COMPUTERWORLD

NEWS

More than 80% of healthcare IT leaders say their systems have been compromised

Only half of IT managers feel they are adequately prepared to prevent future attacks

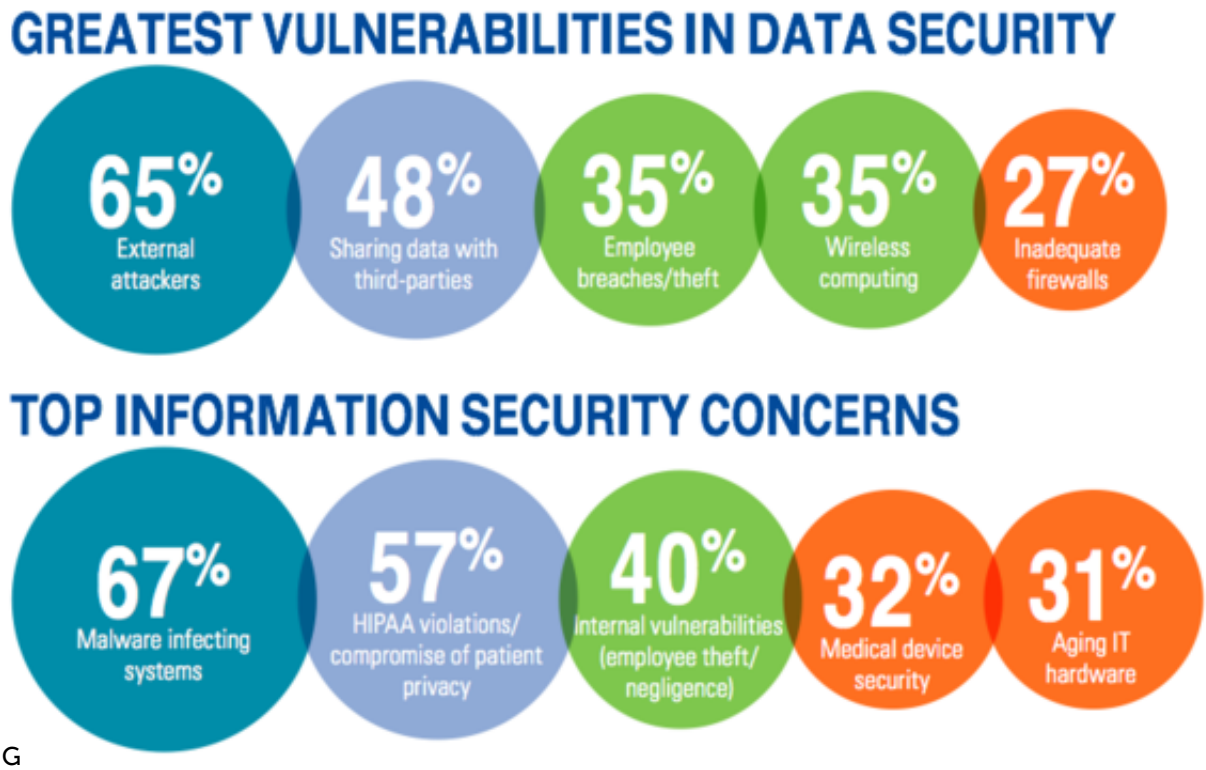
By Lucas Mearian FOLLOW

Computerworld | Aug 27, 2015 3:13 AM PT

Eighty-one percent of healthcare executives say their organizations have been compromised by at least one malware, botnet or other kind of cyberattack during the past two years, according to a survey by KPMG.

The KPMG report also states that only half of those executives feel that they are adequately prepared to prevent future attacks. The attacks place sensitive patient data at risk of exposure, KPMG said.

The 2015 KPMG Healthcare Cybersecurity Survey polled 223 CIOs, CTOs, chief security officers and chief compliance officers at healthcare providers and health plans.



KPMG

Sixty-six percent of the IT executives at healthcare plans who were surveyed said they were prepared to fend off attacks. Based on revenue, larger organizations are better prepared than smaller ones, KPMG said.

Compared with past KPMG polls, the one released Wednesday showed that the number of attacks on healthcare IT systems has increased, with 13% of respondents saying they are targeted by external hack attempts about once a day and another 12% seeing about two or more attacks per week.

"More concerning, 16% of healthcare organizations said they cannot detect in real-time if their systems are compromised," the report said.

Malware, which is designed to disrupt or gain access to private computer systems, was the most frequently reported line of attack during the past 12 to 24 months, according to 65% of survey respondents. Botnet attacks, where computers are hijacked to issue spam or attack other systems, and "internal" attack vectors, such as employees compromising security, were cited by 26% of respondents.

The areas with the greatest vulnerabilities within an organization include external attackers (65%), sharing data with third parties (48%), employee breaches (35%), wireless computing (35%) and inadequate firewalls (27%).

The KPMG survey found that spending to prevent cyberattacks has increased at most institutions, but it has to be on the right initiatives and fit the organization's strategy, said KPMG's Gregg Bell. "There are no cookie-cutter approaches to security. An organization with a mobile workforce may have a far different technology need from an organization that processes healthcare claims, for example."

"The vulnerability of patient data at the nation's health plans and approximately 5,000 hospitals is on the rise and health care executives are struggling to safeguard patient records," Michael Ebert, who runs KPMG's Healthcare & Life Sciences Cyber Practice, said in a statement. "Patient records are far more valuable than credit card information for people who plan to commit fraud, since the personal information cannot be easily changed."

KPMG listed five main reasons healthcare organizations are facing increased security threats:

- The adoption of digital patient records and the automation of clinical systems.
- The use of antiquated electronic medical records (EMRs) and clinical applications that are not designed to securely operate in today's networked environment -- and software vendors who push that problem to the provider.
- The ease of distributing electronic personal health information both internally (via laptops, mobile devices, thumb drives) and externally (third party firms and cloud services).

- The heterogeneous nature of networked systems and applications (i.e. network-enabled respirator pumps on the same network as registration systems that can browse the Internet).
- The evolving threat landscape, where cyberattacks today are more sophisticated and well-funded, given the increased value of the compromised data on the black market.

Healthcare organizations not experiencing an increase in cyber attacks are also more likely to underestimate the threat, according to Bell, who leads KPMG's Cyber Practice.

"The experienced hackers that penetrate a vulnerable health care organization like to remain undetected as long as they can before extracting a great deal of content, similar to a blood-sucking insect," Bell said.

Lucas Mearian — *General assignment and storage*

Lucas Mearian covers consumer data storage, consumerization of IT, mobile device management, renewable energy, telematics/car tech and entertainment tech for Computerworld.

Free course: Hack yourself first (before the bad guys do)

View Comments

YOU MIGHT LIKE

The Most Exciting MMORPG You've Ever Played. Don't miss this!

Sparta Online Game

Adobe Flash must die, die, DIE. Firefox shoots gun loaded by Facebook (and potholer54)

Top 16 Reasons You Should Date a Man with a Beard

YOLO Report

X-47B completes first air-to-air drone refueling

Build Your Own Website In Only 10 Minutes !

Wix.com

Shaking up outdated work practices

Financial Times

The Dark Side of the App Store

Wibki.com