Official IT Security

Government Level IT Security - while maintaining your sanity, your humanity, and some of your budget

Robin Laurén - Reaktor

Hello World! I'm Robin ツ

- Mac & Linux and sysadmin at Reaktor
  - ~600 specialists: developers (~50%), designers, data scientists, graphics, usability, coaches, bizdev, support …
  - Finland, Netherlands, USA, Japan, Dubai
  - Teams > Hierarchies

Find me on the Interwebz

- Slack: @llauren
- Twitter: @RobinLauren
- Web: https://robin.lauren.fi
  https://robin.lauren.fi/talks/macaduk2019

What's "Official"?

- Also known as The Public Sector
- Government, state, Crown, border, police, military...
- Paid with taxpayer money

Spoiler alert!

- I’m talking from a Finnish perspective
- It’s yuge and complicated
- Lot of work involved
- Generally applicable, commercial and personal use
- There’s an alternative to the top-down imperative

Confidential? Restricted? Top secret?

- In books and movies they look cool
- Between friends it depends on the social context
- In a company, lose business or get fined (or fired)
- In official context these mean serious business
    - Restricted: “disadvantageous” if revealed
    - Confidential: personal security, public harm
    - (Top) Secret: national security at risk

Designations and considerations

- Protection levels assigned by the Authorities
- Management, Physical, Information systems
- Documentation by committee but still pretty useful
- Common sense is not only suggested but even recommended

Why listen?

- White hat or a black hat, a gray hat or no hat at all
- Spoil your movies
- Some of it is actually pretty good
- It’s your money!

Hello KATAKRI!

- Information security audit tool for Finnish authorities
- Public document, from 2015, third iteration, in effect
- Covers management, physical security and infosec
- Other countries have similar requirements
  - Sweden (KSF) http://isd.fmv.se/Sidor/FM-MUST-KSF.aspx
  - Germany (BSI: IT-Grundschutz) https://www.bsi.bund.de/grundschutz > English
  - UK https://www.gov.uk/government/publications/government-security-classifications

Protection levels & Security classification

Protection level		If unauthorised disclosure or use could ….
1	**Top Secret**	cause particularly grave prejudice to a public interest (stuff that can lead to war)
2	**Secret**	cause significant prejudice to a public interest (eg National security)
3	**Confidential**	“cause prejudice to a public or private interest” (eg undercover police name lists)
4	**Restricted**	“be disadvantageous to a public or private interest” (Stuff you need clearance to see)

Decree 681/2010 § 11

And now, a deep dive into KATAKRI

Stay frosty, or have a 15 minute nap now

Picture by and of Scott Meyer

Management practices

- Principles exist, and somebody’s responsible
- Have enough expertise to actually be secure
- Plan ahead: risk management, continuity plan, handling security events, communications plan…
- Security education and awareness
- Document and label everything

Physical security

- Multi-level, complementing “onion design”
- Structures, doors, locks and security systems
- Access rights management
- Manage your keys and codes
- No eavesdropping
- Document it all

Network security

- Separate different functions to different networks
- Only allow specific traffic between networks (especially so if traversing protection levels)
- High-sec nets can’t connect to the Internet
- Document fiercely

Wireless insecurity

- Wireless = public
- Wireless makes you visible
- Public is bad opsec
- Best to ban everything wireless

System Administration

- Admins only
- Use per-admin accounts
- Only encrypted protocols
- Enumerate thy hardware
- Change management

Know thy users

- Have an Identity and access management system
- Separation of duties and Principle of least privilege
- No shared accounts
- Not all users are humans
- Have a sensible password policy

Log and monitor

- Log everything, centrally
- Monitor and have a baseline
- Examine the logs regularly
- Keep them secure

Hardening

- Apply secure settings
- Patch and update
- Malware protection
- Encrypt sensitive data
- Remove anything that isn’t strictly necessary
- Keep people educated

Quality control

- Only use approved security products
- Take care of your secrets
- Poke, test and audit
- Be resilient

TEMPEST

- No eavesdropping of electromagnetic waves
- ...or any other kinds of waves

Information security: Everything else

- Treat your copies and backups like originals
- Security over lifespan
- Store and handle stuff only where allowed
- Travelling with secrets

Phew!

What's not in KATAKRI?

- Actual hard requirements
- HOW to actually create a secure environment *)
- WHY you should do these things

*) For that, consult VAHTI, IT-Grundschutz, CIS, or DISA STIG

A fair warning

- Cheap, easy, good: pick one
- Security is not a checklist
- The return of the on-prem or in-org engine room
- You will need to be agile
- Requires money, personnel, time, dedication (and your soul)

Get your gear together

- Start small and grow as needed
- Get a proper firewall and managed switches
- No recycling
- Save your configs and … document fiercely

Essential software

- Learn to love the command line
- Password management
- Version management
- Virtualisation
- Open source software
- Configuration management

Security is about people

- Turn top-down security on its head
- You are the enabler
- Make everybody’s life bearable
- Encourage a secure culture and behaviour
- It gets lonely in a bubble, but on-site is social

An alternative to despair

- Plan
- Protect and prevent
- Monitor, test and audit
- Mitigate and be resilient
- Educate
- Iterate and improve!

Four sources of threats

- Ignorance
- Incompetence
- Malice
- Mistakes

Malice is the obvious threat

- Most people are usually nice, some just have a different agenda
- Rational, on-purpose, clever attac
- Social engineering
- Educate yourself
- Wear a black hat

Scott Meyer drew this picture

Ignorance prevents bliss

- Those too lazy, too busy, or too important
- Beware of Broken Windows and Slippery Slopes
- Teach why security is important and for everyone
  (This includes yourself)
- Make it possible to do “important” things securely

Incompetence can be cured

- Stop feeling ashamed that you don’t know
- Incompetence is temporary and can be cured by education
- Teach those who don’t know they don’t know

To errr is human

- Everybody makes mistakes
- Design for secure behaviour
- Create a culture where making mistakes is allowed
- Learn from mistakes
- Make sensible security

Foster a secure culture

- Understand why it’s important
- It’s everybody’s responsibility
- Be honest to yourself, your peers and your customer
- Don’t hide your mistakes, learn from them
- Teach the people to be resilient

Any practical advice?

Practical hardening

- KATAKRI tells you what
- VAHTI, CIS, DISA STIG tells you how (but nobody tells you why)

Thank you!

(#) llauren
(@) Robin.Lauren@reaktor.com
(w) robin.lauren.fi /talks
(t) @RobinLauren

Pictures in this presentation
by and © Scott Meyer
Basicinstructions.com