The Security Blanket

(Ya Gotta Love Security!)

Issue 6, February 2002

In This Issue:

From the CISO

As we move further into an environment in which services are provided electronically via the Internet, other opportunities are provided for those who have malicious intent. For instance, new privacy concerns are presented in a variety of forms, financial information becomes more at risk, and apparently the electronic con man can think up even more ways to take your money. The Michigan Department of Treasury received an alert from the IRS that an e-mail is going around (from a non-IRS source) indicating that the recipient is under audit and needs to complete a questionnaire within 48 hours to avoid an assessment of penalties and interest. The e-mail refers to an audit and references the IRS Form 1040, while asking for social security numbers, bank account numbers, and other confidential information. This is not a valid e-mail from the IRS, as they do not conduct this type of business via e-mail. It is more likely an attempt to steal identities and money.

We will continue to see this type of activity, and you owe it to yourself to educate yourselves on how to identify fraudulent e-mail of this type. Pay attention to our

publications, read our Web site, and if you ever have a concern or even an "icky" feeling about a message, please give us a call – we'd love to help you out.

Kip Peters

Return to Table of Contents

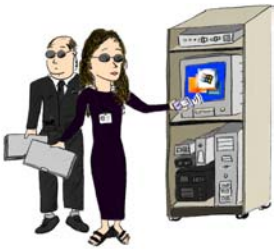
Current Activities

ISO personnel are currently involved with many projects. We are currently assisting with the five charter projects envisioned by Governor Vilsack, which are designed to provide better governmental services to the citizens of Iowa while decreasing the costs associated with those services. ISO personnel also support various security efforts within ITD and in other departments, and our Security Awareness efforts continue to grow.

Information Security Office Service Offerings

Service rates are now available for ISO Services.
Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates!
(Security Services are listed in the last quarter of the web page.)
*You can't buy Love, they say, but you **can** invest in a secure network.*

Security Consulting
Vulnerability Assessments
Physical Security Vulnerability Assessments
Network-Based Intrusion Detection System
Enterprise Business Continuity
Incident Response
Test Lab
Awareness Briefings
Enterprise IT Business Continuity



Descriptions of each service are available at: http://www.itd.state.ia.us/security/ops.html

UPCOMING SERVICES ***On-Line Awareness Training*** (end of February 2002)
Vulnerability Profile Database (early 2002)
Risk Assessment

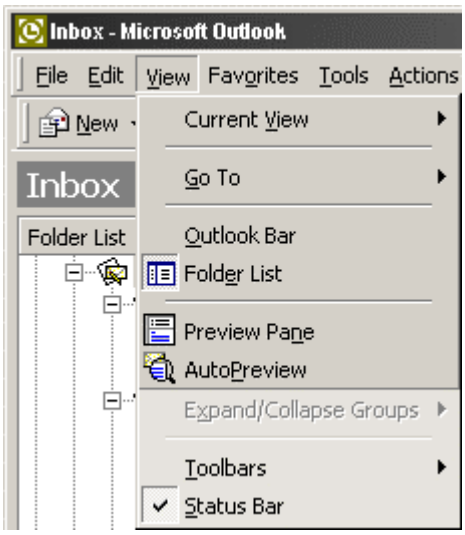
OTHER ACTIVITIES

Enterprise Security Website

Have you been here? From this you have access to a plethora of security information: Security Awareness Resources, Operational Services, Procedures, Recommended Reading, and Mobile News. It's the place to be for Security!

Return to Table of Contents

Helpful Hints



Using the Preview or Auto-Preview Pane in Outlook and other email applications or services can be a nice, convenient way of quickly discovering what an email message refers to. Unfortunately, these two functions can also automatically open certain types of email viruses or launch an application, without any assistance from the user. (For example, the Zoher worm in December 2001 could infect unpatched systems in this manner.) One way to decrease the security risk of this function is to turn off the preview and auto-preview panes in your email application's Inbox folder. For Outlook, simply highlight the 'Inbox" folder, go to the "View" tab on the menu bar, scroll down to "Preview Pane" and "Auto-Preview" make sure they are unselected. By doing this, you can at least mitigate the risk by being able to judge yourself whether or not you want to open a potentially malicious message, such as a message form an unknown source or one with an unexpected attachment.

William Hubbard

Return to Table of Contents

Upcoming Classes and Consultations

Looking for a Romantic Dinner? You won't get it at the Lunch & Learns, but you can learn about security tricks and services, and about vulnerabilities and being secure. That's as close to a Valentine's theme as we can get!

Want to get to know someone better? Bet you wish you could use something as easy as Knowledge Access! It

can't help you with relationships, but it can help you find security (and perhaps happiness?) in applications and systems.

Looking for classes or seminars? Check out the vendor announcements to read about some learning or business opportunities.

Lunch & Learns

The Information Security Office's Lunch &Learn Program continues… These bi-monthly, informal get-togethers cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. The current schedule is as follows:

Date and Time	Topic and Location
Feb. 26 12:00pm-1:00pm	Business Continuity Planning Grimes Bldg., South Conference Room
March 12 TBA	Security for Application Development (Tentative) TBA

Change of location or time will be announced via e-mail, and sent to departmental L&L security contacts. The past presentations (lots of them - in .pdf, .ppt, and/or video) and an updated schedule are available at the Lunch & Learn site.
Questions regarding the Lunch & Learn program can be directed to William Hubbard.

. . . . . .

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing information.

. . . . . .

Vendor Announcements

SANS Offerings

SANS Conference on March 18 - 23, 2002 at the Fairmont Kansas City Hotel in Kansas City, MO. Geared toward those who are starting out in the world of computer security, SANS Kansas City will be offering Track 1: SANS Security Essentials. This course provides the vital information that is necessary to build a foundation that can act as a springboard into information security.

Please plan to attend the SANS Kansas City conference if you are looking to gain the knowledge that is essential to provide solid information security throughout your organization. In addition to this exceptional training opportunity, you will also have the ability to network with industry peers and share experiences, tips, and tricks. If you are

interested in pursuing one of the industry's most recognized certifications, then attending SANS Kansas City will prepare you to attempt the GSEC (GIAC Security Essentials) certification. For more information on this rapidly growing security certification, visit GIAC's new website at www.giac.org.

(From Steven Northcutt.) I hope you can join us in Kansas City this March as we bring SANS Security Essentials to the Great Plains. For more information on this conference please visit: http://www.sans.org/KansasCity.

McAfee and Sniffer Seminar

McAfee Anti-Virus

Find out how to protect your users, your company and your customers from virus infections and malware in Internet traffic. Learn more about our NEW e500 WebShield product, NEW Personal Firewall/VPN, ePO, NetShield and GroupShield, and how they will benefit your business environment.

Sniffer Technologies

Network Associates presents the industry leading solution for network monitoring and analysis. Learn how the suite of Sniffer products can isolate and resolve the IT problems that impact the business of government in your organization. 2002 product road map will be highlighted including introduction of intrusion detection capability.

When: Tuesday, February 19, 2002
Where: Mariott Downtown, 700 Grand Ave
Des Moines, IA 50309
Time: 8:00 am – 12:00 pm
Registration and Continental Breakfast Begins at 7:30AM
RSVP: www.nairegistration.com
Reference Seminar Number: MCA 87545

Agenda

7:30 am – 8:00 am Registration and Continental Breakfast
8:00 am – 10:00 am Sniffer
10:00 am – 12:00 am McAfee

Space is limited. Registration Deadline: **Thursday, Feb. 14th**

Return to Table of Contents

Feature Articles

Wireless Technology

As technology advances, you may be looking to expand your network to support wireless connections. Wireless technologies advance network computing to unmatched ease of use and convenience. When combined with PDA's or laptops it can make for totally mobile computing with the power to manage your network on the move. Though the potential is great, the current wireless Ethernet standards have some security problems that you need to be aware of before integrating wireless nodes into your Ethernet.

The most popular wireless Ethernet standard is 802.11b with its high-speed brother 802.11a. The 802.11b is a 11MB per second maximum transfer rate that operates in the 2.4GHz radio range. The faster 802.11a is a 54MB per second maximum transfer rate that operates within the 5GHz range. The wireless connections of 802.11 are piped through a wireless access point that then connects the nodes to your wired network. The access points will broadcast the Service Set Identifier (SSID), which is the network name. To use an access point, a wireless user must enter a SSID matched with a password that is then transferred in plain text. Once a network is up and running, administrators have the option of running Wired Equivalent Privacy (WEP) to ensure safe network transmissions by using encryption and access controls on node connectivity to the wireless LAN.

Now that we have covered the basics of how a wireless LAN runs, let's discuss the security issues concerned with each part. First of all, there is a huge inherent security concern in sending your network's data over the airwaves outside the confines of those tiny copper wires. Every packet sent over the network is broadcast to anyone within the range of your access point. When within the range of a wireless LAN, anyone snooping around can pick up the SSID of your network because it is sent out in plain text and broadcasted to the entire access point. The passwords that are matched with those SSID's may also be in plain text. If you're following along you'll realize that now any person snooping into the unencrypted traffic of your network has already gained enough information to hop straight onto your LAN without even entering your building or doing any real work.

Can we protect our wireless LANs by using WEP??? The sad answer is no. The current WEP encryption standards are based on RC4 encryption created in 1987 by RSA from 40 bits up to 128 bits. This was chosen because it is cheap to license and easy to implement. The implementation of RC4 used by 802.11 standards makes it quite weak and simple to crack. It has been demonstrated that the 40bit WEP implementations of RC4 can be

cracked open in as little as 30 seconds using programs that can be downloaded for free over the Internet. Even the 128bit WEP implementations can be broken in a matter of minutes with the same software.

So now how do we protect our wireless networks? First of all, find a good physical location on your network to place the access point. Find a place that will allow users to take advantage of the wireless setup and far enough away from the borders of your building so that no one outside can snoop your wireless traffic. Beyond physical protection, the system administrator needs to implement a way to securely tunnel traffic on the wireless nodes. IPSec is a capable protocol with built in support on Windows 2000. IPSec outperforms 64-bit WEP in benchmarks performed on 11mb/s wireless networks while adding heightened security. It can be difficult to keep good speed while implementing improved wireless security, so this is an encouraging statistic. Using any kind of VPN can help keep out unauthorized access. By separating your wireless access point from the wired network by a firewall, you can set up access to only allow VPN traffic into your network. Finally, it is good to try and snoop your own traffic to ensure that you are running a tight setup. There are programs on the Internet that will allow for sniffing wireless connections. IBM even offers a handheld solution to checking wireless security called "Wireless Security Auditor." For those of you still waiting a while until considering wireless, a new 802.11i draft is in the process of being standardized and will include a much better encryption system to ensure safety in wireless transmissions.

Wireless networks have great potential for future network deployments. I hope that this helps raise some concerns that should be addressed before implementing an unprotected wireless LAN. Insecure wireless solutions can leave a wide open door on your network to hackers while a secure setup will let you ensure safe traffic and add total mobile convenience to your users.

Jared McLaren

Useful Links for Wireless Issues:
http://www.80211-planet.com/
http://www.research.ibm.com/gsal/wsa/
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Critical Infrastructure Assurance - Interdependencies

One of the crucial issues in Critical Infrastructure Assurance is the concept of interdependencies. An interdependent system means that both systems are mutually dependent upon one another for successful operation and function. That may seem obtuse, but the following scenarios will hopefully illustrate the point.

Hypothetically: January 20, 2003
Let's say that there is a HUGE ice storm across all of Iowa, and that this ice storm took out much of our electric power grid. Due to the scale of high power lines down, the

electric companies say that it could be days before they can get the lines back up and running. In actuality, there is enough distributed electrical generation across Iowa so as to provide most communities with energy for daily needs, but let's suspend that actuality for this illustration.

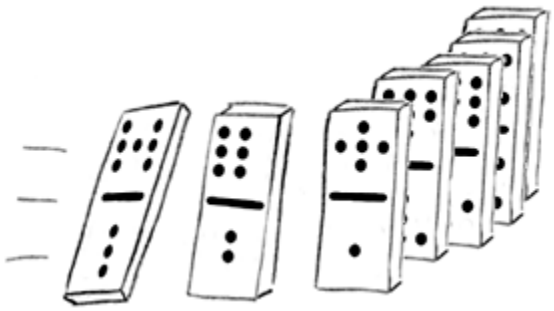
I am in my house, snug and warm in my bed reading Order of the Phoenix, the most recent Harry Potter book. Eventually, I tear myself away from the riveting story, turn out my bedside lamp and go to sleep. Early that morning, the ice storm hits Iowa, taking down the statewide electricity grid. At about 4:00 AM, I wake up to a freezing house. Heading downstairs with my flashlight, I can see my breath in the air, and check the thermostat for the furnace. Being a digital thermostat, there is no reading as there is no power to the house. Hmmm. I had not thought that the furnace would be affected by the blackout, as the natural gas system is still providing gas service to the area. Remembering a McGyver episode, I rig the thermostat with the batteries from my wife's Discman. Ah ha! We have a reading of 42 degrees. I wait, and I wait and I wait, but there is still no heat coming from my vents.

After further examination of the heating system, I can see that my furnace has no pilot light, but it is electrically ignited. So I cannot ignite the burner even if the system is getting the signal to turn on. For that matter, there is no electricity to run the fan that moves the warm air throughout the house. My wife would need MANY more Discmans with batteries to power that!

Later that morning, we decide to leave town to my in-laws house, as the battery-operated radio indicates that the roads are now clear for travel. My in-laws live just across the border in Minnesota, so it is only a couple of hours up I35 to a heated house!

The car is packed and ready to go. As we leave the garage, I notice that there is only a quarter of a tank of gas in the tank, not nearly enough to get us up to Minnesota. Not a problem! I know that the ATM at the Handimart will not be operational, since it runs on electricity, but I have cash so we can fuel up on the way out of town anyway. We get to the Handimart, and they are closed. There is a car leaving the pump area, and I flag her down. The woman in the car informs me that the gas pumps are electrically run, so there is no way for us to get gas out of the pumps. What do we do now?

This illustrates that there are many systems that depend upon one another, and many things that we take for granted. The illustration above was pretty straightforward and simple in its relations. The weather takes out the power lines, the lack of power leads to colder houses, gas pumps can't run, etc., etc. State Government takes threats like this very seriously. Iowa's Department of Natural Resources (IDNR) is mandated by the legislature to maintain and exercise the Iowa Energy Emergency Plan to addresses situations similar to the scenario above.



Unfortunately, not all interdependencies are as obvious and simple as the one above. For example, in 1999 the Worchester Massachusetts airport was unable to activate their

runway lights when a hacker took down the phone system that serviced their facilities. Who would have thought that the airport needed a public telecommunications network to activate their runway lights? The connection was certainly not obvious to me. One question that we in the Office of the Iowa Homeland Security Advisor are asking is "Where else do unintuitive relationships exist that could lead to a critical service being compromised?" This is just one of many difficult tasks that we must accomplish to ensure the security of Iowa's citizens.

Larry Brennan

Lessons Learned with Susie

(Lessons Learned with Susie is a new, ongoing fictional account of an employee learning, sometimes the hard way, about security awareness. The situations Susie finds herself in are quite common, and she, like all of us, finds new ways of practicing good security.)

I've now been working at my new job for a whole month! How exciting! I found that I have really helpful coworkers and a very understanding boss who wants me to learn all that I can, even if it is the hard way.

Everything was going great last Tuesday. I had finished my first big report early and was attempting to print it out to give my boss a hard copy when things went awry… I figured it would be more professional to print my report on the nice color printer. Unfortunately, after I hit print, I realized I had no idea where this printer was located. I checked next to the regular printer, but it was nowhere in sight. As I was looking around, another lady I'd seen around the office asked if I needed some help. I told her I was looking for the color printer, and she took me right to where my report was waiting. What a nice person!

I thanked her and went on my way back to my desk. When I got back to my computer, I began entering my username and password to unlock it. I couldn't remember locking it before I left, but I must have since it was now locked. I checked my email and saw there was a message from me! How odd! I didn't know I could get email from myself. I opened it and read the warning:

> "This message is from the Security Team. We were doing some physical assessments of your work area and found your computer unlocked and free for anyone to use. This is very dangerous due to the fact that anyone walking by has access to or can change not only your files, but could also access or change things on our company network. This access could be used to gain confidential information or to execute programs that can harm our computer systems.
>
> We used your own email account to send you this email, but someone else could have sent an email to anyone, saying anything they wanted, and it would look as if it came from you.

These are just a few of the security risks you are contributing to by leaving your workstation unlocked. If this practice of leaving your workstation unlocked continues to happen, we will be forced to take disciplinary measures to keep the company's network and information secure."

Wow! I never knew I could contribute to all of those security risks just by not locking my workstation while I was away from my desk for a few minutes. I never intended to be a security risk to my own company. From now on I'll always lock my workstation, regardless of whether I plan to be gone for an hour or only a couple minutes. It's very easy to get stopped by a coworker with an issue that needs to be discussed and not return to my computer for a while. This would give someone else plenty of time to access whatever he or she wants to on my computer. I would rather be safe than have someone compromise the company network because of something I did or did not do.

Amy Wilmeth

Return to Table of Contents

Linked Articles

Can PC sleuths dig up Enron data?
Paper shredding doesn't help cover tracks when most documents are originally created on a PC. Computer forensics should help investigators dig out deleted data from Enron's machines. (ZDNet, Feb. 4, 2002)

'Dangerous' hole discovered in Morpheus
Security experts warn MP3 fans that a security hole in the Morpheus file-sharing application could allow a malicious hacker to access a user's computer. (ZDNet, Feb. 4, 2002) (Note: Peer-to-peer file-sharing applications should not be used in the State network without the consent of the CISO.)

Vulnerability Assessment Raises Alarms
Data collected on cyber attacks during the past six months by a security firm that monitors corporate networks all over the world shows that companies in the energy industry suffer attacks at twice the rate of other industries, and many of those attacks appear to be sponsored by governments or organizations in the Middle East. (ComputerWorld, Jan. 21, 2002)

Update: Gates Wants Security Top Priority At Microsoft
Bill Gates, Microsoft's chairman, has issued a call to the software giant's 49,000 employees worldwide asking them to make "trustworthy computing" the company's highest priority. (ComputerWorld, Jan. 17, 2002)

Microsoft Coders Take a Month Off
Microsoft has announced that it has called a halt on new code creation during February as part of its move towards heightened security. (ITToolBox, Feb. 5, 2002)

Security, Now!
A new, bluntly realistic report underscores how insecure the nation's IT infrastructure is. Don't ignore the findings, and use them to help boost your organization's information security - recession or not. (ComputerWorld, January 14, 2002)

CERT: Security Incidents More Than Double In 2001
CERT said it received more than 52,000 reports of security incidents last year, compared with more than 21,000 in 2000. A CERT analyst explained the sharp rise as a result of heightened awareness by users. (ComputerWorld, January 11, 2002)

Port 12345: Hacker haven or Net X-File?
Increased activity on port 12345 could be due to hackers, an anti-virus product, or something else altogether, argue security experts (ZDNet, Jan. 22, 2002)

"Git Along, Little Virii"
This article explains how to protect your computer from dastardly attacks. (ITToolBox, Jan. 7, 2002)

Overview of new Federal Security Legislation
(Also includes ramifications to businesses, government, and the CIO perspective of these changes.) Fighting terrorism has put executives on the front lines to defend their company's IT infrastructure and help the government smoke out terrorists. But the rules of engagement are still emerging. (CIO Magazine, Jan. 15, 2002)

Despite more security spending, Internet a more dangerous place
Spending on Internet security continues to grow, yet the worldwide super network remains more vulnerable than ever to viruses, break-ins and terrorism.
Simply put, hackers are getting smarter, and computer networks are getting more complex and difficult to keep safe. (ITToolBox, Jan. 21, 2002)

Return to Table of Contents

Points of Contact

Kip Peters: Chief Information Security Officer (CISO), Enterprise Security
Consulting, enterprise security, policy, standards, overall security issues
515-725-0362

Marie Hubbard: Chief, Security Operations
Vulnerability assessments, intrusion detection, incident response, test lab
515-281-4905

Larry Brennan: Critical Infrastructure Assurance Coordinator
515-725-0365

Wes Hunsberger: Certified Business Continuity Planner
Business continuity, physical security
515-725-0361

William Hubbard: Security Awareness
515-725-0452

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/

The awesome Enterprise Security website. You can find tons of state or ITD security information here. Policies, procedures, guidelines, educational resources, lists of services, useful links, and more!

http://www.cert.org/nav/index.html

Homepage for CERT (Computer Emergency Response Team)

http://www.sans.org/newlook/home.htm

SANS (System Administration, Networking, and Security)

FBI and SANS List Top Twenty Vulnerabilities and Free Scanner

Security leaders from 30 organizations, led by the FBI's NIPC and the

SANS Institute published a list of the top twenty Internet security vulnerabilities (7 general, 6 Windows NT/2000, and 6 UNIX/Linux), along with instructions on how to fix them.

Iowa Homeland Security

This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more.

Return to Table of Contents

If you have questions or comments relating to this newsletter, or if there is a topic you would like to see an article on, please contact William Hubbard.
Cool artwork provided by Sam Wong.

The ISO Code:

Integrity…Service…Excellence