GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Incident Response Planning for Smaller Financial Institutions

Yvonne Bryce
5/18/04
GSEC – Version 1.4b Option 1

Abstract

Incident Response Planning is now a requisite exercise for smaller financial institutions. In order to create an effective incident response capability a number of broad areas must be considered. These areas include incident classification, the role and responsibilities of a Computer Incident Response Team, incident discovery and reporting, the incident response process, and reducing exposure to future incidents.

Introduction

Information security has become a growing focus for financial services companies. In most financial institutions, the staff recognizes the importance of protecting customer data and the issues involved if the data are compromised. However, few employees have adequate training to properly detect or prevent all possible information security incidents.

The organization's Incident Response Plan is to be used when an information security breach is detected or suspected. Preventative activities based on periodic Vulnerability Assessments can lower the number of incidents, but not all incidents can be prevented. NIST Special Publication 800-61 states "An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services."[1]

Making use of documented standards for information security can help guide an organization as they create their incident response plan, training plans and security procedures. A survey conducted by KPMG in 2002 said that forty-two percent of the surveyed financial services organizations had either implemented ISO17799, or were in the process of implementing it. The KPMG study states, "ISO17799 [The Code of Practice for Information Security Management] is the only international accepted standard in the management of information security, covering such areas as security and organization, access control, communications and operations and compliance."[2]

While the information in this document may apply more widely, the focus will rest on financial institutions ranging in asset size from $750 million to $5 Billion. The goal of this paper is to help smaller financial institutions begin the process of creating an incident response capability.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Incident Classification

Due to the high volume and variety of attacks, incidents occur in countless ways. It is not practical to address each attack individually, so, incident classification and severity ratings may be used as the basis for creating a manageable set of procedures for incident handling. Details of incident handling will be discussed later in the "Incident Process" section. Attacks may be categorized as follows:

Malicious Code – A worm, virus, Trojan horse, or other malicious scripting created to infect systems.

Denial of Service (DOS) – An attack preventing the authorized use of networks or servers by exhausting the system's resources. Viruses, worms and SYN packet attacks, are common methods used to produce Denial of Service conditions. A recently announced TCP vulnerability could also allow hackers to create Denial of Service attacks by causing premature termination of TCP sessions.[3]

Unauthorized Access – This category includes any access to the network, hosts, data or physical locations without permission. This also covers using an account or credentials that do not belong to the user. Often, the intention is to steal information or disrupt business operations. Weak passwords, shared passwords and social engineering are typical examples of how this may occur. Phishing, trying to trick people into giving out personal data like passwords and account numbers has increased in popularity on the internet. As corporate security grows tighter and the intruders find it harder to penetrate a network, customers become a more frequent vector for data theft.

Inappropriate Usage – Behavior in violation of employee policies can be one of the most frequent causes for an incident. Examples include: downloading or installing software from the internet, Peer to Peer file sharing programs such as Kazaa and Morpheus, bringing in infected media or hosts like laptops and workstations from the outside, and setting up VPN or modem connections to bypass firewalls without the permission or review of the Information Security group.

Natural Disasters and Terrorist Attacks – Earthquakes, tornados, terrorist attacks or other acts of god or man may cause anything from a minor power outage to fire, explosion or wide spread destruction. Events in this category are usually the subject of a Business Resumption Plan and may require relocating during recovery.

Severity Levels

Each incident should have an assigned severity level, which is determined by the level of impact on business operations. The severity level affects how the CIRT

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

would respond to the incident. The severity level is assigned by the CIRT and it should be reviewed and modified throughout the incident response process.

Severity – High

1. Disruption of business continuity and critical business process of communications.
2. Business data theft through physical or virtual attacks.
3. "Impacts on long-term perception of the organization, either in part or whole"[4], stated by the Information Security Team at DePaul University.

Severity – Medium

1. Disruption of non-critical business processes.
2. Non-intrusive activities like web site defacement (Code Red) or spoofed email addresses (Netsky variants). This type of attack generally does not target a specific entity.
3. Inappropriate use of company property resulting in installation of P2P or other potential malware to the hosts.

Severity – Low

Incidents at this level have very little impact on business operations. For example, real-time virus detection and quarantine prevents a virus from spreading to the network, and there is evidence of such activities on the host or network.

Severity – Very Low

Incidents with very low impact and no forensic evidence may be logged and reported to monitor trends. A sudden increase in low impact events could be the beginning of a Denial of Service attack.

Example Incidents

Example 1 -- Blaster worm infects Financial Institution Network

Malicious Code (Worm)
Denial of Service
High severity

At one financial institution, this incident infected eighty percent of network hosts. The vulnerabilities in the Remote Procedure Call (RPC) function allowed a Denial of Service (DOS) to their network. The worm caused every infected network server to reboot every five minutes throughout the day. Most of workstations also had the same problem. Even though perimeter defenses blocked the worm, a consultant's ad hoc VPN connection to an infected network allowed the worm to bypass the firewall and Intrusion Prevention System.

Without a practiced incident response plan, the recovery process lacked a coherent team effort. There was a single point of authority to quickly make critical decisions and communicate the incident status to other departments.

© SANS Institute 2004, Author retains full rights.

There was not a trained CIRT to document the whole process and select the most responsive way to mitigate the incident. An incident which should have been eradicated within four hours, took an entire business day to resolve.

Example 2 – FDIC email scam targets bank customers
Unauthorized Access (Phishing)
Low severity
Consumers and financial institutions are being warned of a new e-mail scam that purports to be from the Federal Deposit Insurance Corporation. The email advises consumers to click on an attached file for more information about alleged fraudulent activity in their bank accounts. Instead, according to a FDIC spokesman, "the attached file is either a computer virus or a program that can steal personal information from a computer and send it to the scammer."[5]

These types of emails are becoming very common and increasingly clever and deceptive. These types of activities are virtually impossible to monitor from security devices. Because this form of attack starts between the attacker and a bank customer, prevention and mitigation are best accomplished by educating users. However, vigilance is necessary to discover wide spread occurrences early in order to provide timely warnings to the customers and staff.

Computer Incident Response Team (CIRT)

Establishing a CIRT is a significant task and many points must be addressed and customized to fit a particular financial institution. Ideally, the CIRT is well trained and equipped with computer incident response knowledge that can be quickly applied when the inevitable occurs. This section will document the many details which must be addressed when forming a CIRT.

1. Who should be on the CIRT?
   The CIRT is a group consisting of employees with expert knowledge from various departments. Not only are Information Technology staff needed to handle incidents from the technical aspect, CIRT members should include key staff from many areas of the organization.

   Information Security: The Information Security team is a subset of Information Technology staff that has undergone security training. They fill the role of first responder and begin the initial steps of incident assessment and handling. The team members should be selected so as to cover key areas of critical system knowledge. They will make decisions during the other stages of incident handling and take actions, such as, reconfiguring firewalls, analyzing logs or preserving forensic evidence should the incident call for law enforcement involvement.

© SANS Institute 2004, Author retains full rights.

Help Desk: The help desk group provides an excellent hub for communication. Communication within the organization is important to prevent anxiety due to the uncertainty caused by an incident. Demonstrating confidence during the incident response process is reassuring to both employees and customers. Additionally, members of the Help Desk group will continue to collect evidence and help document each report of a possible incident.

Telecommunications: Some incidents may involve telephone lines, WAN connections and other telecommunications equipments.

Legal/Internal Audit: With increasing information security regulations and liability, it is more important now than ever to include the legal and internal audit representatives on the CIRT. The legal and internal audit representatives should review the incident response plan and procedures to ensure their compliance with State and Federal regulations. The CIRT should also consult with the legal department on procedures involved with evidence collection, prosecution of a suspect, or lawsuits.[6] It is important to show the effort made to secure the network and confidential data when defending against a lawsuit.[7]

Public and Media Relations: California law, SB 1386, now requires a financial institutions to notify Californians when it is known or reasonably believed that personal information stored on the entity's computer system has been disclosed to an unauthorized source as a result of a security breach. According to Don Hewitt, in Washington Technology, SB 1386 states that, "The notice should be given, 'in the most expedient time possible and without unreasonable delay.'"[8] This law requires quick action on the part of a financial institution.

Financial Institutions may need to communicate with the public and media regarding an incident. This includes reporting incidents to organizations such as the Federal Computer Incident Response Center (FedCIRC) and the CERT coordination Center (CERT/CC), contacting law enforcement, and fielding inquires from the media.[9] Separate policies and procedures should be established for sharing information with various outside parties.

Human Resources: The Human Resources group should define employee policies to govern appropriate usage of company hosts and network resources. When an employee violates the policy and causes an incident, the HR team will be involved in employee counseling and discipline.

Physical Security and Facilities Management: Some incidents may occur through physical theft of company property. Regular review and maintenance of physical security is required of Financial Institutions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Physical security and facilities team members most often required when handling an incident caused by a breach of physical security.

Management: It is important to communicate with senior management throughout each incident when it is classified as “severity high” or “severity medium”. Management can empower the CIRT by establishing an incident response budget, staffing the CIRT, reporting an incident’s status to the Board of Directors, and by making critical high-level incident response decisions. Without the support of senior management, the CIRT is bound to fail.

2. What are the major responsibilities?
Many tasks will be carried out by CIRT at three different stages: before, during and after an incident. Many details must be addressed by creating procedures and acquiring assistance from external incident response providers, by preparing hardware and software tools, and obtaining adequate security training. Then the whole process must be tested by performing well-coordinated drills. This section will outline many of the points, for each stage of an incident, to address in the incident response plan document.

Before an incident - Preparation

Procedures and policies: Strong documentation is the key to success. Current network and server documentation is invaluable during an incident.

Basic items: Be sure that all CIRT members have ready access to a copy of the incident response plan and procedures. CIRT members should be strategically located and able to respond to the incident location within a short time. Document contact information for outside parties including all key vendors, law enforcement and media. CIRT members should be able to readily gain access to all physical locations (e.g. telecommunications closets) that may be involved in an incident response.

Master copies of server disk images: Have good backups for all systems and document their location and retrieval procedures. Ensure that the backup and retrieval procedures are adequate for various incident scenarios.

Network and system baseline data: Establish network and system baseline data and logging. It is important to know what one’s network and systems look like when they are running properly so that any deviations may be explored. During an incident response, it may be valuable to compare baselines and logs prior to the incident to what is happening during or after the incident.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Network time synchronization: In order for log time stamps to be accurate all network devices must be synchronized using Network Time Protocol (NTP). Ideally, the network time servers will also synchronize to an atomic clock.

Training: Information security staff members must be familiar with the laws and regulations involved in incident response. Document a curriculum and training plan adequate for each role on the CIRT.

Tools: Establish a forensically sound procedure for collecting system evidence to help prosecute a suspect. Determine what spare devices may be required to replace the production devices involved in an incident. Learn to use tools that may be necessary to correctly identify an incident.

CIRT phone list and on-call information: Keep an up to date phone list and make sure that CIRT members have quick access to it. Include "call tree" information and identify the "first responders."

Incident handling checklist: Develop a checklist to ensure that the important steps of incident handling do not get overlooked during an incident.

Incident response drills: Create procedures for incident response drills. Consider frequency of the drills and whether the drills will be scheduled or surprise. Make sure that a goal or mission statement is established for each drill and determine some measure for success.

Outside experts: If necessary, establish contracts with vendors to assist with incident handling.

Incident database: A help desk system or other database can be a valuable tool for documenting incident details. Make sure that the entire CIRT has access to the systems and understands how to use it. Because this incident documentation may contain highly sensitive information, determine adequate methods to protect the data.

During an incident – Incident Handling

Incident analysis: Document procedures for incident identification and classification. Be cautious of false positives.

Documenting incident: Designate a CIRT team member to coordinate documentation of the incident. Establish guidelines to determine what information should be included in the documentation. When in doubt, document it.

Severity assignment: Assign a severity level to the incident.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Incident notification: Create notification procedures to document who gets notified, when they get notified and how they get notified. Set guidelines to help determine what information can be released internally and externally.

Containment: Document containment procedures for each major type of attack. Determine when it is appropriate to disconnect the infected hosts from the network or disable certain services on the hosts.

Evidence handling: If the incident may result in criminal prosecution or civil liability, procedures must take into account the laws and regulations for collecting evidence. Determine what tools are required and consider contracting with an outside vendor when appropriate. Document procedures to aid in determining the systems compromised by an attack.

Mitigation and Recovery: Establish recovery procedures for all critical systems. This may include restoring systems from backups or using spare devices to temporarily replace production hosts. Document resources that may be necessary to sanitize infected systems.

After an incident – Lessons Learned

Document the lessons learned after each incident and hold meetings for process improvement discussion.

3. Tools and Training

One of the most important resources required for incident response, are system logs. Logs are normally kept individually in each network device. Reading and gathering this information to find traces of problems would be very time consuming. Utilizing a centralized logging tool can dramatically expedite this process. And better yet, log analysis software can parse the logs and send alerts to warn of conditions that may require attention, sometimes before an incident has occurred. Products such as netForensics, Contego or ArcSight, may be considered for this process.

Another important tool to consider is computer forensics and security software. When an incident is suspected, forensics software allows you to take a snapshot of a system, capturing and preserving live data, such as, local data storage, open ports, system registry and a RAM dump. Then, working on the captured snapshot of the affected systems, one may do a variety of things. For example, one may view deleted files, locate hidden malware or search for sensitive data. This allows the CIRT to immediately respond to the incident without taking the system off-line. During an incident response investigation, the analysis must be rapid and accurate in order to mitigate the potential loss of money and possible disruption of operations. Security experts often recommend EnCase Enterprise Edition from

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Guidance Software and SaveBack from New Technologies Inc. Both are recognized, effective computer forensic tools.

Many CIRT members may be technically savvy but lack incident handling skills. An incident handler without proper training could do more harm than good to the evidence. For example, running commands from affected hosts can be dangerous because these commands may have been replaced or altered to damage the hosts. Computer forensics training is essential for incident handlers. Other beneficial topics include, "Analyzing Computer Security Incidents" and "Understand Hackers' Technique, Exploits and Incident Handling". These classes can be found at www.cert.org, www.sans.org and www.guidancsoftware.com. Security awareness training should be available to the CIRT, and can be accessed online at www.sans.org and csrc.nist.gov.

4. Practice Incident Response
   According to the U.S. Securities and Exchange Commission, federal regulation requires, "…firms in the other critical financial markets should strive to achieve a four-hour recovery time capability for clearing and settlement activities in order to ensure that they will be able to meet a within the business day recovery target."[10] To comply with the regulation, incident response drills must be performed by the CIRT to ensure the team members know exactly what to do when disaster strikes. These drills should be continued until a 4-hour recovery time capability is established.

   Scheduled drills with well-documented incident handling procedures are used to get CIRT members proficient with incident response. To raise the CIRT's comfort level with incident handling, these drills are performed with a pre-planned script through the mock incidents. These drills may be designed to minimize the impact on business operations. Each drill may involve CIRT members from one or two specific operational areas and concentrate on their specific roles. Following the scripted drills, a surprise drill may be carried out and may even include some degree of company-wide participation. However, this kind of test needs to balance the amount of protection, the cost of business disruption and staff time.

   A realistic test schedule for most environments is every three to six months. The test results provide the lessons needed for improvement. Feedback from each person involved in the drills is important and will be used to modify the existing procedures.

Discovery and Reporting

It is common to overlook incident symptoms due to the high volume of network device log data and alerts produced by Intrusion Detection Systems each day. One of the most challenging parts of the incident handling process is accurately

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

detecting and assessing potential incidents. Here are some of the signs one should be looking for:

- Fraudulent activities by way of electronic means
- Stolen company hosts containing critical data
- Web site defacement or crashes
- Discovering threatening or harassing e-mail messages
- High system utilization rate and unusual network traffic flow
- Increasing numbers of failed user login attempts
- Processes or large numbers of unknown processes run at an unexpected time
- User rights or ACL changed unexpectedly
- Previously disabled or removed services are mysteriously turned on
- Log or system files removed, modified or renamed unexpectedly
- Unusual access by system accounts
- Higher volume of virus detection, bounced-back messages with suspicious content and spam messages
- Unexpected system configuration change
- Unusual port scanning activities
- A newly announced exploit that targets a vulnerability of the web servers, mail servers, database servers or other critical servers
- Any other abnormal activities

How does an employee report or help others to report an incident? Most employees do not have the training to determine if what they suspect is really an incident. Identification and classification of incidents is one of the CIRT's main responsibilities. The best practice is to train staff to report any suspicious activity immediately through the appropriate channel. Typically, the report would be made to the security department or help desk. Staff should be trained to provide details of when, where, and how the incident occurred. If known, they should also give an indication of who is impacted by the incident and what damage is suspected.

Incident Response Process

Identify Threats

After each incident is reported, the incident handlers begin the incident process by identifying threats. This process can be difficult as some of the incident

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

symptoms are subtle and unclear. This could mislead the incident handlers resulting in an incorrect judgment. For instance, a web server crash could happen because of administrative errors or a security breach. The enormous amount of information logged by network devices makes finding the few real security incidents a real challenge. A good incident handler treats each finding like an incident until it has been determined benign.

As soon as an incident is identified by the CIRT, it is important to start recording all of the activities that have occurred in the incident. Incident handlers should work together to record and log the events into the incident database while others perform the technical tasks.

The next step is to determine the scale of the incident impact and to assign an appropriate severity level. This initial analysis seeks to determine information about what systems are affected, the source or vector of the attack and how the breach is occurring. Information collected at this stage should allow the CIRT to further classify the incident and provide appropriate communication to others within the organization. Notification may extend to the following:

1. CEO
2. CISO
3. CIRT
4. IT Managers
5. System Owners
6. Human Resources Department
7. Legal Department
8. Public Relations

California Senate Bill 1386 took effect on July 1, 2003. This law requires a person or organization to notify Californians when it is known or reasonably believed that personal information stored on the entity's computer system has been disclosed to an unauthorized source as a result of a security breach. The notice should be given in the most expedient time possible and without unreasonable delay.[11] Proper procedures need to be established for sharing information with external parties like the media, ISPs, law enforcement, software vendors, affected external parties and security contacts from where the attack originated.

Containment

After initial analysis of the information gathered and documented, the containment strategy must be quickly determined. The most common containment measures still apply to today's ever changing incident response challenges. Unless the analysis indicates otherwise, consider these options:

- shutting down involved network devices
- disconnecting infected hosts from the network

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- containing the hosts within an isolated (test) network
- applying security patches
- disabling offending or attacked services on the device

Any decision to delay executing containment procedures should always be made after consulting with the legal department and senior management. If an organization knows about an attack and allows the attacker to continue in order to monitor the attacker's activities, it may be held legally liable if the delay results in an attack to other organizations.[12]

Investigation

The evidence collecting process begins after containment. This is often the weakest link in an organization's incident handling process. Network tool sets like server logging, network IDS, firewalls and sniffers are not adequate for computer security forensics analysis. Because some incidents may involve prosecution by state or federal authorities, it is best to treat all evidence as though it will be used in court. According to Guidance Software, "An ISO 17799-compliant enterprise should employ the best methods and tools available to respond to breaches or suspected breaches of its information security, and must collect and preserve the resulting evidence in a forensically sound manner."[13] Computer forensics software is essential to use at this stage of the investigation.

When properly employed, the forensics software creates an image of all system data and calculates a checksum used to validate the unaltered state of the image. This image may be used by the investigator to view and analyze all information in the image including deleted files and directories, hidden information, and other traces left behind by the attack.

As the evidence is gathered make sure all activities occurring during this process are properly documented. Several images of the evidence should be made to write once media.

The evidence collected during this phase of the investigation may be crucial to locate the source of the attack. This analysis process may be completed at this stage if circumstances allow, or if necessary, it can wait until the recovery is complete. The pressure to resume normal business operations can be greater than the importance of identifying the hackers during an incident.

Recovery

The recovery process can be shortened by using master copies of images created prior to the incident. Keeping current system images on hand will dramatically shorten the recovery time. While, a clean-install of the OS, patches and applications gives the best opportunity for system stability, this method is time-consuming and more likely to result in configuration mistakes. The patch-

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and-go method, though faster, is risky because one cannot always be sure that every trace of the attack has been eradicated and the system may not be stable or secure.

Before the recovered systems are brought back into production, carefully examine the services running on the systems and disable all services that are not required. Take extra effort to ensure that the vulnerability that allowed the attacker to exploit the systems has been eliminated. Systems that have been comprised once tend to have a higher chance of getting attacked again. As a result, these systems require more monitoring and auditing than most of the other systems.

Lessons Learned

Using the records of the actions performed during the incident, the CIRT should document lessons learned from the incident. "This practice can result in continued improvement of the organization's security stance."[14], is stated in an article from CERT Coordination Center. Holding a post-mortem meeting with the entire CIRT after each major incident is also helpful in improving the incident handling process. The procedures and other documentation should be refined with any positive changes identified through this final process.

At the end of each incident, a summary report should be created by the CIRT for future reference. Calculate the incident cost and present this analysis in addition to the incident summary report to the management as the basis for further security improvement.[15]

Reducing Exposure to Future Incidents

Periodic vulnerability assessments by a reputable information security company will identify many security weaknesses in an organization. The resulting report of vulnerabilities should be prioritized by risk and remediation should be scheduled as appropriate. Careful tracking and documentation is very important to ensure that all remediation tasks are completed in a timely manner. It is advisable to have the information security company retest all findings from the original report once remediation is complete.

Even when remediation is costly, the potential financial losses are much greater when an incident results in compromised business data or a disruption of business operations. Often more severe than financial loss, is the loss of customer confidence and reputation.

Management should be made aware of the major threats identified during a vulnerability assessment. Sometimes further risk analysis and cost benefit analysis will be required in relation to identified vulnerabilities. This information will be useful to management when prioritizing improvements in security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As you plan activities aimed at preventing information security incidents, make sure that you have the fundamentals well covered. The following section lists some of the requisite points to address and provides a brief description of possible mitigation methods:

Keeping track of new vulnerability announcements and vendor patches: Apply up-to-date operating system and application patches. This is one of the most important mitigation steps to take. Patch management software like HFCheckPro may be necessary to manage the distribution of patches to un-patched network hosts. Monitor and evaluate the new vulnerabilities reported by vendors and security companies by subscribing to e-mail notification services. Staying abreast of newly reported vulnerabilities will allow an organization to act quickly to mitigate the risk before an exploit is developed.

Hardening security for internet-facing servers: All services on internet facing servers must be reviewed and all unnecessary services should be disabled. The goal is to make these devices as transparent to the internet as possible. Security guidelines and templates from various sources like Microsoft (www.microsoft.com), Center of Internet Security (www.cisecurity.org) and SANS (www.sans.org), etc. should be used to harden security on these devices.

Data encryption: Email communications, sensitive business data and network authentication require appropriate levels of encryption. It is important to educate staff as to the proper methods of transferring data to 3rd parties. Many vendors will encourage the transfer of data by insecure means and an uneducated staff can put the organization at risk. All laptop users in the organization must be educated regarding the necessity of encryption when storing confidential data on their local drives.

Securing clients and remote users: Centrally managed anti-virus, spyware detection and removal, and desktop firewall software should be deployed to any workstation that connects to the network; special care should be given to laptops. Establishing firewall-to-firewall VPN connections with 3rd parties is preferable to allowing a VPN that terminates at a workstation. VPN's that terminate at a workstation are more difficult to filter and secure. It is ideal to use tool like Microsoft Connection Manager to prompt remote users to download and apply the most recent patches. If a user does not download the patches within a reasonable amount of time, network access may be denied.[16]

Intrusion detection and auditing: Critical servers in the core domain should have host-based intrusion detection devices and scheduled security audits in place to ensure their integrity. Products like Tripwire for host-based intrusion detection and Contego for security event management are examples of tools suited for this purpose.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Restricted admin accounts: It is all too common for network administrators to share super user accounts. This practice, while convenient, invalidates security logging by tainting the audit trail. All network administrators should have both a standard user account and a personal admin account with the minimum level of rights necessary to do their job. Admin accounts should only be used when performing tasks that require the added privileges. This helps to prevent accidents like inadvertently deleting or moving a large folder.

Security awareness training: Security awareness training classes should be provided to everyone in the organization. The classes should be customized to address issues unique to each job function. This is one of the least expensive methods of defense, yet it is also one of the most effective safeguards. For instance, on April 13, 2004, Microsoft issued 14 security patches and in a Network World article, Ellen Messmer stated that this, "…raised fears that worm-based attacks would follow and sparked discussion on how to better build code." She continued, "But the way to eliminate such vulnerabilities isn't via patches, but in creating tools and processes for building more secure code and weeding out problems in the development phase."[17] It is vital for developers to know how to apply the best security practices while developing web applications to minimize vulnerabilities and limit attacks. Average users should know the importance of best practices related to passwords and securing their workstations. They should be tested periodically on their knowledge of the information security policies and procedures applicable to their job function.

Physical security on premises: All staff must be trained to keep an eye out for suspicious activities. Be very cautious when non-employees enter restricted areas, even when they have a legitimate reason to be in the area. All non-employees, such as repairmen or telecom technicians should be escorted at all times. When groups of workers are in the building, if possible, ask the crew to stay together so all activities can be monitored more easily. All restricted areas should always be locked. Sensitive data packages waiting to be shipped should be stored in a secure area and monitored by security staff.

Conclusion

The endless security alerts do not stop coming in for an IT department that is overloaded. Vulnerabilities will continue to grow as software and networks become more complex and attackers become more sophisticated. It is imperative for financial institutions to overcome these factors through careful planning, practice, response and process improvement. The well designed and well practiced incident response plan is the ultimate defense to mitigate the impact of an information security incident.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[1] Grance, Tim; Kent, Karen; Kim, Brian; "Computer Security Incident Handling Guide" January 2004, p. ES-1, URL: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (May 9, 2004).

[2] KPMG. "ISO 17799 Implementation." 2002. URL: http://www.kpmg.com/microsite/informationsecurity/iss_secpol_iso.html (May 9, 2004).

[3] Roberts, Paul. "Expert Warns of TCP Vulnerabilities." April 20, 2004. URL: http://www.nwfusion.com/news/2004/0420experwarn.html?nl (May 9, 2004).

[4] DePaul University. "A Framework for Incident Response (Draft)" December 13, 2002, p.8, URL: http://security.depaul.edu/doc/policy/pub/irtfwk.pdf (May 9, 2004).

[5] Weiss, Todd R. "FDIC warns of scam targeting consumers' bank accounts." April 8, 2004. URL: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,92050,00.html?from=story_kc (May 9, 2004).

[6] Grance, et. al., p. 2-13.

[7] Reuters. "Cybersecurity liability seen increasing" March 28, 2004. URL: http://news.com.com/2102-7348_3-5180855.html (May 9, 2004).

[8] Hewitt, Devon. "Infotech and the Law: New California privacy law has nationwide ripple." July 7, 2003. URL: http://www.washingtontechnology.com/news/18_7/infotech-hewitt/21129-1.html (May 9, 2004).

[9] Grance, et. al., p. 2-4.

[10] U.S. Securities and Exchange. "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" April 8, 2003. URL: http://www.sec.gov/news/studies/34-47638.htm (May 9, 2004).

[11] Savi, Jerald M. "Identity theft bill brings nightmare for businesses. (An Advertising Supplement).(a discussion of California's privacy law)" May 12, 2003. URL: http://www.findarticles.com/cf_dls/m5072/19_25/102112044/p1/article.jhtml (May 9, 2004).

[12] Grance, et. al., p. 3-18.

[13] Guidance Software. "Incident Response Requirements Under ISO 17799" June 2003, p.2, URL:

© SANS Institute 2004, Author retains full rights.

http://www.encase.com/corporate/whitepapers/downloads/iso17799.pdf (May 9, 2004).

[14] CERT Coordination Center. "Dealing with External Computer Security Incidents" 2001, p.4. URL: http://www.cert.org/archive/pdf/external-incidents.pdf (May 9, 2004).

[15] CERT Coordination Center. et. al., p. 4.

[16] Microsoft Security. "Incident Response: Managing Security at Microsoft" January 1, 2003. URL: http://www.microsoft.com/technet/itsolutions/msit/security/msirsec.mspx (May 9, 2004).

[17] Messmer, Ellen. "Security holes force firms to rethink coding processes." April 19, 2004. URL: http://www.nwfusion.com/news/2004/0419codereview.html?docid=1647 (May 9, 2004).

© SANS Institute 2004, Author retains full rights.