SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Portuguese Cibersecurity Healthcare Landscape

Ricardo Cabecinha
Hospital do Espírito Santo de Évora, Portugal

Brussels, 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

Summary

- Portuguese Health Ministry Cibersecurity Strategy
- Cyber Attacks in the Press
- Global Threats in 2018
- Underground Economy
- Cibersecurity Incidents reported to SPMS
- Hospital Processes and Systems (crucials)

Health Ministry Cibersecurity Strategy

- ***Resolution of the Council of Ministers nº 62/2016* – October 17**

  Defines the National Strategy for the 2020 Health Information Ecosystem – Enesis 2020

- ***Office n.º 1348/2017* - February 8**

  The Secretary of State for Health Establishes Mandatory Centralized Notification of Security Incidents in all institutions - Appointment of RNOs.

- ***Signed Cooperation Protocol between GNS / CNCS and SPMS* – 21 February 21 of 2017**

- **May 12 of 2017**

  Very important day for the cibersecurity in the world

Health Ministry Cibersecurity Strategy

Resolution of the Council of Ministers nº 115/2017 – August 24

Health Cyber Security Strategy establishes channels of communication between the Ministry of Health's cybersecurity team and the institutions

Term of Institutional Commitment for Cybersecurity in Health

70% of the SNS / MS Entities signed the document with SPMS.

Office n.º 8877/2017 - October 9

The Secretary of State for Health establishes the Governance Model for the implementation of the Health Cybersecurity Policy

Portugal Health Summit

International event about cybersecurity in the healthcare sector

Coming Soon will had a Computer Security Incident Response Team (CSIRT)

Cyber Attacks in the Press

- Ministry of Health deactivated the electronic mail to avoid damages by the virus responsible for this attack.
- System where images taken from medical examinations such as X-rays or CT from a hospital were stored. The unit ensures that patient records have not been stolen.
- INEM (medical emergency) exchange computer system of ambulances by radio to prevent attacks.
- CUF Hospitals undergo Ransomware computer attack.
- Champalimaud Foundation says it has been targeted by an "unprecedented computer attack" but has been passed without giving in to the attackers' demands (last week).

Global Threats in 2018

- **95% of cyber security violations are due to human errors**

  58% of all violations in healthcare are started by *insiders.*

  The actions that most contribute to the loss of data are due to human error and misuse.

- **65% of the organizations have more than 500 employers that never change your passwords.**
- **75% of healthcare sector was infected with malware at some moment.**
- **The ransomware is responsible for 70% of trying violation incidents.**

Source: Internet security Threat Report by Symantec

Global Threats in 2018

- Web attacks increased 56%
- 10 % of URL are malicious
- Enterprise Ransomware increased 12%
- 48 % of malicious emails attachments are office files, increased of 5% from 2017
- 78% of total malware is executed in Windows Operating Systems
- Malicious powershell increase scripts 100%

Source: Internet security Threat Report by Symantec

Underground Economy

Stolen Information	Value
Hacked email accounts (2,500)	1 – 15$
VPN services	1 – 20$
RDP login credentials	3 – 30$
Stolen or fake identity	0.10 – 1.50$
Medical notes and prescriptions	15 – 20$
Stolen medical records	15 – 20$
Fake health care ID cards	50 – 220$

Cibersecurity Incidents Reported to SPMS

Malicious Code	Infection
Malicious Code	Infection
Collection of Information	Phishing; Social Engineering
Intrusion Attempt	Vulnerability exploitation; Login attempt
Intrusion	Vulnerability exploitation; Account commitment
Fraud	Illegitimate use of third-party names
Abusive Content	Spam

Cibersecurity Incidents Reported to SPMS

Ransomware

Wannacry - present in more than 8 institutions, however without data encryption.

Data Collection – Social Engineering / *Phishing*

Users and passwords of 3 healthcare institutions was published in *pastebin.*

After a user's credentials were stolen, they were used to make a malware attack on the email front-end server of an institution owned by Ministry of Health.

User Enumeration

Is when a malicious actor can use brute-force to either guess or confirm valid users in a system. 3 institutions was victims of this kind of attack.

Fraud – Illigitimate use of third-party names

Email:

From: "Xico maria <xico.maria@gmail.com >"

Subject: URGENT Antonio maria A (June 24, 2019 02:36)

Dear XXXX,

"Thank you for your answer. I'm in Morocco where I had a problems. My luggage where i put my smartphone, passport, money and other documents have been stolen. if you borrow me 500 € to get me out of this situation I will pay you back when I arrive.

Cibersecurity Incidents Reported to SPMS

SQL Injection (3)

Occurs when an attacker inserts malicious code into a server that uses SQL. SQL injections are only successful when a security vulnerability exists in an application's software. Successful SQL attacks will force a server to provide access to or modify data

Exposed Proxys (2)

Is a method of cyberwarfare where the attacking system impregnates the enemy system, intercepting and compromising communications.

XSS (1)

Attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Cibersecurity Incidents Reported to SPMS

- All local network infrastructure (sometimes very complex)
- Network connections with national healthcare databases (i.e. ePrescription, Patients Health Records)
- Electronic Health Records and other clinical databases
- Applications for clinical decision support (LIS, RIS, PACS, etc)
- Datacenters (Some without Disaster Recovery systems)
- Medical devices linked to Network
- Access controls and authentications (Domain Controllers)
- IoT devices (the latest big challenge)

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

Ricardo Cabecinha
Hospital do Espirito Santo de Évora - Portugal
rjcabecinha@hevora.min-saude.pt

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