



STORMSHIELD

THE HOSPITAL SECTOR

CRITICAL SYSTEMS, HIGHLY SENSITIVE TO CYBERATTACKS

Marco Genovese
Product Manager,
Stormshield

It's a terrifying paradox: despite the fact that trust and confidence is a central aspect in the relationship between hospitals and their users, **80% of health organisations have suffered a successful attack between 2016 and 2018 according to an article by Orange Cyberdefense and Orange Healthcare.** How can we explain this vulnerability and above all how can it be countered?

DATA AND CRITICAL OPERATIONS MAKE THE HOSPITAL SECTOR A PRIME TARGET

Health organisations are particularly attractive to hackers because they process ultra-sensitive data concerning patients. **Ransomware, denial of service attacks, "medjacking", or botnets,** hackers will try anything to compromise access to this sensitive information or to get their hands on it. However, data isn't the only thing of interest to cyberattackers. Because disrupting the different activities carried out in these healthcare establishments, putting lives at risk, offers a powerful means of blackmail enabling them to get what they want.



STRUCTURAL AND HUMAN FACTORS TOGETHER CONSTITUTE A VERY REAL SECTOR-SPECIFIC VULNERABILITY

How can it be that systems which are so sensitive - and which are known to be under threat - can still be so vulnerable? It all comes down to a complete mishmash of failings.

The permeability of front-line networks

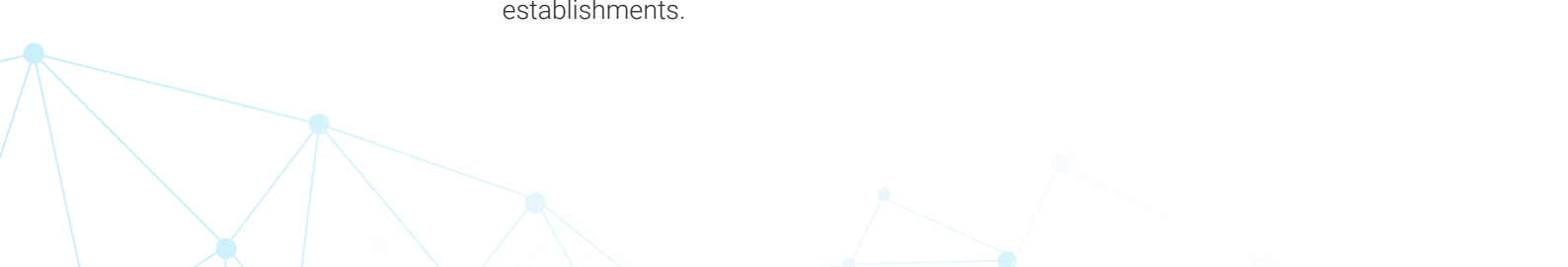
In hospital environments, it's by no means rare to find several networks with different privacy levels existing side-by-side. For example, **from a Wi-Fi hotspot**, it's easy to connect to the patients' network. From there, it's possible to intercept the medical network and from there to access the administrative network. Where it exists, this lack of segmentation constitutes the first flaw in the system, which can be exploited by hackers.

Emergencies take priority

Hospitals and other health organisations have an obligation to ensure business continuity. This means that they cannot interrupt treatments in progress. For this reason, when their IT infrastructure changes, most of them are reluctant to switch into maintenance mode or to switch off certain devices, even briefly. This way of working often leads them to make do with older solutions rather than view the IT system as an all-embracing project with its own governance. To appreciate the problem at first hand, the next time you visit a hospital, **have a quick look at the browsers or applications used**. In a report the British National Audit Office (NAO) examined the impact of WannaCry on the National Health Service (NHS). At the time, *"most of the infected NHS equipment used supported versions of Windows 7, which hadn't been patched"*. At the same time, working under emergency conditions also results in basic security measures being neglected on a daily basis, such as closing your session when away from the workstation. The information contained in the patient's record then becomes accessible and administrative access may also be compromised in some cases.

Very few in-house cybersecurity experts

In addition to insufficient governance, another problem is simply the absence of IT security experts in health establishments. However, this problem may soon be a thing of the past as the sector is now making a considerable effort to catch up. In France, the colloquium for the **Association for the Security of IT Systems in the Health Sector** (APSSIS) held in early October showed that this theme is now assuming greater importance during the debates among the different health and medical-social establishments.





BYOD: a common but uncontrolled practice

Another factor increasing the vulnerability of hospital environments is directly linked to the way the doctors work: many split their time between a private practice and the hospital, but use the same computer and smartphone. As this equipment has not been supplied by the hospital, it does not always comply with the security measures the hospital has put in place.

New and relatively insecure medical technologies

Connected medical devices are becoming increasingly common in the best-resourced hospitals. However, the attention paid to security when designing these devices is still insufficient, **leaving an open door to “medjacking”**.

The increasing use of technical management systems for buildings

Among other things, technical management systems in buildings make it possible to remotely control equipment such as the air conditioning systems, fire detection systems or the lifts. If such a system gets hacked, this can result in the forced evacuation of the hospital for example. Designed based on “*physical*” security standards, these systems are not sufficiently resilient from a digital security viewpoint.

HOW CAN THE HOSPITAL SECTOR BECOME MORE RESILIENT TO CYBERATTACKS?

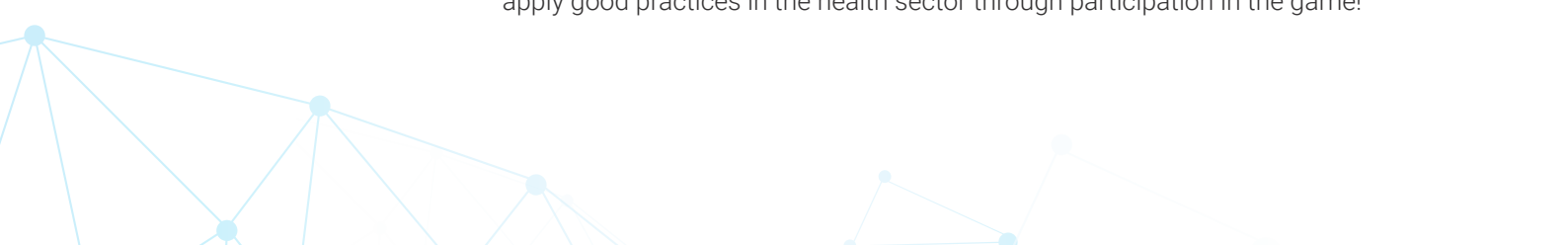
The first necessity is to **fully appreciate the vulnerability of these health establishments and to make cybersecurity a key concern within the organisation**, with everything this entails in terms of investments (human resources, governance, equipment, and dedicated budget, etc.).

Use certified and qualified security solutions for networks and hardware

At a more practical level, it's vital to use solutions designed to secure networks, to protect them against intrusions and to guarantee business continuity, but also to guarantee the security of workstations. These solutions must be compulsory for all equipment involved in patient care, whether the organisation owns this equipment or not.

Raising awareness among staff

To convince health staff to comply with best practices in the cybersecurity field, it's vital to regularly remind them of just what is at stake and to clarify the different procedures with them. With this in mind, the Pays de la Loire's e-health healthcare cooperation group (GCS) worked with Orange Cyberdefense on the creation of **an escape game known as Sant'escape –Digital Security**. Its principle? To explain and apply good practices in the health sector through participation in the game!



Reporting incidents to the Regional Health Agency (ARS)

In France, health establishments are obliged to report any health or cybersecurity incident or suspected incident by means of a portal provided for them by the government. The regional health agencies then have the task of forwarding this information to the “*Cybersecurity Support for Health Organisations*” unit (ACSS - Accompagnement Cybersécurité des Structures de Santé). In addition to allowing for better monitoring, the purpose of this national assistance system created by the French Digital Security agency (ASIP) is to put forward recommendations.

Hospitals and the health sector in general are today caught between the need to cut costs and the need to fully exploit the potential offered by digital technology, such as for example the launch of new services **like teleconsultation**. However, the insufficient security offered by their IT systems can have a particularly severe impact on privacy and security for patients. Unless cybersecurity is treated as a health-related priority in its own right.



STORMSHIELD



Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com