Assessment of users’ IT security awareness in light of the GDPR

Dr. Ferenc Leitold
managing director, Secudit
fleitold@secudit.com

Dr. Attila Kiss
lawyer specialized in ICT Law and IT security
kissati121@gmail.com
• The Secudit system as an example
• How the Secudit system is affected by the GDPR?
• What can we do?
The Secudit system as an example
Apple watch saved Alberta man's life, makes international headlines

'I bought the watch two weeks before the heart attack, so it was the right time'

By Walis Snodden, CBC News  Posted: Mar 17, 2016 8:21 AM MT  |  Last Updated: Mar 17, 2016 12:22 PM MT

A Morinville, Alta. contractor who says his life was saved by a smartwatch is making headlines the world over.

Dennis Anselmo says the high-tech gadget warned him of an impending heart attack.

Now, six months since he was released from hospital, dozens of news outlets, including The Sun and The Daily Mirror in Great Britain, have picked up his story as an example of the merits of wearable technology.
The CIA model
Our IT Security model

- Confidentiality
- Integrity
- Availability

- IT User Behavior
- Deployed Security
- Enterprise Wellbeing
- Protected IT
- Malicious Activity
Our IT Security model

- IT User Behavior
  - Policing
    - Preventing Malicious Activity
  - Patching
    - Protected IT

Enterprise Wellbeing
Vulnerability assessment within the context of overall cybersecurity
Vulnerability assessment within the context of overall cybersecurity
Triunal Model of Cybersecurity Vulnerability

Three contributing sources, or triunes:
• malicious activity
• protected IT
• facilitating adverse user behavior
The vulnerability level of the infrastructure is defined as a probability of at least one threat is able to be executed on at least one device used by the given users in the infrastructure.
Mathematical background

K. Hadarics, K. Győrffy, B. Nagy, L. Bognár, A. Arrott, F. Leitold:
Mathematical Model of Distributed Vulnerability Assessment

9th International Scientific Conference, Security and Protection of Information, 2017, Brno, Czech Republic

F. Leitold, A. Arrott, K. Hadarics:
Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility

24th Annual EICAR Conference, Nuremberg, Germany, 2016

more information: www.secudit.com
How can we use this calculation?

• customized metrics
• identify dangerous users’ behavior
• identify vulnerable IT elements
• estimate different contributions
  • users’ groups
  • devices’ groups
  • threat types
• “what if” estimations
How the Secudit system is affected by the GDPR?
Legal aspects of personal data processing under GDPR

- World Economic Forum (2011):

  „Personal data will be the new “oil” – a valuable resource of the 21st century. It will emerge as a new asset class touching all aspects of society. (...) personal data represents a post-industrial opportunity.”

- Legal uncertainty, costs and administrative burden

- Development of privacy-invasive tools

- Public distrust in emerging technologies
ACCOUNTABILITY
(demonstrate compliance)

• lawfulness, fairness and transparency
• data minimisation
• purpose limitation
• appropriate security
• Shocking sanctions – 2 years of transition period

➢ Directly applicable
➢ Wide scope
How to get ready?

- Awareness
- Data Protection by Design and by Default
Awareness (planning and documenting)

1. Create a road map (PDCA)
2. Inventory
3. Risk assessment framework
4. Data security and breach notifications
5. Rights of data subjects
6. Policies, DPO and trainings
7. Third-party and customer contracts
Description of the envisaged processing

Monitoring and review

Documentation

Assessment of the necessity and proportionality

Measures envisaged to demonstrate compliance

Measures envisaged to address the risks

Assessment of the risks to the rights and freedoms
Art. 25

(... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures (…) which are designed to implement data-protection principles

• Goods or services
• Risk based – impact assessment
• Privacy engineering
What can we do?
What can we do?

Perform a lot of paper works required by the GDPR

... see above

+ create document samples for the users

Data protection by design

- decrease the amount of personal data
- limit the time for store the data
- provide possibility to check personal data for stakeholders
An example
An example

One of the most important element in the user behavior assessment is to identify what the user does with an attachment in the email.
One of the most important element in the user behavior assessment is to identify what the user does with an attachment in the email.

Two information sources:
- email attachments
- executed programs/opened files
An example

One of the most important elements in the user behavior assessment is to identify what the user does with an attachment in the email.

Two information sources:
- email attachments
- executed programs/opened files

For this purpose we do NOT need the email or the attachment itself, we need only the hashes of the attachments and the executed programs/opened files.