Peer to Peer

Risky Business

10 mar jun sep dec

Peer to Peer March 2010

Gotcha! Offense Is the Best Defense Against Security Vulnerabilities

DONNA PAYNE PAYNEGROUP

Attorney John Doe receives an attachment via e-mail and opens it on his computer. The attachment is blank, so he closes it and continues to work. He visits websites, the firm intranet and goes about his business. John doesn't know it, but his computer, as well as the firm's intranet, have been compromised. The attachment had a keystroke monitoring software program embedded. Keystroke monitoring can be run remotely or by an attached device that resembles a USB drive. If you think this is unlikely, consider that this type of activity has already been used against celebrities and in corporate espionage attempts. This is just one type of security vulnerability that the legal industry must be vigilant against. Let's take a look at others as well as some necessary steps toward becoming more secure.

DARK CLOUDS

"Cloud computing" is the latest buzz phrase. We're now looking at more companies providing software as a service (SaaS), storage on demand and remote server capacity. As a result, some firm and corporate data may reside outside a firm's network and outside of the direct control of IT administrators. While you will vet vendors as much as possible, there will always be challenges; and frankly, there may not be a way to ensure 100 percent enforcement of your firm policies on a system that you do not have complete control over. For a look at some insightful questions that should be raised with vendors, visit this article, "Gartner: Seven Cloud-Computing Security Risks," which covers risk issues outlined in a 2008 Gartner report ((http://www.networkworld.com/news/2008/070208-cloud.html).

No matter how good a piece of software is, there are always vulnerabilities. Around our office, we've become numb to receiving weekly updates from certain vendors. These often fix recently discovered security holes — ones that could have left us vulnerable to attacks before the patch was released and installed. As long as there are hackers, we must remain vigilant; and since cloud computing takes control out of our hands, we must rely on third parties to maintain this vigilance.

SOCIAL BUTTERFLIES BEWARE

Social networking is great. (If you haven't reserved your Twitter name, jump over to www.Twitter.com and reserve your name

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.

before someone else grabs it.) Twitter is useful for marketing your firm, keeping up with ILTA members, following the industry and for just being in the know. LinkedIn is great for business, too, because you can use it for networking and staying in touch. That said, there are definite security risks associated with these types of sites. First, there is the lack of control by the firm over what gets posted by the individual. Too often people don't filter what they post, and those posts can come back to bite them. They can also reflect poorly on the firm. For this reason, some firms have started to distribute written employment policies regarding social networking. For an excellent article on the ethical risks and pitfalls of social networking sites, visit http://www.mygazines.com/issue/6117.

Hackers have also found ways to compromise social networking sites. Often when accounts are compromised, messages are sent to all of the contacts for that account with an embedded link to click within the message. Once someone clicks the link, his device also becomes infected, and the virus spreads. This leads us to the next security concern.

PASS THE WORD

In October 2009, Microsoft confirmed that phishers stole at least several thousand Hotmail passwords. This was bad news in itself, but what made it worse was that many of these victims used the same passwords for other accounts, such as their MySpace, Facebook and Twitter accounts, where they would be victimized again.

Craig Ball, an attorney, forensic technologist and Certified Computer Forensic Examiner, was an administrator for a website with 47,000 lawyers who signed on with passwords they selected. He says, "I saw firsthand how little caution lawyers brought to their password choices. Sports teams, alma maters, children's names and birth dates were the norm." Based on his subsequent experience as a forensic examiner, Ball estimates that anywhere from a quarter to a third or more of the registrants used the same password for the website that they also used for their personal e-mail accounts. He explains that many don't know that forensic examiners rarely gain access to encrypted files by decryption because it takes so long; instead, they gather the passwords from less protected applications. These passwords are typically the same as, or closely resemble, the password used for the encrypted material.

Firm administrators, in conjunction with the trainers and support staff, should educate all members of the firm regarding the need for robust password protection. Policies can also be set to provide a little more heavy-handed encouragement for compliance. For instance, consider setting policies such as:

- **Forcing a password change every "x" number of days**
- **Setting a minimum password length**
- **Requiring that passwords meet complex and pre-defined criteria (alphanumeric and special character mix)**

You would be surprised at how many passwords are simply set to 'password.' Even more surprising is that some IT professionals who use netbooks have no password set at all (the default). Password security is important, and it is something that you cannot be sure your users are applying correctly. A general rule of thumb is that if any firm document is sent, or if any e-mail connection is ever made, to any computer, netbook or device, it should have a resilient password applied.

WHAT YOU SEE IS NOT WHAT YOU GET

In the movie "Catch Me if You Can," Leonardo DiCaprio plays the character based on Frank Abagnale, Jr., who, before he turned 19, had posed as a Pan Am pilot, a doctor and a lawyer, and had stolen millions of dollars. He was adept at fitting into any environment by slipping on a uniform and blending into his surroundings. Criminals are good at this, and there are some unbelievable stories about law firms that have been victimized this way. For example, there is the story about one firm that had a telephone equipment room cleaned out because the receptionist let in a man with a service bag and telephone company uniform; he said he was there to repair the telephone system. Another firm had all the attorney laptops stolen by someone wearing painting coveralls who came in carting paint cans on a hand truck. Apparently he piggybacked through the door behind an attorney and didn't go through reception.

If a firm doesn't take precautions, simple lapses in security can happen. As Craig Ball notes, "When I'm working late at these firms, I'm amazed by how many lawyers leave their doors open and their systems logged in."

MALICIOUS MARAUDERS

Some of the newer viruses are easy to get and difficult to remove. One of the more aggressive ones that we've seen with clients is Antivirus Live, which looks just like antivirus software. Once you click Perform Scan, your computer becomes infected via Trojans, and it will load every time your Windows operating system starts. Make sure to educate your staff about this virus because even the professionals have a difficult time removing it. Remind them not to click any unfamiliar button or run any unknown program or virus scanning software. There's an

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.

Outlook Web Access look-alike virus, too. The security company M86 Security identifies this at http://www.m86security.com/labs/i/Don-t-Update-Your-Email-Settings,trace.1215~.asp.

It's not enough to stay up-to-date on virus protection, but it helps, and is well worth the effort. You should also keep current on information from industry experts. Visit websites such as United States Emergency Computer Readiness Team http://www.us-cert.gov/cas/tips/, and communicate regularly with the entire IT staff so they can make firm personnel aware of any real threats.

THE ARTFUL LODGER

Once while staying in a Chicago hotel, I ventured into the hotel's business center to print handouts for a meeting. I did a double take when I saw some files that had been saved on the computer desktop. They were titled FirstNameLastNamePassport, FirstNameLastNameVisa, and FirstNameLastNameBirthCertificate. The files were scanned copies of all these documents, and, as you can imagine, if they were to fall into the wrong hands, could have exposed the person to identity theft. I notified the manager of the hotel, and he told me that this happened all the time. He said he would get legal documents, medical records and all types of files he'd rather not see. This particular set of files did not belong to a guest of the hotel, and he could only surmise that it belonged to someone who was representing this person. Fortunately for this individual, the files were destroyed and no harm was done. This goes to show, however, that when traveling, certain protocol needs to be followed when working on, as well as disposing of, documents. Files should never be saved locally to a computer that is not secured.

THE BIGGEST LOSER

Careless people may be the biggest security threat that organizations face today. They don't intentionally set up themselves and/or their firms to be vulnerable, and they always think that a security breach won't happen to them — until it actually does. Steve Fletcher, CIO at Parker Poe, says, "Security is about people, not technology. It's about people who leave laptops in airports or rental cars; people who can't be bothered with passwords on PDAs; people who refuse to make regular password changes unless they are forced; people who connect (or try to connect) personal devices to office networks after hours or on weekends; people who use their kid's highly unsecure home PC to draft confidential client info or work product; people who don't look carefully at an e-mail recipient's address or carelessly reply to all; people who leave confidential work product all over the office, in conference rooms, etc. While it's true that we have to deal with cybercrime, hacking, etc., from a network ops standpoint, many of the entry points of our systems result from those items mentioned above."

Craig Ball agrees and adds, "People are the weakest link in any effort designed to secure information. It's especially easy to prey on their egos and insecurities through what's called 'social engineering.' I bet you could gain access to almost any law firm's network by leaving a thumb drive holding malware and labeled 'Payroll' on the bathroom floor. You might have to do it a few times to succeed, but you can bet someone will ultimately pick it up and pop it into a machine. If it holds self-executing spyware, forget the firewall; it's already inside and tunneling through the system sending secrets who-knows-where."

WHAT'S A FIRM TO DO?

What are some of the things you can do to address security concerns? If you are going to be contemplating cloud computing and other such endeavors, you cannot just take the word of consultants. Know the tough questions to ask and when to challenge their answers. Set an internal policy that is right for your firm, and see that it is passed to the attorney and staff population throughout the organization. Make sure virus protection is in place and kept up to date. Maintain firm software and updates. Determine what the firm policy will be for social networking and then create and distribute the policy. Train your trainers and support staff on security issues. Training should not be just for networking and administrative staff, but for your entire team. Finally, you can't be successful if you just look at security matters every five years; this has to be an ongoing process. If you audit your practices regularly, you will be more successful, better prepared and less vulnerable. **ILTA**

Donna Payne is CEO of PayneGroup She was the recipient of the first ever Consultant of the Year award given by *Law Technology News*, and the Lex Proficio award for lifetime service advancement of legal software and publishing. She is a frequent speaker at legal and technical conferences worldwide and has spoken to Congressional committees, the Senate, and at international judicial conferences on the subject of metadata and preventing accidental disclosure. Donna writes the Test Drive column for *Law Technology News*. She can be reached at donnapayne@payneconsulting.com or Twitter @Donna_Payne.

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.