cyberwatching.eu

The European watch on cybersecurity & privacy

Security and Privacy by Design for healthcare Problems and overview of the proposed Solutions

Webinar | 10 December 2020

Funded by the European Commission
Horizon 2020 – Grant # 740129

cyberwatching.eu Topics

The European watch on cybersecurity & privacy

- Security and Privacy by Design for the healthcare sector? Yes, now!
- Problems
- How DEFeND, PANACEA and PAPAYA solutions may help: an overview
- Conclusions

Security and Privacy by Design for the healthcare sector? Yes, now!

- **Systems are mission-critical, but still poorly protected and vulnerable**
  - ICT and connected Medical Devices in last years have become mission-critical for healthcare operations. Therefore, cyberattacks and staff mis-behaviour are **growing risks for business continuity, patients' safety and data privacy**.
  - **Current level of privacy protection and security must be improved,** also because most of the **existing assets were designed when data privacy and cybersecurity were not an issue**
- **Covid offers the opportunity to renew the systems**
  - A way to radically improve is to **invest, to substitute/upgrade "obsolete" assets, adopting a "Security & Privacy by Design" approach**.
  - Question: is there the money and the "push" to do these investments?
  - Answer: probably YES. A positive side-effect of **Covid in Europe** is that it has surfaced the weaknesses of the national health services and the **need to invest in e-health and tele-health**.

Problems

- **Hospitals and digital service providers need «protocols» for secure integration**
  - Systems developers and medical device manufacturers obviously need to apply **Security & Privacy by Design** approaches
  - However, **also hospitals and digital service providers need to master Security & Privacy by Design, when they procure and deploy the assets**
  - **Let me give an example**
    - **My hospital during last 30 days received 20+ offers for new ICT platforms**, including
      - a system to manage the delivery of drugs to Covid patients quarantined at home
      - a system to tele-transmit the data collected by remote oximeters
    - **My hospital needs "methods and tools"**
      - to **assess how good are the 20+ platforms** from the privacy and cybersecurity perspective.
      - to **ensure that, when a new asset is deployed** and integrated into our hospital context , **is privacy and cybersecurity compliant**.

Problems

- **All healthcare actors need to comply with EU regulatory framework**
  - **GDPR (EU) 2016/679**

    Art. 25 Data protection by design and by default: ... 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, … designed to implement data-protection principles

    Art. 30 Records of processing activities: **…** Each controller … shall **maintain a record** of processing activities under its responsibility…Each **processor** .. shall maintain a record of all categories of processing activities carried out
  - **DIRECTIVE (EU) 2016/1148 (NIS) concerning measures for a high common level of security of network and information systems across the Union**.

    Whereas 50): … manufacturers and software developers … play an important role in enabling operators of essential services and digital service providers to secure their network and information systems.
  - **Medical Device Regulation (EU) 2017/745**.

    Requirements regarding design and manufacture . 17.2: For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
  - All above is reinforced by the **Cyberact Regulation (EU) 2019/881,** which establishes an EU-wide cybersecurity certification framework for digital products, services and processes**.**

Problems

- **Covid-like context raises specific requirements, pointing to Security & Privacy by Design**
  - **Telemedicine:** the policy to keep non severe COVID patients at home + the need for telemonitoring, expand the use of telemedicine, that has low level of security.
  - **Smart working**: Risk may come from technology illiteracy of the staff at home and increased risk of infection due to connections from home devices potentially defenceless; carelessness to exchange credentials with colleagues to VPN or shared folders.
  - **Use of new staff**: newly hired healthcare personnel have inexperience of company cybersecurity and privacy policies sudden arrival of massive new staff can weaken the provisioning, de-provisioning and profiling processes, leading to security issues.
  - **Need for ad-hoc IT solutions fast design:** Healthcare sector needs to rapidly design and deploy Apps and back-end systems. Fast design risks to deliver non secure solutions.
  - **Infection monitoring data flows**: there has been a major request of data flux to monitor infections, to do epidemiological reporting, etc. These data fluxes take place between many institutions; information sharing has low level of security.
  - **Non-healthcare sites used for healthcare operations**: Temporary Hospitals, Churches, nearby Hotels, other empty but usable spaces have been upgraded to “hospital level”. WIFI systems of these structures in general are not secure. Hackers can monitor traffic over air to steal access credentials

How DEFeND, PANACEA and PAPAYA solutions may help: an overview

- **European response**
  - EC response to the need for Security and Privacy by Design, includes not only the **revamping and strengthening of ENISA (**the EU Agency for cybersecurity, through Cyberact 2019/881) and **regulatory measures** (GDPR, MDR, EU Directive 2016/1148, Cyberact 2019/881), but also the funding, through the **Horizon 2020 programme**, of **research and innovation projects** to develop solutions that are effective and usable in the healthcare context. DEFeND, PANACEA and PAPAYA are three of them.
    - The ***DEFeND*** *(Data Governance for Supporting GDPR)* project provides an innovative data privacy governance platform which supports healthcare organizations towards GDPR compliance using advanced modelling languages and methodologies for privacy-by-design and data protection management.
    - The ***PANACEA (****Protection and Privacy of Hospital and Health Infrastructures with Smart Cyber Security and Cyber Threat Toolkit for Data and People)* project provides all healthcare actors with a assessment and system monitoring audit workflow to easily run conformity assessment and engineering assessment
    - The ***PAPAYA*** *Platform for Privacy Preserving Data Analytics)* project is developing privacy-by-design solutions and a dedicated platform for data analytics tasks which are outsourced to untrusted data processors.
  - In this webinar they describe what they have developed

cyberwatching.eu
The European watch on cybersecurity & privacy

How DEFeND, PANACEA and PAPAYA solutions may help: an overview

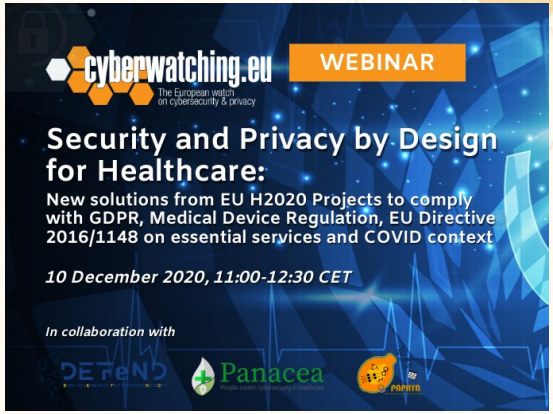
Problem areas		Envisaged users of the proposed Solutions				Solutions		
Contextual factor	Challenge	Healthcare Organizations	Medical Device Manufacturers	Sw developers	Digital service providers	DEFeND SbD/PbD	PANACEA SbDF (CST, SDSP)	PAPAYA PbD
Investments	• New systems assessment and deployment	✓			✓	✓	✓	✓
GDPR	• Data protection by design and by default (art.25)	✓			✓	✓	✓	✓
	• Records of processing activities (art.30)	✓			✓	✓	✓	
MDR	• Development process compliance		✓	✓			✓	
	• Product compliance		✓	✓			✓	
EU Directive	• HW and SW products compliance	✓	✓	✓	✓	✓	✓	
	• Digital Service compliance	✓		✓	✓	✓		
Covid	• Telemedicine, Smart working	✓			✓		✓	
	• Use of new staff	✓					✓	
	• Need to rapidly develop ad-hoc IT solutions	✓		✓	✓		✓	
	• Infection monitoring data flows	✓			✓			✓
	• Non-healthcare sites used for healthcare operations	✓					✓	

Conclusions

- **In all European countries, Next Generation EU and the related recovery plans and investments** will have among their objectives the **upgrading of healthcare systems and medical devices.**
- These investments are an **opportunity to reduce cyber risk <u>if and only if</u> Security & Privacy by Design approaches are adopted by all involved parties**
- While waiting for the definitive indications on how to implement the Cyberact, hospitals could **set-up pre-requirements for contracts** with medical device manufacturers and system/service providers. These should **state that,** in face of similar products**, preference is given to those that comply with Security and Privacy by Design approach**.
- To be in line with this policy, **all parties can count on the solutions proposed by these three projects: DEFeND, PANACEA, PAPAYA**.

Thank-you and keep in touch

Sabina Magalini
Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli IRCCS (FPG) and Professor of Surgery at the Rome Catholic University School of Medicine (UCSC).
Sabina.Magalini@unicatt.it



cyberwatching.eu
The European watch on cybersecurity & privacy

www.cyberwatching.eu
@cyberwatching.eu
info@cyberwatching.eu

Trust-IT Services Communicating ICT to markets
UNIVERSITY OF OXFORD
ICT LEGAL CONSULTING
CONCEPTIVITY 360 SECURITY
European Digital SME Alliance
aeiciberseguridad
AON