HOSPITAL NETWORKS:
AT THE HEART OF A MAJOR ATTACK VECTOR

The computer network is a critical part of how a hospital operates. It interconnects all areas and acts as a powerful engine of transmission with the operational network and the outside world. As a result, much sensitive data passes through these various networks, which then prove to be critically important to an equally essential and vital area of activity.

NETWORK VECTOR

DEFINITION

A "network" cyberattack involves exploiting a weakness in the network configuration of a healthcare establishment, or one found directly in its network protocol.

TARGETS

The actual targets of a network cyberattack are the sender or receiver of data carried in an exchange between computers. It can be medical or computer equipment, or even elements of the technical building infrastructure (building/central/electrical management systems).

ACCESSIBILITY

Cybercriminals access data streams locally (by breaking in via the staff's Wi-Fi network, for example) or remotely.

They can remotely break into employees' remote connections via a VPN or into data flows between business applications and third parties (subcontractors, laboratories, insurance companies or other hospitals). This modus operandi is a growing one in the fields of telemedicine and data hosting in the Cloud.

A more brutal approach may also involve launching a denial of service (DDoS) attack. Its goal: to make a server, a service or an infrastructure unavailable.

Read more

By nature, telemedicine involves risks related to the technologies on which it is based. A computerised medical instrument, such as a connected morphine pump, may experience a technical malfunction. But more importantly, it increases cyber risks for the hospital as a whole.

Diego Facchini, IT Director at Health Italia Spa, tells us more about these risks.

IMPACT

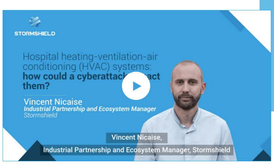
The impacts of a network attack on a hospital are many and varied, ranging from the sabotage of medical equipment to the extraction of health data.

Discover the impacts of cyberattacks that affect the hospital's computer and operational networks.

EXAMPLES OF NETWORK ATTACKS

2021 | A fictitious cyberattack on HVAC systems

In a hospital environment, a cyberattack on the heating-ventilation-air conditioning system could prove disastrous. Vincent Nicaise, Industrial Partnership and Ecosystem Manager (Stormshield), deciphers the flaws in HVAC systems and delivers useful advice for preventing them.



2020 | A DDoS attack on AP-HP services

The services of the Assistance Publique – Hôpitaux de Paris (AP-HP) were targeted by a distributed denial-of-service (DDoS) attack on two of its internet addresses. The result: disrupted access to messaging and applications for employees.

2018 | Patient data extortion with blackmail

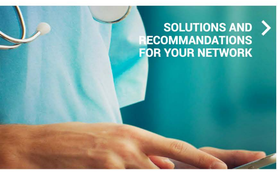
Cyberattackers obtained data from Vastaamo, which operates 25 psychotherapy centres across Finland. Two years later and after having – unsuccessfully – attempted to blackmail the company, the cybercriminals decided to attack the patients… threatening to publish the stolen content.

2017 | Ransomware shakes Britain's healthcare system

WannaCry ransomware attacks Britain's NHS healthcare system. Hackers exploit a Windows vulnerability to infect more than 16 health centres and 200,000 computers (70,000 consultations cancelled, 1,200 items of diagnostic equipment paralysed).

2014 | A DDoS attack on a hospital donation page

The donation page of a US children's hospital is paralysed for several days as the result of a distributed denial-of-service (DDoS) attack. Lost revenue for the establishment: $300,000.



SOLUTIONS AND RECOMMANDATIONS FOR YOUR NETWORK

Preparation, prevention and protection are the key words here. Probes are able to detect vulnerabilities, and firewalls, and to ensure perimeter security, making them the two main solutions to be deployed. On the firewall side, the functionalities of service continuity and availability, secure VPN access, protocol analysis, intrusion prevention system and network segmentation will be central to an effective protection mechanism. At the same time, it is important not to forget the need to raise teams' awareness of good cybersecurity practices.

More about Stormshield solutions

REGULATORY UPDATE

At European level, the NIS directive lists a number of recommendations for operators of essential services (OES), including most health establishments with a medical emergency service. At this same European level, the GDPR, the PSI and the PCI-DSS are all standards that must be complied with... not to mention specific national variants.

To help you find your way through the labyrinth of cyber regulations,

read our dedicated ebook

Want to get in touch with Stormshield? Start a discussion with our technical or sales teams.

Contact Stormshield

Download this webpage in a PDF file