HIN ANAPAYA

Cyber Attacks on Healthcare

May 2023

Johnson Memorial Health, USA

Johnson Memorial Health, located in Franklin, Indiana, experienced a devastating cyberattack in October 2021. The attackers, which left the hospital grappling with the aftermath for months, demanded a ransom of $3 (€2.74) million in Bitcoin.

This incident sheds light on the growing trend of cyberattacks targeting hospitals across the United States, with instances more than doubling between 2016 and 2022.

Aside from the potential exposure of confidential patient information, the attack also inflicted significant financial loss and disrupted patient care, putting lives at risk.

- **Forced hospital to resort to low-tech methods of patient care,** such as using pen and paper for medical records.
- Hospital **forced to disconnect their systems** and rebuild.
- **Led to disruptions in various hospital departments** and even diversion of ambulances to other hospitals.
- Estimated costs approximately **€9.6 million**
- Cyber security **recovery process took nearly six months,** and ongoing costs persist.

February 2023

DDoS Attacks on Healthcare Applications in Azure by KillNet, USA

Amid geopolitical tension, pro-Russia hacktivist group KillNet launched DDoS attacks on various healthcare applications hosted on Azure. Within a span of three months, daily attacks increased from 10-20 in November 2022 to 40-60 by February 2023.

The attacks targeted pharmaceutical and life sciences organizations, hospitals, healthcare insurance providers, and health services. The majority of attacks utilized UDP flood (53%), with 38% being UDP spoof flood attacks and 29% DNS amplification attacks, greatly hindering healthcare services across the USA.

- Increase in daily attacks **from 10-20 to 40-60 within three months.**
- Attack severity ranged **from 1.3 million packets per second to 22,000** sources of attack per target.
- **Attacks used multiple angles of attack,** including multi-vector layer 3, layer 4, and layer 7 DDoS attacks, with TCP and UDP attack vectors targeting web applications.
- DDoS strikes attempted to deplete memory state resources, **slowing down operations** and locking up online healthcare services.

August 2022

Center Hospitalier Sud Francilien (CHSF) Attack, France

A criminal group demanded €9.6 million in ransom following a DDoS strike on CHSF that led to thousands of patient data being stolen.

The government spent nearly €20 million to increase security in French hospitals, and the CHSF faced penalties of over €20 million in GDPR fines.

- Criminal group demanding **$10 million (€9.6 million) in ransom**
- **DDoS used to disrupt IT teams** while data was harvested
- Thousands of **patient data leaked online**
- **€20 million to increase** security in French hospitals
- **Over €20 million** (or 4% of annual global turnover – whichever is greater) **in GDPR fines**

October 2020

DDoS Attack on Universal Health Services, USA

A major healthcare provider, Universal Health Services (UHS), faced a DDoS attack that led to disruptions in their online services and impacted patient care. Although the attack was later revealed to be primarily a ransomware attack, the DDoS component disabled systems and services to pave the way for the strike.

The financial damages and extent of the disruptions were not disclosed, but are anticipated to be in the millions.

- **DDoS attack on** Universal Health Services
- Disrupted online services and **impacted patient care**
- Primarily a ransomware attack **with DDoS component**
- **Temporary unavailability** of some systems
- **Financial damages and extent** of disruptions not disclosed

April 2020

DDoS Attack on Fresenius, Germany

Fresenius, Europe's largest private hospital operator, experienced a DDoS attack that disrupted the company's IT systems, affecting their hospitals and medical services.

The attack came amid the COVID-19 pandemic, making it even more challenging for healthcare providers to respond to the crisis. It provided cover for ransomware to infect and lock up Fresenius' systems.

The attackers demanded over €1.35 million to cease the attack.

- **Disruptions to IT systems** of Europe's largest private hospital operator
- **Affected hospitals and medical services** during the COVID-19 pandemic
- Targeted Fresenius, Germany **the largest private hospital operator** in EU
- **Over €1.35 million** demanded in ransom to stop

May 2017

WannaCry National Health Services Attack, UK

North Korea launched a massive DDoS instigated malware strike against the UK NHS.

The DDoS served as a cover to cause even greater damage and theft. 19,500 medical appointments, 139 potential cancer referrals, and 5 hospitals closed, totalling 81 Healthcare providers and 600 GP offices affected. The damages were over €105 million.

- North Korean **state-orchestrated cyber attack**
- DDoS instigated-malware attack **DDoS used as distraction**
- **£92 million** (€105 million) in damage
- **19,500 medical appointments, 139 potential cancer referrals, 5 hospitals** shut down
- **81 Healthcare** providers and **600 GP** offices affected

Learn more **[insert landing page URL here]**
Contact HIN Representative **[insert HIN representative contact details here]**