ACADÉMIE NATIONALE DE MÉDECINE

Attacks on hospital computer systems endanger patients' lives[1]

Press release from the French Academy of Medicine

October 10, 2024

Cyber-attacks are a new form of criminality that affect many people and an increasing number of public or private organizations. Since the mid-2010s, cybercriminals have been attacking hospitals (1), for vandalism or denial of service, or to demand a ransom, the insertion of a ransomware altering the smooth running of essential services or equipment (2) by making system data unusable.

In France, 1582 health facilities were attacked in 2021 i.e. one in six establishments, twice as many as in 2020. In 2023, the largest public hospitals were targeted (Hôpital de la Pitié-Salpêtrière and Hôpital Saint-Antoine in Paris, Assistance Publique-Hôpitaux de Marseille and Hospices Civils de Lyon). Private establishments were not spared. In February 2024, the Armentières hospital was the target of a cyber-attack with a ransom demand that resulted in the closure of its emergency department for 24 hours (3).

Beyond the extortion of funds or the cost of strengthening the security of hospital information systems, these cyber-attacks endanger patients' lives in several ways: delaying emergency care; impairing the proper functioning of life-support devices, for example in the operating room or intensive care unit; lengthening the time for implementing some diagnostic or therapeutic procedures.

Recent studies have documented the impact of such attacks on delays in patient care, for example in the management of strokes (4) or cancer (5). A recent attack on Guy's and St Thomas' Hospital in London (6) has illustrated these serious consequences: surgical operations were cancelled; blood transfusions could not be carried out, as the required data had been deleted; patients had to be transferred to other hospitals.

Faced with the increasing number of computer attacks against healthcare facilities, actions are being taken in many countries. At national level, this involves the authorities in charge of homeland security, cybersecurity and justice, and at the level of each healthcare establishment, strengthening the security of information systems and raising staff awareness about this risk.

[1] Press release from the Academy's Rapid Communication Platform.

CONTACT PRESSE : Virginie Gustin +33 (0)6 62 52 43 42 virginie.gustin@academie-medecine.fr
ACADÉMIE NATIONALE DE MÉDECINE, 16 rue Bonaparte - 75272 Paris cedex 06
Site : *www.academie-medecine.fr* / **Twitter** : *@Acadmed*

Given the potential seriousness of these attacks on patients' health, the French academy of medicine highlights:

The need to document the health impacts of these attacks on patients in care or awaiting care;

The need for all healthcare professionals using digital technology in healthcare establishments to be aware of and trained in the risks of cyber-attacks;

In addition to the cybersecurity reinforcement measures set out in the CaRE incentive plan (7, 8), the extreme vigilance required with regard to the specific cybersecurity skills of staff in charge of IT services;

The necessary preparation of all healthcare establishments, through anticipatory and organizational measures, to ensure activities continuity in the event of an attack, either in degraded mode, or via a cooperative system between healthcare establishments, prepared and tested in advance;

The criminal nature of cyber-attacks on hospitals, which, in addition to extortion or vandalism, constitute a threat to the life of others, and possibly homicide.

References

1. Argaw, S.T., Bempong, N.E., Eshaya-Chauvin, B. *et al.,* The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Med Inform Decis Mak,* 2019*,* 19, 10.
2. Williams P.A., Woodward A.J., Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, *Med Devices Evid Res*, 2015, Jul 20.8: 305-16
3. Lemaignen J., Romain M. : Cyberattaques dans les hôpitaux, Le Monde, 7 décembre 2022
4. Dameff C., Tully J., Chan T.C. *et al.*, Ransomware attack associated with disruptions at adjacent emergency departments in the US, *JAMA*, 2023: 6(5) e 2312270
5. Keogh R., Harvey H., Brady C. *et al*., Dealing with digital paralysis: surviving a cyberattack in a national cancer center, *Journal of Cancer Policy,* 2024, 39, 100466
6. https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve?CMP=Share;
7. Agence du numérique en Santé, Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2023, 2024, https://esante.gouv.fr/sites/default/files/media_entity/documents/observatoire-incidents-cybersecurite-sante-2023.pdf
8. Agence du numérique en Santé, Cybersécurité accélération et Résilience des Etablissements (CaRE), https://esante.gouv.fr/strategie-nationale/cybersecurite, consulté le 18 juillet 2024

CONTACT PRESSE : Virginie Gustin +33 (0)6 62 52 43 42 virginie.gustin@academie-medecine.fr
ACADÉMIE NATIONALE DE MÉDECINE, 16 rue Bonaparte - 75272 Paris cedex 06
Site : *www.academie-medecine.fr* / **Twitter** : *@Acadmed*