Health care organizations under siege from cyberattacks, study says

February 21 2014

Add this to the list of reasons for consumers to fret over privacy: Health care organizations of all kinds are being routinely attacked and compromised by increasingly sophisticated cyberattacks.

A new study set to be officially released Wednesday found that networks and Internet-connected devices in places such as hospitals, insurance companies and pharmaceutical companies are under siege and in many cases have been infiltrated without their knowledge.

The study was conducted by Norse Corp., a Silicon Valley cybersecurity firm, and the SANS Institute, a security research institute. In the report, the groups found from September 2012 to October 2013 that 375 health care organizations in the U.S. had been compromised, and in many cases are still compromised because they have not yet detected the attacks.

In addition to getting access to patient files and information, the attackers managed to infiltrate devices such as radiology imaging software, conferencing systems, printers, firewalls, Web cameras and mail servers.

"What's concerning to us is the sheer lack of basic blocking and tackling within these organizations," said Sam Glines, chief executive of Norse. "Firewalls were on default settings. They used very simple passwords for devices. In some cases, an organization used the same password for everything."

"A decent percentage of these firms could have been eliminated from the data set if basic network and security protocol had been followed," he added.

The surge in attacks comes as hospitals and doctors across the country are using more and more medical devices that are connected to the Internet in some fashion. It's part of the broader trend known as the "Internet of Things," in which devices increasingly are being fitted with sensors and Internet connections.

In addition, more patient information is being placed online, in part through the growing network of federal and state health insurance exchanges.

"The pace at which technology has allowed our devices to be connected for ease of use has allowed for a larger attack surface," Glines said. "More vigilance is required."

But as the report found, there are often not enough security measures taken to protect these connected devices.

As a result, patient information and privacy can be compromised.

But another troubling aspect is that once attackers gain access to these devices, they can use them to launch attacks on other devices.

Indeed, the report tracked the origin of some of the malicious traffic coming out of medical sites that had been hacked: "The findings of this study indicate that 7 percent of traffic was coming from radiology imaging software, another 7 percent of malicious traffic originated from video conferencing systems, and another 3 percent came from digital video systems that are most likely used for consults and remote procedures."

In following the trails of this malicious traffic, Norse found detailed information about the layouts of hospitals and specifications of various pieces of life-saving equipment.

Glines said the vulnerability can be addressed in many cases. But still, he's worried that health care providers may not move quickly enough.

"It's going to accelerate as we have more and more connected devices," Glines said. "With more health care information coming online, it becomes more valuable and therefore a richer target. We expect to see an uptick of breaches related to health care. It's sort of a perfect storm."