The Security Blanket

(Keep cozy with this Blanket!)

Volume 1, Issue 5, January 2002

In This Issue:

- From the CISO
  - Security Alerts
- Current Activities
- Helpful Hints
  - Email Hoaxes
- Upcoming Classes and Consultations
  - Lunch & Learns
  - Terrorism Conference
  - Security Courses
- Feature Articles
  - VPN Technology
  - Lessons Learned with Susie
- Linked Articles
- Points of Contact
- Links to Resources

From the CISO

This month's *From the CISO* column concerns something that we have to deal with every once in a while. One of the functions we provide is alert notification. We receive and process multiple alerts each day, and have to make a determination with each one on whether or not to send out a notice to the security, technical, or user community. Our sources include the FBI, various computer emergency response teams (CERTs), security Web sites and publications, other state governments, and other groups we are part of. We look at several things in order to make a risk determination: what systems are affected, what the vulnerability itself is, how sophisticated an attack would have to be in order to compromise a system using the vulnerability, and what the result might be. If we think the resulting risk to state computer systems warrant an alert, then we send it out via our Security Alert account so that those who receive it can key off the sender.

The reason we do this is because there are so many things that surface each day, if we were to send something out on everything, we'd be like the boy who cried wolf and nobody would listen to us when something serious came up. In addition, we'd spend so much time sending out alerts we'd never get anything else done. Finally, and most important, each and every vulnerability/virus does not warrant the trouble.

To make our jobs easier, we request that other personnel not send out alerts. Some people see something from the news and forward it on, but it is best to understand that CNN, MSNBC, ABC, (news/media/etc) are not good sources for information like this. While they may be able to raise the visibility of an issue, their information is almost always incomplete and blown completely blown out of proportion. Also, if multiple people propagate alerts, others would suffer from information overload. This is a serious problem in today's world – e-mail is very easy to use and inboxes can become very full. If something needs to be seen, we'd like it to have a good chance of surfacing among all the other mail. We also have to deal with something we call the false authority syndrome. If someone in a certain position, such as a technical or leadership position, sends out an alert or even says something, certain people will take it for the Gospel. The media holds that power over millions. We find ourselves responding to the false authority syndrome quite a bit, usually to soothe someone's mind, but also to defend ourselves as to why we didn't either know about the issue or didn't share it with others. In most cases, we already knew about it and have decided not to bother anyone.

We periodically receive alerts from those in the user and technical community. That is fine, and that is the way we would prefer to handle it. If you see something you think we may have missed, please feel free to forward it to our Security Alert account (securityalert@itd.state.ia.us) and we'll take a look at it.

Happy computing…
Kip Peters

Return to Table of Contents

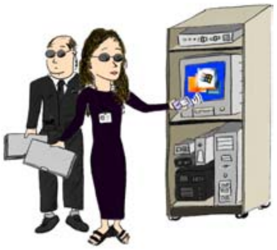
Current Activities

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 pending)

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

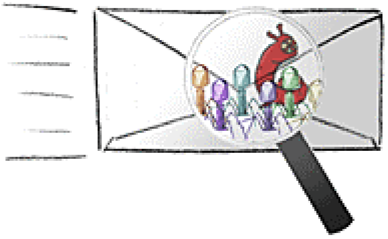
Enterprise Security Website

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 – Email Hoaxes

Is it butter or margarine? Is it an e-mail virus or a hoax? Its usually better in both cases to find out what it is before you get a real taste of it. The way you can determine whether a container holds butter or margarine is to look at the outside of the container, read it, or look for other clues on it. The situation is much the same with viruses and hoaxes. Email filtering at the email server can detect virus signatures and stop most viruses before they enter the network. It looks for and gets rid of most (99+%) viruses for us. Users also need to be willing to not open unsolicited e-mail and unexpected attachments to further reduce the risk of virus infection. Dealing with hoaxes, however, requires a bit different awareness and action on the part of the recipient.



Hoaxes often do not have a file attached to the message; they usually just present false information and try to get the recipient to take some kind of action. Results from this subsequent action may include deleting files (thus damaging the user's system), obtaining confidential information (like a user's credit card number), tying up network system resources, spreading false information, or the hoax originator may simply take perverse joy in sowing the seeds of chaos in our ever-increasingly electronically connected world.

So, how do you recognize a hoax? Well, the following guidelines on hoax characteristics should help you with that determination:

- ALL CAPS – for example: A CHILD NEEDS YOUR HELP
- Catastrophic results, usually in non-technical terms ("eats your hard drive")
- Sometimes a lot of techno-jargon
- A company like AOL or IBM reports it - neither of report viruses
- Asks you to send the alert to all your friends or everyone you know

An article from CNN's Sci-Tech also contains a good list of the Top Ten Cyber Hoaxes and scams since the Internet began. Some of these hoaxes have appeared in slightly different formats several times, and probably will do so again, so it's a good idea to become familiar with them. You can also visit sites like Vmyths.com, Hoaxbusters (CIAC/Dept. of Energy), or Symantec Virus Hoax List to learn more about hoaxes.

Remember, the best defense against hoaxes and is your own education, diligence, and healthy skepticism. It's not nice to 'fool Mother Nature', nor is it nice to fool people with hoaxes. Be forewarned and wary, and know what kinds of things can be spread around.

William Hubbard

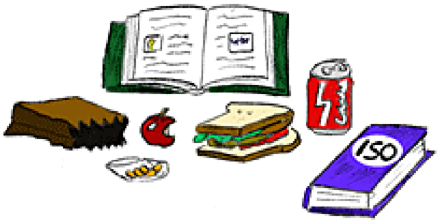
Return to Table of Contents

Upcoming Classes and Consultations

This section includes announcements of security training opportunities, classes, and conferences that are available to State of Iowa employees. Some events will be geared toward all employees, while others may be more appropriate for server administrators or security contacts. Also included are security-related links to vendor announcements for seminars.

Lunch & Learns

The Information Security Office continues its Lunch &Learn Program! These bi-monthly, informal get-togethers cover a variety of security-oriented issues. No sign-ups or registration is necessary, just come on down! The current schedule is as follows:



Date and Time	Topic and Location
Jan. 22 10:30am – 11:30am	Home Computer Security Grimes Bldg., South Conference Room
Feb. 12 11:30am-12:30pm	Vulnerability Assessments and Security Scans 1LC and 2LC, Hoover Building
Feb. 26 12:00pm-1:00pm	Business Continuity Planning Grimes Bldg., South Conference Room

Change of location or time will be announced via e-mail, and sent to departmental L&L security contacts. The past presentations (Introduction to the Information Security Office, Critical Infrastructure Assurance and Cyber Terrorism, Top Security Issues for Windows 2000, and How Attacks Are Perpetrated Against Us - 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.

Terrorism Conference

January 16, 2002. STARC Armory, Camp Dodge, Johnston, Iowa. Sponsored by EMD.

Topics and presenters currently planned include:

Public and Private Partnerships	American Red Cross
Cyber Terrorism	ITD, State of Iowa
FEMA's Updated Responsibilities	FEMA Region VII, Eric Jenkins
Public Health Support for BIO Terrorism	Iowa Dept. of Public Health
Civil Support Team	LT. Col. Dan Robbins
Terrorism Planning	IEMD, Dan Lee
National Pharmaceutical Stockpile "Thinking outside the box"	CDC, Steve Reissman
Training and Exercises	Connie Gilbert
Incident Command/Unified Command	Chuck Eddy and Scott Siberski
Facilitated WMD Tabletop Exercise:	DOJ Tech Assist from contractor.

To view the Conference Flyer and Application, see: http://www.itd.state.ia.us/security/education.html#conference. Other questions? Contact: Thomas Baumgartner.

Security Vendor Announcements

Interested in SANS Conferences? See http://www.sans.org/ for details on courses, locations, and dates. (SANS is one of the foremost security educational programs.)

Windows 2000 Security - *Hands on Technology Transfer Inc. (2/5/02)*
Date: February 5-26, 2002
Location: Various Cities

This hands on Windows 2000 Security training class will allow the students to understand the main issues arising from the Windows 2000 security model. Many security weaknesses are exposed and the students get to identify what steps can be taken to eliminate the security risk. Advice will be given on set-up and system auditing processes to assist the administrator in trapping passive and active attacks from external and internal threats.

ITD's Knowledge Access also 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 detail and pricing information.

Return to Table of Contents

Feature Articles

VPN Technology

Virtual Private Networking is a technology that allows the transport of data through a foreign network, most often the Internet, to another network in a tunnel that will not allow anyone on the foreign network to see the data in the VPN. VPN's can be deployed from a very small scale to a very large scale.

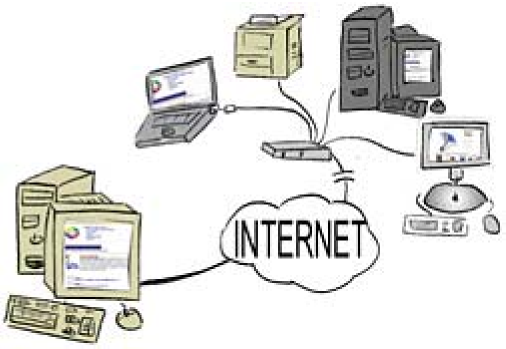
The common theme in all VPN's is the desire to save money. Bandwidth costs are one way to save money. The most expensive part of a wide area network is almost always the ongoing cost of circuits. A point-to-point circuit (which can connect one remote network to another) is most often more expensive than an Internet connection. The cost difference becomes more pronounced as distances increase. It also may be possible get DSL or broadband Internet connections in remote areas (often residential) where carriers do not currently provide other services, such as point to point circuit availability.

Another common area of cost savings is that of managing a dialup service/modem pool for remote users. By utilizing a VPN, networks may reduce the number of modems required or eliminate them altogether. This also brings the possibility of saving money on toll or 800 phone charges if the remote users have access to an ISP that is a local call to the remote user. When this is the case a remote user may be able to get unlimited access to the network for the price of an ISP connection, which is often $20 a month or less. A small office might be able to get a DSL connection to the Internet, often $100 or less, and substitute this for a fractional T1 that may cost several hundred dollars per month.

Types of VPN's

VPN can be deployed to connect many different devices. One of the most common devices is a dedicated device called a VPN Concentrator. This device is designed and optimized for the maximum encryption/decryption of traffic passing through it. VPN's of VPN tunnels, as they are often called, can run from a single PC to a VPN concentrator, between two VPN concentrators, or from a firewall to a VPN concentrator. There is also a version of Cisco router software that will allow the router to serve as one end of the VPN. There are several more combinations of the different types of endpoints mentioned above.

All the different combinations either break down into a user-to-LAN or LAN-to-LAN connection. The user-to-LAN connections are the most common and the simplest. They consist of client software on a PC that establishes a connection to a remote network through a foreign network. The remote network device can be a router, firewall, or VPN Concentrator and the connection will function pretty much the same with similar security concerns. The difference among these will be in the performance and speed available for the connection. In a LAN-to-LAN connection either endpoint can be any of the devices listed above, and as above the main difference will be performance.



Mechanics of the VPN

VPN's can be implemented with several different protocols. One of the most common is IPSEC, short for Internet Protocol Security. Other common protocols are Microsoft's Point to Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP). Each of these is actually a group of protocols that provides the tools necessary for a VPN. All these solutions use well-known encryption methods. The IPSEC protocol suite was developed by the IETF (Internet Engineering Task Force - this is the standards body responsible for Internet standards) and not surprisingly exceeds the others when it comes to interoperability. For that reason it is becoming the most common. IPSEC is used in the ITD VPN solution.

The ITD VPN solution is designed for maximum availability. Dual VPN concentrators are deployed and are protected by dual firewalls. For this reason any part of the solution can be taken down for maintenance without disrupting users. If either VPN concentrator or either firewall fails the redundant component will take over seamlessly. It is also designed to scale to a large numbers of users. Unlike a firewall or router, which uses the main CPN for encryption/decryption, VPN concentrators have dedicated processor modules to perform encryption and decryption. If the concentrator approaches capacity another module is simply added. The ITD solution can be seamlessly expanded to four times the present capacity in the existing chassis.

VPN Security Concerns

Vigilance is the order of the day. When deploying a VPN, a network is actually being extended to include the remote device. It is important not to view a VPN as an end all solution to security. It really only provides encryption through a foreign network, and to an extent, some authentication. It does little or nothing to protect against what may be done using the devices that the network has been extended to include (a remote PC, for example). There are somewhat different security concerns for user-to-LAN and LAN-to-LAN VPN's. The user-to-LAN connection involves a VPN client, which operates directly on the device communicating and may provide some additional protection against intruders. The LAN-to-LAN VPN typically starts at the border of a network and terminates at a remote network. In this case the two networks could potentially have access to everything on the other network. The VPN simply encrypts the traffic as it moves through the foreign network.

In the case of a remote field office, all the normal concerns of physical security in a remote office are still valid, just as if the traffic came in on a dedicated circuit. While the incoming traffic is encrypted, this in no way lessens risks associated with a remote office. These risks might include, but are not limited to things such as relaxed physical security and unattended PCs during the day, or a remote office that is not staffed around the clock. These concerns are not unique to a VPN connection, but they can be forgotten or neglected if VPN's are thought of as "secure".

All of the concerns that apply to a PC on a local LAN are just as important with a VPN as well. For example, it makes no sense to allow PC's without virus software to access a network through a VPN, just as it is unwise to allow an unprotected PC to have a direct connection to a network. As soon as any unprotected PC connected to a network it could infect other devices on the network.

In addition to all the concerns that any other circuit would bring there are some additional concerns with the VPN. One concern would be that since there is exposure to a foreign network someone could break in through the VPN. Wherever there is exposure to risk someone will eventually attempt to break in, so careful management of passwords and keys are essential. Monitoring of failed attempts and disabling of associated accounts can mitigate this risk. Token-based security for individual users' VPN connections strengthens authentication.

Another risk is a technique called split tunneling. This would allow an authorized user to use the connection to the Internet while at the same time accessing the VPN through the same Internet connection. This is recognized as a significant risk in the industry. If a PC using the VPN is compromised, the intruder could then use that PC to attack the main network because the PC would be authenticated through the VPN and would appear to be a legitimate user.

Conclusion

A VPN can be a versatile tool to help in managing your communication costs while enabling staff to have access to information. Individual users can use a VPN instead of expensive dial-up connections. A LAN-to-LAN may be able to replace a small office dedicated connection with a less expensive Internet connection. Contact the ITD Networking Team if you have questions or comments regarding this service.

Dave Rowen

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.

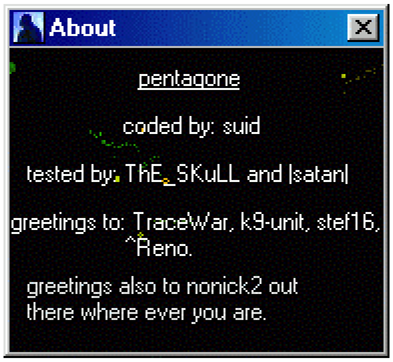
Lessons Learned with Susie

What a week it has been. The first week on a new job is always crazy. Learning a whole new system and not messing things up, at least not in front of the boss. That was my goal for the week. It started out pretty well, but on Wednesday things got a little hairy.

I started the day checking to see if I had received any email messages. To my surprise I did have an email waiting for me! It was from someone that sounded familiar, but I just couldn't place the name as anyone I knew. The subject appeared as "Hi", so I couldn't get any information there. I figured it must be the name of someone in the company that I couldn't remember, so I opened it.

The following message appeared: "How are you? When I saw this screen saver, I immediately thought about you. I am in a harry, I promise you will love it!" It had a screensaver attached called gone.scr.

That made me curious. Who here at work knew enough about me to know what I liked? What made them think of me? I had to know, so I clicked on the attached screensaver. A box popped up with what appeared to be a credit to the authors, but then an error box came up. As I clicked to get rid of the box, I vaguely wondered if this could be one of those viruses I had read about. I dismissed that thought, quickly telling myself that would never happen to me.



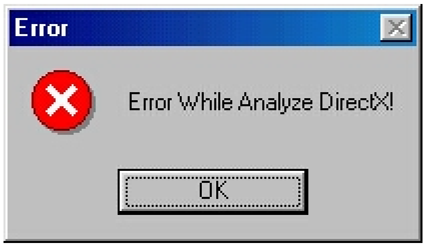
pentagone

coded by: suid

tested by: ThE_SKuLL and |satan|

greetings to: TraceWar, k9-unit, stef16, ^Reno.

greetings also to nonick2 out there where ever you are.



Error While Analyze DirectX!

I continued reading my email and saw another message from my boss. It was a message he had received from the security department about a new email virus that had made it past the firewall and the virus detection program. As I read the warning, a sense of dread began to build in the pit of my stomach. This was describing the very email I had received. I noticed under “Ways to Detect the Virus” that the subject line of this virus-infected message would be “Hi”, and there would be an attachment called gone.scr. Uh-oh, that worried me even more. But then the alert also said that other employees might reply to virus messages and inform the person with the infected workstation, as well as the security department, that their system had been hit. No one had contacted me! Maybe I didn’t activate it! A sense of relief washed over me as I blew a huge sigh of relief.

Then I noticed I had more email. Twelve new messages in fact. I counted five of them with the subject “Hi” from people I didn’t know. I wasn’t about to open those after being warned about the Goner virus. Then I noticed the other emails had subjects like “You have a virus” or “You sent me the Goner virus.” Then my phone rang. I regretfully answered the phone, and the caller identified herself as a member of the security department and said they had received reports that I was sending out the new virus. I reluctantly told her what had happened. She told me not to do anything else with my computer and someone would be there to get rid of the virus for me.

It seemed simple for the tech person to fix the problem. It took him only a few minutes to get the virus detection software running again, which the Goner virus had uninstalled, and get rid of the virus for me. It was pretty embarrassing to send an email virus to the entire company my first week on the job. My boss seemed to understand how awful I felt. He just told me that, even though I and a few other people had opened the virus, it could have been much worse, and that for my sake he hoped I had learned an important lesson on email viruses. Believe me I did - I won’t be opening any more mysterious email attachments!

Amy Wilmeth

Return to Table of Contents

Linked Articles

Open-Source Security Tools Gain Favor
Open-source security tools are gaining appeal in the enterprise as IT managers and CIOs search for ways to step up security while holding down costs.
Many of the tools have been available for years and are used in niche environments or small offices. But only recently have enterprise MSSPs (managed security service providers) begun incorporating them. (ZDNet, Jan. 8, 2002)

Instant Messaging Viruses Set to Soar
Antivirus experts are predicting that Instant Messaging will become an increasingly popular way to spread computer viruses, and warned companies that they face more of the same dangers that struck during the first half of last year. (ITToolBox, Jan. 2, 2002)

Security: IT Locks Down
This year, some of America's most forward-looking IT security managers will be responsible for rewriting the book on corporate enterprise security and helping to guide their industry colleagues through the uncertainty of the year ahead. (ComputerWorld, Jan. 1, 2002)

Homeland Defense and Crisis Management Conference: Info Sharing
Panelists at the Homeland Defense and Crisis Management conference said local, state and federal law enforcement agencies, intelligence organizations, and government officials at all levels need to share information to forestall future terrorist attacks. Certain obstacles need to be overcome, however; groups use differing methods of communication, radio frequencies and terminology. (ComputerWorld, Dec. 19, 2001)

The Survivors Guide to 2002
Security is a process, not a product. And it touches every aspect of an organization. Yet security is often an afterthought. Even worse, some organizations' idea of security is the firewall sitting at the network edge or the virus scanner integrated into the mail servers. Security is none of these things. Security is an approach to allowing authorized access to resources. Resources can be a Web page, an FTP site or access to the central computing facility. It should be obvious that with the wide variety of entry points into your network, a layered approach to network security is required.

Professors Hash Out Cyberterrorism Strategies
Although the potential for cyber terrorism continues to grow, terrorist groups now use the Internet more to distribute information about attacks rather than to carry them out, Georgetown University information security expert Dorothy E. Denning told a crisis management group Thursday.

Quantum Cryptography Moves Forward
The possibility of quantum cryptography has taken an important step forward with the development of a device capable of emitting single photons. (BBC News, Dec. 13, 2001)

Intrusion Detection Systems

This article describes how intrusion detection systems (IDSs) enhance network security infrastructure, explains the difference between host- based and network-based systems and enumerates IDS detection techniques. (Security Focus, December 6, 2001)

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