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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Robin Stuart
GSEC Version 1.2e

The Enemy Within; The Role of the Security Administrator in Apprehending and Terminating the Malicious Insider

Preface

The following information is set forth to generally describe the tools available to security administrators to facilitate the apprehension and participate in the resolution of internal threats to your organization's sensitive or restricted resources. This discussion will include references to United States Labor Code and California state law. It must be stated clearly and unequivocally that I am not a lawyer. The information contained herein is meant to serve as a guideline reference. Nothing in this document should be relied upon without consulting your own or your company's counsel.

What Is A Malicious Insider?

While external threats to commercial networks continue to rise, the insider threat is still going strong. The Computer Security Institute/FBI annual Computer Crime and Security Survey for 2001 indicates that 31% of surveyed businesses reported internal system attacks while 91% of respondents detected Internet and email abuses by employees[1].

Generally, the term "insider" implies a user with a legitimate presence and purpose within an organization's perimeter defenses. However, the definition is potentially controversial. A user may be considered an insider as to specific resources while an outsider to others. This is addressed in The Challenges of Insider Misuse[2]:

> Clearly there are different degrees of logical insiders, relative to the nature of the systems and networks involved, the extent to which authentication is enforced, and the exact environment in which a user is operating at the moment. A user may be an insider at one moment and an outsider at another. A user may be also be an insider within one operational frame of reference and an outsider at another…Thus, everything is relative to the frame of reference -- what the user is trusted to be able to do, what privileges are required, and what data or programs are being referenced, whether the user authentication is strong enough to add credibility to user identities.

---

[1] CSI press release. "Financial Losses Due to Internet Instrusions, Trade Secret Theft and Other Cyber Crimes Soar." 12 March 2001
URL: http://www.gocsi.com/prelea_000321.htm. 24 July 2001

[2] Neumann, Peter G. "The Challenges of Insider Misuse." 23 August 1999
URL: http://www.csl.sri.com/users/neumann/pgn-misuse.html. 24 July 2001

© SANS Institute 2000 - 2005 Author retains full rights.

For ease of reference, hereinafter the term "insider" will refer to the ordinary end user with no superuser or system administration privileges.

The word "malicious" is much simpler to define. The term refers to the intent of the user, as in one who intentionally operates outside the parameters of acceptable behavior. The groundwork for delineating such parameters is laid by your company's employee handbook, specifically, the information systems' acceptable use policy.

Planning Ahead

The most crucial and often overlooked stage in securing the availability, integrity, and confidentiality of data is planning. This includes defining the processes and procedures governing worst-case scenarios, such as employee abuses of information systems. But I'm getting ahead of myself.

It is incumbent upon the Security Administrator to be involved in the creation of an organization's statement of acceptable use of computer systems, email, and the Internet. Sample elements to include are:

- Complexity requirements of passwords
- Protection of confidential information (physical security standards and encryption requirements)
- Backup policies
- Software installation/download policies
- Acceptable uses of email

These are just a few examples. Your company's business and practices will dictate your specific needs.[3]

Just as important as defining the types of activities that are acceptable is providing guidelines for determining misuse. When itemizing behavior that is unacceptable, a prudent prefacing phrase is "including but not limited to." By stating that this, that, and the other activities are unacceptable, it is arguable that the ONLY unacceptable behaviors are those listed. The phrase, "including, but not limited to," clearly describes the listed behaviors as exemplar. Among the items to include in the category of unacceptable behavior:

- Viewing, storing, downloading or forwarding objectionable materials (such as pornography)
- Using email to send or forward confidential or unauthorized information
- Sending sexually explicit or offensive email

[3] e.g., financial institutions are now subject to the Gramm-Leach-Bliley Act which sets forth "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information." [16 CFR Part 314, 314.1(a)].

© SANS Institute 2000 - 2005 Author retains full rights.

- Online gambling
- Playing games
- Entering non-work-related chat rooms
- Attempting to gain unauthorized access to restricted resources

Finally, the acceptable use statement should describe the consequences of unacceptable behavior. If failure to comply with the policy could potentially result in termination of employment, say so in the policy.

It is advisable to have new hires initial or sign the documentation to indicate that each person has read and understands organization's policies. This establishes a clear record that employees are aware that your company expects them to adhere to standards of conduct and that they understand the possible consequences of violating those standards.

In addition to acceptable use statements, the computers themselves provide another opportunity to exercise your security standards. Of course, any blanket "welcome" at the system sign-on should be avoided on all platforms. Legal dogma popularly holds that "welcome" infers an invitation, thus undermining any claims of trespass or intrusion. Warnings are also helpful, particularly if your company intends to prosecute users who engage in illegal activities using company computers or attackers (both insiders and outsiders). Such warnings should specifically state that unauthorized use or access is prohibited and that signing on is the user's consent to being monitored. The actual language should come from your company's legal department.

Does all of this seem like a lot of legal positioning? It should. That's exactly what you're doing. Remember, planning is crucial. The stage needs to be precisely set to enforce a secure environment. Enforcement requires consequences of non-compliance. Punishing an employee without providing evidence of wrongdoing is asking for trouble.

United State Labor Code 2922 provides the basis for at-will employment. It states:

> "An employment, having no specified term, may be terminated at the will of either party on notice to the other. Employment for a specified term means an employment for a period of greater than one month."[4]

According to the Code, an employer can terminate and employee without cause or justification. However, this rule has been successfully challenged. The case of *Cleary v. American Airlines, Inc.*[5] provides the legal basis for employee wrongful discharge lawsuits in California (and sometimes beyond). While a detailed legal analysis is outside the scope of this document, not to mention my area of expertise, the court in *Cleary* held:

---

[4] As amended by Stats. 1971, ch. 1580, section 1, p 3186; Stats. 1971, ch. 1607, section 2, p. 3459
[5] *Cleary v. American Airlines, Inc.*, 111 Cal.App.3d 443 29 October 1980
URL: http://caselaw.lp.findlaw.com/ca/calapp3d/111.html (free registration required)

© SANS Institute 2000 - 2005 Author retains full rights.

> "Termination of employment without legal cause…offends the implied-in-law covenant of good faith and fair dealing contained in all contracts, including employment contracts."

In plain English, this means that in order to fire someone, you better have a reason. To satisfy this requirement, preparing for the worst is necessary.

Most companies are savvy enough to have a termination process in place whereby objectionable conduct is handled systematically. The steps are typically a verbal warning, a written warning, then final termination. The Security Administrator plays a role in each stage of the process in cases where the misconduct involves the information systems or resources. As we've discussed, the Security Administrator supplies documentation as to foreseeable abuses while leaving open the possibility of the unforeseen. He or she has an ongoing role by implementing the tools and practices that provide the checks and balances to monitor employee behaviors. This is all accomplished with a security policy.

The security policy is the cornerstone that documents the guiding principles, procedures, roles and responsibilities required to establish and protect the confidentiality, availability and integrity of an organization's computing environment. A full discourse on security policies is beyond the scope of this document. For more information, Carnegie Mellon's CERT Coordination Center offers excellent references in evaluating resources at risk and security policy elements[6]. At this point, we will focus on the aspects integral to identifying the malicious insider. The key to this is auditing.

To decide which resources to audit, look at your network to determine where sensitive, confidential, and/or mission-critical data reside. Financial institutions, for example, are legally required to treat customer data as confidential and protect the information accordingly. Therefore, auditing participating resources, such as storage and customer account services, is a priority. Which servers provide mission-critical services? If your company offers web-based services, auditing of all Apache servers is paramount.

For the purposes of this document, it is assumed that perimeter defenses, such as firewalls and intrusion detection systems, are in place and that your proxy servers are secure. But how do you protect your internal resources from your employees? There are two ways: monitor traffic and monitor the resources themselves. A large enterprise organization with high bandwidth availability may opt to implement both methods. Manageability of data to analyze is also a question to consider. Too much information is often just as bad as not enough. An overwhelmed security analyst is more likely to miss subtle details indicating an intrusion attempt.

The next question is how often to review the audit data. That's easy – as often as

[6] URL: http://www.cert.org/security-improvement/

© SANS Institute 2000 - 2005 Author retains full rights.

is possible and reasonable. Daily is ideal. Filters help in keeping the tedium of this task to a bearable level. Events of interest would be logon failures and successes, security policy changes, and startup/shutdown.

Finally, the security policy should address the management of the audit data itself. Where do you collect and store audit data? Protection of collected data is paramount; audits are meaningless if they can be tampered with.

The security policy works in partnership with the company's overall acceptable use statement by delineating procedures to establish and preserve the evidence of employee misuse. Such procedures include preservation of the integrity of log files or collected data, the type of data collected, and a record of the handling of the data, known as a "chain of custody." In his article, An Introduction to the Field Guide for Investigating Computer Crime, Part 1, Timothy E. Wright defines the chain of custody and its importance:

> …this means accounting for who has touched a given piece of evidence, when they touched it, and what they did to the evidence. It's a way of demonstrating that evidence hasn't been damaged or tampered with while in the care of the investigator. In his book, *Criminalistics: An Introduction to Forensic Science*, Richard Saferstein notes, 'Failure to substantiate the evidence's chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it (pg. 48).' As one would imagine, changes to the chain of custody can quickly ruin a case.[7]

Those with the authority to preserve and maintain the data should be identified in the security policy. User ID's specific to the task of chain of custody should be created and assigned to those people, used only for this purpose.

Caught In The Act

It's time to put this all together.

Let's say Company X is an asset management firm and has an acceptable use policy signed by all new hires. The Security Administrator (hereinafter "SA") has documented and follows an audit policy whereby she monitors certain production NT servers on a daily basis. These servers store customer financial records and account information. In User Manager for Domains, in Audit under the Policies menu, she has enabled the security log to audit all events for success and failure. Using the resource kit tool `dumpel`, the SA dumps copies of the security logs to an Access database on her secured workstation to which only she and one backup information security administrator have physical and remote access. She routinely filters the collected data for logon

[7] Wright, Timothy E. "An Introduction to the Field Guide for Investigating Computer Crime." 17 April 2000. URL: http://www.securityfocus.com/focus/ih/articles/crimeguide1.html 27 February 2001

© SANS Institute 2000 - 2005 Author retains full rights.

successes, failures, policy changes, and shutdowns.

It's late afternoon on a Thursday and our SA reviews the day's audit logs before she goes home. She's thinking of her evening plans when she spots this:

> 8/2/01,1:35:11PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
> CUSTOMERDATASVR,bad guy customerdatasvr 3 KsecDD
> MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

In fact, she spots three similar entries in a row.

Disseminating the record, line by line:

Line 1: date (August 2), time (1:35 pm), category (16 = logon/logoff), logon (2), event ID (529), log type (Security), unrecognized username or password (NTAUTHORITY\SYSTEM).

Line 2: Servername (CUSTOMERDATASVR), user id (bad guy), domain name (customerdatasvr), logon type (3), kernel security device driver (KsecDD)

Line 3: NTLMv1, originating desktop (bad guy's machine's NetBIOS name)

Translated, from his own workstation, Bad Guy attempted to log on to the server CUSTOMERDATASVR over the network, using his own account name and password. The event ID of 529 indicates that his attempt failed. The domain name and the server name being identical indicate that the user attempted to gain local access to the server.

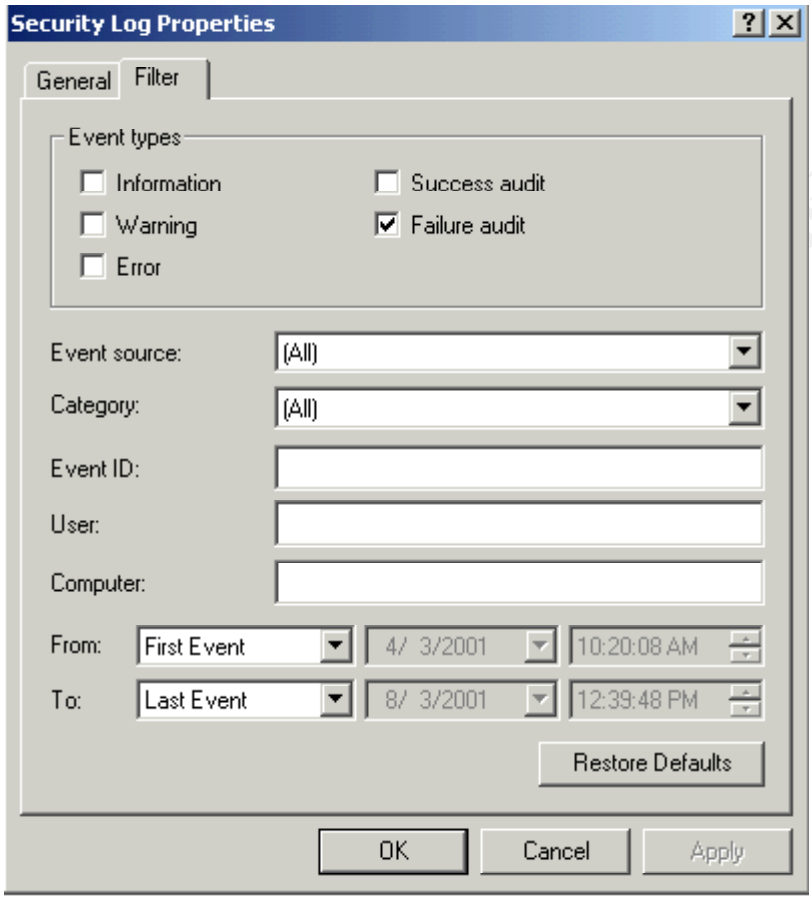
This is potentially worrisome but not the end of the world. The user had no business attempting to gain access to the server but, buoyed by his failure, our trusty SA is not going to sound an alarm just yet. The fact that Bad Guy attempted access with his own user ID indicates that the logon attempts may have been misguided or, at worst, attempted out of curiosity. The SA's thoughts return to the night ahead. That is, until she reviews the `dumpel` output on Friday and sees a repeat performance by Bad Guy. Three more bad logon attempts.

The data now establishes a pattern of an ordinary user attempting to gain unauthorized access to a restricted resource. Such behavior is clearly prohibited in the employee handbook under the information systems' acceptable use guidelines.

The security policy's evidence handling guidelines spring into action. The SA copies the complete `dumpel` logs for the days in question to a new file on a secured hard disk set aside for evidentiary purposes, configuring the NTFS permissions on that file to exclude everyone but the authorized evidence collection IDs. She also copies the logs into a zip file on a floppy disk. Next, as is documented in her procedures, she remotely logs

© SANS Institute 2000 - 2005, Author retains full rights.

onto the server and opens the event viewer. She filters the view of the Security log to show only failed logons (View – Filter Events, checking the "Failure Audit" box as shown).



The SA does a print screen of the resulting event viewer log and saves it as a bit-map file to the same newly created evidence directory. The SA copies the evidence to a zip file and stores it on the floppy disk containing the `dumpel` log zip file, prints the contents of the disk and locks the floppy and hard copy of data into a desk drawer to which only she has the key. Finally, she creates a written log of the data collected, the date and time collected, and the whereabouts of soft and hard copies of the data collected.

Now she's ready to notify management that a violation has occurred. This notification process is also documented in the security policy. She calls the human resources person assigned to this task and provides a printed copy of the evidence to the HR representative.

According to the company's policies, the SA's role in the first warning to the employee is complete. A meeting will be scheduled between the HR representative and the employee wherein the transgression will be pointed out and the employee will be warned that these incidents violate the company's information systems' acceptable use

© SANS Institute 2000 - 2005 Author retains full rights.

policy.

The SA goes about her business, not giving the episode another thought until several days later when her daily audit turns up the following:

8/7/01,10:27:11AM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,Administrator customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

In fact, she spots three similar entries in a row, followed by:

8/7/01,10:34:33AM,16,2,539,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,Administrator customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

What's different this time? A couple of things. First, Bad Guy is now attempting to gain access to the server using the Administrator account. Second, in the last record we see the error event code of 539. This indicates an account lockout; Bad Guy used up his chances in guessing the administrator account password.[8]

It's getting more serious. Bad Guy – or someone at Bad Guy's workstation - is attempting to gain root access to a restricted resource. This is an absolute violation to the company's policies. The SA wastes no time. She collects the data, once again following the data collection and evidence non-repudiation procedures as dictated by her security policy. She records her every move on the written log, as she did following the first incident. Upon notifying her HR contact, her role is once again completed. The HR representative will meet with Bad Guy again, this time to issue a warning in writing and obtain Bad Guy's signature on the warning.

Our faithful SA continues her regularly scheduled activities. Surely Bad Guy has gotten the message. A few weeks later, she sees something out of the ordinary in her daily audit:

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,Administrator customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,Administrator customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,

[8] The true administrator account should always be renamed and the default Administrator account should be disabled. In this example, a bogus "Administrator" account with no permissions has been created as a means of identifying unauthorized privilege escalations, hence the resulting account lockout.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

CUSTOMERDATASVR,Guest customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,Guest customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 \\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,IUSR_CUSTOMERDATASVR customerdatasvr 3
KsecDD MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,IUSR_CUSTOMERDATASVR customerdatasvr 3
KsecDD MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,IWAM_CUSTOMERDATASVR customerdatasvr 3
KsecDD MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,IWAM_CUSTOMERDATASVR customerdatasvr 3
KsecDD MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,SecAdmin customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

8/30/01,5:53:19PM,16,2,529,Security,NTAUTHORITY\SYSTEM,
CUSTOMERDATASVR,SecAdmin customerdatasvr 3 KsecDD
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
\\BADGUYWKSTN

Several details stand out. Each user ID is tested twice. The attempts are default users and a legitimate account, namely, the Security Administrator's. And all attempts bear the identical after-hours time stamp. Bad Guy had used an automated utility to identify and attempt access under each local account, within the account lock-out limit of 3 attempts.

There is nothing harmless indicated here. The SA follows the escalation procedure documented in her security plan, immediately notifying her management contact of the

© SANS Institute 2000 - 2005 Author retains full rights.

attempted security breach. She collects her data and logs the evidence. A meeting is called, attended by the SA, management, the legal department and human resources. The employee has been sufficiently warned, following company guidelines and in satisfaction of common employment law standards. In-house counsel takes custody of the evidence. The employee will be terminated. The only question is whether or not to prosecute.

The SA has a few things left to do. Immediately disable the user's account. Confiscate and preserve the desktop machine from which he conducted his activities for forensic study and evidence, should legal proceedings follow. As a precaution, change all passwords within the organization.

Conclusion

The scenario presented here is not altogether implausible. In real life, however, malicious insiders can and will be much more savvy. This paper began with a promise to illustrate the tools available to information security professionals to facilitate the apprehension and participate in the resolution of internal threats to your organization's sensitive or restricted resources. Those tools, as I've described, are planning, procedure, and practice. A security plan is meaningless without procedural guidelines. Working with legal professionals will help give your policy teeth and help determine your escalation and evidence-handling guidelines. But all of it is just a bunch of paper unless the words are put into practice.

References

CSI press release. "Financial Losses Due to Internet Instrusions, Trade Secret Theft and Other Cyber Crimes Soar." 12 March 2001
URL: http://www.gocsi.com/prelea_000321.htm. 24 July 2001

Neumann, Peter G. "The Challenges of Insider Misuse." 23 August 1999
URL: http://www.csl.sri.com/users/neumann/pgn-misuse.html. 24 July 2001

Federal Trade Commission 16 CFR Part 314, Standards for Safeguarding Customer Information, RFC period ending 9 October 2001.
URL: http://www.ftc.gov/os/2001/07/stansafecustinfofrn.htm. 31 July 2001

United States Labor Code §2922 as amended by Stats. 1971, ch. 1580, §1, p 3186; Stats. 1971, ch. 1607, §2, p. 3459

Cleary v. American Airlines, Inc., 111 Cal.App.3d 443 29 October 1980
URL: http://caselaw.lp.findlaw.com/ca/calapp3d/111.html (free registration required)

Wright, Timothy E. "An Introduction to the Field Guide for Investigating Computer

© SANS Institute 2000 - 2005 Author retains full rights.

Crime." Parts 1 through 7. 17 April 2000 through 26 February 2001.
URL: http://www.securityfocus.com/focus/ih/articles/crimeguide1.html
27 February 2001

Tan, John. "Forensic Readiness." 17 July 2001
URL: http://www.atstake.com/research/reports/index.html. 3 August 2001

Carnegie Mellon University CERT Coordination Center. "Establish a Policy and Procedures That Prepare Your Organization to Detect Signs of Intrusion." 18 October 2000
URL: http://www.cert.org/security-improvement/practices/p090.html. 1 August 2001

Computer Crime and Intellectual Property Section (CCIPS). "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." January 2001
URL: http://www.usdoj.gov/criminal/cybercrime/ 8 August 2001

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.