Ruijun Lei
2/5/2024

Cyber Attack on German Hospital: A Case Study

a. Introduction

In September 2020, a cyberattack occurred at University Hospital Düsseldorf in Germany, resulting in system failures. Tragically, one patient lost their life due to delayed treatment, serving as a stark reminder of the importance of cybersecurity in public health.[1]

b. Facts of the Case

On September 10, 2020, University Hospital Düsseldorf (UHD) suffered a cyberattack that resulted in the encryption of 30 hospital servers, which caused a gradual system failure and the loss of data access. This incident caused the hospital to disrupt emergency care services and divert incoming patients to other facilities.[1] One patient who required urgent admission had to be transferred to a hospital from approximately 30 kilometers away, which led to a delay of about an hour in her treatment and ultimately contributed to her death. The cyberattack resulted in significant costs, which include damage to infrastructure and response efforts. Those total costs are currently under investigation.[2] It took nearly two weeks for the hospital to restore essential services and reopen emergency care, and an even longer time to fully recover and become operational again.

c. Epidemiological Aspects of the Event

Unfortunately, there is limited information available regarding the specific epidemiological study methods, measures of association, or analytic approaches used to investigate the cyber attack.[2] As of now, there does not appear to be a comprehensive epidemiological study conducted on this event. Consequently, details regarding potential sources of biases are not available. However, the significance of such an epidemiological investigation in understanding the impact of cyberattacks on healthcare systems and patient outcomes remains paramount.[2] Future research in this area could concentrate on designing observational studies. It may involve the utilization of appropriate measures of association to quantify relationships. Additionally, researchers should be diligent in addressing potential biases that might affect the validity of their findings.[2] Finally, the establishment of effective analytical approaches will be crucial in providing a comprehensive assessment of the implications of cyber threats on both patient care and hospital operations.

d. Management of the Event

The hospital's prompt cooperation with law enforcement and subsequent acquisition of decryption keys were critical in mitigating the attack, which also served as an example for the preparedness cases. However, there were large gaps in emergency response for cyberattacks that need to be addressed.[3]

e. Communications of the Event

In terms of communication, the hospital's approach was transparent and prompt in their public notifications. Furthermore, their willingness to communicate with the attackers in order to have the ransom demand withdrawn showed a responsible and well-prepared approach in handling the crisis. This open and effective communication played a vital role in keeping patients safe and preventing additional harm[3].

f. Summary

The Düsseldorf Cyber Incident underscores the need to enhance defenses against cyberattacks, especially in vital sectors like healthcare. It underlines the crucial significance of planning for the changing technology and cybersecurity landscape in order to assure a secure

future. It is critical that we strengthen our preparation and resilience in the face of increasing threats.

Ruijun Lei
2/5/2024

References

1. Ralston W. The untold story of a cyberattack, a hospital and a dying woman. WIRED UK. Published November 11, 2020. https://www.wired.co.uk/article/ransomware-hospital-death-germany
2. The Düsseldorf Cyber Incident. Accessed February 5, 2024. https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident
3. Eddy M, Perlroth N. Cyber Attack Suspected in German Woman's Death. The New York Times. Published September 19, 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html