CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Inadvertent Data Disclosure on Peer-to-Peer Networks

Key Message: Peer-to-peer networks are being used today to unintentionally disclose government, commercial, and personal information.

Executive Summary

Peer-to-peer software clients are increasingly being installed by users on home and business computers but can sometimes be installed without your knowledge. These clients are being used by millions of users to share music, video, pictures, and other information. Most users do not understand that having these clients on their computers can cause the contents of their entire hard drive to be shared publicly in the peer-to-peer network. This is a particularly high risk when work computers are used at home.

In this podcast, M. Eric Johnson, Director, and Scott Dynes, Senior Research Fellow, both with the Center for Digital Strategies within Dartmouth's Tuck School of Business, discuss this growing class of information security breaches and what users and business leaders can do about it.

PART 1: Understanding the Threat

Inadvertent and Unintentional Disclosure

In their paper "Inadvertent Disclosure – Information Leaks in the Extended Enterprise," Eric and Scott state that while hacks on poorly secured networks do happen, many of today's security breaches result from inadvertent disclosure – lost laptops, mis-posted web entries, and losses in peer-to-peer (P2P) file sharing networks.

The result is the same – information leakage leading to embarrassment and possible financial loss.

Peer-to-Peer File Sharing Networks

What is P2P? These are networks where people share music and other types of files and documents. Napster, LimeWire, and eDonkey are several examples.

Inadvertent disclosure via P2P happens because people are unfamiliar with the technology and that in sharing a single directory, you can end up sharing your entire hard drive. Kids are much more adept than their parents.

How does this happen? P2P clients come with wizards that allow you to expose specific directories. What some people don't understand is that when you share a directory, all of its sub-directories are also shared.

In addition, the basis of P2P is sharing so P2P clients provide incentives for sharing a substantial number of files (faster service, better search results, larger networks to access).

P2P use most commonly occurs in home computing and as work life merges with home life. People take work files home, put it on their home computer, and the P2P client software automatically shares them.

They are hard to control in home or public networks, even with the use of firewalls.

PART 2: DETERMINING IF A PEER-TO-PEER DISCLOSURE HAS OCCURRED

Why We Don't Hear More About P2P Breaches

An inadvertent disclosure is often unknown and invisible until something surfaces to make it known (such as a news article). The unintentional sharing of financial information via P2P can lead to identity theft but users don't typically know that this action is the cause.

Legal Consequences – Breach Notification

Companies may find themselves having to notify customers and employees if a breach of personal information occurs as a result of peer-to-peer file sharing.

How Do You Find Out If Your Data Is Out There?

There are commercially available services that will monitor P2P networks, similar to services than monitor for brand and other copyright violations.

The downside is that each report is a snapshot. At any point in time, there may be upwards of 10 million simultaneous P2P users who are all sharing information. The user mix, their access, and the documents they share are constantly changing. This makes surveillance more challenging.

User awareness and training, strong content management practices and software, strong access control, and blocking the use of P2P services can help prevent inadvertent disclosure.

PART 3: THE UPSIDE AND THE DOWNSIDE OF PEER-TO-PEER

Recovering Disclosed Information

Recovery of information disclosed via P2P is quite difficult, as documents propagate throughout the network. The only option currently is to ask those who have your information to remove it from their systems.

Benefits of Using P2P

P2P can be effectively used for widespread content distribution, allowing rapid dissemination of information both within an organization and outside.

The useful features that come with new technologies almost always have associated risks.

Finding P2P Clients on Your Computers

In most cases, you know if a client has been installed but once it's there, it's often not clear that the client is sharing information when it is executing. Even when you think you've shut a client down, it may still be sharing.

The U.S. Patent & Trademark paper, testimony, and a supporting appendix (see Resources below) describe specific P2P clients and their features.

A Final Word of Advice

Keep computers that you use for handling sensitive information separate from computers that you use for routine web surfing and file downloading, particularly at home. Don't keep your bank records on the family machine.

Resources

Sydnor II, Thomas D.; Knight, John; Hollaar, Lee A. "Filesharing Programs and 'Technological Features to Induce Users to Share, v1.1.'" A Report to the United States Patent and Trademark Office from the Office of International

Relations. November 2006.

Testimony before the House Committee on Oversight and Government Reform. Thomas D. Sydnor II, Office of International Relations, United States Patent and Trademark Office, July 24, 2007. On the subject of inadvertent file sharing.

Appendix A to the testimony above, discussing each of the five "features" described in the USPTO Report "Filesharing Programs and 'Technological Features to Induce Users to Share v1.1.'" (redistribution, search-wizard, share-folder, partial-uninstall, coerced-sharing)

Johnson, M. Eric & Dynes, Scott. "Inadvertent Disclosure – Information Leaks in the Extended Enterprise," Proceedings of the Sixth Workshop on the Economics of Information Security, Carnegie Mellon University, June 7-8, 2007.

Johnson, M. Eric; McGuire, Dan; Willey, Nicholas D. "Why File Sharing Networks Are Dangerous." Forthcoming in Communications of the ACM, 2007.

Greenemeier, Larry. "Beware P2P Networks With A Tunnel To Confidential Data, Study Warns." Information Week, May 15, 2007.

Pessin, Jaime Levy. "Citi Unit Info Leaked Onto P2P Network." Dow Jones Newswires, September 21, 2007.

Terese, Adam. "Internet sharing exposes secrets." The Washington Times, July 25, 2007.