HealthManagement
Promoting Management and Leadership

Shocking Finds: HIMSS Cybersecurity Report

Remember that any connected device or system can be hacked. This is a central message of the latest HIMSS Healthcare and Cross-Sector Cybersecurity Report.

A Reddit post describes how "connected" coffee machines got infected and took factory systems down. "The coffee machines are supposed to be connected to their own isolated WiFi network, however, the person installing the coffee machine connected the machine to the Internal control room network," the anonymous Reddit poster wrote. "And then when he didn't get internet access remembered to also connect it to the isolated WiFi network."

What does this incident have to do with healthcare, anyway? Hospitals have coffee machines, for one. But also it's among the unexpected findings HIMSS Director of Privacy and Security Lee Kim discovered while compiling the new HIMSS cybersecurity report.

Coffee machines are not the only susceptible devices, either. "Basically, if you have something that is a connected computer-implemented or computer-enabled device, it can get infected," Kim said. "Then, it turns into a quest of what else can get infected. What's also connected to that same network?"

These important cybersecurity revelations are highlighted in the latest HIMSS report:

- New SMB (server message block) vulnerability: SMBLoris, which manifested in July, affects every Microsoft operating system since Windows 2000. Microsoft has not shared plans to address this vulnerability with a security update, but the software giant recommended enterprise customers consider blocking access from the internet to SMBv1.

- Win32/Industroyer, aka CrashOveride, which Kim described as sophisticated malware currently geared toward industrial control systems. The code is eye-opening because of its "highly configurable payloads" that hackers could tweak to target other industries as well.

- Some devices running Android.Triada.231, researchers found, have malware embedded into the libandroid_runtime.so system library. Yes, that means it could have an impact on just about every Android app. The researchers recommend that users install all possible updates for such devices.

In addition, infosec pros should be aware that Adobe said it will cease updating the Flash player in 2020. Once that happens, the company will no longer issue security patches and HTML5 will take over as the new web platform.

Another takeaway from Kim's report: Keep those software patches up to date but don't rely too heavily on vendors.

"Nothing replaces good cyber hygiene and defence in depth," Kim noted. "Unfortunately, as we have more things that are connected, there are more things that an attacker can compromise. Having things connected to super sensitive networks is never a good thing."

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 8 Aug 2017