EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY IN HEALTHCARE AND ENISA ACTIVITIES

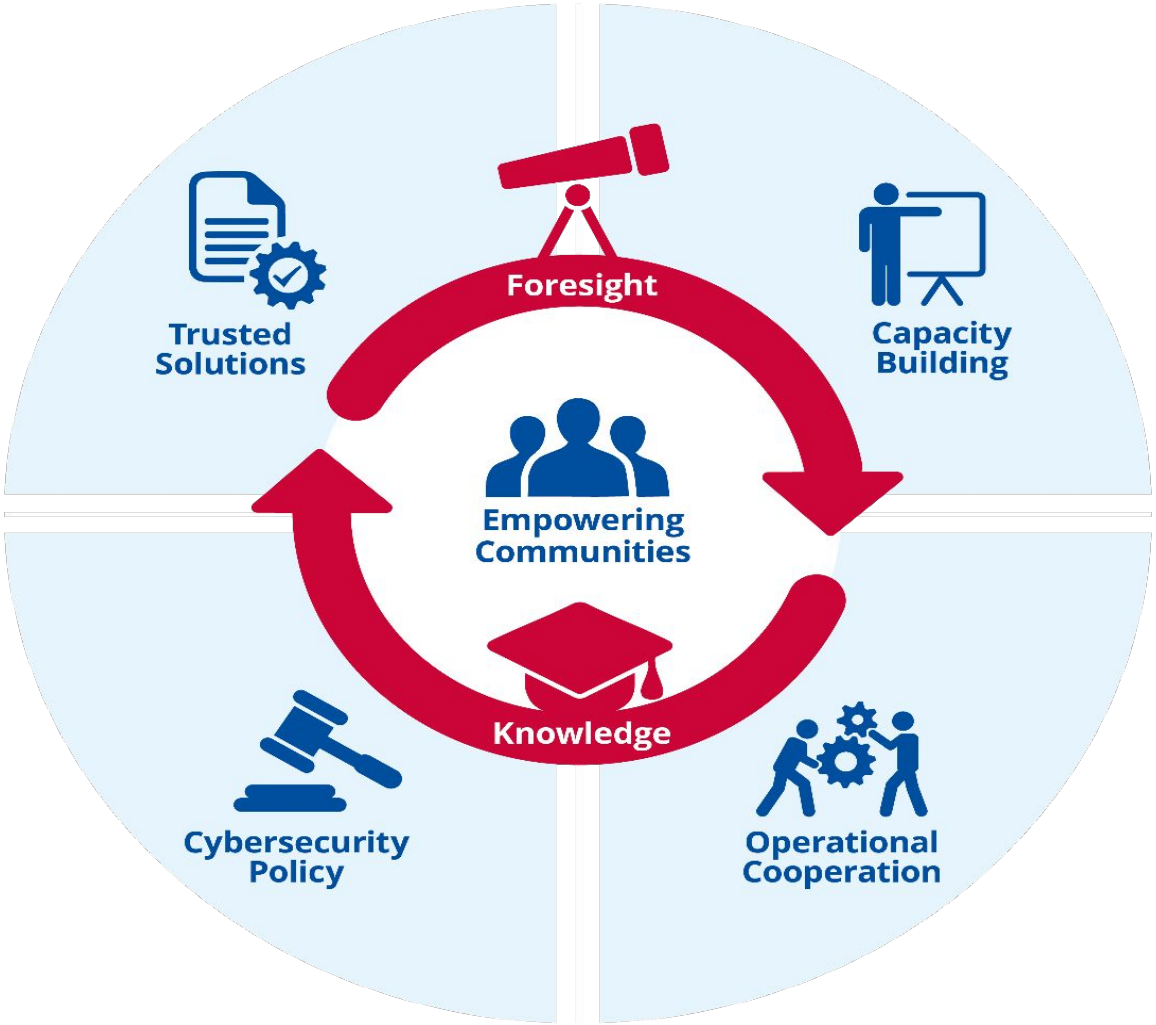
Dr. Athanasios Drougkas
Cybersecurity Expert

SAFECARE 2nd Awareness Event
01 | 02 | 2021

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

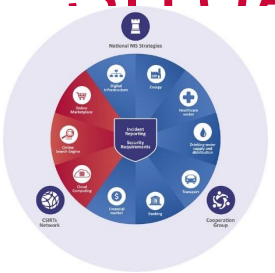
Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



HEALTHCARE UNDER ATTACK

- 150+ countries
- 230K+ computers
- Significant impact on NHS!
  - Computers
  - MRI scanners
  - Blood storage refrigerators
  - Etc…

EHEALTH CYBERSECURITY – SITUATIONAL ANALYSIS



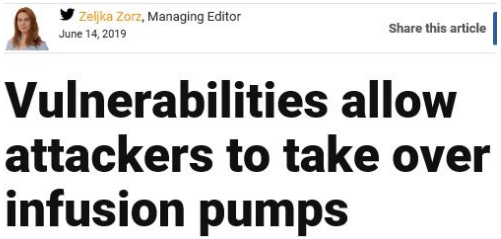
- **200%** increase in software supply chain attacks
- **600%** increase of attacks on IoT devices, 29% on ICS
- **46%** increase in ransomware variants
- Surge in crypto-mining malware hijacking processing power

Source: Infoblox - Cybersecurity in Healthcare, 2019

- **Confidence** in response: **92%** up from **82%** two years ago
- **Patching**: **87%** claim to frequently patch systems
- **Investment**: More healthcare organizations (28%) are spending **11-20% more** on cybersecurity than in 2017
- **Outdated systems**: Number of devices running on Windows XP has fallen from **1 in 5** to **1 in 10**

Source: Infoblox - Cybersecurity in Healthcare, 2019

Source: IBM, Cost of a Data Breach, 2018



Source: Kaspersky, 2018

CYBERSECURITY IN THE PANDEMIC

Increase of COVID-themed phishing attacks

Cybercrime & ransomware against hospitals

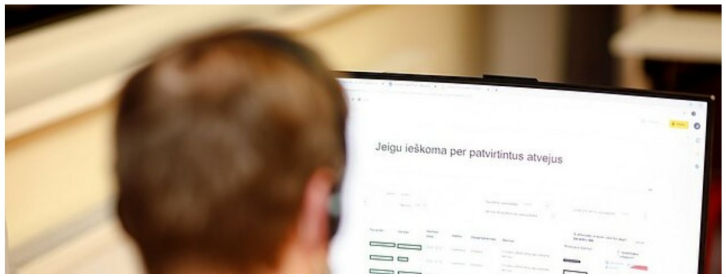
Coordinated EU efforts

Lithuania's public health body comes under cyber attack

updated

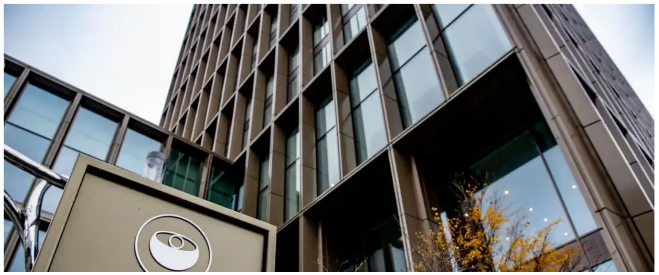
31

Jūratė Damulytė, Ignas Jačauskas, BNS
2020.12.30 09:22



Hackers accessed vaccine documents in cyber-attack on EMA

Papers relating to Pfizer/BioNTech vaccine reportedly targeted in attack on European Medicines Agency



Hackers targeted EU Commission to infiltrate coronavirus vaccine 'cold chain'

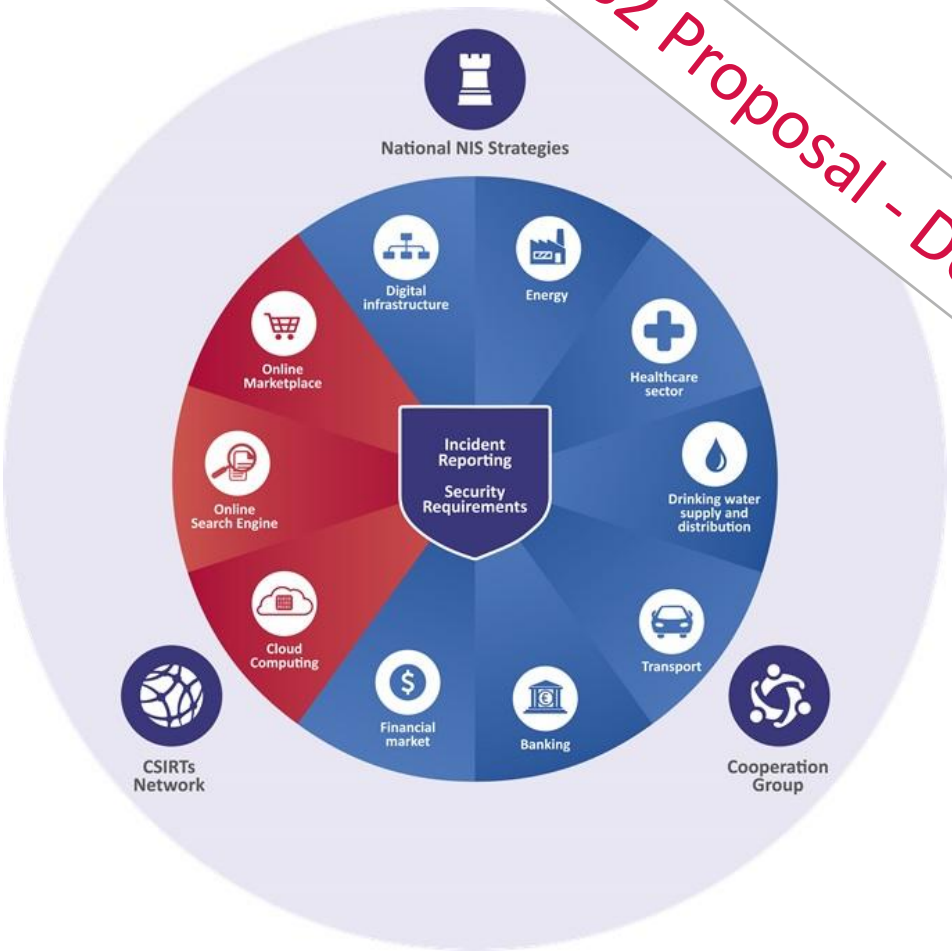
Attacks were likely state-sponsored, says US tech giant IBM.

Belgian coronavirus test lab hit by cyberattack

Hackers reported to demand a ransom to unblock computers at Antwerp facility.

THE NIS DIRECTIVE

NIS2 Proposal - Dec. 2020



NIS COOPERATION GROUP

NIS Cooperation group
Chair: Rotating with EU presidency
Secretariat: European Commission
Biannual work program

Multiple work streams on different topics:

WS1: OES Identification criteria (led by DE)	WS2: OES Security measures (led by FR)	WS3: Incident reporting (led by RO) (previously NL/PL)	WS4: Cross-border dependencies (led by EE)	WS5: Digital service providers (NL previously IE)
WS6: Cybersecurity of EP elections (led by EE/CZ)	WS7: Large scale incidents (blueprint) (led by FR/ES)	WS8: Energy sector (led by AT)	WS9: National Cyber capabilities (led by AT/UK)	WS10: Digital infrastructure (led by PL)
			WS12: Health Sector (led by PT)	WS on 5G cybersecurity (FR/CZ/NL/FI/NL/SE/RO)

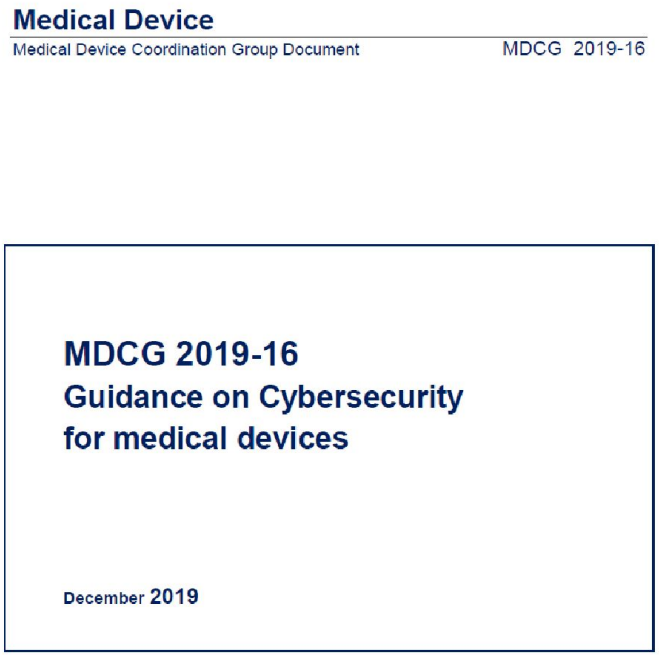
ENISA supports all work streams with drafting, research, analysis, surveys, exercises, etc.

MEDICAL DEVICES REGULATION

European Commission

Medical Devices Regulation

EU MDR



- **IT Security requirements pre-market and post-market**
- **Incident reporting for MD security incidents**
- **MDR Cybersecurity Task Force**

EHEALTH – ENISA ACTIVITIES

November 2016

February 2020

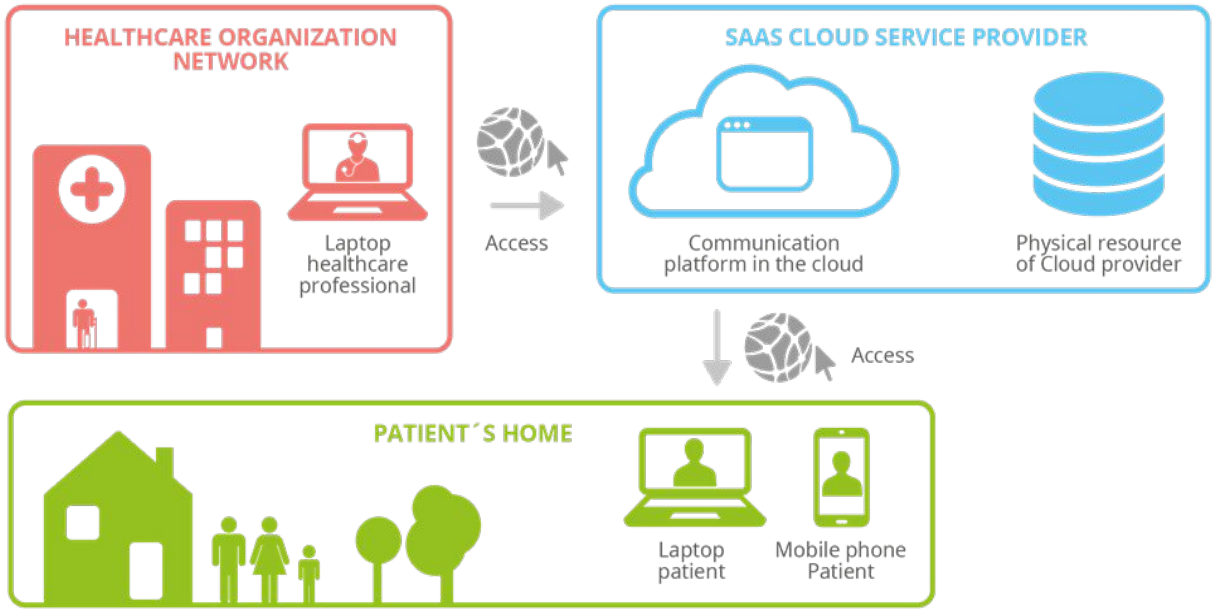
Just published!

CLOUD SECURITY FOR HEALTHCARE SERVICES

- Policy context
- Cloud security considerations
- Data protection considerations
- Use cases
- Measures

CLOUD SECURITY FOR HEALTHCARE SERVICES – USE CASES

- UC1: Electronic Health Record
- UC2: Remote Care - COVID19
- UC3: Medical Device software



CLOUD SECURITY FOR HEALTHCARE SERVICES – MEASURES

- 17 Security Measures
- Application per Use case
- Data protection considerations

SM-09	Enable data encryption for data at rest and data in transit			
Ensure data in the Cloud service provider's location is encrypted during the whole data life cycle (creation, storing, using, sharing, archiving, deleting). Review the Cloud provider's encryption practices to ensure they meet the required encryption level, are compatible with other cryptographic protection, and meet regulatory requirements. Ensure data transfer from and to the Cloud service for all incoming and outgoing connections is encrypted. (note for the author: Encryption in transit is always a shared responsibility- the Cloud customer needs to take the appropriate measures to ensure that encryption will function properly (i.e. provider or patient using outdated browsers with known vulnerabilities in encryption protocols will result into breaking the encryption measures applied by the CSP)				
Reference to Good Practice Procurement		GP 10. Encrypt sensitive personal data at rest and in transit		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider	x	x	x
Additional data protection considerations		Ensure data at rest including backup and data-in transit is encrypted. Advise on client side encryption.	Ensure data-in transit is encrypted. Advise on client side encryption.	Ensure data at rest including backup and data-in transit is encrypted. Advise on client side encryption.

CLOUD SECURITY FOR HEALTHCARE SERVICES – MEASURES

- SM-01 Identify security and data protection requirements
- SM-02 Conduct a risk assessment and data protection impact assessment
- SM-03 Establish processes for security and data protection incident management
- SM-04 Ensure business continuity and disaster recovery
- SM-05 Termination and secure data deletion
- SM-06 Auditing, logging and monitoring
- SM-07 Implement vulnerability and patch management
- SM-08 Manage assets and classify information
- SM-09 Enable data encryption for data at rest and data in transit
- SM-10 Ensure security of encryption keys
- SM-11 Data portability and interoperability
- SM-12 Client and endpoint protection
- SM-13 Authentication and access control
- SM-14 Information security awareness, education and training
- SM-15 Network Security
- SM-16 Review isolation between tenants
- SM-17 Physical and environmental security

OTHER RELATED ENISA ACTIVITIES

eHealth Security Experts Group

Cyber Europe ~~2020~~ 2021?

Annual eHealth Security Conference

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu