HUMANS:
THE GATEWAY OF CHOICE FOR CYBERATTACKS AGAINST HOSPITALS

Cybercriminals are no longer reticent about attacking medical organisations. One way in which they do this is to use real people at the heart of their digital attack. To this end, patients, families and the staff of hospitals and other health establishments can be manipulated to deliver a cyberattack.

HUMAN VECTOR

DEFINITION

Cyberattacks that exploit the human vector use or target one or more individuals (doctors, nurses, agents, administrators, or even patients themselves).

ACCESSIBILITY

Perpetrated remotely – for example, via phishing or spear phishing techniques – these cyberattacks can take different forms: a fraudulent phone call, a falsified e-mail or even a corrupted USB key, deliberately left in a car park in the hope that it may be picked up and brought into the hospital. But a "human" attack can also be made when a patient connects to a fake Netflix site via the Wi-Fi in their room, a login by a surgeon from home, or maybe a subcontractor in charge of remote maintenance.

TARGETS

While such cyberattacks use the human vector – very often the employees or subcontractors of healthcare establishments – this is generally only an entry point. Ultimately, their aim is to target the health structure itself: how it works, the data it processes, its patients, etc.

IMPACT

The use of the human vector to conduct a cyberattack has several objectives: to extract information as part of a reconnaissance phase, to play the role of intermediary to reach specific equipment, to corrupt a particular individual's computer, or to deploy ransomware.

EXAMPLES OF ATTACKS ON THE HUMAN VERCTOR IN A HOSPITAL ENVIRONMENT

2020 | A fake e-mail from the WHO to exploit a flaw in a Windows component

Cybercriminals pretending to be the World Health Organization (WHO) used an email attack to exploit a flaw in the ActiveX controls of the Windows operating system and held several Canadian healthcare organisations to ransom.

Learn about the inside story of this attack in pictures.

2020 | Pharmacy wholesaler falls victim to CEO scam

At the same time in France, a pharmacy wholesaler in Rouen was hit by a scam involving false transfer orders, placing an order for 6.6 million euros' worth of gel and masks. The order was placed with cybercriminals who had impersonated known suppliers.

2020 | Ryuk storms American hospitals

Cybercriminals conducted a massive phishing campaign in the United States to carry out a coordinated attack specifically targeting several hundred American healthcare facilities in 2020. Their goal? To infect them with Ryuk ransomware.

2019 | Clop: the ransomware that shook the Rouen University Hospital

Following a phishing campaign, the TA505 criminal group succeeded in paralysing not only the office automation system but also the medical imaging and analysis systems of the University Hospital of Rouen. Only the Linux servers and the telephone network, isolated from the IT infrastructure, were spared.

SOLUTIONS AND RECOMMENDATIONS TO GUARD AGAINST ATTACKS THAT EXPLOIT THE HUMAN VECTOR

Raising awareness among teams remains essential to reduce the risks of exploitation of the human vector in cyberattacks; and the same is true of the implementation of digital hygiene procedures in support of new working practices (external devices, BYOD, etc.). Network segmentation and behavioural analysis are also recommended, along with the use of IPSec and SSL VPN and data encryption.

Finally, strengthening protection and security means implementing two-factor authentication or even authentication filtering, by configuring access restrictions on a per-user basis.

More about Stormshield solutions

REGULATORY UPDATE

In view of the major challenges, the regulations that apply to the medical sector are very strict: CE marking for medical devices, approval of machines, compliance with the "Health safety in healthcare establishments" standard, and also the GDPR, the ISSP (mandatory information systems security policy in healthcare establishments), the ePHI (electronic Protected Health Information) and the American HIPAA (Health Insurance Portability and Accountability Act) standard.

For more information about them,

read our interactive ebook

Want to get some extra input or talk through your specific issues with our experts? Start a discussion with our technical or sales teams.

Contact Stormshield

Download this webpage in a PDF file