



Welcome to

# **Privacy, surveillance and hacking, protect yourself**

## DANSK IT IT-sikkerhed 2019

Henrik Lund Kramshøj [hlk@zencurity.com](mailto:hlk@zencurity.com)

Slides are available as PDF, [kramse@Github](https://github.com/kramse/dansk-it-2019)  
`dansk-it-2019.tex` in the repo `security-courses`

# Happy New Year 2019



- Same problems
- Repeat last year?
- ... or try something new!
- 2019 will become a nightmare of breakins and data leaks
- GDPR is here and the snow ball is rolling

Try not to panic, but there are lots of threats



Try something new



**Do you think like an attacker?**

**Why not.**

- This talk will try to convince you to start attacking yourself, your company, your life.
- Start using Nmap, Wireshark, Kali Linux
- Learn some hacking skills, so you can recognize bad and insecure design

# Hackers don't give a shit

Your system is only for testing, development, ...

Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

**Think like attackers - don't hold back**

# Hackers don't give a shit:



**KIWICON III**  
28<sup>TH</sup> & 29<sup>TH</sup> NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

# Secure Laptops



Start with your laptops (and mobile devices if you wish)

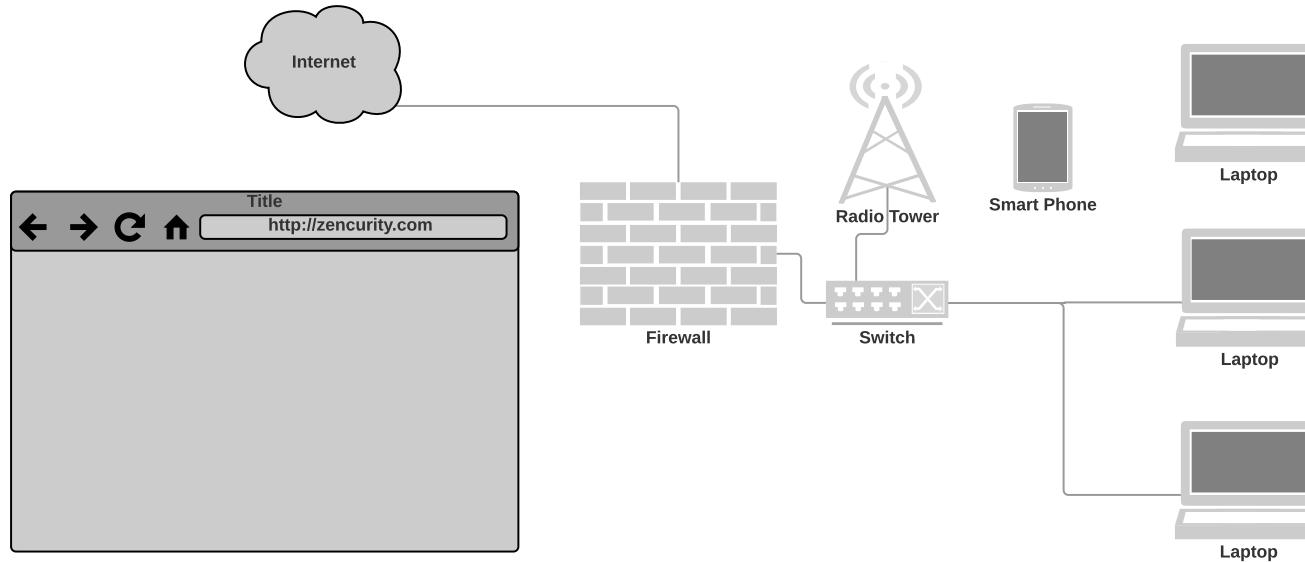
Are they *secure*, and to what extent

# Comply Everywhere



- **Laptop storage must be encrypted**
- Firewall must be enabled
- Suggestions
- Try sniffing data from a laptop, setup Access Point/Monitor port
- Portscan your laptop networks - use Nmap
- Write an email to everyone in your organisation:  
"Hi All, we need to identify laptops without full disk encryption  
- come see us, we have christmas cookies left, Best regards IT"

# Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

## Data found in Network data



Lets take an example, DNS

Domain Name System DNS breadcrumbs

- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

Advice show your users, ask them to participate in a experiment

**Join this Wireless network SSID and we will show you who you are on the internet**

**Maybe use VPN more - or always!**

# Data from Day 1



- 
- 
-

# Start Attacking from the Inside



- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?  
Having a large open network may cost you 1.9 billion DKK - ref Maersk
- Try scanning everything, start in a small corner, expand
- Scan all your danish segments, one by one, then the nordic, then the world
- Yes, things may break - FINE, BREAKING is GOOD

**Better to break while we are ready to un-break**

# Questions?



Henrik Lund Kramshøj [hlk@zecurity.com](mailto:hlk@zecurity.com)

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email