PANACEA PROJECT

Project administrative information

Project Acronym: PANACEA

Full project title: **P**rotection and priv**A**cy of hospital and health i**N**frastructures with sm**A**rt Cyber s**E**curity and cyber threat toolkit for d**A**ta and people

Website: https://www.panacearesearch.eu

Start date: January 2019 End date: February 2022

European H2020 Project Number: 826293 Call identifier: H2020-SC1-FA-DTS-2018-1

Type of project: Research and Innovation Action (RIA)

Consortium:

Coordinator: UNIVERSITA CATTOLICA DEL SACRO CUORE	UCSC	IT
Partners:		
FONDAZIONE POLICLINICO UNIVERSITARIO AGOSTINO GEMELLI IRCCS	FPG	IT
RINA CONSULTING SPA	RINA-C	IT
FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	FORTH	GR
IDEMIA IDENTITY & SECURITY FRANCE	IDEMIA	FR
RHEA SYSTEM SA	RHEA	BE
UNIVERSITY OF NORTHUMBRIA AT NEWCASTLE	UNAN	UK
AON SPA INSURANCE & REINSURANCE BROKERS	AON	IT
STELAR SECURITY TECHNOLOGY LAW RESEARCH UG	STELAR	GE
UNIVERSITA DEGLI STUDI DI ROMA LA SAPIENZA	UROME	IT
TRUST-IT SERVICES LIMITED	TRUST-IT	UK
DIOIKHSH YGEIONOMIKHS PERIFEREIAS KRHTHS	7HRC	GR
HEALTH SERVICE EXECUTIVE HSE	HSE	IE
IRISH CENTRE FOR EMERGENCY MANAGEMENT	ICEM	IE
INNOVATION SPRINT	iSPRINT	BE

Project challenges and scope

Healthcare organizations are especially sensitive to cyberattacks. This is due to their infrastructure as they have a large attack surface and they handle highly confidential and valuable data, and to human factors such as “medical culture” that put patient care topics far above cybersecurity. On top of this, exceptional situations such as the COVID-19 pandemic make healthcare organisations even weaker. It is therefore not a surprise that in France, the number of cyberattacks against hospitals has doubled between 2020 and 2021[1], and numerous large-scale cyber-attacks were reported in 2022. In order to cope with this threat a crisis management plan will be prepared in Q1 2023 with ANSSI[2].

It is now clear that cyber risks on hospital are not only financial. Cyber-attacks may have a critical impact on healthcare services, as they can completely disorganize the hospital, prevent patients to be admitted, make medical analysis and surveillance impossible, make medical records no longer available, delay important and urgent treatment, and eventually may cause patient death.

Project approach and results

PANACEA has adopted a socio-technical approach to hospital cybersecurity, developing nine tools to address:

1. the technology, i.e. proposes new tools to reduce the vulnerability of the ICT components,
2. the people, i.e. helps people understanding how cyberattacks happen and how to behave,
3. the organization, i.e. helps management to make cybersecurity related decisions

The end TRL is 6, i.e. the tools have been demonstrated in relevant environment and in co-operation with relevant end-users, that have given positive feedback on their performance and usefulness.

The tools have been developed according to the requirements of the PANACEA stakeholders. They have been tested in the three healthcare organisations that were part of the PANACEA Consortium,

[1] les cyberattaques contre les hôpitaux ont doublé en 2021

[2] Préparation plan blanc numérique pour les hôpitaux Mars 2023

either in real world conditions, or in emulated environment reproducing faithfully the IT environment of the hospital. The project has developed of a toolkit including following tools:

PANACEA tools			Healthcare Organisations components		
			Technology	People	Organisation
Solution Tools	DRMP	Dynamic Risk Management Platform	✓	✓	
	SbDF	Security by Design Framework	✓		✓
	SISP	Secure Information Sharing Platform	✓		
	IMP	Identification Management Platform	✓	✓	
	SBNT	Secure Behaviour Nudging Tool		✓	
	TECT	Training & Education for Cybersecurity Tool		✓	
	RGT	Resilience Governance Tool			✓
Delivery Tools	C-ROI	Cybersecurity Return on Investment			✓
	IGT	Implementation Guidelines Tool			✓

PANACEA has delivered the toolkit as planned[3]. It is now promoted by the PHCAS (PANACEA Healthcare Cybersecurity Advisory Service), a collaborative organization set-up by the PANACEA consortium members (https://www.panacearesearch.eu) after the end of the project[4]

Scientific learnings

The human and managerial factors are claimed to be key to ensure cybersecurity. However, the available solutions only propose training, control checklists, the Chief Information Security Officer (CISO). And, for the technology, only the technical vulnerabilities are taken into consideration. PANACEA, as an applied research project, instead has developed new concepts[5], including:

1. The identification system (IMP) is based on facial recognition and has been designed to avoid the burden to remember and input the password, thus contrasting the bad behaviour of nurses and medical staff, that tend to "stick" the password on the workstation and to use all the same password (this happens when the same workstation is used by many users many times in a day).
2. The vulnerability assessment tool (DRMP) 1) has a strong visual analytics interface that help the IT staff to take action and identifies the vulnerabilities affecting the system both at the technical and non-technical level, that is, human interactions with IT and medical systems.
3. The methodology to deal with people behaviour (SBNT) provides tools to identify human bad behaviour and to implement "nudges" that influence the individual behaviour vs the cyber risk
4. The governance model (RGT) adds to the CISO the "security angels", i.e. staff appointed in each office/clinical ward that act as an interface between the CISO and the staff (their colleagues)

Future research perspectives

A finding of PANACEA (thanks to the application of the SBNT) was that the most risky users are doctors, not nurses, not administrative personnel. As doctors were students once, we believe it is required to educate them in the field of cybersecurity – and more generally educate health professional on cybersecurity. We think that it is important to define and validate an approach to deliver effective training inside the university curriculum, during the "residency" period (for the new doctors), in the Continuing medical education (CME) sessions (for the "mature" doctors). Examples teaching content include: vulnerability of patients in healthcare as consequence of cyberattacks, other potential consequences of cyber-attacks (with a variety of cyber-attacks natures), how to adopt a secure behaviour, how to help others (e.g. nurses) adopting a secure behaviour in the hospital, phishing, cyber risks management in healthcare (prevention of cyber-attacks and planning for business continuity).

Presentation and Demo

The presentation at the RESSI 2023 will be delivered by IDEMIA, that will also produce a demo of the Identification Management Platform (IMP).

---

[3] see https://www.panacearesearch.eu/panacea-toolkit).

[4] Most of the tools developed by the PANACEA project will be adopted in 2023-2024 by the Fondazione Policlinico Gemelli within the project CYBERHIMPREX, co-funded by the European Commission-Digital Europe Programme

[5] see articles published in the context of PANACEA project: https://panacearesearch.eu/publications/