Beyond the Firewall:

Using a Layered Security Strategy to Address Internal Security Threats

Introduction

The Internet has become a key tool for business communication and information sharing, and many organizations would cease to function if e-mail and Web access was denied for any significant period. All Internet Content you read, send, and receive carries a risk. The number of potential security risks has increased at the same time that dependence on information technology has grown, making the need for a comprehensive security program even more important. Likewise, the job of those persons tasked with network security, often system administrators, has never been harder.

The number of reported security incidents continues to grow and there is little indication that this trend will improve at any time in the near future. In 2001, there were 52,658 reported incidents. By the end of the first quarter of 2002 there were already 26,829 incidents reported. A reported incident can be as simple as a single computer being compromised or as severe as a complete network compromise involving hundreds of client computers. The number of reported security vulnerabilities has continued to grow at the same alarming rate with 2,437 vulnerabilities reported in 2001 and 1,065 reported by the end of Q1 2002 [1].

Unfortunately, many companies have stopped short of implementing a more secure “layered” approach to network security and have chosen to rely solely on the firewall/virus scanner approach. While firewalls and virus protection are necessary, by themselves they address only one portion of potential security risks and may contribute to a false sense of security. A more complete approach integrates these technologies with other effective tools including Web and e-mail filtering, intrusion detection, PKI, and artificial intelligence tools. Advanced tools can automate many tasks and increase the efficiency of a security program while reducing demand on network administrators.

Major Threats to Networks

Experts discover new security vulnerabilities almost every day. These newly discovered vulnerabilities may be due to flaws in software or they may be the result of software configuration errors. Hackers or other malicious individuals can exploit these vulnerabilities to gain access to network assets. Administrators must spend a lot of time and energy just staying informed about and dealing with new vulnerabilities. Often the result is that they are unable to take the time to monitor and educate staff. Enforcement of security policies may be non-existent or rely on the honor system. Failure to defend against the key threats to data and network assets can result in disaster.

Employee Behavior

Companies can face significant risk due to the behavior of their employees. Whether malicious or accidental, security incidents due to insiders are becoming more frequent. Insiders may present a more likely threat to many organizations than an attack by hackers or other malicious outsiders. Often even when internal security compromises occur, many organizations decide not to report the incidents due to fear of negative publicity. Failure to address employee behavior as part of internal network security leaves an organization exposed in a variety of ways.

Employees accessing offensive or illegal material from a company's network can leave the organization exposed to litigation. Employees visiting porn sites or sites with other offensive content create a hostile work environment, affect morale and may lead to costly litigation. If personnel access illegal material, such as child pornography, an organization may be held liable, have network assets seized in an investigation, and suffer negative publicity.

Millions of people subscribe to free webbased e-mail services such as Hotmail and Yahoo! mail. Allowing personnel to access webbased e-mail accounts from a corporate intranet increases the risk of damage to data and assets by a virus. While an organization may scan for viruses at its e-mail gateway, employees downloading attachments from web-based accounts circumvent this protection and may unwittingly receive and execute malicious code.

Software downloaded from the Internet and installed without consent poses a threat. Employees may inadvertently create a security hole by using ICQ or chat software. Disgruntled personnel can download and install hacking software that may allow them to circumvent security and delete or steal data. Downloaded games can contain malicious code, and illegal copies of software (warez) can result in fines and litigation.

Employees can negatively affect productivity of the entire organization by abusing or misusing e-mail to forward jokes, chain letters, or perpetuating hoaxes. Organizations can be liable for forwarding of material that is threatening, harassing, defamatory or that violates HR policies. Companies must educate employees about security and IT policies to avoid many of these problems. Usually this burden to instruct and notify personnel falls upon IT staff, adding to their workload and frustration. Advanced tools automate these and other functions, freeing IT to do other projects.

Disgruntled employees may share intellectual property or competitive information with the press or with the competition. Customer lists, proprietary data, financial data, research, and other types of confidential information are also vulnerable. Employees can easily undermine a company's competitive edge with a few forwarded e-mails.

Consider employee behavior a prime risk when designing a layered security program. The potential damage done by an insider is often considerably greater than the risk posed by an external threat. Later we will discuss tools that will mitigate these risks and make management of the program easier and more efficient.

E-mail

E-mail is definitely the Internet's "killer app" or the application that has driven adoption of the Internet to the greatest degree. Most people depend heavily upon e-mail, and many organizations could not operate effectively without it. While employee behavior can account for the majority of serious abuse, it is not the only threat to this resource.

Unsolicited commercial e-mail and unwanted junk mail or spam can quickly fill up inboxes and be an excessive burden to e-mail resources. It is often difficult to stop spam despite attempts to legislate against it. Employees should be discouraged from posting or using their work e-mail addresses for Internet shopping or special offers.

Many new Internet worms exploit bugs in Microsoft Outlook and other SMTP e-mail servers to replicate and spread from inbox to inbox. Virus Scanners at the gateway can minimize the risk but may not always intercept new viruses. Instruct personnel to avoid opening unidentified or suspicious e-mail attachments.

Viruses

Viruses and other malicious code can be devastating to network assets, data, and productivity. Each year, viruses grow more sophisticated and programmers that create malicious code are creating more viruses, worms and Trojans that take advantage of and exploit software vulnerabilities. The "Code Red" and "Klez" worms are recent examples of this trend.

Almost as damaging to productivity are the numerous virus hoaxes. Well meaning employees forward warnings for non-existent viruses to other members of the organization as well as friends and family, compounding the problem of this false information, wasting mail server resources and creating an additional burden for IT staff that must respond. Perpetuation of virus hoaxes can be limited or stopped by addressing employee behavior in your security program and using the proper screening tools.

Hackers

A hacker is an individual with a great deal of technical knowledge about computer systems and their security. Originally, the term had no negative connotations; in fact, it was a compliment in recognition of a great deal of technical prowess. Today, the term is frequently applied to cyber-criminals, to the dismay of legitimate hackers. Hackers prefer to call criminal hackers "crackers" and wish that the press would do the same.

Hackers are the most publicized threat to enterprise security. Hackers make great headlines and companies have spent millions of dollars improving existing security programs or creating new ones in reaction to the threat. While malicious outsiders are a risk to an enterprise, in comparison to other risks faced by an organization, it is less likely that an outsider will compromise network assets.

Focusing entirely on hackers may lead an organization to overlook a more likely threat, that of an insider compromising security intentionally, due to mistakes, or through negligence. Even in cases where an outsider actually penetrates network security, more often than not, someone within an organization has enabled the attack intentionally or through negligence. Adding additional layers of security that complement firewalls and virus protection will allow an organization to mitigate internal risks.

Assessing risk to your organization

The majority of companies would privately admit that their IT security is not as comprehensive as it should be. Security policies and procedures are often far behind technological advances, and adequate staff education is rare and infrequent. In fact, many organizations only develop or update policies and procedures in reaction to a security compromise. As a result, many companies are vulnerable, despite spending large sums on security products and consultants. A more proactive approach involves identifying risks specific to your organization and regularly auditing to address known risks and deal with new risks proactively rather than reactively.

Before an organization can protect something, it has to know that it is at risk. It is impossible to plan for the security of assets if you do not know the threats against them. Risk analysis is a process of identifying assets that need protection and evaluating the threats against those assets. Risk analysis can be simplified and broken down into five steps: [2]

1. Identify assets
2. Determine the value of each asset and identify the cost associated with its loss
3. Identify threats to the asset
4. Determine the vulnerability to those threats
5. Prioritize assets by level of importance

Following these steps, you can identify assets that are at risk and plan for their protection. Do not overlook the possibility of threats from within your organization. Too often, organizations emphasize external threats, specifically hackers and viruses, and ignore the more likely threats from within an organization. The majority of threats come from within a company and recent trends demonstrate this. [3]

Sources of insider security problems include malicious action, negligence, disdain of security practices, and ignorance of security policy and practices. [4] Misuse of computer systems by employees may result in liability if they use internal systems to access illegal or offensive material, or to commit computer crime. Intentional or accidental public dissemination of sensitive information can result in lawsuits or loss of revenue. Laws concerning protection of privacy data make monitoring employee behavior more important than ever before.

How does your organization address internal network security? What is the liability involved if your organization's data is compromised? Your level of exposure to internal risks will dictate the steps you must take to mitigate the risks. A security policy and program must include steps to mitigate the risks from disgruntled employees, risk of liability due to employee behavior or damage to systems from employee error. As mentioned before, the job of enforcing the policy and educating personnel usually falls upon the shoulders of an already burdened IT staff. Automated security tools can inform and enforce, making a security program more efficient while reducing the cost in man-hours.

Inside Attacks Examined

Recent surveys indicate that security breaches originating from within an organization may account for up to 80% of all incidents. These same surveys indicate the losses suffered from an external intrusion amount to $60,000.00 on average and that the average “inside job” cost in excess of $2.7 million! [5]

The risk from within certainly seems to outweigh the seemingly more dangerous threat posed by hackers. An insider often has the motive, knowledge and opportunity to do far greater harm to IT assets than any outsider. A hacker must spend a great deal of time and effort to gain significant intelligence on a well-protected network. An insider has intimate knowledge due to their position in the company and can often compromise security or destroy data even after they no longer have physical access to the network. Consider this threat a prime risk to network security; the following real world examples demonstrate why.

The Saboteur

On July 31, 1996 a software “time-bomb” went off on the primary file server of Omega Engineering’s Bridgeport N.J. manufacturing plant. The malicious program deleted manufacturing programs that Omega depended on to conduct business causing them to lose an estimated $10 million in business and $2 million in programming costs in order to resume business. Omega engineering suffered loss of market share, and had to lay off many employees. Even now, it is still recovering from the sabotage. [6]

Tim Lloyd, a systems administrator who worked at Omega for over 11 years, wrote the software “time-bomb.” He had intimate knowledge of the network and critical systems and was able to use that knowledge to cripple his former employers. Lloyd, a trusted and loyal employee, had access to senior management. As Omega grew, he became disgruntled at his own loss of influence and eventually lost his job. This apparently prompted his act of sabotage, and no procedures were in place to protect against an individual with his access damaging the systems from within.

A jury convicted Lloyd and a Federal Judge sentenced him to 41 months in federal prison and $2 million in restitution, but the damage inflicted upon his former employers can never be undone. Omega has put security systems in place to mitigate the risk of future sabotage, and multiple backup systems to provide for recovery of data. However reacting to a security incident has certainly cost Omega far more than a proactive security program would have ever cost.

The Leaked E-mail

In Okinawa, Japan, the United States Marine Corps was embarrassed when an anonymous employee leaked the contents of an e-mail message sent by Lt. General Hailston to the local press. Relations between the U.S. Military and the citizens of Okinawa were already strained due to several incidents involving U.S. Marines, including the rape of an Okinawan schoolgirl by three marines. Lt. General Hailston conveyed his thoughts about local Okinawan officials in his e-mail. “I think they are all nuts, and a bunch of wimps,” he stated in his e-mail. Of course, this aggravated an already volatile situation, and damaged relations between the U.S.M.C and the people of Okinawa even further. [10]

In this case, a single forwarded e-mail further damaged public relations and cast the U.S. Military in a bad light both in Japan and the United States. A proactive content security program may have prevented a sensitive (or insensitive) communication from compromise.

Dealing with new threats

New threats to networked computers appear almost daily. Hackers may discover weaknesses in software and post these exploits on several websites. [7] There is a good and a bad side to this activity. The good side is that the information is available to everyone and security personnel or system administrators can act to secure computers with the security hole. The bad side is that the information is available to everyone and malicious hackers can attempt to use it to exploit and gain access to systems before system administrators patch them.

Often the threats are variants of previous threats, i.e. modified worms and viruses, in which case they will take advantage of known weaknesses in operating systems or applications. This underscores the need for personnel to stay aware of software vulnerabilities that may affect their systems and update software accordingly. Security applications that automate updates to their own databases can significantly improve efficiency in this regard by assuming responsibility for this task and freeing IT personnel for more important duties.

Beyond Firewall and A/V technology

The first and last word in security for many companies is firewall. Many administrators regard the firewall as a magic bullet that will somehow make their networks impervious to risk. A firewall is a necessary and important part of any security program; it can limit access to your private network from the public Internet, as well as divide your internal network into zones thus limiting employee access to network areas that they require to perform their jobs. However, a firewall by itself cannot effectively deal with the majority of insider threats.

The second ingredient in the most popular security programs is anti-virus software. With the proliferation of viruses, worms and other malicious programs, anti-virus software is also a necessary part of network security. Even a simple e-mail worm (i.e. the Love Bug) can waste bandwidth and crash mail servers, or entire networks. Some worms, such as the Code-Red worm and its variants, inflicted unexpected collateral damage upon many networked print and storage devices, causing them to crash or hang despite the fact that it did not target these devices specifically. Properly maintained and updated anti-virus software can go a long way in protecting a network from this damage but insiders can intentionally, or inadvertently, circumvent anti-virus applications leaving your network vulnerable.

As prevalent as the firewall/anti-virus security model is, alone it cannot adequately protect organizations from the risk of an external attack and does little to provide security against malicious insiders. The answer to this problem is the addition of security layers using advanced tools that complement the firewall/anti-virus approach while addressing the areas of greatest risk.

The Layered Approach

Using successive layers of protection allows an organization to provide adequate protection against the majority of threats that it faces, thus minimizing risk. Implemented technologies should complement one another, with one component addressing threats that other components do not, as well as securing paths around (or through) other components. This comprehensive approach can mitigate risk more effectively as well as improve the efficiency of the security program.

Take care to carefully select tools that perform the required functions without adding unnecessary complexity to the system. Increased complexity often results in decreased security not in a more secure network environment. Avoid unnecessary redundancy; this is not the goal of a layered program, and may increase complexity or create conflict between components of the system. If one anti-virus package is good, that does not mean that two running on the same gateway would be better. Duplicating function would most likely result in conflict and wasted computing resources.

For an example of complementary technologies, we can look at anti-virus software and content security using Web filtering. An anti-virus product installed on an e-mail gateway may provide adequate protection from e-mail-borne viruses and malicious attachments. However, if employees can access Web based e-mail accounts, they can circumvent this component and compromise the network by downloading attachments.
A Web filtering solution can prevent employees from accessing Web based e-mail accounts, closing this backdoor past the anti-virus solution.

This is the strength of a layered program: each component acts to protect the network against specific threats while adding to the effectiveness of the other components. The different tools, like layers of armor, work to exclude unauthorized access, and prevent compromises from within the network.

Select automated tools that will handle reporting as well as enforcement of the security policies. A Web filtering tool that informs the user that they cannot access a specific website as well as notifying the administrator of the attempt, saves time and allows fewer IT personnel to invest time monitoring and educating employees. Real-time reporting is especially desirable because it allows an administrator to detect and react to attempts to compromise security before they succeed.

Intrusion Detection Tools

An intrusion detection system (IDS) monitors systems and analyses network traffic to detect signs of intrusion. An IDS can detect a variety of attacks in progress as well as well as attempts to scan a network for weaknesses. An IDS can be a dedicated network appliance or a software solution installed a host computer. A network intrusion detection system (NIDS) monitors all traffic on a network segment and is most affective when use in conjunction with a firewall, placed near remote access servers and on wide area network (WAN) backbones: although traffic on a WAN backbone may be too fast for an individual NIDS to keep up with. [8]

A NIDS/IDS can detect attempts to scan a network for intelligence gathering purposes. Hackers often scan networks to detect services running on ports of specific hosts. This can allow a hacker to identify the operating system of the host(s) and detect any exploitable services. There are many types of port scanning applications. Some can bypass a firewall and attempt to scan hosts within a private network. A NIDS/IDS can detect these stealth scans, complementing your firewall and providing an added layer of security.

A NIDS/IDS may use anomaly detection to discover intrusion attempts. This involves monitoring resource use, network traffic, user behavior and comparing it to normal levels. If a user that normally only accesses the system between 9 am – 5pm, suddenly logs on at 3 am then this may indicate that an intruder has compromised the user's account. A NIDS/IDS would then alert administrators to the suspicious activity.

PKI

PKI enables organizations to communicate securely using software, and services that rely on public key encryption. PKI systems use digital certificates and digital signatures to identify parties in a transaction, and allow for secure signing of messages, confidentiality of communication, and secure remote access to network assets.

Public key encryption uses pairs of encrypted keys (public and private) to allow parties to communicate securely. Using an individual's public key, anyone can encrypt (scramble) a message that can only be decrypted (unscrambled) by that person's private key. A digital certificate is a digital ID that certifies that a particular public key belongs to a specific individual or organization. PKI relies on trusted third parties called certificate authorities (CA) that issue digital certificates to identify individuals and organizations over a public network.

Much of the software already in daily use supports PKI, including browsers and e-mail clients. Properly used PKI can secure remote access to systems, communications, and financial transactions. Digital signing of software can ensure that software downloaded from the Internet has not been tampered with and establish who wrote the software. Digital signatures can ensure the integrity of a message so that recipients know that a third party has not altered it. By ensuring the integrity of documents, digital signatures can satisfy legal requirements for non-repudiation in some states.

PKI can be an important part of a comprehensive security program but it is not a cure-all for security woes. PKI solutions vary in complexity and no single approach is right for every organization. PKI has its weaknesses and some PKI solutions are more secure than others are. By itself, PKI does not adequately address the threat posed by malicious insiders.

Content security

Content security using filtering technology provides the key protection against risk due to employee behavior and abuse of IT resources. Filtering solutions can protect an organization from employee error including:

- Inadvertent disclosure of confidential or sensitive information
- Malicious compromise of information
- Compromise of information due to negligence
- Accessing illegal or offensive material
- Compromising security by downloading unauthorized software

Filtering solutions allow management to control who may access and distribute information. This limits the amount of damage that individuals can do and aids in the enforcement of both security and privacy policies. Even when an acceptable use policy (AUP) is in place, administrators often lack the means to enforce it. Filtering solutions enable management to enforce security policies, privacy policies and AUPs while managing staff productivity and minimizing wasted network bandwidth.

Web Filtering

Internet access is necessary for many employees, however abuse of this access can waste network bandwidth, decrease productivity and expose an organization to legal liability. Internet Filtering manages harmful and unnecessary Web and email content according to your policy. Web filtering can increase the security of a network by preventing circumvention of other security software i.e. anti-virus software via the Internet, and blocking the download of unauthorized or illegal software.

To maximize the benefits of a filtering solution, it is essential that the chosen solution is configurable and gives administrators maximum flexibility in managing content security. Administrators must be able to configure blocking by user and group. There is no such thing as a “one size fits all” policy, and organizations differ in their need for blocking even between individual departments. A solution that does not allow this level of customization will quickly outgrow its usefulness or worse, administrators may circumvent it if it seems to be a burden.

Software should allow for blocking by file extension or true MIME type. This is extremely useful if your staff collaborates on documents via the Web and you want to allow Microsoft Word and PowerPoint documents, but not executable files or image files. Again, if the choice is all or nothing, the result will be that administrators will block no files if the software prevents staff from doing their jobs.

Administrators should be able to define rules for blocking for maximum flexibility. Management can pre-determine the level of trust for each employee or group of employees and allow selective blocking based on employee need and level of trust. Flexibility is one of the most important factors relating to acceptance of a filtering solution.

Automated reporting increases the efficiency of policy enforcement, allows management to stay informed of employee activities and reduces the workload of administrators. Reports should be customizable to allow for different information requirements and reporting to different levels of an organization. Automatic scheduling of periodic reports as well as real-time notification and reporting of abuses are essential and will increase the ROI of the program.

Many filtering applications block Web addresses based on a list of keywords or phrases. These keywords may indicate obvious offensive or illegal material such as “porn,” “sex,” or words that are more explicit. Keyword blocking is limited in its effectiveness and can result in over blocking or erroneous exclusion of sites. An example of this would be a breast cancer site blocked because of the word “breast” appearing on the page. Such obvious mistakes are rare as the technology has improved but software that blocks based on keywords alone is insufficient as tool in an enterprise security program.

Software intended for use in an enterprise security program will usually rely on an extensive database maintained by real people in addition to blocking based on advanced A.I. and keyword recognition. These databases consist of millions of sites pre-screened by professionals to determine their content. The best solutions organize sites into groups and categories that allow administrators to define access to very specific types of websites while blocking others. Due to the nature of the Internet, updates to the database should be available frequently (daily is best).

By implementing content security through Web filtering an organization will minimize the risk of litigation, reduce wasted network bandwidth, and improve productivity. The use of advanced automated tools will increase the ROI, reduce the burden on IT staff, and improve the enforcement and efficiency of security, AUP and privacy policies.

E-mail filtering

The second key component in the content security program is an e-mail filtering solution. Access to e-mail is necessary for arguably every employee in a company. E-mail provides an efficient means for all levels of the organization to communicate and collaborate on projects. However, abuse of e-mail will result in loss of productivity, exposure to liability, wasted bandwidth and an increased burden on mail servers.

Often abuse of e-mail leads to the termination of personnel. In 1999, the New York Times fired 23 employees for sending inappropriate e-mail and the U.S. Navy disciplined over 500 sailors for sending sexually explicit e-mail. [9] Clearly, an AUP or security policy will not enforce itself. Depending of the honor system for enforcement increases risk and undermines the credibility of policies and procedures.

An e-mail filtering solution must allow managers to control which employees can e-mail particular information, and to whom they may send it. The software should provide real-time monitoring and quarantine of suspect messages. The software must be configurable to allow managers to review e-mail, remotely if necessary, and provide automated notification so that administrators can monitor attempts to send unauthorized information or attachments.

Advanced text and content analysis is necessary to reduce the likelihood of users sending sensitive information to unauthorized parties. Analysis should be customizable, and allow for examination of attachments including those that are compressed (zipped files).

Solutions that allow for multiple dictionaries, are context sensitive, and include the ability to filter by keyword and phrase will reduce the number of “false positive” alerts and increase the efficiency of the system. Customization is key, as in Web filtering, and the solution that allows administrators the most flexibility in determining rules will be the most successful.

E-mail filtering tools are the most reliable way to enforce e-mail procedures and policies, while reducing the workload on IT staff. This is the best technology decision for mitigating the risk of employee abuse of e-mail services and possible liability resulting from that abuse. Together with a Web filtering product, an e-mail filter provides a complete solution to secure content in an organization. Securing content is necessary to prevent incidents and liability due to employee behavior.

Summary

Perhaps the most overlooked threat in a security program is the threat posed by employee behavior. As much as 80% of security compromises are the result of actions by an insider. Whether incidents are due to malicious intent or inadvertent employee error, the result is the same: loss of revenue, productivity and potential liability.

The threats to networks will only continue to grow. This is in part due to the increasing complexity of enterprise systems, which results in greater possibility of unexpected interactions and software faults. The ability of administrators to keep up with the growing number of threats is decreasing due to increasing demands on their time. The only way to alleviate the burden on IT staff and increase security at the same time is to implement a proactive security program that automates as many functions as possible. Automated content security tools help to effectively and efficiently secure network assets against threats from within an organization.

About SurfControl

This white paper was commissioned by SurfControl plc, the world's Number One Web and e-mail filtering company. SurfControl is the only company in the security market offering a total content security solution that combines Web and e-mail filtering technology with the industry's largest, most accurate and relevant content database and adaptive reasoning tools to automate content recognition. Analysts estimate double-digit growth in the security market with forecasts predicting it will reach $14.6 billion by 2006.

SurfControl's Internet monitoring and policy management solutions are flexible, scaleable and interoperable to meet the diverse needs of all its markets -- corporate, education, home and OEM. SurfControl offers a choice of platform independent or integrated solutions, and the software can be installed in any network environment. With world-class partners such as AT&T, Intel, Cisco and IBM, as well as a customer base that includes many of the world's largest corporations, SurfControl offers the most sophisticated yet easy to use technology, the best understanding of market needs and a global reach unmatched in the industry. For further information and news on SurfControl, please visit http://www.surfcontrol.com.

About the Author

Jack McCullough is a co-author of “Access Denied: The Complete Guide to Protecting Your Business Online”, in addition to papers and articles about information security. He is the founding consultant of Razorwire Information Security Consulting which provides cutting-edge computer security expertise, threat assessment, training and security policy/program analysis and development. He speaks regularly on the subject of information security and provides security awareness training to all levels of management. He can be reached via email: Jack.McCullough@rzrwire.com

References

1. CERT Statistics: http://www.cert.org/stats/cert_stats.html
2. *Access Denied: the Complete Guide to Protecting Your Business Online*, Cathy Cronkhite & Jack McCullough, Osborne/McGraw-Hill Aug 2001, pg. 210
3. *Insider Attacks: The Doom of Information Security Methods to thwart insider attacks,* Anton Chuvakin Ph.D. available at: http://www.sinc.sunysb.edu/Stu/achuvaki/internal-attacks.html
4. *DoD Insider Threat Mitigation: Final Report of the Insider Threat- Integrated Process Team* pg1 executive summary
5. *Insider Attacks: The Doom of Information Security Methods to thwart insider attacks,* Anton Chuvakin Ph.D. available at: http://www.sinc.sunysb.edu/Stu/achuvaki/internal-attacks.html
6. *Computer Saboteur Sentenced to Federal Prison,* Sharon Gaudin Network World Fusion available at: http://www.nwfusion.com/news/2002/0226lloyd.html
7. An example of a useful site for tracking exploits is: http://www.securityfocus.com
8. *Access Denied: the Complete Guide to Protecting Your Business Online*, Cathy Cronkhite & Jack McCullough, Osborne/McGraw-Hill Aug 2001, pg. 135
9. *Access Denied: the Complete Guide to Protecting Your Business Online*, Cathy Cronkhite & Jack McCullough, Osborne/McGraw-Hill Aug 2001, pg. 51
10. *Access Denied: the Complete Guide to Protecting Your Business Online*, Cathy Cronkhite & Jack McCullough, Osborne/McGraw-Hill Aug 2001, pg. 51