Charles Rhodes GSEC

The Internal Threat to Security
Or
Users Can Really Mess Things Up

On one hand, the media is replete with reports of hackers exploiting various weaknesses in order to gain access to a network and the data it houses. Most, if not all, network administrators and engineers secure their intranets against outsiders these days. On the other hand, many administrators and engineers don't do the same thorough job of securing network resources against the people in the best position to do the most damage to a network, the legitimate users of the network. This paper will outline some of the threats posed by the "insider" and safeguards against these threats.

The following paragraphs describe some of the security measures you can implement which will help insure the availability of your network despite the users actions. These chapters are broken into several categories, which are: Data input security, basic security controls, session security, Internet security, physical security, desktop security, data security, and malicious activity.

DATA INPUT SECURITY

One threat area is data input. In today's "collaborative" world, many industries rely on the accuracy of data input into specialty or home grown software solutions which feed databases. These specialty programs are generated and maintained specifically for the given business or corporation. These applications have not undergone the rigorous testing and subsequent trial-by-fire of similar off the shelf solutions. As a result, the specialty program may not be as robust or "bullet proof" as it's off the shelf cousins. Examples of this threat can be seen in typos, stuck keys, and incorrect or incomplete data accidentally or intentionally entered. The results can range from inaccurate or incomplete data to crashing the entire program.

While obvious, the best defense against this threat is often difficult to implement. All programs, whether off the shelf or home grown should be thoroughly tested and some form of change management enforced. Additionally, during the engineering of these applications special attention should be paid to the following areas:

- Narrowing Data Types: In requirements documentation data types are spelled out. In the absence of formal requirements, ask the user or manager. These data types should be narrowly defined in the code. If a specific field requires a non-negative integer between one and one hundred, the code should not use a long floating-point variable. Similarly a field requiring a word or name should be checked to ensure it is within a reasonable length. Few words or names are longer than 20 characters. Additionally, the code should check to ensure the input is in that range and give the user a helpful error message if it isn't. While this is a classic buffer overflow vulnerability, it is often overlooked. Additional information on buffer overflows can be found at the Network Magazine web site at: http://www.networkmagazine.com/article/NMG20000511S0015 (1)

- Limit User Input Capability: A good way of insuring the user does not input invalid data is to use checkboxes, radio buttons, canned queries, dropdown lists, or other non-text based entry devices where possible. This solution is often employed in web pages with great success. Not only will this solution allow for better accuracy of data, it tends to speed up data input, thus saving time.
- User and Programmer Education: During the design process, the programming staff should listen to the users as well as management. This will keep the users from attempting to find ways around a product that does not fulfill their needs. Additionally, users must be trained on the application as it relates to their position. Users can be expected to incorrectly use an application if they have not been shown how it works. Simply handing someone a quickly produced user manual should not be considered training. A training plan should be produced and given to all users of the application consisting of both documentation and hands on training.

People are curious by nature. Users are no exception to this rule. However, when networks shares are involved curiosity is not a good trait. Users can and will browse network shares. This browsing may be just to see what is there. Or, it could be for more sinister reasons such as corporate espionage.

Regardless of the reason, this activity must be reduced to a minimum and controlled. The resulting information leakage could include coworker's salaries and personnel files, credit card numbers, proprietary company information, or medical record. The legal concepts of Due Diligence, and Due Care hold corporate officers responsible for the information under their employee's control. These legal concepts are evident in the Health Insurance Portability and Accountability Act (HIPPA), and title 5 of the Gramm Leach Bliley Act. (2) (3)

In order to provide sufficient security for the data on a network while legally protecting the company, several issues must be addressed. The extent and severity of the security controls in place must be dictated by the sensitivity of the data. Additionally, the security controls must be balanced with the usability of the system. While it's true that the only secure system is one that is still in the box, this system does not offer any benefit. It is a tradeoff that must be handled and "tweaked" to the needs of each organization.

BASIC SECURITY

The appropriate security measures to prevent network-browsing range from administrative policies and procedures to technical controls placed on the data itself. Some possibilities are:

- Acceptable Usage Policies: During the hiring process most companies have new employees sign certain agreements. These agreements range from medical benefits to expected codes of conduct. This orientation process is an excellent time to have the user acknowledge and sign an acceptable usage policy that states the user is not allowed access to data that does not pertain to their job. Additionally, both Windows and Unix systems offer a log on banner or message of the day.

These can, and should, be used to remind the user of acceptable usage policies. In order for these policies to be affective, they must be accepted, supported, and enforced by upper management.

- Strict access rights: Simply telling the users not to look at certain data is not sufficient to meet the due diligence standards imposed by law. These standards dictate restricting access via either discretionary or mandatory access controls. However, both Windows and Unix systems don't do a good job of restricting access out-of-the-box. The administrator must set them up correctly. Good examples of this fact are the Windows "Everyone" group is given full permissions to all directories and files by default, and the Unix operating system frequently uses a file "mask" of 755 which produces read and write access to files by default.
- Implement Security Restrictions: Plan for and activate all security restrictions prior to placing new resources online. In the rush to implement new systems, many companies will setup the system and start using it prior to securing the system. This temptation must be resisted in order to ensure the system is secure. Once users are given access to something, taking that access away is often a politically difficult and administratively cumbersome task.
- Periodically verify access restrictions: Once established, these access rights and restrictions must be verified. Users and administrators alike will create files and directories that do not have proper access restrictions in place. These security weaknesses must be identified and corrected periodically. One alternative to manually dumping the access control lists for each server and computer are group policy objects in Windows 2000. Group policy objects can enforce the desired security settings throughout the domain. Likewise Unix users user, group, directory, and file level permissions should be manually reviewed. If access is a paramount concern you can implement proprietary programs such as "Suid" which adds defensive layers to your system. Explanations of setting permissions in the various file systems can be found at:
  - Linux http://www.userlocal.com/secfileperm.shtml (4)
  - Unix http://www.mcsr.olemiss.edu/unixhelp/tasks/access_permissions.html (5)
  - Windows http://www.utexas.edu/its/windows/resources/secure.html (6)
- Audit Logs: Once access controls have been implemented, auditing should be used to ensure users are adhering to them. Successful and failed login and file access attempts should be recorded. Almost all systems have some form of security logging capability today. Many network designs provide security logging of various activities on these machines. Often there is no mechanism in place to securely archive and maintain these logs. Detailed documentation of all activities to be logged and a log management plan must be in place prior to standing up the network. Today's operating systems are capable of generating logs reaching into hundreds of megabytes per day in an uncompressed state. In order to use these logs effectively they must be centrally maintained in a way that will guarantee they are genuine and have not been tampered with in any way. Additionally, a mechanism must be in place that will provide for manually reviewing these logs. The most thorough logging combined with good log management does no good unless the logs are actually reviewable. There are Windows products on the market such

as EML log manager, or Sun's "Proudat –l<logname>" Unix command, that will help with this task. http://www.tntsoftware.com/support/WhitePapers/ELMSecurity.pdf (7)

- Encryption of Sensitive Data: In addition to restricting access via access control lists, some data may need to be encrypted. The act of encrypting data is becoming more user friendly. Windows operating systems and most relational database management systems now natively support data encryption. Additionally, there are many Unix encryption programs commercially available such as PGP, MD5 etc. While encryption increases the load on hardware, it is often worth the added expense to protect.
- Segregation of Sensitive Data: Finally, if assigning access controls or encryption isn't sufficient, the data may need to be segregated from other less sensitive data. This can be achieved in several ways. The data may be placed on separate servers on a different LAN. The data could also be placed on a separate subnet protected by IP address filters on the router or server handling the data. SSL connections with authentication architectures can be used to segregate the data as well.

Once security is in place and audited, the network administrator and / or security professional must keep a watchful eye to ensure the security measures are not avoided or subverted. These same professionals must remember that most users who avoid or subvert security measures do not have malicious intent. They are merely attempting to do their job with as little inconvenience as possible. As a result, a heavy-handed response in this department can be counterproductive. So remember, unlike computers, users typically don't like to be told what to do.

SESSION SECURITY

Some of the many problem areas in security that tend to be avoided or subverted are passwords, unauthorized devices, and quick fixes by help desk personnel. Passwords are often weak, reused, or written down. They can be shared between employees, or the user may simply never log out. The issue of unauthorized devices is exemplified by user installed modems or wireless devices. While help desk personnel are often bullied into providing users with improper access or assign access rights too liberally. Some methods to identify and correct these weaknesses are:

- Password Policies: The lifetime, complexity, and reusability of passwords can be dictated by the operating system. These password attributes should be set prior to placing the system in use. However, there settings should be a balance between security and the user's ability to log on. Passwords that are too complex or changed to often will result in increased user lock out and user complaints. A good overview of the problems associated with passwords can be found at http://www.smat.us/sanity/pwdilemma.html (8)
- Automatic Session Termination or screen lock: A good defense against users leaving unattended computers logged-on is automatic log out settings or screen savers that require a password. These measures are both easy to apply, and add security to an office environment where distractions take people away from their computers often. This policy can be set at the domain level to ease the administrative burden.

- Password Cracking: The same programs used by hackers to attempt access to your network can be used to verify the complexity of passwords used on your system. These programs should be used judiciously. Additionally, the cracked passwords are also highly sensitive data that should never be stored, especially on your network. A good starting point for cracking passwords is the password cracking FAQ file located at: http://www.password-crackers.com/pwdcrackfaq.html (9)
- Hardware Verification: If a LAN or WAN solution is in use, all modems should be removed or disabled on workstations prior to placing them in service. Users should not be given the administrative privilege necessary to install these devices. Additionally, workstations should be periodically surveyed to ensure users have not installed these devices. There are many software packages available to assist in this inventory process. These packages can be centrally managed, and detect changes in hardware profiles.
- War-Dialing / War-Walking: These practices will detect devices missed by hardware verification procedures. Periodically all analog telephone numbers within the organization should be dialed to ensure they are not hooked up to unauthorized modems. This process can be automated using war-dialing software. Additionally, the telephone bill for the organization should be reviewed to ensure a complete list of phone numbers is used. The practice of war-walking is designed to detect wireless access devices. By "walking the halls" with a laptop equipped with a wireless network card, wireless access points can be located with ease.
- Security Education: One of the often-overlooked solutions is education. This includes initial training and mandatory periodic refresher training. Many users are unaware of the security measures in place or the reasoning behind them. Once informed of these details users may be less likely to subvert these security measures. The training provided should be tailored to the audience. Network administrators and help desk personnel should be given more in depth training than users. This training can range the gambit from formal classes to organization wide emails and pop ups.

INTERNET SECURITY

Another touchy security issue facing network personnel is web surfing by users. The Internet has permeated modern society. This fact is evident by the number of Internet connected computers in homes and offices all over the industrialized world. This Internet connectivity can be productive by allowing workers to look up data such as addresses, phone numbers, driving directions, or research data. However, this access must be controlled and safeguards must be in place to ensure it remains productive.

If these Internet connections are not controlled, productivity may actually decrease. Instead of working, users may choose to surf the Internet instead. This web surfing not only reduces that employee's productivity, it uses bandwidth and hard drive space that may be needed for legitimate business purposes. This misuse adversely impacts other employees who are attempting to conduct legitimate business. While the bandwidth issue is often easy to see, the hard drive space taken up in temp files is somewhat less obvious. Over time, these files can, and will, build up to the point of impacting the system; especially if file servers are used for home directories.

Any Internet access opens the network to infestation by viruses, trojan horse programs, and worms. Most people are aware of the existence of viruses and propagation of email worms. However, they may not be aware of the dangers associated with web surfing. Users may not realize that clicking on a link may surreptitiously download a malicious program. If they do realize this fact, some of them may be willing to take the risk; or have been lulled into a false sense of security by the antiviral software loaded on their workstation. By it's very nature, antiviral software is reactive. When a new virus is discovered, the software is updated to identify it. Under the best circumstances there is a window of vulnerability on your network.

Web surfing by employees can also pose a legal threat to the organization. These employees can download pornography or copyrighted material such as songs or programs. While it's generally understood that business computers should not be used for pornography, many employees do not see the harm in storing music on company computers. File-sharing software such as napster opens more avenues of attack on your network. Additionally, if this music is copyrighted it opens the door to legal question most companies would rather not face. These issues arise out of the Digital Minimum Copyright Act of 1988 (10)

These risks do not outweigh the benefits associated with allowing users access to the Internet. Internet connectivity must be safeguarded to keep it from impacting productivity. In order to ensure Internet connectivity is used in a safe and productive way, several steps may be taken:

- Limit Surfing Capabilities: By limiting the capability of users to surf the Internet many threats can be avoided or minimized. Proxy servers are a solution designed specifically for this task. Today's proxy servers can be finely tuned to allow granular control of users and groups. Specific groups of users can be allowed access to specific sites or domains while denying Internet access to others entirely. Microsoft's Internet Security and Acceleration server is a good example. Unix users often implement a firewall system such as Gauntlet (CAI) that controls protocol, port, domain, and IP access to and from your network.
- Antiviral Software and Updates: Any network should have antiviral software installed and regularly updated. A properly implemented antiviral plan should include automated virus warnings from vendors and a daily review of vendor cites for new virus definition files and information. All servers and workstations should be routinely scanned for viruses. Mail servers should automatically delete or quarantine the suspicious files and forward a message to the recipient or sender. In addition, scanning should include cross-platform searches for viruses. Most antiviral software allows for automating the scan and update processes. The automation of these processes should be documented and followed. Additionally, periodic random checks of workstations should be used to ensure they are being scanned and updated.

- Scan for Unauthorized Files: If music files are not allowed on the network, scripts can be used to identify known file extensions such as MP3 or AVI. The results of these scans can be fed into a file which should be manually reviewed to ensure they are not a false positive and provide documentation in the event an employee must be counseled.
- Close Ports: Closing ports associated with Trojans, files sharing software, and backdoor programs may reduce their impact on your network. This should be done on the border router between your network and the Internet. In order for this approach to be effective, the list of suspect ports must be periodically reviewed against the configuration on the router. A listing of ports can be found at the Internet Assigned Number Authority. http://www.iana.org/assignments/port-numbers (11)
- Internet Activity Monitoring: Software is available which will monitor and document Internet usage. Depending on the product, this software can discreetly monitor or overtly block access to specific sites. Examples of this type software are Net Nanny and Big Brother for Windows based networks and Gauntlet for Unix.
- Acceptable Usage Policy: Users should be informed of exactly what is considered acceptable and unacceptable usage of their Internet access privileges. This training should be part of the new employee orientation process. Additionally, a user acknowledgement form should be signed by all users of the network to ensure they have been informed and understand the policy.
- Hard Drive Cleanup: If the operating system does not automate the cleanup of "temp" folders or temporary Internet files, scripts can be employed to automate the task. An example of this is the /sageset switch that automates disk cleanup in Windows 2000.
- Internet Kiosks: A final alternative is to place Internet access from kiosks or shared workstations through the organization on a separate network. This will allow the legitimate usage of the Internet while reducing the threat to your production network. This solution is expensive, but has the effect of reducing Internet surfing to a minimum.

PHYSICAL SECURITY

The physical placement and security of LAN wiring and hardware represents a potential problem when users are added to the scenario. Users have been known to use overhead LAN wiring as close rods, hanging their coat on it. LAN wiring running along the floor, especially under carpet or rugs is at risk as well. Users will inadvertently roll over the wires with chairs or walk on it until the wiring shorts out.

Wiring closets represent another area of concern. Employees often use wiring closets as storage bins for mops, brooms, or coats if nothing else. If allowed access, employees may add LAN drops or move their drop from one port to another as they see fit. While typically not done maliciously, this represents a threat to the security of the network especially if VLANs are in use.

In order to protect the network against these risks, several steps must be taken:

- Physical Restrictions: All remote network equipment should be placed in wiring closets. These closets should be locked with either a cipher lock or a key that is controlled. If this isn't possible, a locked network rack should be used.
- Wire Management: All network cabling should be run in the ceiling, walls, or under raised floors to keep it out of the way. Wire should never be taped to the floor in accessible locations. If a patch cable needs to be ran along the outside of walls, it should be attached to the baseboard if possible.
- Configuration Management: All wiring and port assignments should be properly identified and noted on a schematic diagram. This network mapping should be maintained and updated any time the network is modified. This solution will help ensure network drops stay where they are placed. It will also assist in planning for future growth and troubleshooting issues as well.

DESKTOP SECURITY

The desktop represents another avenue for problems to creep into the network. Users have been known to delete files either on their desktop or from file and application servers. Additionally, users will often modify environmental variables and / or load software from outside the organization. Once again, these acts are typically not done with malicious intent. However, at a minimum, they will increase help desk utilization, often for applications that help desk personnel have not received formal training on.

In order to protect users from causing these problems on your network, their local desktop privileges should be controlled. This control is often politically easer to implement at startup before the users grow accustomed to those privileges. Good configuration management will allow the implementation of these controls with the least amount of manpower. These controls include:

- User Rights Assignments: Following the concept of least privilege, users should never be granted any more access to the local desktop, or network system than they need to do their job. While this may seem harsh, it will go unnoticed if done correctly. Users should not be allowed to load programs on the local machine.
- User Access Restrictions: Users should not be allowed the necessary permissions to delete files they do not author or own. In many cases, the default file permissions are applied to local systems and network shares. These permissions allow full control to everyone on the system. They should be modified or locked down to ensure only the proper individuals or groups have the ability to delete the files or directories.
- User Education: Educating the users to the dangers of bringing outside applications into the work environment may alleviate some of the issues associated with this activity. At a minimum it will inform them that this is not acceptable behavior.
- Disabling removable drives: If the situation warrants, floppy drives and CD-ROMS can be disabled or removed. An alternative is to control access to these devices via hardware or software.

DATA SECURITY

Another problem worth noting is the user who becomes a pack rat. These are users who never delete anything. They save all their mail and old files without any regard to the size limits of their hard drive or network shares. While it's true that data storage alternatives continuously get larger and cheaper, file sizes have more than kept pace. These days it isn't uncommon to see a Power Point presentation with a file size over 10 megabytes. Video files are often larger still. It doesn't take long for these files to build up on a hard drive or network share. In addition to single files building up, users often email multiple people copies of these files. This replicates the file when people download it into their hard drive as an email attachment. Additionally, if the data is being stored locally on the hard drive it probably is not being backed up. Should the local hard drive fail, the user and organization will loose that data.

Storage isn't the only part of the system with size limitations. Once users personal mail files get too large, they become unstable. Microsoft Outlook is one example. The mail package has been known to become unstable and start crashing with a gigabyte of data stored locally.

Some of these emails and files probably need to be kept on line and readily accessible. Others may need to be kept for historical value or other purposes. Many of them are not needed at all. A determination needs to be made on each file. It is not possible for the administrator of a network or help desk personnel to make these decisions. However, the users can be encouraged to make these decisions by implementing the following solutions:

- Local Hard Drive Lockdown: The access control list for the local hard drive can be manipulated to keep users from storing data where it does not belong. While this approach is not foolproof, it will discourage many users from writing files outside of a central location.
- Centralized Storage: Users main document storage can be redirected to a central location under some operating systems. On other operating systems the users can be given a drive mapping to file storage servers with the appropriate permissions on each user's folder. Many programs can also be configured to store data on remote servers as well. This will centralize the problem and allow for backup of the data.
- Drive Storage Limits: The amount of storage allocated to an individual user can be tracked and capped at a predetermined limit or quota. These disk quotas encourage users to police their own files.
- Offline Storage: Offline storage can be implemented for files of historical value or other data that is not often used. This offline storage can be as elaborate as storage area networks or magneto-optical drive or as simple as a CD writer. Old emails can be burned to a CD-ROM and deleted out of the user's mailbox. This will reduce the size of the mailbox and allow access to the old emails when needed.
- User Education: Educating the users about the dangers of storing information locally will encourage more utilization of centralized storage. Additionally, teaching users how to send a link to documents instead of sending the document itself will reduce replicated documents on the network; thus reducing the problem.

MALICOUS ACTIVITY

While far less likely than the situation already stated, malicious activity by users must be guarded against as well. The likelihood of this type of activity is low; however, the possible damage is tremendous. Corporate espionage and monetary theft are two prime examples of the harm users can do. However, these headline-catching activities are just the tip of the iceberg. Disgruntled employees are capable of deleting files, encrypting files, or modifying the data contained within them. (12)

In addition to the solutions outlined already, there are several security precautions that can be taken to minimize the possibility of this type activity occurring. Or if it does occur, assist in detecting it.

- Separation of Duties: By dividing duties of employees you can minimize the number of people who are in a position to conduct these crimes by themselves. The fact that someone would have to conspire with another employee in order to commit these types of crimes provides a strong deterrent.
- Employee Exit Procedures: The opportunity an ex-employee has to damage data on the network must be minimized. Upon termination, all employees should follow a standard set of procedures that include removing their access to all systems. These procedures should be followed regardless of the terms of the termination. Additionally, warning an employee that they are going to be terminated on a specific date gives that individual an opportunity to cause harm. Thus employees should not be forewarned of this activity.
- Background Checks: By implementing a policy requiring background checks for all employees during the hiring process, individuals with a history of criminal behavior can be screened out. This will reduce the chances of it occurring in the future.
- Screening Outbound Email: Email can be screened prior to releasing it out of the confines of the organizational network. This screening can look for key words indicating possible information leakage.
- Tripwire Programs: Tripwire programs make hashes of all key executables on a system. You store these hash figures on another machine and periodically compare them against the hash values of the executables running on the production machine. Any variance in the hash value represents a change in the executable. This will alert you to the possibility of infestation by malicious software.

While the measures outlined above will not guarantee your network remains safe from it's users, they will minimize the problems associated with users. They will improve the availability of the network for all users while providing for increased confidentiality.

References

1. Farrow, Rik. “Blocking Buffer Overflow Attacks” Network Magazine. 11/01/99 http://www.networkmagazine.com/article/NMG20000511S0015

2. “PUBLIC LAW 104-191 AUG 21, 1996 HEALTH INSURANCE PORTABILITY AND ACCOUNTABLITY ACT OF 1996” HIPAA.ORG, Aug 21, 1996, http://aspe.hhs.gov/admnsimp/pl104191.htm

3. “Financial Services Modernization Act Gramm-Leach-Bliley Summary of Provisions”, US SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS Information regarding the Gramm-Leach-Bliley act of 1999”, http://www.senate.gov/~banking/conf/grmleach.htm

4. UserLocal.com http://www.userlocal.com/secfileperm.shtml

5. “Controlling Access To Your Files And Directories”, “UNIXHelp for Users”, http://www.mcsr.olemiss.edu/unixhelp/tasks/access_permissions.html

6. “Windows Services File Security”, “Information Technology Services”, Jan 8, 2003, http://www.utexas.edu/its/windows/resources/secure.html

7. “EFFECTIVE SECURITY MANAGEMENT WITH ELM LOG MANAGER”, “TNT Software”, http://www.tntsoftware.com/support/WhitePapers/ELMSecurity.pdf

8. Smith, Richard, E. “The Strong Password Dilemma”, “Authentication: From Passwords to Public Keys” Aug 9, 2002, http://www.smat.us/sanity/pwdilemma.html

9. SemJanov, Pavel, “Password Cracking FAQ” 1999-2000, http://www.password-crackers.com/pwdcrackfaq.html

10. Cobel, “DIGITAL MILINNIUM COPYRIGHT ACT CONFERENCE REPORT”, Oct 8, 1988, http://www.copyright.gov/legislation/hr2281.pdf

11. “PORT NUMBERS”, March 14, 2003, http://www.iana.org/assignments/port-numbers

12. Anderson Robert H., Bozek, Thomas, Longstaff, Tom, Meitzler, Wayne, Skroch, Michael, Van Wyk, Ken, “Research on Mitigating the Insider Threat to Information Systems - #2: Proceedings of a Workshop Held August, 2000” Aug 2000, http://www.rand.org/publications/CF/CF163/