HOSPITAL EQUIPMENT:

THE FRAGILE TARGETS OF **PHYSICAL ATTACKS**

Far from the cliché of the cyber-criminal, hidden behind a screen miles from the intended victim, some attackers get up close and personal to their target. Their technique: to attack hospital equipment directly, whether computer or medical equipment, and exploit its vulnerabilities. This is called a physical cyberattack.

PHYSICAL VECTOR

DEFINITION

Physical cyberattacks include attacks that specifically target the hardware aspect of medical, IT or operational equipment.

ACCESSIBILITY

These cyberattacks all share a physical dimension, with the cyber-criminal gaining physical access to the equipment in question and connecting to it to disrupt its operation.

TARGETS

In hospitals, physical cyberattacks target not only medical equipment (medical imaging equipment, anesthesia machines, breathing apparatus, insulin pumps, etc.) but also more traditional computer equipment for hospital staff (computers, laptops, etc.).

Learn about cybercriminals' key hardware targets and find some practical advice for preventing attacks with Mathieu Demont, Cybersecurity Expert at Siemens Smart Infrastructure France.

IMPACT

From the sabotage of machines to the alteration – or even theft – of health data, the impacts of a physical attack on a hospital are manifold.

Decipher them using a real-world scenario of a cyberattack on a hospital's fire safety system.

EXAMPLES OF SOFTWARE ATTACKS IN HOSPITALS

2020 | Conficker returns to compromise connected objects

This computer worm, which appeared in 2008, was detected by an American firm on connected medical equipment using obsolete versions of Windows. These included mammography machines.

2020 | Medical devices hit by "SweynTooth"

A series of vulnerabilities in the Bluetooth Low Energy protocol, called SweynTooth, affect chips in certain medical devices. These include certain cardiac pacemakers, glucometers, ultrasound systems and even insulin pumps, which can then be controlled remotely or blocked.

2019 | Alterable medical imaging data

Israeli researchers simulated a "man-in-the middle" attack by physically smuggling a Raspberry Pi into a hospital. In this way, they were able to intercept medical imaging data transmitted via the DICOM protocol and demonstrate that it could be altered.

SOLUTIONS AND RECOMMANDATIONS FOR PREVENTING A PHYSICAL CYBERATTACK

To guard against such attacks, it is necessary to provide optimal protection for machines at workstation level. The recommendation is therefore to implement systems for access control, external device control, and even behavioural analysis. This can mean installing "sheep-dip" stations which act as a decontamination area for USB keys. As a last resort, network segmentation makes it possible to limit propagation in the event of infection.

More about Stormshield solutions

REGULATORY UPDATE

In addition to the "Health safety in healthcare establishments" standard, hospitals must use approved machines to ensure patient safety. Medical devices must bear the CE mark – a sign of compliance with European legislation.

To find out more about the applicable legislative framework,

read our interactive ebook

Do you want to go deeper into certain issues involving the physical vector? Want to know more about workstation protection and behavioural analysis? Start a discussion with our technical or sales teams.

Contact Stormshield

Download this webpage in a PDF file