The chilling ransomware threat facing hospitals

Earlier this year, multiple hospitals in Germany fell victim to ransomware attacks, which disabled their IT infrastructure. While these attacks are far from being limited to hospitals, these cases gained media attention due to the relevance of healthcare for the general population. In addition, as hospitals are required to thoroughly protect health data, these attacks have raised additional concerns. Jana Grieb and Claus Färber of McDermott Will & Emery explain the legal implications of such attacks and how hospitals should respond.

Over the last few years, there has been a steep increase in ransomware attacks across all industries, and the healthcare sector has not been spared. Ransomware is malicious software (malware) that encrypts files stored on a computer, rendering them unreadable by the user. The software then goes on to demand payment of a ransom for the decryption of these files. Thereby, it essentially takes the data of the user hostage. Like other malware, ransomware usually infests computer systems through unpatched security vulnerabilities of the software installed on the computer, or by tricking the user into opening an email attachment that contains malicious software.

Response to ransomware attacks

Healthcare providers confronted with a ransomware attack face a much harder decision than other businesses and institutions.

Even outside of the healthcare sector, opinions are divided on whether victims should pay the ransom to regain their data. While the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) clearly advises against making any payment, some German police offices have made the recommendation to pay if there is no other way to decrypt the data. From an economic perspective, paying the ransom is usually more cost-effective. Even though there is no guarantee that the individuals responsible for the attack will honour their promise to decrypt the files, experience shows that they usually do.

For hospital operators, there are two additional major aspects to take into account besides cost-effectiveness. Firstly, hospitals have to ensure proper patient treatment - i.e. they are to ensure that treatment of already admitted patients is not endangered by software failure or unavailability of relevant data, and they have to provide alternatives if patients cannot be admitted to the hospital in the first place due to a ransomware attack that renders hospital facilities unserviceable. The referral of patients to alternative locations for treatment will be facilitated if hospitals maintain partnerships with other healthcare providers. If such schemes are not yet in place at the time the ransomware strikes, the hospital may have no other choice than to pay.

Secondly, although the malware attacks discussed here mostly consist of data encryption where the hospital is blackmailed to pay for the decryption of the data, such attacks are generally accompanied by concerns that it might be possible to abuse the data. Even if the ransomware in question does not upload the data, the sheer fact that it was possible to infect the computers indicates that the security measures are deficient and that it is possible for an outsider to infiltrate the systems. Data used and stored in hospitals are health and social insurance data, hence, if they are personalised, data of specific sensibility that trigger stricter provisions under data protection laws. At the same time, they are subject to the physicians' professional secrecy, violation of which is a criminal offence. Additionally, such data may be within the scope of social insurance law, where German courts set high standards for protection. Consequently, a hospital that has suffered a ransomware attack will not only have to restore service but also remedy the security deficits that made the attack possible in the first place.

Regulatory aspects

Besides data protection laws and laws regarding professional secrecy, some healthcare providers may be subject to additional requirements for so-called critical infrastructures ('KRITIS').

Just last year, the German Parliament established a scheme to protect critical infrastructure with the IT Security Act (IT-Sicherheitsgesetz) 2015 (BGBl. I 1325). The new provisions introduced to the German Act on the Federal Agency for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, 'BSIG') will, in certain cases, also cover entities in the healthcare sector. Whether an entity is subject to the provisions under the BSIG, however, depends on the importance of such entity in the general healthcare system. Only where a hospital is considered as important to the general public, which is the case if it might cause a supply shortfall or pose a risk to public security if the entity is not able to fulfil its tasks, may it qualify as a KRITIS entity. In the healthcare sector, this means that outpatient physician practices will hardly be concerned, whereas larger hospitals, particularly in rural areas with a greater distance to other healthcare facilities, are not unlikely to qualify as KRITIS entities. However, it will be up to the courts to determine the borderline in future case law. At the moment, there are a broad variety of opinions being expressed and it is uncertain whether many or even most hospitals will be covered, or whether hospitals will only be considered critical infrastructure in exceptional cases, where no other healthcare facilities can be reached in due time.

Precautions and preparation

Hospitals that are KRITIS entities are required to ensure, within a period of two years from the Act's effective date, compliance with the IT Security Act by creating organisational measures to prevent disruptions of availability, integrity, authenticity and confidentiality of their IT systems, components and processes, to the extent they are required for the functionality of their critical infrastructures. This means that such hospitals have to update their policies and systems to - at least - state-of-the-art standard by July 2017. In order to maintain an up-to-date IT infrastructure, certification has to be obtained and be presented to the Federal Agency on a biannual basis.

In order to ensure its capacity for action in case of a cyber attack, a hospital should know where to refer patients in case they cannot be treated due to software failure

Furthermore, affected hospitals are obligated to establish a contact point that is notified to the Federal Agency for IT Security. Severe disturbances have to be brought to the attention of the Federal Agency via the contact point. At the contact point, an IT expert has to be permanently available. However, an attack does not trigger regulatory penalties for the hospital if reported correctly, as the IT Security Act does not provide for fines or other sanctions.

For the majority of hospitals, which are not KRITIS, the requirements are less strict. The data protection laws only mandate appropriate technical and organisational measures, without going far into the details. As there is no public certification system, compliance is the sole responsibility of the respective entity and its data protection officer. The German Federal Office for Information Security has published a guide regarding IT security, the IT-Grundschutz Catalogue, but this is only a recommendation and not mandatory. However, following this guide or alternative codes of conduct such as ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) - and documenting any deviations will make it easier to show that appropriate technical and organisational measures have been taken. This may be advisable to reduce liability risks.

However, while these measures decrease the likelihood of an attack, a hospital should also employ a strategy to mitigate the effects of an attack or system failure. This strategy will include regular backups that are kept in a secure (off-site) place to ensure that the computer systems can be quickly restored. In order to ensure its capacity for action in case of a cyber attack, a hospital should know where to refer patients in case they cannot be treated due to software failure. Where no hospitals are located close enough, this may require partnerships with physician practices. In addition, it may also be worthwhile to retain non-computerised solutions as a last resort to keep the hospital running in the meantime. Such fallback solutions may play an important role in the risk management regarding cyber attacks, and the old-school paper patient file we used to see in the doctor's hand during ward round may not be so obsolete after all.

Jana Grieb Counsel
Claus Färber Associate
McDermott Will & Emery Rechtsanwälte Steuerberater LLP, Munich
jgrieb@mwe.com
cfaerber@mwe.com