IoT, smart cities and cybersecurity

Digital Transformation for Cities and Communities Webinar Series - Episode #9: Addressing the Security Risks of Digital Transformation on IoT

(CC) 2021

Matej Kovačič

Jožef Stefan Institute
Ljubljana, Slovenia

United Nations Educational, Scientific and Cultural Organization

IRCAI International Research Centre on Artificial Intelligence under the auspices of UNESCO

Personal blog:
https://telefoncek.si

Cybersecurity

Security is not a product (to buy, install and "forget"), it is a process.

Security culture should be developed and maintained continuously.

Security is a combination of people, process, *and* technology.

Cybersecurity and traffic safety: it is not enough just to have a good car and get a driving license, knowledge about safety needs to be renewed, updated and used regularly.

Aspects of cybersecurity

Different aspects of cybersecurity:

- Technical aspects (usually overemphasized, because we can not solve social problems with technology only).
- Human aspects (very important part of any security system are people).
- Processes supporting technology and people.
- Social aspects of security (broad societal consequences of IT systems).

Technology

Hardware security (tampering protection), physical hardening and manufacturing standards.

Weak password protection.

Insecure interfaces, lack of firewall protection, old protocols and poor software and OS security.

Insufficient data protection (communication and data storage), lack of strong encryption and authentication mechanisms, lack of data integrity measures.

Possibility of hijacking of devices and abuse them for other attacks (DDoS, attacks on energy consumption,...), rogue IoT devices.

People

Users and operator's knowledge, understanding and awareness (the IoT skills gap).

IoT devices are still not seen as computers.

Belief that advancements in technology is the only factor that guarantees security.

Humans are prone to making mistakes, they fall for social engineering, scams,...

People tend to circumvent security regulations (to make their life easier).

Processes

IoT manufacturers lack cybersecurity knowledge, and they do not spend enough time and resources on security.

Rushing to deploy new technologies often comes without the right security measures.

Lack of secure default settings.

Lack of regular patches and updates and weak update mechanisms.

Poor IoT device management.

Security of supply chains?

Lack of vulnerability disclosure.

Lack of (user's and manufacturer's) training and education.

Broader social aspects

Technology is often deployed without reflection what are the needs of people and what will be the long term social consequences.

What will be the long term sustainability of these projects after the initial funding is finished?

Use of clouds, closed technology and standards, limited interoperability. Vendor lock-in.

We are becoming more and more dependent from the technology.

Rise of digital feudalism.

Rise of surveillance society.

Technology is only a part of solution

When we talk about the cybersecurity in a broader sense, technology, people and processes matter.

We should not start talking about technology first.

First are needs, processes and effects on a broader environment. Technology should follow.

Questions?

Matej Kovačič

Jožef Stefan Institute
Ljubljana, Slovenia

United Nations Educational, Scientific and Cultural Organization

International Research Centre on Artificial Intelligence under the auspices of UNESCO

Personal blog:
https://telefoncek.si