SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Vulnerability Assessment as a Service

Meeting place: **Brussels**
Meeting title: **Workshop on Cyber Security Situation Awareness for Health Organisations**
Presenter name: **Yannis Nikoloudakis**
Presenter organisation: **HMU (prev. TEIC)**
Date: **July 10, 2019**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Vulnerability Assessment as a Service

* **Presentation Structure**
  1. Introduction
  2. Cyber Security Facts
  3. Problem Formulation
  4. Required Solution

Vulnerability Assessment as a Service

Introduction 1/3

Large scale infrastructures, especially Healthcare ICT environments, face inherent issues:

- Fast adoption of digital systems/solutions
  - expert systems
  - remote medical consulting
- proliferation of IoT paradigm/technology
  - health sensors
  - medical devices in hospitals/homes
- host different networks
  - multi-cloud IaaS/PaaS
  - different context
  - different characteristics
- Large number of devices and services
  - Servers
  - medical devices
  - User terminals
  - Virtual machines
  - Tele-medicine equipment
  - IoT Gateways

Vulnerability Assessment as a Service

Introduction 2/3

Large scale infrastructures, especially Healthcare ICT environments, face inherent issues:

- Wide heterogeneity of devices and services
  - OSs
  - Data I/O
- Connection to other networks (corporate or not)
  - Corporate
  - Client
  - DMZ
  - Public
  - Remote
- IoT devices
  - Heart-rate monitors
  - Blood-Pressure monitor
  - Oxygen levels -sensor
  - etc.
- Intermittent connectivity of network entities
  - Wi-Fi clients come and go

Vulnerability Assessment as a Service

Introduction 3/3

Large scale infrastructures, especially Healthcare ICT environments, face inherent issues:

- Critical and non-Critical systems/devices/services coexist in the same infrastructure
  - Medical devices
  - Operator terminals

- Users/operators of devices are not always aware of (cyber) security rules, best practices
  - Susceptible to attacks

Vulnerability Assessment as a Service

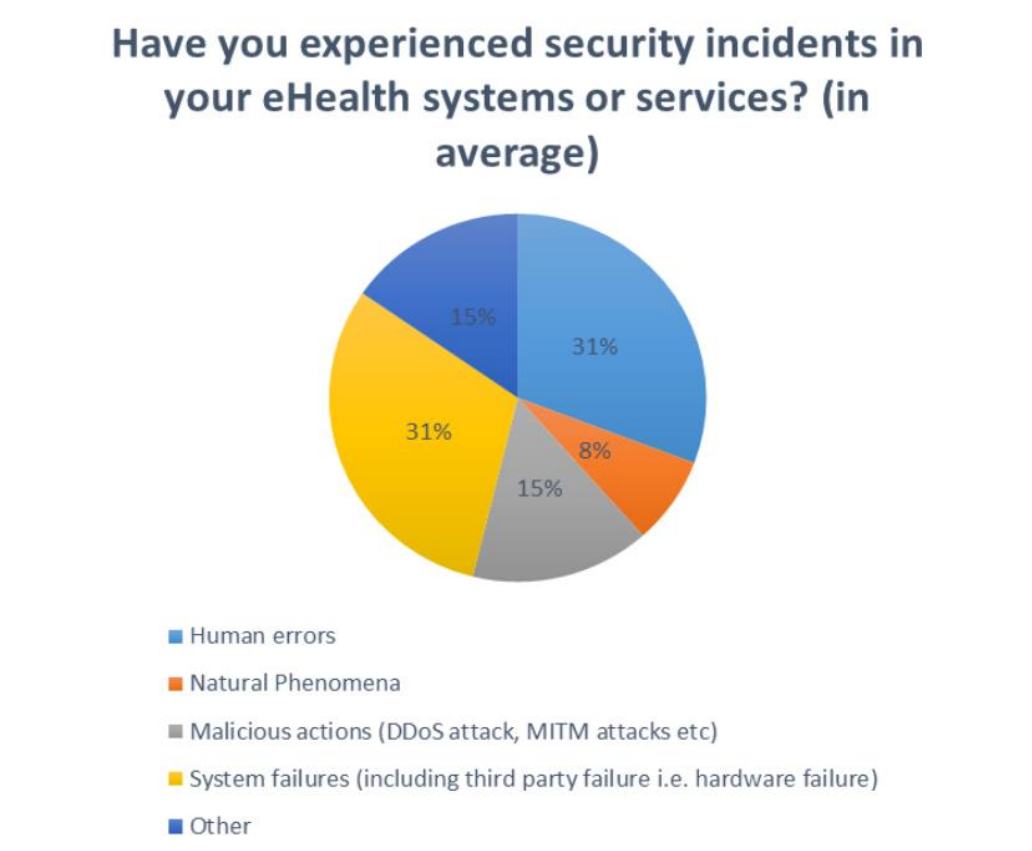
Cyber Security Facts 1/3

- Approximately, healthcare faces twice the number of attacks, compared to other ICT infrastructures
- During 2017, an average of 32000 attacks per organization was observed:~14.000 in other types of industries
- During 2017, 18% of cybersecurity events, occurred in healthcare institutions: 63% of those were caused by cyber-criminals

Vulnerability Assessment as a Service

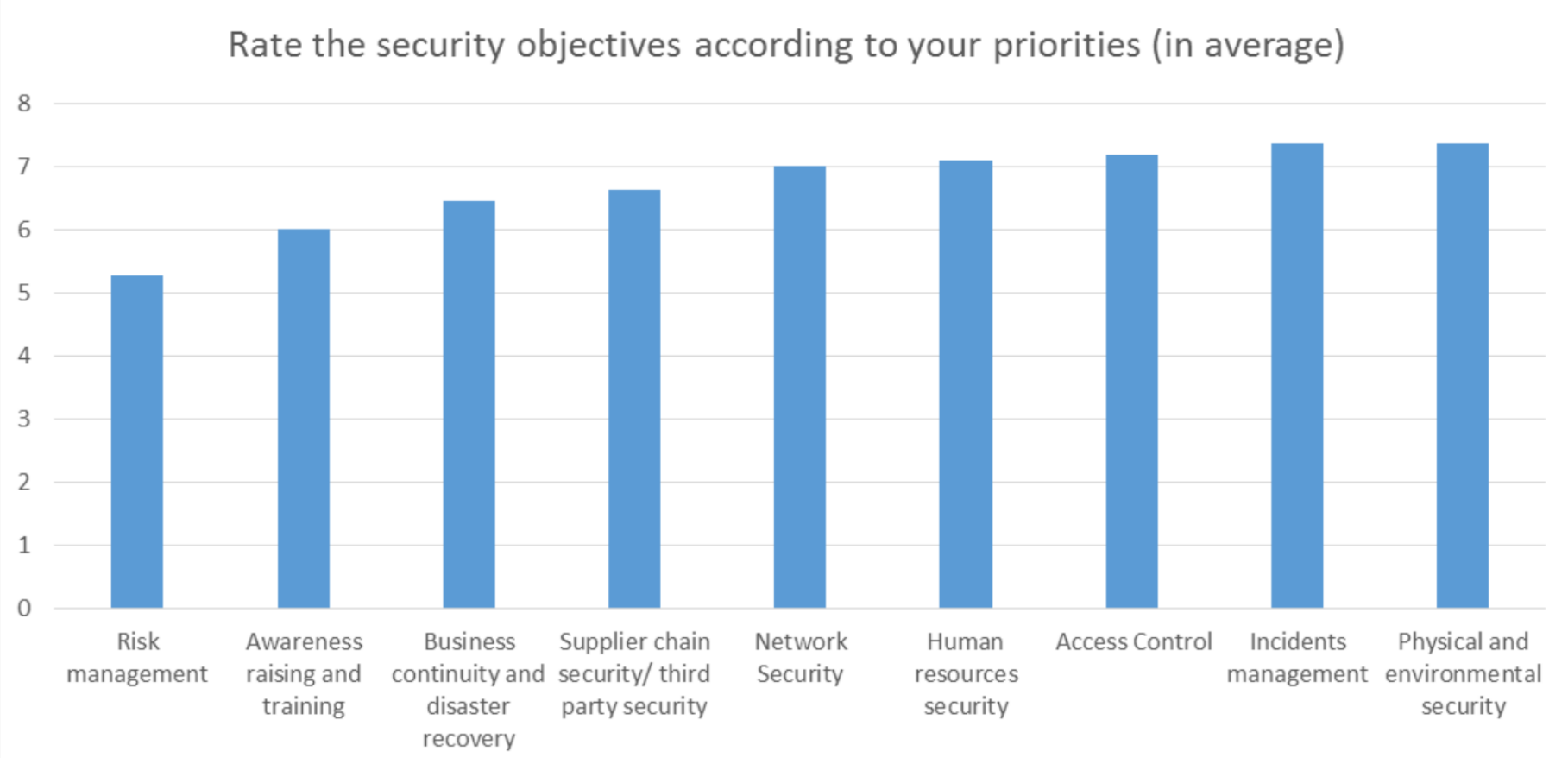
Cyber Security Facts 2/3

- Natural Phenomena 8%
- Malicious Actions 15%
- System Failures 31%
- Human Error 31%
- Other 15%



Vulnerability Assessment as a Service

Cyber Security Facts 3/3



Vulnerability Assessment as a Service

Problem Formulation 1/2

Administrators and maintainers of these infrastructures struggle due to:

- Number of devices
  - 10-15 connected devices per bed
    - 500 bed hospital
  - Updates, patches, penetration testing, etc., becomes almost impossible => ~75000 devices
  - Personnel is always limited
- Extremely large attack surface
  - Impossible to manually maintain
- Configuration of dedicated cybersecurity appliances
  - Specialized knowledge/certification is required
- Outdated operating systems and firmwares
  - render systems vulnerable

Vulnerability Assessment as a Service

Problem Formulation 2/2

Administrator and maintainers of these infrastructures struggle due to:

- Pre-assessed devices, may become vulnerable/dangerous at any point, thus requiring re-assessment
  - Initially "safe" devices can become dangerous in time
- BYOD paradigm allows users to work on their personal devices, which may be infected
  - Personal computers are a great source of vulnerabilities
- Users, who are inexperienced with cybersecurity issues/best-practices, are highly susceptible to attacks
  - Social engineering
  - Trojan horse
  - Malware
  - Ransomware

Vulnerability Assessment as a Service

Required Solution

There is a raging need for an proactive, automated system that:

- Monitors all existing and newly introduced network entities, within the ICT infrastructure
- Assess entities against known and state of the art vulnerabilities
- Utilize the large pool of knowledge that can be acquired within a healthcare institution
  - Attacks
  - Vulnerabilities
- Certify entities against cybersecurity standards
- Provide comprehensive reports for administrators
- Provide detailed input for Decision Support Systems

Vulnerability Assessment as a Service

References

[1] Ladi Adefala, *Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries*, Fortinet, March 6th 2018, https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

[2] *2018 Cyber Claims Study*, Net Diligence, Version 1.0, https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf.

[3] Dimitra Liveri, Anna Sarri and Christina Skouloudi, *Security and Resilience in eHealth – Security Challenges and Risks*, European Union Agency for Network and Information Security - ENISA, 2015, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services.

[4] Nikoloudakis, Y., Pallis, E., Mastorakis, G., Mavromoustakis, C. X., Skianis, C., & Markakis, E. K. (2019, January 24). Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. Peer-to-Peer Networking and Applications, pp. 1–9. https://doi.org/10.1007/s12083-019-0716-y

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

Presenter Name: Yannis Nikoloudakis
Organisation: HMU (prev. TEIC)
Email: nikoloudakis@pasiphae.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing