HealthManagement
Promoting Management and Leadership

New ransomware threats

Hackers and cybercriminals always try to outsmart their targets. The best way to keep your organisation safe is to stay one step ahead of these attackers, according to an IT expert.

"There's a new ransomware variant making the rounds, and it may prove more productive for attackers and more problematic for healthcare security teams. Rather than the “spray and pray” type attacks we saw in the past, the new twist is focusing on select, high-risk targets," said Kevin Conklin, who is a vice president at software company Ipswitch.

He describes “spray and pray” ransomware attacks as a volume game. Attackers target a very large audience with a spear phishing scheme and hope to fool a relatively small percentage of people. Once files are encrypted, the attackers ask for hundreds of bitcoins/dollars to unlock them.

Now attackers focus on high-value targets, Conklin said. A high-value target has access to high-value data or performs a function that is critical to the business. Encrypting their data means a much higher payout for the attackers.

Defray is an example of this new targeted ransomware attack. The ransomware is being spread through a phishing email. It recently emerged in August targeting healthcare organisations.

Protecting your organisation against these targeted ransomware attacks is an imperative, notes Conklin, who shares these security tips:

1. Know the difference between a hacker and a cybercriminal

The big difference between hackers and cybercriminals is the level of effort and persistence they are willing to invest for the reward. Cybercrime is an industry with criminal organisations run very much like businesses. Hackers can be viewed more like hobbyists. "Cybercriminals will invest resources to design around your defences. They'll spend the time to know your organisation and create a campaign with a high probability for success so they can achieve much bigger payoffs," Conklin explains.

2. Backup with regularity

You should back up data daily, and you should have multiple backups in multiple locations. If you have quick access to a backup of data that was just encrypted in a ransomware attack, you significantly cut your losses.

3. Raise awareness throughout an organisation

Instil a culture of suspicion regarding emails with attachments and links throughout your organisation. Often, a 10-second pause to scan the email for funky “from” addresses, weird file types or suspicious URLs will help identify 99 percent of attacks. Make sure your employees are trained in how to identify these telltale signs of a spear-phishing attempt.

4. Keep systems updated

There is a continuous race for cybercriminals to identify and exploit security vulnerabilities in systems and software before they are identified by the vendor and patched. Keeping up to date with patches significantly improves your defences, according to Conklin.

Source: Health Data Management
Image Credit: Pixabay

Published on : Tue, 12 Sep 2017