HealthManagement
Promoting Management and Leadership

Deception technology in battle against cyber-threats

According to an annual study on privacy and security of healthcare data, Ponemon Institute reports that nearly 90 percent of healthcare organisations have been breached. More importantly, the approximate average cost of each data breach for these organisations is nearly $2.2 million.

It is expected that in 2018, cyberattacks will become even more sophisticated and will probably cost heathcare providers even more than before. A survey by Deloitte reveals that more than a third of 370 medical device professionals had experienced a cybersecurity incident in the last 12 months. The frequency of these incidents is likely to increase.

The problem is that healthcare organisations are lucrative targets for hackers because they have sensitive patient data. In addition, most healthcare providers have IT systems that are relatively easy to infiltrate. The chances of such infiltration can be minimised if healthcare providers would give their cybersecurity practices a thorough review more regularly.

There are several factors that make a healthcare provider more vulnerable to cyberattacks. These include:

- Medical devices with IoT capability make traditional network security monitoring more difficult because of transient connectivity.
- Electronic medical records may increase patient satisfaction but pose a major security risk.
- Healthcare IT teams are limited by budgets and resources and lack the tools they need to combat cyberattackers.

Healthcare providers need to focus on increasing network security. For this, they need new and advanced tools to defend their network perimeter and to proactively detect and respond to in-network threats.

One such technology tool is deception technology. This is an emerging category of security tools that is designed to prevent an attacker who has entered your network from doing any damage. Deception technology also allows IT teams to automate routine security tasks. Overall, deception technology is a comprehensive and authentic technique that can improve attack analysis as well as the ability to improve incident response.

By placing deception at the both the end-point and inside the network, one can detect threats across all vendors including stolen credentials, Man-in-the-Middle ransomware, phishing and insider threats. Deception technology is also effective at misdirecting attackers and creating deceptions to draw in attackers.

It is thus important for healthcare providers to enhance their cybersecurity by implementing deception technology and other multi-faceted cybersecurity initiatives.

Source: HealthDataManagement
Image Credit: Pixabay

Published on : Tue, 27 Mar 2018