HealthManagement.org
Promoting Management and Leadership

Ten Ways to Keep Your Networks Hacker Proof

As healthcare continues to be a target for cyber attacks, the European Union cybersecurity agency the European Union Agency for Cybersecurity (ENISA) has issued a guide of recommendations for protecting hospital computer networks.

You might also like: **Staff Training Urgently Needed for HealthcareCybersecurity**

Called 'Procurement Guidelines For Cybersecurity In Hospitals- Good Practices for the Security Of Healthcare Services', the 51-page report addresses issues that include types of procurement, identification of possible threats, risks and challenges related to procurement in hospital organisations and good practices related to healthcare procurement in order to meet cybersecurity objectives.

The guide is suitable for CIOs and CISOs of healthcare providers, medical device manufacturers, insurers and other healthcare related organisations.

ENISA say that two-thirds of healthcare organisations suffered cyber security incidents in 2019.

Medical data is highly sensitive and, with lives at risk, healthcare is one of the most vulnerable sectors and prime targets for cyber hackers. Bur monitoring hospital cyber security is a difficult task because of the vast ecosystem of devices, equipment and systems that often connect to external parties.

"Protecting patients and ensuring the resilience of our hospitals are a key part of the Agency's work to make Europe's health sector cyber secure," said ENISA Executive Director, Juhan Lepassaar.

ENISA outlines ten good practices in the guide as follows:

1. Involve the IT department in procurement

Involve the IT department in the different stages of procurement to ensure that expertise in cybersecurity aspects is considered.

2. Implement a vulnerability identification and management process

Ensure that vulnerabilities are considered before procuring new products or services and that vulnerabilities of existing products/services are monitored throughout their lifecycle.

3. Develop a policy for hardware and software updates

Develop an update policy to ensure that the latest patches to OS and Software are applied and that the antivirus Software is updated.

4. Enhance security controls for wireless communication

Access to the hospital's Wi-Fi networks should be limited and strictly controlled. Number of devices connected should be monitored and in the case of medical devices should be verified and restricted. Non-authorised personnel should not have access to the Wi-Fi.

You might also like: Fighting Cyber Threats With A Global Community

5. Establish testing policies

The healthcare organisation should establish a minimum set of security tests to be performed on acquired products or system, depending on the product/system type. It is also important to note that a newly acquired or newly configured product must undergo a penetration test in its actual installed environment. In the same way, remediating action taken must be inline with the operational parameters of the actual environment.

6. Establish business continuity plans

Business continuity plans should be established whenever the failure of a system may disrupt the hospital's core services and the role of the supplier is such cases must be well-defined.

7. Take into account interoperability issues

Interoperability is one of the greatest cybersecurity risks for healthcare organisations. The hospital's IT ecosystem is comprised by different components medical devices, networking equipment, remote care systems etc. Some of these components exist already (legacy IT) and connection with new components might result into security gaps.

8. Enable testing of all components

Information systems should be thoroughly tested to guarantee they deliver what is promised: verify easiness of use, check the correctness of results under load, and check for security flaws (weak password policy, SQL injection). Testing should be a requirement in procurement as well as monitoring

during testing. Testing should be aligned with testing policies.

9. Allow auditing and logging

Logs are a crucial part of the secure-test-analyse-improve strategy of security. If you assume that sooner or later your system will be compromised, logs are one of the most useful tools that you can use to trace back how attackers gained access to your system.

10. Encrypt sensitive personal data at rest and in transit

To ensure compliance with the General Data Protection Regulation, and to ensure the safety of both patients and staff, sensitive information should be encrypted, so that if outsiders do get access to the systems, it's likely to be useless to them.

Source: ENISA

Image credit: iStock

Published on : Wed, 26 Feb 2020