar, StarSSL...
- How can we change this?
  - As customer
  - As a professional

- All the Anonymous, Lulzsec J3st3r and others
  - Are we really prepared?
  - What’s about the daily skiddie?

- Predictions, who will fall next?

- Thanx for listening