Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Security: Handling Compromises

As the Information Systems Security Manager (ISSM) for an organization within DoD, I am responsible for ensuring the overall security stance of our network. This includes physical security and network security. Part of maintaining our security stance is ensuring that information considered sensitive to national security does not reside on the unsecured network. Occasionally this information of this type is introduced onto the unsecured network and it is my job to create and implement the procedures that erase the data ...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Information Security: Handling Compromises

Craig L. Bowser

August 15, 2001

As the Information Systems Security Manager (ISSM) for an organization within DoD, I am responsible for ensuring the overall security stance of our network. This includes physical security and network security. Part of maintaining our security stance is ensuring that information considered sensitive to national security does not reside on the unsecured network. Occasionally this information of this type is introduced onto the unsecured network and it is my job to create and implement the procedures that erase the data from the network to ensure it cannot be recovered if an unauthorized user gains access to our network.

While the corporate sector may not be guarding national secrets, they are protecting valuable information such as trade secrets, financial documents and personal information. Often this information is kept (or should be kept) sectioned from each other. In the case of trade secrets or financial documents such as earning forecasts, this information could only be available to a select few. Similar to the DoD, companies would want to make sure that this information did not get onto an unsecured part of the network and if it did, make sure it got cleaned in such a way that no one, from the casual user to the determined hacker, could recreate the data. Therefore, corporations need to create and implement procedures to prevent the contamination of networks, contain contaminations and eliminate contaminations from unsecured areas of their networks just as much as government organizations.

While researching this topic, I found several articles mentioning that corporations should sanitize their drives when the computer changes ownership along with suggestions of which software tools to use. This is and always should be a mandatory task. There are stories about some school receiving a Government computer and finding classified information still residing on the hard drive. The government has written several regulations, instructions, and manuals that address what the standards are for cleansing and what methods are appropriate. However, in my Internet search efforts, I did not find any articles of any type (and surprisingly no Usenet hits either) discussing exactly how companies should go about eradicating confidential information from unsecured areas of their network. So even though I am not in the corporate world, I will apply what I have learned to suggest some policies and procedures that can apply to both sectors, government and civilian. I will also share some lessons learned. Please note that while the terms "corporate" or "corporation" are used throughout the writing, this paper does apply to both the government and civilian sectors.

Before I begin, I would like to reference the reader to Robert E. McFarland's paper "Incident Handling: The Art of Containing Compromised Information" (http://www.sans.org/infosecFAQ/incident/containing.htm) as I will use several of his terms. His article is straightforward and instructive, but I believe there are several areas that he missed and other areas that should be

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

expanded. McFarland introduces the concept of an Incident Coordinator (IR) who is responsible from initial call to the restoration of services. However, before this IR can begin to respond to the initial call regarding a compromise, there are several tasks he or she should accomplish before a compromise that will make his job easier during a compromise. These are listed below:

1. User Education
2. Building separate LANs for highly critical data
3. User Education
4. Content Filtering software (email, FTP)
5. User Education
6. Pre-Approved policy with specific Standard Operating Procedures (SOPs)

I know 1, 3 and 5 are the same, but the point is that you can't emphasis user education enough, it is your first line of defense to prevent compromises. This is one of those areas of security that you must depend on the user knowing how to correctly handle sensitive information. If the user knows what type of information he is working with and how he needs to protect it and follows through with that protection, you have solved 70 – 75% of your problem. I have found that most of the compromises I deal with occur because the user does not realize what the sensitivity is of the information he is handling. User education also increases user awareness; they go hand-in-hand. This prevents the fail-to-check syndrome, the next largest group of compromises I have seen. These happen when someone does not look at what is in the email or attachment he just got and forwards it onto someone(s) else. Then the user learns later that something in the email or attachment is sensitive in nature. Educating users to know what they are handling and to be aware of what (and how) they are sending it can significantly reduce your number of compromises. The last type of compromises I have seen are mostly out of your control. These happen when someone from outside your organization sends you sensitive information. Hopefully, your content filtering software catches it and then you only have to scrub one machine. But if it doesn't, then you are launched into you SOPs regardless of how well you are set up.

Secondly, physically separate networks that have critical information and networks that house your everyday network. Everyone knows the government has separate LANs for handling different levels of classification. If your company is not doing this and can afford to set such a system up, it may be worth the effort especially if there is an airgap between the two networks. Provided you had no other remote access points, an airgap would really prevent any malicious outsiders from getting in!

Next, look into installing content filtering software at strategic points on your network. Place email content filters at your gateways to check for key words and block or quarantine mail containing those words. Do the same with FTP and Telnet servers. These content filters often are able to look several layers deep into files even if they are zipped. Run all web page and bulletin board postings past an Information Assurance Public Affairs person. This will

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

give you another layer of security to stop information compromise. Lastly, McFarland mentions having a pre-approved site policy, but what you need to include in this policy is a pre-approved Standard Operating Procedure (SOP) that tells *how* the Incident Response Team (IRT) will react and *who* will do *what, when.* This way when a compromise happens (and if you work in a corporation that deals with sensitive data, it's only a matter of time), anyone can pick up the SOP and act as the IR.

When writing the SOP, it is important to clearly state to order in which work will flow and the order in which to make decisions. These must be shown and people trained in a manner everyone involved can understand or events will happen out of sequence creating chaos. Chaos will only result in longer recovery times and missed tasks. The other thing to make sure of is that each position is not one deep and the contact information for everyone is include in the SOP or somewhere within reach. Keep this information up to date! It will not look good because you cannot do a server restore because the person responsible is on vacation or no one has the number of the new employee yet. The SOP needs to take into account if a spillage occurs during business hours, after business hours or on the weekend. Remember, there might be a different chain of events and contact personnel for each scenario. One final word on the SOP, the IR, or someone designated by him, should be the central contact. This central contact makes sure that procedures don't get our of step, decisions are not made prematurely, the right people are called and whoever is next is standing by. The coordination effort done by the central contact creates a smooth process from beginning to end.

Now what happens when a compromise occurs? The IR person is contacted and he should collect all the information suggested by McFarland AS WELL AS the Notifier's contact information. I can't tell you how many times we needed more detailed information to accomplish a cleansing only to find no one knows how to get in touch with the Notifier, who has that information or thinking his job is done, the Notifier has gone home! So I strongly suggest getting as much contact information as you can in the beginning, the Notifier, his Boss, etc and the cleansing will go smoother later.

Now that the IR has all the information about the compromise, here is where having the SOP pre-approved makes a big difference. Since the SOPs are pre-approved, everyone on the IRT should have a copy and as soon as they get the call can run off and do what they need to do. Everyone is one the same sheet of music and if your boss comes by and wants to know how things are going, you are able to immediately point to the step in the procedure you are at and give a status report. The first step that needs to be done is determine how extensive is the contamination and what needs to be done to stop it from spreading any further. This gives you an idea of how much effort will be needed for cleanup.

With everyone marching to the same beat, only one thing can slow the procedure down; determining cleansing level. There needs to be a step in your SOP where a decision is made to determine what type of sanitization should be done. This is an individual corporation decision, what may fit for one

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

corporation will not fit for another. Some corporations may feel the all its sensitive information is of such a level that if a compromise occurred, the media should be protected in the most stringent manner possible. Other corporations may feel they have different levels of data, some requiring stringent overwrites and others simply deletions. However your corporation feels, a decision must be made either before hand (a decision matrix included in SOP) or the decision maker must be contacted to render her judgment.

Based on that decision, there are several options to cleansing the media. First, you can just delete the data and continue on with business. This is short and sweet and will get you up and running again fast, but keep in mind that this will not get rid of the information as the data still physically resides on the disk. A malicious user can use commonly available software to retrieve that data remotely or locally from the hard drive.

The next level of cleansing is to overwrite the data. Since just deleting the data does not get rid of it, a number of vendors have created software that overwrites the spot on the hard drive where the data resided. With these products you can either select to overwrite the freespace on the hard drive, or you can choose a specific directory or file. To create a high degree of certainty that the information will be unrecoverable, you should have the software run at least three passes. The first pass should be bytes of 1s, the second pass bytes of 0s and the third pass bytes of a random mix. This method will prevent anyone sitting at the console or gaining remote access from recovering the deleted data. Several of these products claim to adhere to government standards. If the manufacturer shows you that their software overwrites according to the pattern above, they are conforming to government overwriting standards. However, if someone gains physical access to the media, they can still recover some or all of the information residing on it. The methods are tedious and time consuming, but if your enemy has the motivation and the money, it is possible.

Therefore, the last cleansing level is for the paranoid. The usually only applies to the government, but perhaps you owned a large software development company somewhere out west. If you were getting rid of computers that had been used to develop the latest version of your new OS, I think your competitors would have the motivation and money to invest in the tedious and time consuming methods needed to extract information off those hard drives! Consequently, you probably want to destroy any media with such sensitive information. This can be done by several methods including burning, sanding, sledgehammer and degaussing. (A note about degaussing: it is possible for certain types of media using the proper degaussing device to be degaussed without destruction. Please see "A Guide to Understanding Data Remanence in Automated Information Systems" NCSC-TG-025, http://secinf.net/info/rainbow/tg25.htm for more details). This will virtually ensure the data is unrecoverable in any kind of convenient time period, if ever.

You must have procedures in place to clean other media as well. The first thing is the backup tapes. You must properly handle all the contaminated tapes. Decide if the tapes should be labeled and stored in a secure area in case

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

non-sensitive information is needed off them or if the tapes should be destroyed. Tapes can also be erased or immediately (that night) overwritten. Also, consider if the data has been printed, saved to floppy or other removable media or put on a PDA. If it has been printed, collect the paper copies. If copied to a floppy, then you must delete, overwrite or destroy the floppy. The PDA needs to have its memory cleaned according to manufacturers instructions. This usually involves a hard reset. If the data was burned to a CDROM, the CD needs to be destroyed. This is accomplished either by breaking the CD or sanding it down so the data cannot be read by any CDROM drive.

Now that you have eradicated the sensitive data, you must bring everything back into operational status. Sometimes this is as simple as rebooting the PC. However there may be additional steps for certain systems. If the hard drive was destroyed then a new one needs to be installed. Email systems and databases may need to be restored from the last uncontaminated backup. The IRT needs to be prepared for each of these contingencies to minimize network downtime. Your boss is primarily concerned with two things: a clean system and getting back to business as quickly as possible. In my experience, he mostly will be more concerned with the latter. Therefore, it is your job to make sure your procedures expedite a quick return to full operational status after a proper cleansing.

The last item is to prepare an after action report. This report should tell who did what when and how big an effect the compromise caused in personnel, dollars and/or equipment. Then upper management should decide if any punishment is merited and what that punishment should be. Again, this should have been spelled out beforehand in policy so no one can claim ignorance or bias. The reports generated can be used to keep statistics. This way any upward trends in the number of compromises are noticed and actions taken to reverse the trend. Such actions might include increased user education, increased consequences or better network controls.

Here are some final tips. Constantly review your SOP. Each compromise that occurs will give you a chance to refine them further. I have had to work a number of compromises and our SOPs now can be run without my even being present. Be flexible, your boss might change how he wants the SOPs carried out due to what is happening on the job that day. However, do not give up on the goal of cleansing the systems. Always look for ways technology can make your job easier and quicker. If a technology comes out that shortens your overwrite time in half, you boss is more likely to support that option. If you plan well and show how smoothly your SOPs work, your boss will take confidence in the procedure and have faith in you enabling you to accomplish the task of restoring the system to full operations as quickly as possible while ensure the confidentiality of the information on it.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Sources:

Boran, Sean (1999) An Overview of Corporate Information Security, Retrieved August 15, 2001 from the World Wide Web:
http://secinf.net/info/policy/coverstory19991213.html

A Guide to Understanding Data Remanence in Automated Information Systems NCSC-TG-025, Retrieved August 15, 2001 from the World Wide Web:
http://secinf.net/info/rainbow/tg25.htm

Williams, Jim (2000) Deleted Files – Still There, Retrieved August 15, 2001 from the World Wide Web:
http://netsecurity.about.com/library/weekly/aa070300a.htm

CSL Bulletin Advising users on computer systems technology (1992), Retrieved August 15, 2001 from the World Wide Web:
http://csrc.nist.gov/publications/nistbul/csl92-10.txt

McFarland, Robert E., (2000) Incident Handling: The Art of Containing Compromised Information, Retrieved August 15, 2001 from the World Wide Web: http://www.sans.org/infosecFAQ/incident/containing.htm

Haley, Kelly S., (2001), The Unintentional Disclosure of Digital Data, Retrieved August 15, 2001 from the World Wide Web:
http://www.sans.org/infosecFAQ/incident/disclosure.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**