



Common employees' privacy expectations pitfalls

Dominik Pantůček
`dominik.pantucek@trustica.cz`

Trustica s.r.o.

14.11.2017

- What is privacy
- Employees' data
- Customers' data
- Pitfalls
 - Deadly, Mostly harmless, Non-obvious
- Documents
 - Storage, Transfer
- Databases
- Conclusion
- Q&A

- Protection of private information
- CIA
 - Confidentiality
 - Integrity
 - Accessibility
- Information privacy levels:
 - aggregated
 - anonymous
 - pseudonymous
 - personal
 - sensitive

■ Generic

- Name
- Gender
- Address
- Phone
- Salary
- Health status

■ Behavioral data

- browsing history
- security cameras

■ Location data

- Laptop
- Mobile phone

- Similar content
- Employees' work with them
- Accessibility versus confidentiality
- Judging by comparison

- Contractual data
 - Contracts
 - Payrolls
- Storage
 - Encrypted storage – not enough?
 - Backups – not enough?
 - Encrypted backups – mostly.
- Transfer
 - Email ...
 - Encrypt?
 - Sign?
- Usage
 - Temporary files
 - Locally saved files



Mostly harmless pitfalls

- Behavioral data
 - Firewall logs
 - Security cameras
- Storage
 - Encrypt
 - Backup
- Transfer
 - Usually not applicable
- Usage
 - in case of incidents

- Enterprise Wireless LAN Network
 - WLC in the cloud
- Outsourcing IT support
 - Firewall as a Service
- Mobile devices
 - Location data
 - Network traffic and behavioral data

- Encryption
 - Key management
 - Accountability
- Access Control
 - Accountability
- Backup
 - Encryption (see above)
 - Access Control

- Email
- Removable media

- Improper use of hashing functions
 - Hashing name for public ID usage
 - Brute force search
 - Rainbow tables
- Salting
 - Complex-enough salting lowers the brute force speed
 - Important for data that can cause collateral damage
- Homomorphic encryption
 - Only for aggregated data
- Retention management

- Game the system
- Ignore laws ...
- ... don't get caught



Q&A



Thank you.