SECUREPURDUE NEWS
www.purdue.edu/securepurdue

January 2010
Volume 5, Issue 1

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Today's topic is "Cloudy, With a Chance of Security." I know I have talked about this before but it seems like every article I read, every presentation I attend, and now even television commercials have something to say about "cloud computing." Everyone wants to believe clouds provide everything good, eliminate costs, and have no risk. I hope I can convince you to question that position.

On the up side, there is certainly reduced capital cost to deploy cloud computing services. Note this is "reduced" and not "eliminated" costs. There is also reduced management requirements for infrastructure staff because massive data can potentially be consolidated on cloud provider storage space. There can be some security options like Data Loss Protection (a.k.a. DLP) that cloud providers may bundle into the base package. One could even argue that cloud providers may be better prepared to protect against some of the advanced web-based security threats. On the down side, there is additional network latency to access the cloud and there may be greater cost in providing the bandwidth necessary to effectively use the cloud. Minor changes in the cloud infrastructure (if we can even define such a thing) may have significant unintended consequences as could providers who become less concerned about individual users.

As I thought about all of this and the message that I wanted to communicate, I decided on five things you should know when discussing cloud computing:

1. Clouds can be secure, but that doesn't mean they are always secure. Placing an application in a cloud means that application security must be the strongest possible since other layers of security may not be present.

2. You MIGHT save money but, then again, you might not. In the end, you usually get what you pay for and using cloud computing puts a HUGE burden on accurately specifying your requirements and expectations in the contract or memorandum of understanding (MOU)

3. You probably can't pass a compliance audit with an application in a cloud. At best, it is going to be almost impossible to properly perform an audit. At worst, the cloud really isn't compliant. Some major cloud vendors already state as much right up front.

CISO cont. page 2

In this issue

Wi-Fi Security Presentation

ITaP's Networks and Security is hosting a presentation about Wi-Fi security to be held February 16th from noon to 2:30 p.m. in Stewart Center room 310. Dr. Bob Morrow will be presenting information that he teaches in wireless courses that he presents around the country. Bob has a PhD in Electrical Engineering from Purdue. He is a retired Air Force Academy professor with wireless networking expertise. This presentation is regularly a 3 day course, but will be offered in a condensed version for us at no charge. Below

"he will provide a summary of simple ways that wireless security can be improved"

is an overview of what Morrow will present.

Wi-Fi (IEEE 802.11) is by far the most common wireless computer network, and the relentless tide of sophisticated attacks make security of this system critically important. Dr. Bob Morrow will address several Wi-Fi security threats, including disclosure, data integrity, and denial-of-service attacks that can bring a network to its knees. Simple propagation analysis can determine a target network's vulnerability to eavesdropping and jamming. The weaknesses of wired equivalent privacy (WEP) are legendary, and Morrow will discuss how these are addressed through the IEEE 802.11i standard with improved authentication, key distribution, and encryption methods. Finally, he will provide a summary of simple ways that wireless security can be improved beyond simply implementing 802.11i.

Please join us for this presentation. Stop by the Union for a carry out lunch and join us for this informative session on Wi-Fi security.

CISO continued

4. Cloud computing means different things to different people. Don't use this as an "industry standard term" that you expect everyone will understand.

5. Regardless of what you think about clouds, your data still exists in a physical location somewhere and there may well be local laws that could make data transfer and/or storage subject to legal requirements. Encryption in the cloud may just be a way to keep you out of jail.

So, to paraphrase the great Judy Collins,

"We've looked at clouds from both sides now
From up and down and still somehow
It's clouds illusions we recall
We really don't know clouds at all"

As always, thanks for reading and be careful out there.

SPOTLIGHT

International Data Privacy Day

On January 28, 2009, the United States, Canada, and 27 European countries will celebrate international Data Privacy Day. According to www.dayatprivacyday2010.org, "Data Privacy Day is an international celebration of the dignity of the individual expressed through personal information."

"Individuals must take steps to protect their data, particularly when engaging in business and transactions online or participating on social networking sites," said Joanna Grama, Information Security Policy and Compliance Director at ITaP Networks and Security and a Certified Information Privacy Professional (CIPP/IT). "One part of protecting data is making sure that your computer's security settings are sufficient and operational."

In recognition of Data Privacy Day, ITaP's Networks and Security group offers their top security guidelines for protecting data privacy while on the Internet:

-Install and use daily anti-virus software and set your computer to automatically update anti-virus applications daily.

-Install firewall security software.

-Apply operating system security software patches and updates regularly. Windows users can use Microsoft's Windows Update Service. Apple OSX users should install security updates when prompted by "software update." Also apply patches to application software such as word processors, IM clients, and other programs.

-Set the security settings to the highest level on Internet browsers.

Use adware and spyware removal programs.

-Be suspicious of any unexpected e-mail requesting personal information, or of any e-mail attachment, even if it is from someone that you know. Never comply with requests for personal information from an e-mail unless you initiated the contact (these are often phishing scams trying to steal your personal information). Be suspicious of any unexpected e-mail attachment even if from someone you do know because it may have been sent without that person's knowledge from an infected machine.

"Another way to protect your data is to read up on privacy issues," Grama said. Internet-based educational resources on privacy issues include:

-The Privacy Rights Clearinghouse, http://www.privacyrights.org/. Navigate to their "Fact Sheets" page for detailed information on a number of subjects.

-Data Privacy Day 2010, http://dataprivacyday2010.org/ . Navigate to their "Education and Resources" page for additional reading on privacy issues.

-On Guard Online, http://www.onguardonline.gov/. Navigate to their "Topics" page for detailed resources on a number of computer security issues.

Additional information regarding computer security can be found on the SecurePurdue web site: www.purdue.edu/securepurdue. If you have questions regarding the security settings for your Purdue University workstation, contact your local IT support staff.

NEWS UPDATES

Targeted E-mail Scams Continue to Plague Purdue

The New Year has brought resurgence in e-mails scams targeted specifically at Purdue University e-mail users. "These scams continue to plague campus," said Greg Hedrick, Director of Security Services in ITaP Networks and Security. "Users should continue to question whether or not these e-mails are authentic before taking the action requested in the e-mail."

The e-mail scams appear to come from various authoritative Purdue University administrative departments, such as the "Purdue Webmail Team," "Purdue Management Team," or "Purdue Support Team." Often times these e-mails will look highly authentic, using Purdue logos, screenshots, or common Purdue terminology.

Some variations of these types of e-mails ask users to respond to the e-mail to confirm their e-mail address and to provide their computing login information and password. In most variations, the e-mails threaten that if the user does not respond or take some required action that their e-mail account will be somehow deactivated.

Not all of the e-mail scams are phishing attempts to gain user names and passwords. One of the latest scams targeted at Purdue attempts to download malicious software onto the end user's computer. This scam specifically targets Outlook Web Access (OWA) users. The e-mails direct users to navigate to a specific URL. Navigating to the web pages indicated in the e-mails and following directions on those web pages can potentially install malware on the user's computer. Many anti-virus products, including McAfee, will detect and delete the malware.

"Users who receive these types of e-mails should question whether they are from the university," Hedrick said. "Users should immediately delete the e-mails and should not reply or take the action requested in the e-mail. In addition, IT units at Purdue will never ask users to divulge their passwords to university IT resources."

Users who have responded to e-mail scams such as the ones described here should immediately reset their Purdue Career Account password. Users can go to the password reset page located at www. purdue. edu/securepurdue. (Click on the "Change Your Password" link on the bottom right hand side of the page.) Users who believe that they have been infected with malware should contact their local computer support groups for further assistance.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

- The Privacy Rights Clearinghouse
http://www.privacyrights.org/
- Data Privacy 2010
http://dataprivacyday2010.org/
- Change Your Password
http://www.purdue.edu/securepurdue
Click on the "Change Your Password" link on the bottom right hand side of the page.
- On Guard Online
http://www.onguardonline.gov/