Blog review – Hospial Center Sud Francilien ransomware attack – Michael Geiger

In his blog post, Cluley (2022) drew attention to the ransomeware attack on the French Hospial Center Sud Francilien, which took place on August 20, 2022. A ransomeware attack aims to encrypt or steal important information or systems in order to demand a ransom for the key or non-disclosure of the data (Collier, 2017).

As a result of the attack, the hospital was no longer able to access important digital patient treatment infrastructure. In addition to the patient admissions information system, business software for diagnosing and treating patients and their storage systems were affected. Due to the failed digital infrastructure, the hospital employees had to resort to pen and paper.

As a result, patient care was massively affected, patients were asked to consult other hospitals, were referred to other hospitals and surgical procedures were postponed.

The hackers demand a $10 million ransom from the hospital. It is not known whether, in addition to the encryption of the hospital's digital systems, sensitive patient information was stolen as a result of the ransomware attack. The National Cybersecurity Agency of France (ANSSI) was involved for clarification and technical support in this case.

While the culprit is currently unknown, it is suspected that the Ragnar Locker ransomware group was behind the attack. In addition to encrypting the systems, this group is also known for stealing data and threatening to publish or sell it, which could lead to further damage in the event of a data leak of sensitive patient data.

According to the French Criminal Code, there is reason to assume that the perpetrators of the predatory extortion made themselves punishable under Art. 312-1

or Art. 312-2. “Extortion is committed by anyone who obtains, by force, the threat of force, or coercion, a signature, an obligation, a waiver, the disclosure of a secret, or the delivery of money, valuables, or any property. The rapacious extortion is punishable by seven years in prison and a fine of EUR 700,000.” (Bijus, 2016).

In addition, the hackers could be guilty of sabotage according to Art. 411-9: "Anyone who destroys, damages, misappropriates documents, devices, buildings, pieces of equipment, facilities, machines, technical systems or systems for automated data processing or causes defects in them will be punished with 15 years imprisonment and a fine of EUR 1,500,000 if these actions are capable of harming basic national interests. If the same act is committed to serve the interests of a foreign power, a foreign or foreign-controlled enterprise, or a foreign or foreign-controlled organization, it is punishable by 20 years imprisonment and a fine of EUR 2,000,000.” (Bijus, 2016).

If the ransomeware attack puts patients in serious danger, which is possible if the medical systems fail, the criminal offense of negligent attack on life under Art. 221-6 could also have been committed under French criminal law: ”carelessness, inattention, negligence, or by breach of a duty of safety or care imposed by law or other regulation, causes the death of another, commits negligent homicide and is punishable by three years in prison and a fine of EUR 300,000. In the event of a deliberate violation of a security or duty of care imposed by law or other regulations, the penalties increase to five years in prison and a fine of EUR 500,000.” (Bijus, 2016).

Renferences:

Bijus (2016) Französisches Strafgesetzbuch / Code penal. Available from: https://www.bijus.eu/?p=10720 [Accessed 01 September 2022].

Cluley, G. (2022) Hackers demand $10 million from Paris hopital after ransomare attack. Bitdefender. Available from: https://www.bitdefender.com/blog/hotforsecurity/hackers-demand-10-million-from-paris-hospital-after-ransomware-attack/ [Accessed 01 September 2022].

Malecki, F. (2019) Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security*. *2019*(3): 8-10. Available from: https://www.magonlinelibrary.com/doi/abs/10.1016/S1361-3723%2819%2930028-4 [Accessed 01 September 2022].