- Preface

- Who am I

- What is a Incidet

- How do we prepare
  - The Policy
  - The Incident response plan
  - Creating a Computer Security Incident Response Team
  - External Forensic Partner

prevent.
Materials. Seats. Interior.

- Incident Response and Forensic techniques

- Ressponsible disclosure

- Now how does this look like in real life?

- The Good

prevent.
Materials. Seats. Interior.

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…

prevent.
Materials. Seats. Interior.

- Preface

  - Why bother?

  - The fisrst Virus was progammed1986 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?

prevent.
Materials. Seats. Interior.

- Who am I

    - CIO

    - Computer nerd since the mid 70's

    - A Hacker

    - Spearhead and founder of BerlinSides

    - A nobody

prevent.
Materials. Seats. Interior.

- What is a Incidet 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

prevent.
Materials. Seats. Interior.

- **How do we prepare**
  - **The Policy**
    - What is a incident
    - Who to report to
    - What to report
    - Wich mesurements 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.

prevent.
Materials. Seats. Interior.

- **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)

prevent.
Materials. Seats. Interior.

- **Ressponsible disclosure**

  - To the Police

  - To our staff

  - To our business Partners

  - To the Public

prevent.
Materials. Seats. Interior.

- Now how does this look like in real life?

    - You're most likly into infosec, look for yourself

    - How many of you know your companies Incident response plan?

    - From those who had their hands up, are you sure all emploees know the IR Policy?

    - Why is that so?

prevent.
Materials. Seats. Interior.

- 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
    - http://blog.phpfog.com/2011/03/22/how-we-got-owned-by-a-few-teenagers-and-why-it-will-never-happen-again/

  - Comodo
    - http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/ (March 23)
    - https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

prevent.
Materials. Seats. Interior.

- The Bad

  - Kernel.Org
    - Can't find a statement on their webside 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

prevent.
Materials. Seats. Interior.

- ## 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

prevent.
Materials. Seats. Interior.

- 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...

prevent.
Materials. Seats. Interior.

- 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

prevent.
Materials. Seats. Interior.