Attacking is easy, defending is hard

ir. Walter Belgers, CISSP, CISA

Walter Belgers

- Principal Security Consultant and Partner at Madison Gurkha B.V.
- Has been working in the IT security field for over 16 years

Madison Gurkha

- Madison Gurkha supports organisations with high quality services to efficiently identify, decrease and prevent IT security risks
- With a focus on technical security aspects
Physical layer

Solutions
- Have a policy for physical security
- Don’t buy locks from the local hardware store

Software
- Firmware
- Operating system
- COTS Add-on packages (backup software, database, web server)
- Homebrew applications (web application)
Firmware

- Override boot sequence using hardware
- Evil Maid attack
- (P)DoS attacks a/k/a "phlashing"

Solutions

- Trust your vendor :-)
- Do not leave your laptop unattended, even if you use (full) disk encryption

Software

- Trust your vendor :-)
- Do not leave your laptop unattended, even if you use (full) disk encryption

Speed to Market

Complexity
Monoculture

Software

Patching

- For OS and some packages: automated
  - For many add-on packages: not automated

- For homebrew software: ???
- Security audits

- Lot of work: test, accept, production cycle
- Dependency on specific version
- High costs when updates cause downtime
A6 Security Misconfiguration

Hardening

- Installation ≠ Configuration
- Almost always overlooked
- Default deny
- Users, file permissions, installed software, configuration settings regarding functionality

Homebrew software
Solutions (technical)

- Deny all, except (safe installation/hardening)
- Separation of duties/modular approach
- Restrict permissions
- Simplicity/ergonomics

Solutions (other)

- Functional requirements and security requirements
- Also for 3rd party software
- Use cases and abuse cases
- Educate programmers in secure programming
- Security testing

Other things to do

- If All Else Fails... (and it will)
- Multiple layers of defense (prevention)
- Logging and monitoring (detection)
- Have a plan ready (reaction)
Insider attacks

- A malicious person becoming an insider
- Physically
  - Burglary
- Logically
  - Hacking

Insider attacks

- Malicious insiders
- Insiders being (unknowingly) abused by outsiders
Insider attacks

- Active
- Social Engineering
- Phishing
- Passive
- Drive-by hacking
Educating users

- A process, not just an awareness session

Attack vectors

- Browser plugins
- Screensaver, picture in an email
- Codec to play a clip
- P2P-software
- Anti-malware
Solutions

- Find all known risks and act on them
- Fix bugs on all systems for all software
- Keep doing this
- Do secure installations (configurations)
- Embed security in the devpt process
- Educate and screen users and keep on doing this
- Monitor and be ready

walter@madison-gurkha.com