HealthManagement.org
Promoting Management and Leadership

How to Defend Against a Cyber Attack

Recent malware attacks on a hospital in Hollywood and a second in Germany have highlighted the role of human error in paralysing the IT of healthcare and the urgent need to train staff to recognise a cyber-threat.

Last month Hollywood Presbyterian Medical Centre was forced to pay ransom after malware froze its IT systems while Lucas Hospital reverted to phone and fax after a cyber-attack brought operations to a standstill.

Both facilities had to transfer critical patient cases to other hospitals although each stressed that patient data had never been at risk. In each case, it took several days for experts to control the situation.

Malware can infect a hospital's IT systems through a simple email opened mistakenly by staff. This has been the case in several such recent attacks.

"When you think of the pressure staff at a hospital are under is it any wonder that one may open a malicious email by mistake? They aren't the IT experts," European Association of Healthcare IT Managers Secretary General, Christian Marolt told *HealthManagement.org.*
See Also*:* IT Community Leader: "Don't Give in to Cyber-Blackmailers"

Now more than ever it is critical that healthcare providers and companies invest in cyber security training

Prioritising detection and response is the first step but protection is necessary for these two steps to be effective.

Healthcare IT News recently detailed the main causes of cyber hackers succeeding in accessing healthcare IT:

- A lack of proper and real segmentation;
- Weak access controls and protections of credentials;
- Lack of discipline in hardening, patching and change control processes;
- Lagging refresh cycles and end-of-life equipment;
- Shadow IT and rogue applications;
- Inadequate user education and awareness;
- Not adhering to recognised standards based approach to controls;
- Irregular testing and assessment;
- Lack of external review;
- Inadequate oversight or governance.

In terms of being prepared for an attack, the same publication outlined the following steps:

- Train users to know how to identify unusual behaviour and avoid common threats through practical training and regular exercises;
- Keep the IT environment up-to-date and adhering to standards;
- Use multiple layers in protective technologies and controls at all system levels;
- Deploy signature-based and heuristic-based detection solutions;
- Use next generation firewalls, malware filters, A/V filters, automate log management and IDS/IPS;
- Plan for worst case scenarios and be prepared with effective back up;
- Put external support relationships in place in the case of a real event;
- Introduce objectivity into security by getting third parties to perform regular readiness audits, testing of controls and assessments.

“We urge any hospital to reject a ransom attack,” Marolt said. “The emphasis must be put on better security. There are hospitals in Europe operating on such outdated security that they aren’t able to deal with these kinds of attacks.”

Sources:
HealthManagement.org
HealthcareIT News

Image Credit:
WikiCommons

Published on : Mon, 29 Feb 2016