CYBERSECURITY IN HOSPITALS

How Dräger will help keep your hospital safe

Networked information technology in hospitals ensures rapid exchange of information and automated processes. However, it also increases the risk of attacks from cyber criminals. At Dräger, we continually strive to implement cybersecurity best practices and have implemented a comprehensive consideration of cybersecurity throughout every stage of the product development cycle.

Cyber-attacks: risk for healthcare facilities

Hospitals have fallen victim to cyber-crime on several occasions. Blackmail attempts with ransomware where important hospital data are encrypted and a high amount in cryptocurrencies such as bitcoin were demanded as a ransom to get the decryption code is the most common. However, there are a whole host of other cyber-attacks on hospital networks (see blue box).

EXAMPLES OF CYBER-ATTACKS ON IT NETWORKS:

- Viruses, trojans, worms, spyware, spam, ransomware
- Advanced persistent threats: complex, targeted attacks on critical IT infrastructures such as medical networks. Once the attacker has initially penetrated a computer, they advance further into the victim's local IT infrastructure, wanting to remain undiscovered for as long as possible, so that they can spy on sensitive information or do other damage over a long period of time.
- Botnets: this involves attackers introducing trojans onto your computer, taking control and combining the infected systems into one network that is then controlled by remote access.
- DDoS (Distributed Denial of Service) attacks aim to overload a server's resources with large volumes of simultaneous requests from different locations on the internet in such a way that the server is no longer accessible or drastically slowed down.

Simulated attacks have also shown that medical devices are often inadequately protected against manipulation. Apart from the risk to life and limb for the patients, there is the threat of service failure, financial loss, loss of sensitive data and a negative reputation for the hospital.

To mitigate cyber-threats, medical device manufacturers need to add security requirements throughout the development cycle.

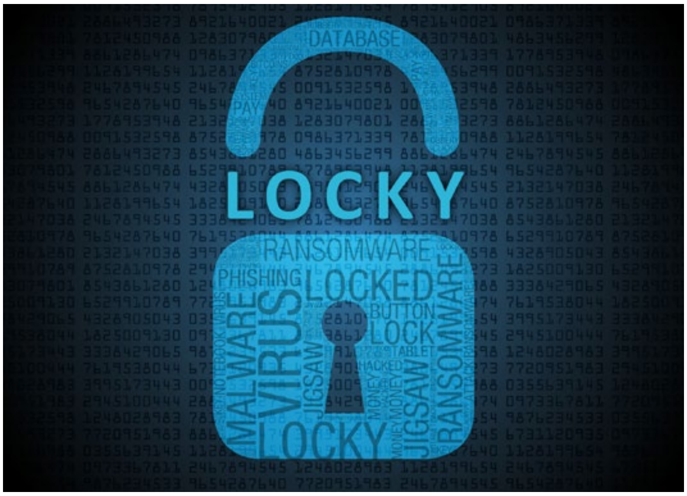
In May 2017, there were reports of a global cyber-attack that hit hospitals in Great Britain especially hard[1]. The hospitals of the National Health Service (NHS) that were brought to a standstill included those in London, Blackpool, Hertfordshire and Derbyshire. The IT systems were infected by what is known as ransomware. The spreading of the malware through the IT network led to a complete shut down, which forced staff to revert to pen and paper. Several patients had to be referred to other, unaffected hospitals. Many hospitals were overwhelmed with delays.

> *“Our Dräger products have survived this attack unscathed and I have no reason to expect that there will be any problems with this in the future”*
>
> Hannes Molsen, Product Security Manager at Dräger, on the 2017 WannaCry Ransomware Attack [2]

“A key reason for this is undoubtedly that we design security into our devices right from the start. This offers our customers a distinct advantage – alongside the security itself: the documented security properties of Dräger devices facilitate obligatory IT-security risk management, as stipulated by, e.g., the German IT Security Law.” Furthermore, according to Molsen, even if you have an unexpected attack like the one in May, Dräger is able to provide advisories that contain all the information the customer needs to put safeguards in place.

Digitisation trend: accelerated by monitoring devices

The level of digitisation still greatly varies from country to country. The US is leading this unstoppable development, as is Scandinavia. Molsen explains: “In the Scandinavian countries, we find by far the highest level of digitisation throughout Europe.”



Even in countries where digitisation is not yet so advanced, such as Germany for example, there are nevertheless several very sensitive areas in hospitals. Thus, the capture of X-ray and MRI data is now mostly digital. In Germany, active medical equipment such as anaesthesia machines and ventilators have until now been rarely connected to a network. However, in the medium-term, this too will change. Nevertheless, by and large, European hospitals are still significantly less connected to a network than US healthcare facilities.

Clinical monitoring has significantly accelerated the trend for digitisation. Sensitive monitoring data from the intensive care unit is entered in the patient data management system (PDMS), the OP system or even the anaesthesia system. In the US, the capture of patient data electronically is mandatory. In view of growing patient numbers, this presents a huge challenge for software companies, with high production volumes. “I doubt that sufficient attention can ever be paid to cybersecurity at this rate,” Molsen points out in view of this development. He continues: “Dräger has been committed to cybersecurity since medical devices have been connected to each other in a network.“ In the meantime, clinical cybersecurity is one of the key quality attributes of the Dräger portfolio.

MORE AND MORE ATTACKS ON THE DIGITAL STRUCTURE OF HOSPITALS ARE RECORDED WORLDWIDE. HERE ARE TWO EXAMPLES FROM FEBRUARY 2016:

– Hollywood Presbyterian Medical Center in Los Angeles, a hospital affected by ransomware, had to pay a ransom for its IT systems. According to a statement made by the hospital director, 40 bitcoins were paid, worth around 15,000 euros[3] at that time. The affected systems were operational again after a week of shutdown.

– When hospitals in Germany were attacked, they were forced to use methods from the last century. Patient data was recorded using paper and pen, documents were sent by fax and patients had to collect their examination results in person, instead of receiving them by email.

Security systems: standard requirements for our devices

Until a few years ago, securing medical devices against cyberattacks was done more in the context of individual projects. Today, system security is included in our comprehensive list of requirements and is deeply embedded into our development processes. Patient safety is the top item on the Dräger agenda, and should be a top priority at all times. It does not matter whether the appropriate device is linked up directly via the WLAN or a poor network in the daily running of the hospital: “We changed our mindset. We acknowledge that our devices will be attacked at some point, and it doesn‘t matter whether the attack is targeted or accidental, patient safety must be preserved.” says Molsen. Any point where data can enter a device is a possible point of attack. These include for example, interfaces through which an attacker can manipulate the device, such as the user interface, the network integration or the USB ports.

The environment in which it is operated is also one of the safety issues for a device. However, attacks on actively used medical devices are as yet unknown and these are likely to be the exception even in the future. There is a much higher risk as a result of collateral damage through viruses and malware, such as the above mentioned ransomware. To provide protection from this, operating systems in medical devices are usually “hardened”: they consist only of reduced, specific components and in this way offer less of a target for viruses.

Successfully fend off hacker attacks

If a clinical network acts as an intranet and therefore does not access the public internet, how are hacker attacks even possible? Molsen answers this question, giving evidence of potential “leaks”:

- “A lot of hospitals use a wireless internal network. Here, the level of security can vary extremely. In the worst case scenario, an attacker can record, manipulate or illegally pass on internal hospital data from outside the building with the appropriate equipment.
- However, IT configuration errors or simple negligence can also lead to security being put at risk and systems that are actually insular can be infiltrated from outside.
- Within the hospital, there is also a way of accessing the intranet undetected via a network socket.”

Dräger offers a wide range of safeguards against network damage as a result of these kinds of attacks. The aim is to find the best possible compromise between security and user-friendliness (usability). “However, it is of course these compromises that offer opportunities to hackers,” explains Product Security Manager Hannes Molsen. The fact that IT departments and medical technology are still acting relatively independently from each other is also problematic. Because requirements are increasingly merging against the background of increasing digitisation, such cooperation should be significantly expanded and optimised.

ON A STANDARD WLAN BASIS

How patient safety, device security and networking can be brought together becomes clear when we take Sunderby Hospital in Luleå, Sweden as an example, where Dräger has implemented a hospital-wide patient monitoring system. Careful planning and modern technology ensured that the quality of patient care was improved and an optimised clinical workflow for the staff achieved. In the video https://youtu.be/yLQ-BZ6dnHc the staff from the IT department of Sunderby Hospital explain the advantages – but also the challenges – of implementing a new patient monitoring and telemetry system into the existing in-house LAN and WLAN network.

Dräger secure development lifecycle: multi-layered protection

We design our devices in such a way that the system offers only a very limited attack surface. Consistent omission of unnecessary software components means that many of the vulnerabilities that have and/or will become known cannot be exploited. This also reduces the number of patches necessary and therefore the devices' maintenance costs.

Here is a ventilation example: while a patient is being ventilated, various service functions are automatically deactivated and thus inaccessible, even over the network. Inbound access via the interface is only possible if the ventilation is switched off. In this way, the risk of possible harm to patients through external manipulation can be reduced to an absolute minimum.

In our discussions concerning cybersecurity, we undertake the following measures:

- Evaluation of data protection and data security of our solutions
- Penetration tests performed by independent experts (white hats)*
- Security training courses for staff involved in the development lifecycle
- In-house cybersecurity team that coordinates our commitment on a global scale.

Another important component of our security strategy is the "Coordinated Vulnerability Disclosure Policy", a kind of direct line to our security experts through which anyone can communicate any potential weak points they've discovered.

Note: on our website https://www.draeger.com/cybersecurity we provide you with further information about cybersecurity in hospitals. We also provide you with security information on current threats on our Coordinated Disclosure Statement page (https://static.draeger.com/security).

The importance of ongoing training

All professionals working in hospitals need to be aware of potential vulnerabilities and how these weaknesses allow cyber criminals to easily commit malicious actions. They should regularly refresh their knowledge, for example, about the following:

- How to deal with e-mail attachments
- How to deal with passwords
- Behaviour in public internet forum
- Dealing with USB sticks

Because healthcare cybersecurity is an ongoing concern, even IT specialists and medical device technicians should receive regular training. After all, the best way to stay safe is to stay educated.

Rethinking cybersecurity

The cooperation concerning security between medical technology and IT should continue to intensify in the next few years. One indication is the international standard IEC 80001-1 "risk management for medical IT networks" which particularly applies to operators and users, focused on cooperation with manufacturers based on partnership. A further indication that security requirements will increase is provided by the US Food and Drug Administration (FDA). They refer to the guidelines of the NIST (National Institute of Standards and Technology) on securing critical infrastructures against cyber-attacks[(4)]. The FDA first published a "Premarket Guidance" in October 2014 with IT security requirements for the development and marketing of medical devices. At the end of 2016, a 30-page "Postmarket Guidance", a guideline for the management of IT security risks for networked medical devices after they have been brought onto the market, was published. In Germany, the German Federal Office for Information Security (BSI) published the guideline "Protection of critical infrastructures: risk analysis of hospital IT" in 2013[(5)].

Conclusion: effective protection against cyber criminals can only be achieved if all those involved work together: system administrators, software manufacturers, medical device manufacturers, users and data protection officers. It is time to rethink cybersecurity.

*Penetration tests performed for selected products since 2015, mandatory for all new product developments since 2019

PUBLISHING DETAILS

GERMANY
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23542 Lübeck

www.draeger.com

PDF-8938

SOURCES:

(1) *NHS cyber-attack: GPs and hospitals hit by ransomware at http://www.bbc.com/news/health-39899646 (downloaded on 26/07/2017).*

(2) *Expertengespräch Hannes Molsen, Product Security Manager, Drägerwerk AG & Co. KGaA, 19/05/2017*

(3) *http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf (downloaded on 26/07/2017).*

(4) *FDA outlines cybersecurity recommendations for medical device manufacturers, www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm (downloaded on 26/07/2017)*

(5) *www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?_blob=publicationFile ((downloaded on 26/07/2017)*