HEALTHCARE EQUIPMENT IN A WORLD OF **SOFTWARE FLAWS**

Computer software provides countless services in increasingly connected hospitals. But the loopholes they contain can also help cybercriminals.

SOFTWARE VECTOR

DEFINITION

Software cyberattacks are any kinds of attack that exploit a weakness, flaw or obsolescence in software installed on computer equipment or a computerised medical device.

ACCESSIBILITY

These cyberattacks can made locally, provided the cybercriminal has physical or network access to their target within the hospital. But they can also occur remotely, if the same target is accessible via a computer network. This is, for example, the case with some medical equipment monitored by old operating systems.

Learn about the different ways in which software attacks can access hospital equipment.

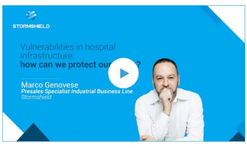
TARGETS

The majority of software cyberattacks target medical equipment. However, in some cases, the first machine to be attacked is only an intermediate step in reaching the real target: patient data, other medical or IT equipment, or even installations relating to the centralised building management system (BMS) or electrical technical management system.

IMPACT

The consequences of a software attack on a hospital can be varied, and often disastrous. They can take many forms, from industrial sabotage of health machines to the installation of ransomware, and including the extraction or corruption of health data.

Flat networks and lack of segmentation, obsolete operating systems, failure of updates: there can be many vulnerabilities in a hospital. It only takes one to be exploited for a virus to spread and bring the entire hospital infrastructure to be frozen. Focus on the subject with Marco Genovese, Presales Specialist Industrial Business Line Stormshield.



EXAMPLES OF SOFTWARE ATTACKS IN HOSPITALS

2020 | Tragic attack at Düsseldorf hospital

A German hospital fell victim to ransomware which was deployed by exploiting a software flaw in a Citrix network gateway. The cyberattack turned into a tragedy when one of the patients who could not be treated died during her transfer to another hospital.

2020 | Security breaches at Dedalus

In 2020, a controversy uncovered a number of security flaws in a solution from the Dedalus group, specialising in healthcare software. One of them provided access to tickets opened by the company's client hospitals and laboratories, in which remote administration identifiers and passwords could be found.

2019 | Phishing case at the Issoudun Hospital Center

The emergency department at this hospital centre was the first to sound the alarm on an October night when they lost access to their business software. The culprit: Anti Recuva, malicious software which infiltrated the network as an email attachment, paralysing all Windows workstations by exploiting a flaw in the operating system.

2019 | Critical flaw in Medtronic defibrillators

The American authorities issued a warning over potential risks from implantable defibrillators produced by the Medtronic company, whose data transmission system could be hacked to disrupt its operation.

SOLUTIONS AND RECOMMANDATIONS FOR PREVENTING A SOFTWARE CYBERATTACK

To prevent software cyberattacks, it is essential to raise awareness among teams, and also to ensure that workstations comply with best practices in this area: limit application network access to what is strictly necessary, perform a systems audit, tighten configurations, and even perform offline backups. Security can also be delivered through the use of behavioural analysis on workstations and data encryption.

More about Stormshield solutions

REGULATORY UPDATES

Medical devices are thus required to bear the CE marking, a sign of compliance with European legislation. The rules that apply to hospitals to guarantee patient safety are numerous and varied, and include the use of approved machines, and compliance with the "Health safety in healthcare establishments" standard.

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

read our dedicated ebook

Would you like to get in touch with Stormshield for more information on your options? Start a discussion with our technical or sales teams.

Contact Stormshield

Download this webpage in a PDF file