HealthManagement
Promoting Management and Leadership

Trapping Hackers

The "art of deception network" provides an added dimension to the protection of sensitive health information. This new method uses little bits of code – placed at strategic points throughout a network – to lure cyberattackers, slow their progress and ultimately trap them.

“A deception network is numerous sets of lures or traps strategically placed throughout real networks and end-points,” says Alton Kizziah, vice president of global managed services at Kudelski Security. “It is designed to attract, delay and detect an attacker’s movement through the targeted organisation as they try to find the way to their objective.”

Hospital IT systems have become more appealing targets of ransomware attacks, especially because the risk vs. reward scenario highly favours the attacker. When setting up a deception network, a hospital should pay special attention to the lures that can detect ransomware activity and configure managed deceptions accordingly, Kizziah says.

Some attacks, known as advanced persistent threats, can be underway for many months prior to being discovered. “If an advanced attacker makes it past the basic perimeter controls, deception technology provides the next level of defence, safeguarding the crown jewels of healthcare organisations as well as their most sensitive data and zones,” says Ofer Israeli, CEO and founder of Illusive Networks, a vendor of deception network technology and services.

Because the deceptive lures are set on a real and operational machine, when the intruder begins to feel their way around the patient end-point and the networks to which it is connected, the deceptive bait is taken and the adversary caught, Kizziah adds.

The good thing is that deception is easy to deploy and in many cases does not require another agent to be installed on an end-user’s system. Further, there's minimal upkeep and deceptive lures lay dormant on end-points not consuming any precious resources, according to Kizziah.

“If we can accept that even with the best of threat prevention and detection, we will be breached, then adding deceptions can flip the paradigm,” he points out. “Once a deception alert has been triggered, an organisation immediately goes into response mode because the false positive rate is so low.”

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Thu, 20 Jul 2017