HealthManagement
Promoting Management and Leadership

Addressing Cyberthreats in Healthcare Through Collective Action

A new report from The CyberPeace Institute analyses a variety of recent cyberattacks against the healthcare sector around the world, identifies the predominant threats and provides recommendations for improvement.

You might also like: ENISA has released cybersecurity guidelines for hospitals when procuring services, products and infrastructure. Learn more

The CyberPeace Institute is a non-profit, international organisation headquartered in Geneva, Switzerland, whose work focusses on matters of cyberattacks and cybersecurity and aims to ensure responsible behaviour and the advancement of international law at corporate and state level.

The document titled *Playing with Lives: Cyberattacks on Healthcare are Attacks on People,* focusses on three key categories of cyberattacks: disruptive attacks (e.g. ransomware), data breaches and disinformation operations. It explores real-life cases mainly from 2020 and various cybersecurity issues in the context of the COVID-19 pandemic. The analysis of each case comprises information on victims, targets, actors, methods used, etc. Among the examples covered are the ransomware attack on Universal Health Services, USA, in September 2020; WannaCry ransomware attack on the U.K. National Health Service in 2017; or the data breach at the Vastaamo Psychotherapy Center in Finland in September 2020.

The report argues in favour of collective action to contain the damages caused by cyberattacks and hold threat actors to account, and assigns a leading role in this to the states as well as the corporate sector. “Preventing attacks, building resilience and prosecuting offenders requires policy steps from governments and companies alike,” the study notes.

The key findings include the following:

- Attacks on healthcare are causing direct harm to people and are a threat to public health, globally.
- Attacks are increasing and evolving as they continue to exploit vulnerabilities in the healthcare sector’s fragile digital infrastructure and weaknesses in its cybersecurity regime.
- Attacks on healthcare are low-risk, high-reward crimes. Acting with near impunity, criminals and state actors are joining forces against healthcare with varying motives and agendas.
- Healthcare professionals and patients do not benefit fully from legal instruments and existing assistance initiatives designed to protect them.

The document recommends documenting attacks and analysing their impact on populations and societies; investing in healthcare preparedness and resilience improvement; activating technical and legal protection instruments; and holding threat actors accountable.

The report is freely available here.

Source and image credit: The CyberPeace Institute

Published on : Fri, 12 Mar 2021