Print This Article

<< Return to Medical data leakage rampant on P2P networks

Medical data leakage rampant on P2P networks

Angela Moscaritolo
February 11 2009
Updated Thursday, Feb. 12, 2009 at 10:34 a.m. EST

The risk of patient information disclosures on peer-to-peer (P2P) networks is much higher than if a health care worker loses a laptop or removable storage device, according to new Dartmouth College research.

Dartmouth College business professor Eric Johnson has written a report called "Data Hemorrhages in the Health Care Sector" and plans to present his findings later this month at the Financial Cryptography and Data Security conference, Johnson told SCMagazineUS.com Wednesday.

P2P networks are internet-based file sharing networks that allow users to share music or other files -- LimeWire or BearShare are popular examples.

Over a two-week period, Dartmouth College researchers, in collaboration with P2P monitoring vendor Tiversa, searched file-sharing networks for key terms associated with the top ten publicly traded health care firms in the country, and discovered numerous sensitive documents – for example, a spreadsheet from an AIDS clinic with 232 client names, including Social Security numbers, addresses and birthdates.

The researchers also discovered databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact details, and insurance records, along with diagnosis information.

The researchers also found a 1,718-page document from a medical testing laboratory containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients. And in another place relating to a group of anesthesiologists, more than 350 megabytes of data comprising sensitive patient reports were found.

In all, researchers found hundreds of documents revealing sensitive information on tends of thousands of patients, Johnson said.

Robert Boback, CEO of Tiversa told SCMagazineUS.com in an email Thursday that the company has seen millions of P2P-related disclosures from health care organizations and other industries --

everything from Social Security numbers, employee and customer records, executive board minutes, strategic initiatives, security audits and contracts.

“We've found that most health care providers are not aware of the severity of the threat these public networks pose, how they operate, or even the alarming rate at which data is actually being disclosed,” Boback said.

There are numerous ways confidential data can inadvertently get on a P2P network, Johnson said. For example, users could share folders containing sensitive information because of a confusing client interface or because they have music and data in the same folder. Or they could potentially download malware that exposes files or install a vulnerable program that unintentionally shares files the user did not intend to.

Johnson said health care organizations should be worried about the threats of P2P networks. Because even if they ban employee use of P2P, many times patient data winds up on the laptops of individual physicians or partners -- so the potential for any one of those users to participate in P2P goes up, Johnson said.

William Miaoulis, manager of security services at Phoenix Health Systems, a health care consultancy, said the threat of data loss on P2P networks is probably greater from third parties than from internal hospital employees.

Partners doing services for the hospital often have access to the virtual private network (VPN), and while hospitals believe they can secure their own environment, securing those outside of the hospital environment is harder, Miaoulis said.

"Any time you open up your network there are some security risks,” he told SCMagazineUS.com.

Boback said recent Tiversa research shows that 93 percent of client disclosures are caused by workers who have access beyond the enterprise boundaries.

“It all comes down to folks not understanding the severity of risk that data outside the corporate perimeter poses,” Boback said. “Combine this misunderstanding with the fact that this information is publicly available to millions of people, including a large number of criminals, and you have a huge problem.”

Johnson said the root problem causing data leakage in the health care sector is that health care organizations store confidential and highly sensitive data in unprotected and easily portable formats such as Microsoft Excel spreadsheets, Word documents, or PDFs, he said. Preventing users from using P2P networks is just a "Band-Aid" fix for a bigger problem, since there are many other ways data can be leaked from an organization.

Health care firms must implement systems in which users can look up information on a patient but cannot download the data to a spreadsheet, he said. The $818 billion economic stimulus bill passed two weeks ago by the House provides money to computerize health records and also calls for

stringent security and privacy controls.

“The bigger issue is moving toward a robust enterprise data system based on a universal medical record format,” Johnson said.