HealthManagement
Promoting Management and Leadership

2021: Even More Cyber Attacks on Healthcare

2020 saw an unprecedented rise in cyber attacks on healthcare systems and institutions. However, in 2021 the situation might get even worse, and here is why.

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

According to Saryu Nayyar (Gurucul) writing for Forbes, there are several reasons for the healthcare sector being under even more pressure from cyber criminals than usual.

Health data are a known target for cyber attacks, on both individual and institutional levels. For patients, having their data stolen might lead to criminals either getting access to patients' (and their connections') finances, or using those data to directly blackmail them and get a ransom.

For institutions, a cyber attack may literally be a matter of life-or-death, Nayyar notes. In a situation where essential systems in a facility are compromised and every minute counts, paying out ransom might seem like the best option. Therefore, according to Nayyar: "Ransomware is expected to remain a big part of the cybercriminal's portfolio in 2021," and it will spread beyond encrypting endpoint devices, with backup applications and databases being increasingly targeted as well.

On the bright side, Nayyar sees this spike in cyber threats leading to better cyber defence in healthcare and more robust implementation of legal frameworks.

For healthcare, she suggests focussing on the following areas.

Password management. Trying not to complicate user experience too much, healthcare organisations will still be looking to strengthen their password management. Nayyar sees increased deployment of such tools in the future.

Multifactor authentication (MFA). Following the banking sector's example, healthcare is also expected to adopt novel MFA instruments, such as token-based authentication, while relying less on not-so-effective methods like phone-based authentication.

Risk-based access controls. With remote work and care now being on the rise, accessing systems from different locations might burden users with additional authentication requirements. This issue may be addressed by enforcing access policies based on risk.

In conclusion, Nayyar notes that increased cyber threats can potentially be offset by the stronger security measures and policies which should be the focus for healthcare organisations now. "Own your cybersecurity readiness," she urges.

Source: Forbes

Image credit: JuSun via iStock

Published on : Mon, 22 Mar 2021