



The race to make hospitals cybersecure

As medical centres increasingly come under attack from hackers, Europe is bolstering protection.

24 May 2023 - By TOM CASSAUWERS

Amid the Covid-19 pandemic in early 2021, the Irish healthcare system's computers were breached by hackers who gained access to patient files and posted hundreds of them online. As a result, the network had to be shut down.

The reverberations were widespread as appointments got cancelled, people's most sensitive data was stolen and even procedures like CT scans came to a halt. The attack was one of the largest hacks of a healthcare provider in the world.

Mind the gap

'At the moment, there is a major gap in the cybersecurity capacities of healthcare,' said Christos Xenakis, a digital systems professor at the University of Piraeus in Greece. 'Hospitals need to work properly and protect our data.'

From May 2021 to June 2022, the EU's cybersecurity agency – ENISA – detected a total of 623 ransomware incidents in Member States similar to the one in Ireland. Healthcare was the fifth most targeted sector of those attacks.

That in turn has spawned more investment and technological development to secure the industry. Scientists, medical professionals and governments are increasingly taking action to prevent scenarios like the Irish one.

The answer lies not only in better software. Cybersecurity is more often than not about people and changing their behaviour.

That's one of the conclusions reached by Sabina Magalini, a professor of surgery at the Catholic University of the Sacred Heart in Rome, Italy.

She coordinated an EU-funded project called [PANACEA](#) to improve hospital cybersecurity. The initiative ran for 38 months through February 2022.

Human errors

'Human error is one of the main cybersecurity risks for hospitals,' said Magalini. 'The risk lies with people, which is logical. A hospital isn't a nuclear power plant and can't be closed off in the same way.'

Hospitals tend to be busy places. Staff need to perform medical duties and, at the same time, work on a variety of computer systems.

Research during PANACEA showed that, during a single day, nurses often had to log in to computer systems more than 80 times.

This is time-consuming and leads to shortcuts, including the same password being used by a group of people or passwords being written down on a piece of paper next to the computer.

In general, the study demonstrated that hospital staff followed cybersecurity precautions poorly and, in the process, left an opening that attackers could exploit.

'We need to make interactions between healthcare professionals and computers better,' said Magalini. 'As a doctor or nurse, you're treating the patient and using a computer at the same time. It's hectic.'

Safety precautions

PANACEA came up with ways to make it easier for hospital staff to follow cybersecurity precautions. One example is software ensuring a more secure login system.

'The software allows for facial recognition of healthcare workers,' said Magalini. 'This would bypass the need for the problems we're seeing today with passwords.'

The project also experimented with low-tech alternatives. Researchers put up stickers and posters in participating hospitals to nudge healthcare workers into following basic cybersecurity procedures.

Education also needs to play a role, including for doctors, according to Magalini.

'Cybersecurity training should be included in their residency programmes,' she said.

Easier sharing

Another EU-funded project, [CUREX](#), facilitated the sharing of health information among hospitals. Xenakis of the University of Piraeus coordinated the project, which ran for 40 months through March 2022.

'Health data is the most sensitive data there is,' he said. 'Hackers pay more for health data than for credit card information.'

When sending patient information to another health facility, a hospital might not be aware of the extent of the recipient's cybersecurity arrangements.

CUREX addressed that uncertainty.

The project developed a software that can help detect any vulnerabilities in the security of an outside organisation. The system makes it easier for medical facilities to share information in line with EU data-protection rules.

'It's all about risk assessment,' said Xenakis. 'And to do that, you need to know how secure the other organisation is.'

Follow-up work

European researchers and cybersecurity organisations are investing in these types of answers.

As a follow-up to PANACEA and CUREX, the EU is co-funding cybersecurity procurement for hospitals, meeting 50% of the cost of new measures.

So, even while attacks on European hospitals continue on a regular basis, experts see reason for optimism about the future.

'European cybersecurity providers are rapidly becoming more mature,' said Xenakis. 'In turn, hospitals are recognising the necessity to buy new tools and upgrade their security.'

Research in this article was funded by the EU. If you liked this article, please consider sharing it on social media.

More info

- [PANACEA](#)
- [CUREX](#)
- [Digital Europe Programme](#)