HealthManagement.org
The Journal
LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES
VOLUME 20 • ISSUE 4 • 2020 • € 22
ISSN = 1377-7629

COVID-19 Management

Healthcare Cybersecurity in the Time of COVID-19

The European Union Agency for Cybersecurity (ENISA) has just published a cybersecurity guide for hospitals. The body's director, Juhan Lepassaar, explains how the COVID-19 pandemic has made the need for effective cyber hygiene even more urgent.

What has prompted ENISA to release the Cybersecurity Procurement Guide for Hospitals?
The EU Agency for Cybersecurity (ENISA) is working closely with the cybersecurity community across the EU. The activities in healthcare security started in 2014 and one year later the Agency created the eHealth Security Experts Group, a group comprised of representatives from EU healthcare organisations, medical device manufacturers, as well as national healthcare authorities. Following feedback collected from this group but also from the wider healthcare community, it emerged that cybersecurity guidelines for procurement supporting IT professionals in hospitals would be valuable.

What has ENISA identified as the most serious blocks to effective cybersecurity in hospitals across Europe?
There are a number of aspects that are specific to the healthcare sector that can result in impediments to building strong cybersecurity. The situation in the healthcare sector regarding cybersecurity can be summarised as follows:

- Low maturity on cybersecurity in the healthcare sector is evident, as hospitals do not have a Chief Information Security Officer, there are a lack of security policies and of access control mechanisms.
- Hospitals are easy targets for malicious attackers due to the many different ways such attackers can gain access to a system. There are many cases of ransomware attacks in hospitals across the EU.
- Lack of security awareness amongst the involved stakeholders and use of walk-around (ie physicians, administrative personnel, patients can all use their personal devices to connect to the hospital network without following any specific strategy).
- The life span of medical devices in use such as CAT scanners or MRI machines can be outdated (longer than what the manufacturer had foreseen) and the patch management process is usually performed by a third party.
- The vulnerable nature of medical devices. For example manufacturers build them so as to support remote patching and updating of firmware, which creates identifiable loopholes.

The priority is building capabilities and increasing the awareness in the field, and this is exactly what the ENISA has been doing in collaboration with the sector.

The COVID-19 crisis has highlighted how important HIT is. There has been an increase in telehealth and telemedicine deployment for example. With this in mind, how critical is it that healthcare needs to take note of proper, permanent cybersecurity measures?
The current situation has increased various teleactivities. Teleworking, teleconferencing, telegoverenance and e-shopping are some of the activities that are becoming new habits globally. The agency has already created guidelines for a number of these activities, but similarly, healthcare has also become more digitalised. Requirements for telemedicine and remote care are now of paramount importance to society. Indeed until recently, cybersecurity was overlooked as these services didn't score high in the essential healthcare services catalogue. The COVID-19 pandemic proved this to be wrong. ENISA in 2020, will shift its focus to this topic: how can cybersecurity be ensured when telemedicine is practiced? What are the security and data protection measures vendors and providers (ie cloud services providers) should take to meet heavy demand from society while ensuring cybersecurity of the services?

There have been reports that cyber hackers have been taking advantage of the COVID-19 crisis to target healthcare organisations under more strain than usual. What advice does ENISA have for hospitals and healthcare organisations to mitigate this?
Based on information, ENISA has noted a daily increase of ransomware and phishing attacks, all a result of hackers taking advantage of the COVID-19 pandemic. The attacks are widespread and do not only target healthcare organisations but society overall. In these challenging times, hospitals are more vulnerable than ever. ENISA, along with European Institutions, strives to support cybersecurity in the essential systems in hospitals and of healthcare organisations. Some recommendations targeting healthcare IT professionals can

be summarised as follows:

•First of all, raise awareness internally in healthcare organisations and hospitals by launching campaigns even during the time of crisis (ie hospital staff not to open suspicious emails). Campaigns can be targeted or address the wider public.

• Business continuity plans should be established to be put in place whenever the failure of a system may disrupt the hospital's core services and the role of the supplier in such cases must be well-defined.

• Collaborate with vendors on incident response concerning medical devices or clinical information systems.

• It is important to isolate all network connected devices from the rest of the network by implementing network segmentation. With network segmentation network traffic can be isolated and/or filtered to limit and/or prevent access between network zones.

In case of an incident (ransomware/malware), freeze any activity in your systems, directly inform all staff and get in touch with the national cybersecurity authority. They have all the resources and knowledge to support essential operators.

systems from a potential ransomware attack. There is no "one-size-fits-all" solution in the case of healthcare organisations. However, in our report all good practices are measures that have already been implemented in some healthcare organisations with great success indicating a good preparedness level.

Since ENISA started operations in 2015, what changes has it seen in the approach to cybersecurity in healthcare?

Since we launched our activities in the sector we have noticed a shift in the approach healthcare organisations are taking towards cybersecurity. This shift was followed by policy initiatives like the Network and Information Security Directive and the General Directive Protection Regulation, but also by several private sector voluntary activities, ie the eHealth Network cybersecurity group; the cybersecurity task force created under the Medical Device Regulation to support corresponding requirements. Several awareness-raising activities have also taken place at the national level, for example SPMS, the Health Ministry's central purchasing and

ENISA has noted a daily increase of ransomware and phishing attacks, all a result of hackers taking advantage of the COVID-19 pandemic

Where cybersecurity measures are put in place, what has ENISA identified as the most significant failures to effective cybersecurity implementation in hospitals across Europe?

In hospitals, cybersecurity is undeniably not a priority; as in all other cases human error is the most common risk in this sector, based on ENISA reports and feedback from hospital CISOs. Hospital staff who are not appropriately trained, a lack of resources (budget and human) for the IT department and a preference for workarounds are some of the common burdens IT professionals need to overcome.

At the same time, limited flexibility from the medical device manufacturers a lack of contractual obligations related to cybersecurity make the situation even more difficult to handle. The Agency's activities supporting the sector, look into improving the cybersecurity position of all different stakeholders involved in the vast health ecosystem.

Can ENISA provide examples of hospitals that are implementing good cybersecurity practices?

Several large and small hospitals have been implementing good practices that suit their ecosystem, depending on the resources and the priorities they have. We have seen cases where the IT team is comprised of 30 people and cases where there is only one person and could, in both cases protect the

IT authority in Portugal, and on the European level, there is the Joint Action Plan for the eHealth Network activities.

Do you have anything to add for healthcare cybersecurity in light of the COVID-19 crisis?

Amidst the global COVID-19 crisis, the importance of information sharing has become essential; through sharing experiences on cybersecurity issues, in the form of early warnings or even recommendations and good practices, the healthcare organisations ensure resilience and continuity of their vital services.

Across EU Member States, cybersecurity experts are creating task forces to offer their services for free to all hospitals and healthcare organisations that are battling with the pandemic. Reaching out to the national cybersecurity authority or to ENISA will make you part of this larger network for information exchange. All of Europe is in this together. ■

To access the full Cybersecurity Procurement Guide for Hospitals report: enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Interviewee: **Juhan Lepassaar**
Executive Director | European Union Agency for Cybersecurity
info@enisa.europa.eu | enisa.europa.eu | @enisa_eu