Global Information Assurance Certification Paper

ROBERT E. MCFARLAND

Incident Handling: The Art of Containing Compromised Information.

I am going to try and point out some of the issues that are involved in the business of containing compromised information. Whether it is a government site stopping the spread of classified emails or a private business stopping the spread of sensitive proprietary information via attached email document, these user accounts and desktops need to be disabled and cleaned. All of the issues that will be discussed are not unique to any one organization, but are problems that each company would need to address.

The first issue would be an *Incident Coordinator*. Every Computer Security Department should consist of one Incident Coordinator. This person should be able to bring all the resources to bear to contain the compromise. This person would also serve as the point of contact for the organization. If need be, this person would work hand in hand with local law enforcement and any computer crime lab involved in the collection of evidence for later use in the court room. A couple of good sources of information to check would be the Computer Incident Advisory Capability (CIAC) and the National Infrastructure Protection Center (NIPC).

The second issue could be the *Incident Response Team.* The makeup of the IR team needs to be in-depth. The Incident Coordinator will need, depending on the size of the site; a team of say 3 to 5 people. The question of how big the team should be will be answered by the speed in which management wants the people involved back up online. In today's network environment with multiple platforms, they need to be able to tackle all the different situations that may come along. It may be a good idea to have one or two team members trained to a higher level for those OS's that are in small number on the network. There is no need for everyone to be trained on Mac 9.0 OS desktop cleanup when there are only 50 out of 5000 workstations running it.

The first thing the Incident Coordinator person should get from management and put in place is a site policy. This is the only way to run a successful operation in any business setting. Also, you are covered when the boss asks why 15% of the users are disabled due to a compromised newsletter that was emailed or posted on a company Intranet web page. SANS Level One course book, page 5-1 has a good example of a "Basic Security Policy" template for an organization to start with. Another excellent source would be the "Handbook for Computer Security Incident Response Teams" from Carnegie Mellon/Software Engineering Institute. It is a very thorough book and offers several templates.

Another decision is what cleanup software to use and the procedures on the proper use of these tools. Some of the tools on the market encrypt the file, then you can secure delete it, while other software programs wipe the file by government standards or even better. One very good tool is Norton's Your Eyes Only, a very thorough tool that has been around for a long time. It can be used with Windows 3.x, 9x, NT 3.5 and 4.0, but it is not compatible with Windows 2000. There is also a version for MAC. At the time of this

writing, this product is no longer in production. That doesn't mean it is at the end of its life. I do believe that most of this OS's will be in production networks for a long time. BC Wipe and Secure Clean are other fine products for desktop cleanup. Something to consider as the Incident Coordinator is the continued evolution of the different operating systems and how the cleanup software will perform on each one. Some of these cleanup programs wipe the swap file or the slack spaces in a cluster, others don't. This person should be conducting lab tests on all the different variables, this way the Incident Coordinator will be able to consult with management on which program will fulfill the requirements of the site policies.

Lets study and follow an email incident from the beginning to the final report. When the call comes in, the Incident Coordinator should log as much information about the incident as possible. There should be a set of approved forms that are used for each incident. Some of the information that should be collected includes;

Person that notified the team;
Name of Originator:
Level of the Incident: i.e. (Sensitive, Classified)
Time:
Nature of the Incident: i.e. (Copy of the Sensitive Email or document)
IR Team members assigned to the case.

These questions will cover the "Who, What, When, Where and How?". The Incident will need to have a incident tracking number assigned to it. This should be a unique tracking number assigned for each case.

The Incident Coordinator or the designated authority, will need to suspend all User accounts involved in the incident to stop the spread of the compromise, especially when dealing with an email. Again, there needs to be a sound site policy in place that covers the suspension of accounts in the event of an incident.

If it is an email incident, all the mailboxes involved on the Mail Server/s will have to be cleaned before the team members are sent to the user's desktop. Depending on the way the site sets up their email servers, this may be the only cleanup required. If the PST's are mapped to the local hard drives or division storage area, then each user desktop will need to be checked. Also keep in mind the time factor involved in an email server cleanup. The person conducting this doesn't need any distractions around while checking and cleaning up any mailboxes with compromising emails. One other thing is the backup tapes, don't forget to get these checked.

When the IR team member shows up at the desktop in question to do the cleanup, he/she will need a complete understanding of the information that was compromised to conduct the search. Utilizing a good search string that is unique to the email or document will cut down on the time the user is suspended. It is best to use only one word for the search string. Look for a misspelled word in the email or document to use. Also for email, search on the subject. Check for pointers, they may lead to a removable storage device.

Was there any hard copies made by the user? There are several questions the IR team member will need to ask about the compromise. If the user knows nothing of the email or document, then there is a good chance the server cleanup personnel got to it first. If the email or document is found on the desktop, the IR team member will need to load the cleanup software. Depending on the size of the file and your site procedures, it may take several hours to cleanup the hard drive and activate the user account

When all the desktops have been checked by a IR team member, the Incident Coordinator will need to gather all of the paperwork involved in the incident. This may include user statements collected at the desktop by IR members. These incident reports can be used by upper level management to track the root cause of the problems and take corrective action to cut down on production time.

In closing, if the Incident Coordinator has the right IR team members and tools, the cleanups will go a lot smoother, in turn keeping management happy.

Best of luck.

Sources:

SANS Home page URL: http://www.sans.org/newlook/home.htm

Moira J. West- Brown Don Stikvoort Klaus- Peter Kossakowski "Handbook for Computer Security Incident Response Teams (CSIRTs)" December 1998 HANDBOOK CMU/ SEI- 98- HB- 001 Pittsburgh, PA 15213- 3890
URL: http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

SecureClean v 3.12
http://www.whitecanyon.com/index.html

BCWipe v2.31
http://www.jetico.com/

Norton's Your Eyes Only
http://www.symantec.com/index.html

NIPC
http://www.nipc.gov/

CIAC
http://www.ciac.llnl.gov/

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event