SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Cybersecurity Standards for reducing Data breaches

Meeting place: Brussels

Meeting title: Workshop on cyber security situation awareness for health organizations

Presenter name: George Doukas

Presenter organisation: National Technical University of Athens

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

The Changing Phase of Information Security

Traditional View

- The domain of a System Administrator
- Implementing Security Controls was only the task of a Dedicated Information Security Manager
- Task of simply Purchasing a Firewall
- Act Model
- Best practices

Modern View

- The Domain of Business Owners. Business and Security can't be separated
- Security Team Consists of Top Management, IT Managers and a Dedicated Information Security Manager
- Task of Finding out what is AT RISK and which are the right approaches to secure it
- Plan, Do, Check and Act Model
- Integration of standards in conjunction with legislation

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

What is the current protection level

Three broad types of threats that act on the cyber domain

- Software based (viruses, worms, spyware, root kits, exploit scripts, protocol exploits, etc.);
- Hardware based (Hardware Trojans, counterfeit components, etc);
- User-centric (Insider or outsider threats either from malicious or inadvertent actions or inaction).

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

What is the current protection level

Attacks affect data at any stage

- unauthorised disclosure of information (loss of confidentiality)
- unauthorised modification or destruction of information (loss of integrity)
- disruption of access to, or use of, information or an information system (loss of availability)

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

What is the current protection level

Today, cyber security has evolved but its current sophistication and maturity is being offset by:

- Increasingly sophisticated attackers and a threat-countermeasure cycle that favours the attacker.
- Software and systems designed and manufactured from a variety of sources giving rise to the possibility of compromised supply chains.
- Larger attack surfaces, stemming from the increased complexity of systems and use models.
- Social and technology trends, such as the use of IoT devices, which lead to an increased number of insecure devices accessing networks and blurring the perimeters of systems.

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

Cybersecurity Threats

15 Top Cyber threats reported in 2018

- Malware
- Web Based Attacks
- Web Application Attacks
- Phishing
- Denial of Service
- Spam
- Botnets
- Data Breaches
- Insider threat
- Physical manipulation/damage/theft/loss
- Information Leakage
- Identity Theft
- Cryptojacking
- Ransomware
- Cyber Espionage

ENISA Threat Landscape Report 2018

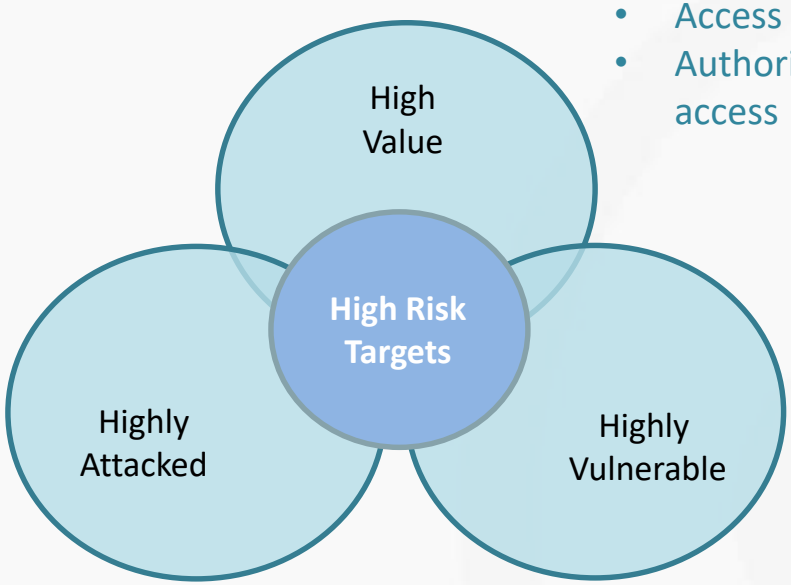
The Potential Targets of the Top Cybersecurity Threats in 2019

- Smartphone
- Internet-of-Things
- Cloud Applications

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

Increased User-Centric Vulnerabilities

- Access to critical systems
- Access to sensitive data
- Authority over teams with access



- Highly targeted
- Highly sophisticated
- High volumes

- Vulnerable devices or networks
- Interacts with malicious content
- Highly visible

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

The Healthcare environment

Opportunity

- Electronic healthcare technology creates huge potential to improve clinical outcomes and transform care delivery.

Risk

- Security of healthcare data and devices.

New legislation and regulations are in place to facilitate this digital transformation.

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

Security of Health data

- Due to their sensitive nature, Health data have always been considered a special category of data and invariably fall under the jurisdiction of data protection regulations.
  - Under the EU's General Data Protection Regulation (GDPR), they are explicitly classed as a special category of personal data, which requires the strict application of the regulation's requirements.
  - In the US, health data fall under the incidence of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), two interconnected acts which together guarantee their protection.

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

What to expect in the future

- Attacks tend to be more opportunistic and difficult to detect or predict.
- Threats are getting more potent because systems are more interconnected and people, business and government will have a greater reliance on ICT to function.
- Effects or outcomes of attacks will not be as obvious and may go undetected for long periods of time.
- A move from code exploitation to manipulation of data is identified.

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

What to expect in the future

- **The answer to the question “can I always prevent an attack”, is probably NO!**

Attackers are always changing their methods, but some trends are clear—identifying these trends will help security professionals with addressing these issues at least for a while.

But is this Enough?

- **The most effective strategy to mitigate and minimise the effects of a cyber attack is to build a solid foundation upon which to grow the cyber security technology stack.**

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

What is a standard

- **The term "standard'** includes a wide variety of technical works that prescribe rules, guidelines, best practices, specifications, test methods, design or installation procedures and the like.
- **The size, scope and subject** of standards varies widely, ranging from lengthy model building or codes to narrowly scoped test methods or product specifications.
- **Key principles** in standard development (according to ISO):
  - respond to a need in the market
  - are based on global expert opinion
  - are developed through a multi-stakeholder process
  - are based on a consensus

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

The goal of Cyber Security Standards

- Improve the security of information technology (IT) systems, networks, and critical infrastructures.
- Define both functional and assurance requirements within a product, system, process, or technology environment.
- Enable consistency among product developers and serve as a reliable metric for purchasing security products.
- Cover a broad range of granularity, from the mathematical definition of a cryptographic algorithm to the specification of security features in a web browser, and are typically implementation independent.
- Address user needs, taking into account the cost and technological limitations.
- Rise security awareness level among users, patients and care professionals

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

Cybersecurity Standards and frameworks

When identifying the most useful best-practice standards and guidance for implementing effective cybersecurity, it is important to establish the role that each fulfils, its scope, and how it interacts with other standards and guidance.

Which one is the Best?

- NIST SPs (Special Publications) 800-53 and 800-171
- ISO 27000 series
- HIPAA - HITECH
- PAS 555
- ETSI
- other

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

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

Presenter Name: George Doukas
Organisation: NTUA
Email: gdoukas@epu.ntua.gr

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