MAIN WEAKNESSES AND PROBLEMATICS OF CYBER-SECURITY IN MEDICAL DEVICES

Ihor Blavatskyi[1], Oksana Blavatska[2]
[1] IT specialist; Lviv, Ukraine
[2] Danylo Galytskyi Lviv national medical university;

PMU 11
Lviv, Ukraine

Advancements in healthcare technologies devices such as infusion pumps and pacemakers are helping patients lead healthier and happier lives. Just as these patients rely on their device to provide safe reliable care. The devices themselves often rely on computer software to function properly and these devices more of which are wireless in nature are increasingly connected to one or other way to hospitals network, internet or to other medical devices. But this connectivity will cost vulnerabilities for hackers, malwares, viruses and other threats. Cybersecurity which is found in medical devices and IT is not very advanced at this point. Cybersecurity specialist should take preventative steps, to this problem. There are several weaknesses in cybersecurity practices of many hospitals, here is 4 most common:

1) An incomplete cyber inventory. Many of the problems with cyber security aren't technical, if you don't know what you have, you aren't going to know how to protect it. This is hard to mitigate risk until you have an inventory of your systems. You should be able to enumerate everything that is on your network and identify your cyber security risk by device in your computerized maintenance management system.

2) Vendors can make security hard, some vendors can take a lackadaisical approach to cyber security. If a vendors answer to cybersecurity is just to tell you: "*to put your device on a secure network or behind the firewall*" this is not fully effective. Awareness and general knowledge of cyber security can be vary by vendor is the vendor doesn't know about medical device security formulas, you should consider whether that vendor has other deficiencies and would leave open backdoors to potential cyber threats.

3) Number of the overwhelming security testing tools. Providers struggle to cope with the volume of security testing tools and can become overwhelmed with vulnerability info they may not know issue to address, how to identify the most important one or even where to start.

4) List of overreliance on segmentation as an answer, while it can be necessary segmentation is not enough. Network segmentation also makes network is harder to manage which again adds to the workload and makes taking inventory more difficult despite all these challenges and they should be monitored.

Security should be design at development and not add later, when it's already on market. This should be handled by medical device developer which applied to risk management.

oksablav@gmail.com blavic2229034@gmail.com