Infosec through People, Process and Technology

Mate Soos
Presentation at kLab, Kigali
About me

- Studied information security in Hungary and France
- PhD in RFID and embedded systems security
- Worked for German security consultancy where we broke A5/1, MiFare, GPRS, 3G, SIMs
- Currently working for Cisco in the UK
1. What are the goals of infosec for a particular product or service?
2. How do people, process and technology help achieve these goals?
3. Technical failures that were saved by process and technology
Goals of Infosec

What

- Prevent unauthorised access (authentication, authorization)
- Prevent data manipulation (integrity checking, separation of duty)
- Prevent denial of service (incentivisation, distributed systems architecture)
- Non-repudiation (audit logs)

For whom

- For the customer (e.g. data encryption)
- For the company (e.g. protect assets)
- For third parties (e.g. regulations)
The three aspects of Infosec

People
- Enabling people to take responsibility, continuous learning, culture of security

Process
- Setting responsibilities, regular meetings using standard cookbooks, managerial oversight and sign-off

Technology
- Use known, tested technology, don’t try to roll your own, keep it simple, think both top down and bottom up
People

- Encourage going to presentations, conferences
- Buy books on security and encourage staff to take them home, read
- Encourage open discussion of known issues
Process

- Call regular meetings with the explicit agenda of security
- Use and adapt cookbooks to needs (OWASP, Sec. Threat Modelling, Security engineering)
- Pick some high-impact TODOs every 2-3 months
- Make someone responsible for watching out for CVEs
Technology

- Tech is bottom up (libraries) and top down (tech stack)
- Use well-known protocols. OpenSSL, REST, HTTP, etc.
- Use well-known tech stack. nginx, MySQL, Redis, etc
- KISS: Keep it simple, stupid
The Oyster card
Fail or success?
A5/1
Fail or success?
Thank you for your time

Questions?