# Fight Cybercrime

from the Hackers Perspective

Florian ‚scusi‘ Walther
Professional Hacker and Penetration tester

# about me

- working as a professional Hacker since 1999
- for a number of international top consultancies for it-security (Stockholm, Berlin, Hamburg, Boston, Tokyo)
- a decade of experience within financial-, corporate- and governmental IT-Systems and networks.

# Some general Insights

(the root of the problem)

- Why Cybercrime is increasing while other crime is mostly decreasing?
- It‘s easy, it‘s simple, more gain, less risk than in the real world

# Some general Insights

(the root of the problem)

- Why is it that easy and attractive to criminals?
- Because nobody takes care!
- Vendors build crap software, making money is more important than quality.
- Companies running Systems don‘t care about IT-Security. „It‘s just costs“

# What to do?

(to solve the root problem)

- Product Liability for commercial Software Products would shift the Risk, and therefore help sustainable to solve the Problem at it‘s root.
- Force IT-System-Operators to take security seriously and care about like they care about profit.

# Let‘s get concrete…

- **Article 3-6**: Not the one who was able to proof that a certain System is unsafe should be prosecuted. The one responsible for the bug(s) making the system vulnerable should be held responsible. The Rest will be fixed by the Market.
- Individuals or Groups that (responsible) disclose security issues should be especialy protected by law. Since their work make us all safer, if we loose them we loose most of our defense.
- Only attacks that are really executed and done for malicious intend should be punishable.

# electromagnetic emissions

- Article 6:
- **receiving electromagnetic emissions should not be punished.** The ones that distribute sensitive information unprotected to the ether should be punished.

# Article 7

- drop it completely, it‘s dumb bullshit!
- Ask yourself two simple questions:
  - What do you do when you loose your home keys?
  - Have increased penalties decreased cybercrime?

# Article 8

- You should make sure that publishing information about a vulnerability can not punished under Article 8. Otherwise public looses vital information necessary to protect our systems
- If trying is punishable, nobody tries things any more. Again we loose important information to defend us, it just helps cybercrime!

# Article 9

- The penalties for cybercrime related offenses have been raised dramatically in recent years.
- Is there any measurable effect on cybercrime?
- NO!
- Do you think raising penalties will work?

# Article 10

- Article 10 turns everything upside down, drop it completly!
- Paragraph 1: should be called the Anonymous Paragraph, and will not help.
- 2: Impact of an Attack is solely based on the Defenders Actions and Precautions. The Attacker should pay for the defenders unability to get his stuff right? => Stupid!

# Article 10 P.3

- Identity Theft:
- Why we have so much - further increasing - identity theft?
- Like with Cybercrime, it‘s easy, works well, not much risk.
- Why is it easy?

# Article 10 P.3 (2)

- Because we have increasing huge databases of private information that are required by (stupid) laws and easy to hack.
- The best defense against identity theft is to protect every ones Identity. Stop collecting these Informations support online anonymity, Establish a harsh regime for those still collect private information.

# Thank you...

- ... for your time an attention.
- Contact me at: scusi@snurn.de
- or florian.walther@gmail.com