Global Information Assurance Certification Paper

Incident Illustration - Magistr Virus/Worm

Christopher Loomis
GCIH assignment version 1.5c option 1

To do business in our interconnected world, companies have to assume a degree of risk. The task of the information security departments of those companies is to manage that risk. We will take a look behind the scenes of the security department of a large company, which we will refer to as "ABC Corp" (Original? No. Sanitized? Yes.). In particular, we will examine ABC Corp's Anti-Virus (AV) Team, in hopes of gaining a better understanding of not only what actions they take when battling a computer virus, but why they take them. Also, we will learn how theory is put into practice by looking at how the AV Team handled the recent Magistr virus/worm, in which I played a very minor part in resolving.

Note: This is not an attempt to determine whether or not the policies and procedures adopted and implemented by ABC Corp are the "right" ones, but instead to illustrate how they correlate and differ from those which are generally acknowledged as best practices as described in the Incident Handling Step-by-Step Guide from SANS. As outlined in the guide, there are six stages of incident handling: Preparation, detection, containment, eradication, recovery and follow-up.

Preparation

Preparation refers to those tasks that should be considered before any actual incidents occur. This is a critical phase of incident handling as the policies and procedures that are implemented here form the foundation for all subsequent incident handling efforts.

1. Post Warning Banners - It is important from a legal standpoint for a company to use warning banners. Investigations are much easier as banners cut through a lot of legal red tape and exclude some potential defenses for transgressors.

ABC Corp displays the following banner at user login:

```
These computer resources are solely owned by the Company.
Unauthorized                  access or use is a violation of
federal law and could result in criminal prosecution. Users agree not
to disclose any company information except as authorized by the
Company. Your use of this computer system is consent to be monitored
and authorization to search your personal computer to assure
compliance with company policies.
```

2. No Presumption of Privacy - This is important for the same reasons as (1)

above. Note that it isn't enough that the company has this policy, but it is also important that they make sure that the users are informed of the company's position.

ABC Corp displays the following in the security policies section on the company intranet:

```
All messages sent over ABC Corp internal computer communications
systems are the property of ABC Corp. To properly maintain and manage
this property, management reserves the right to examine all
information transmitted through these systems. Examination of such
information may take place without prior warning to the parties
sending or receiving such information. Workers should have no
expectation of privacy associated with the information they store or
send through these systems, including deleted files.
```

3. Establish an Organizational Approach to Virus Handling:

A. Preauthorization for actions - During the course of handling an incident, many critical decisions must be made and immediate actions taken. It saves a lot of time and aggravation if management is willing to trust the judgment of the incident handlers and allow them to make some of these decisions themselves. It is very important for all of the parties involved to get together before an incident occurs to lay out (in writing) which calls the incident handlers can and cannot make on their own. Sometimes incident handlers have to work with "micromanagers" who insist on making every critical decision. Repeated, urgent phone calls to them at three in the morning usually help them to come around.

At ABC Corp, the AV Team, in cooperation with other units that assist it, have the authority to do whatever they deem is necessary to fix the problems. In my conversations with them, however, they explained that they would consult management if it looked as though some very drastic measures would need to be taken (i.e. disconnecting from the Internet or shutting down the system). Fortunately, it hasn't come to that, as the AV Team has yet to have to shut down any servers, much less networks, and have never had to format and reinstall anything above the workstation level.

B. Contain & Clear vs. Watch & Collect - This is a real hot button topic in security circles these days. "Contain and clear" means that the company is only concerned with getting the problem contained and eradicated, bolstering defenses, then getting back to business. "Watch and collect" involves monitoring an intruder in hopes of gathering evidence which may be used to prosecute him and attempting to track down his point of origin.

ABC Corp has decided that it doesn't make much sense to go with the "watch and collect" approach with a virus outbreak, since there really isn't anyone to watch. They are instead concerned about getting the mess cleaned up, blocking, or at least hindering, the entry vector of the virus and getting the users back to work.

C. Notify external parties? - Companies these days are torn between involving external parties to help resolve incidents or keeping things to themselves. Many companies that feel they have adequate resources have decided that they are better served to "go it alone" rather than sharing the information and risk the chance of bad publicity by exposing the breach.

ABC Corp works very closely with its AV software vendor during an incident. The vendor is counted on for tips on detection, containment and eradication, but most importantly for updated virus definitions. ABC Corp does not currently notify law enforcement, CSIRTs or ISPs, since they prefer to keep these things in-house and confidential.

D. Clearly define monitoring boundaries - This has become more of an issue with the massive increase in mobile computing and employees accessing company resources from home. It is also an incredible security risk. Companies need to extend their defenses to include these remote users.

ABC Corp is going through this right now. They currently allow employees to dial-in from their home computers. Even though it is made clear to the users that all security policies apply to them regardless of where they are accessing the network from, there is no real way for the company to ensure that the users are adequately defending their computers, and subsequently the ABC Corp network, with anti-virus software and firewalls. Therefore, ABC Corp has decided that it will only allow access from company-provided computers that employees may use from home. These computers will come preloaded with AV and firewall software with auto-update capabilities, which allows ABC Corp to be confident that its perimeter defense is consistent and up-to-date.

4. Develop Management Support - If an incident handling capability is going to be successful, it almost always needs the backing of management (particularly upper management). Without it, you will probably not get the money, resources or authority you need in order to be effective.

At ABC Corp, management is supportive, informed and involved. Being the cynic I am, I asked the head of the AV Team how the heck that happened. He just smiled and said one word - "Pain". It took a couple of pre-AV Team incidents, which did not go so well, before upper management "got it". With their support, the lower-level managers were quick to fall in line.

5. AV Team and Architecture - There are a variety of AV architectures and approaches that a company may choose to combat viral outbreaks.

ABC Corp has decided to go with a combination control structure with four core members for the AV Team. This means that the members of the AV Team coordinate responses and either go on-site to fix problems or use PCAnywhere to get to remote boxes. There is a rotating Primary Point of Contact so that they can provide 24 hour AV coverage, with all members being expected to report for

duty during high-volume incidents. As for software solutions, ABC Corp has implemented a multi-level defense system:

Internet Gateway	: 2 servers	: Handles content filtering and port blocking.
AV Servers	: 9 central repositories	: Signatures are updated here daily from the vendor. Workstations are updated from these central repositories, also on a daily basis.
Mail System	: 16 servers	: Scans all emails. Able to filter and clean.
PCs	: 24,000+ machines	: AV software on all Windows machines (about 95% of the hosts). Able to scan and clean.

To give you an idea of the volume this system is handling, the AV software at the workstation level has intercepted year-to-date over 5,000 infection attempts and over 45,000 infection attempts have been intercepted at the mail system level.

ABC Corp basically relies on scanning to detect viruses. This means that the AV software searches for strings or certain algorithms that are known to exist in each particular virus. The drawback to this approach is that you can only scan for known viruses. There is an additional problem when dealing with polymorphic viruses (such as Magistr), since the signatures and algorithms are becoming increasingly sophisticated in order to avoid detection. The AV Team is well aware of these shortcomings and is resigned to having to fight these types of viruses "one box at a time". They have stepped up education efforts directed at users in an attempt to stop the problem at the best time possible - before it starts. Also, they do run some heuristic scans, which look for virus-like behavior on the system and can detect previously unknown viruses. The drawback with these it that they may return a large amount of false positives. When something suspicious is uncovered by a heuristic scan, a sample is sent to the AV vendor, which is quick to confirm or deny if it is in fact a virus.

6. Emergency Communications Plan - This involves making sure that the right people get the right information at the right time. In times of crisis, it is important to have the capacity to employ various modes of communication in case the primary mode is not available.

ABC Corp uses call lists and call trees in order to inform critical people quickly, with several possible communication methods to choose from. Land line phones, cell phones and pagers may be used for incident handlers. Users may be notified en masse with email, the intranet and a PA system.

7. Encrypted Communications - Used to prevent an intruder, or anyone else not on a "need to know" basis, from intercepting communications between incident handlers.

AV Incident Handlers at ABC Corp do not use encrypted communications. As far as I know, there aren't any viruses in the wild that can intercept

communications (Oh, man. I don't even want to think about that!). Nevertheless, it may be a good practice for ABC Corp's security staff to consider encryption of all security-related communications, as you never really know who may have access to them. The AV Team is currently testing a variety of PKI solutions in order to secure their communications.

8. Provide Easy Reporting Facilities - With all incident handling, and particularly viral incidents, timely reporting may mean the difference between a minor inconvenience and a major headache. Therefore, it is important that users know how to identify possible infections, what they should do with the suspect computer and whom they should notify.

ABC Corp has a simple strategy for reporting - at the security website on the company intranet it directs users who think that their computer may have a virus to call the I/S Help Desk. I will describe user education efforts in more detail in the Identification section.

9. Interdepartmental Cooperation - Before an incident occurs, those areas, which may be involved in the resolution of that incident, should get together so that everyone's responsibilities are clear.

ABC Corp has implemented educational programs for Help Desk workers that clarify how they can determine which events warrant further investigation and need to be forwarded to the AV Team. During an outbreak, the AV Team would notify the Help Desk as to what specific viral indicators they should be on the lookout for, what questions they should be asking users who suspect that they may be infected and what information they should divulge to curious, uninfected users.

Identification

Identification refers to event detection activities, the subsequent investigation of those events to determine whether or not they are actually incidents and the notification of the parties who are responsible for handling those incidents.

1. Incident detection methods:

A. Sensor Platforms - These are a company's hardware and software mechanisms designed to detect and remove viruses and other malicious code.

For ABC Corp, these have been detailed in the 'AV Team and Architecture' section above. I also chose to include some additional information below, since it illustrates how a combination of several small errors can cascade and ultimately result in infection.

ABC Corp displays the following in the security policies section on the company intranet:

```
All personal computer users must keep the current versions of
approved virus screening software enabled on their computers.
```

There was a breakdown at this stage at ABC Corp that left the machines in my particular building vulnerable to the Magistr virus, of which several became infected. It turns out that the software that was used to auto-install the latest AV version failed to update the machines in my building, leaving us running the older version that did not pick up Magistr. At the time, there was no way for the AV team to identify what version of AV software each workstation was running or for users to know if they missed an update. It took an infection to expose the problem. Fortunately, all machines now have software on them that allows the AV Team to quickly identify what version each machine is running along with the capability to do a host of other AV administrative tasks.

B. People - Users need to be trained how to spot potential viral problems, what to do if they suspect an infection and who to notify about it.

There has been an emphasis on this at ABC Corp. With the rise in prevalence of polymorphic viruses and other malware that specialize in avoiding conventional detection by sensor platforms, user education is a continuing and critical component of the anti-virus strategy.

What to watch for - ABC Corp displays the following on the security website of the company intranet:

```
The following examples may be indications that a computer has been
infected with a virus. Although these problems can be caused by a
non-virus problem, they are the most reported symptoms of an
infection.
    - Programs take longer to load than normal.
    - Computer's hard drive constantly runs out of free space.
    - The floppy disk drive or hard drive runs when you are not using
it.
    - New files appear on the PC and you don't know where they came
from.
    - Files have strange names you don't recognize.
    - Program sizes and dates keep changing.
```

What to do / who to contact - ABC Corp displays the following on the security website of the company intranet:

```
If workers suspect infection by a computer virus, they must
immediately stop using the involved computer and call the Help Desk
at extension XXXX.
```

The circumstances that led to my involvement with the Magistr incident are a little complicated. Users "A" and "B" (not their real names), who work in the same area as I do (its not security related), had experienced some indications that their machines had become infected. They dutifully reported this to the Help Desk and were transferred to the AV Team, where it was discovered that they were running outdated versions of ABC Corp's AV software. Once the software

was updated, scans were run on their machines that discovered the presence of the Magistr virus and cleaned it up. It was a mystery, however, how they had become infected. At the same time that this was happening, I received an email from someone outside of the company, who was a mutual friend of myself and another co-worker of mine, User "C". The external party stated that he had received an email with an infected attachment from User "A" and that he had no idea who this was (note: he wasn't infected as he has a Linux system). Using a bit of detective work, I surmised that his address may have been passed from User "C" to User "A", which meant that User "C" was probably also infected. There was a slight problem, though. User "C" was, at the time, in the hospital having a baby. As I proceeded over to her machine, I was wondering how I was going to get past her login screen. When I turned on her monitor, however, it became evident that this was a moot point as I noticed, with some horror, that SHE WAS STILL LOGGED IN! We will need to have a little talk when she returns from maternity leave. I called the Help Desk and was forwarded to a member of the AV Team who PCAnywhered to the machine and we began the assessment.

2. Assessment of the situation:

An event is not officially considered an incident until it is deemed one by experienced professionals. At most companies, this is done by the incident handlers.

At ABC Corp, members of the AV Team conduct the assessment. There are two parts to the assessment. First, a determination needs to be made as to whether or not there really is an infection. Second, if an infection is confirmed, the AV Team needs to develop a containment and eradication game plan. I detail the two phases below:

A. Is there an infection?

The AV Team uses a variety of tools to determine if the event is actually an incident. However, these tools might not be considered a prototypical "jump kit" as most of them are part of the standard Windows installation. Granted, these tools are basic, but since they are on all of the machines, the AV Team is able to go directly to local machines or PCAnywhere to any remote machines and immediately conduct their investigation. Basically, what the AV Team is trying to do is either confirm or deny that the abnormal behavior of the machine as reported by the user is due to a virus.

First, they will attempt to rule out any possible innocent causal factors that may be impairing the proper functioning of the machine. Sometimes a drive is out of space because a user has filled it up. Sometimes a machine is sluggish because a user is running a dozen programs at once. Hardware fails. The AV Team will check the basic health of the system, using tools such as the Task Manager, System File Checker, System Information Utility, and the Device Manager Tab within the System icon of the Control Panel.

Second, the AV Team member conducting the assessment will look for

specific indicators of an infection. These are the telltale signs that point to a particular virus. Because of their familiarity with all things viral, the AV Team keeps abreast of which viruses are making the rounds and the symptoms that may announce their presence. Some tools used here and what they look for are: Regedit for modified, deleted or added registry entries, Windows Explorer for suspicious files or folders, and Find for recent file modified dates, unexplained files or folders and specific text strings.

If not infected - Because the AV Team works so closely with the Help Desk, most of the cases forwarded to them are, in fact, something more than conventional computer problems. Even so, false positives are acceptable. They are used as educational opportunities for the AV Team and contribute to that body of knowledge that can only be built from experience. The AV Team believes that this will help them improve their ability to identify actual infections.

If infected - This is the real deal, and the AV Team needs to move quickly, but judiciously, to properly identify the important components of the threat: The virus type, its transport mechanism and the payload. To assist in this effort, the AV Team will consult with the vendor, Internet resources and their own reference materials. Test machines (non-networked) may also be set up and intentionally infected in order to study the virus in a controlled environment.

For background purposes, I will include a couple of examples from two of the Internet resources used by the AV Team to illustrate the particulars of the Magistr virus.

From the Symantec web site (see references for address):

```
W32.Magistr.24876@mm is a virus that has email worm capability. It is
also network aware. It infects Windows Portable Executable files,
with the exception of .dll system files, and sends email messages to
addresses that it gathers from the Outlook/Outlook Express mail
folders, the sent items file from Netscape, and Windows address
books, which are used by mail clients such as Microsoft Outlook and
Outlook Express. The email message may have up to two attachments,
and it has a randomly generated subject line and message body.
```

From the McAfee web site (see references for address):

```
Indications of Infection:
 - Increase in size in .EXE files (adds 24kb or more)
 - Infected files use a modified access date of the time of the
infection
 - Presence of a newly created .DAT file containing email addresses
    representing those users that were sent the virus
 - Entry in WIN.INI RUN=(App)
 - Entry in Registry, run key value: HKLM\Software\Microsoft\Windows\
    Current
Version\Run\AppName(varies)=C:\WINDOWS\SYSTEM\(App).EXE(varies)
```

B. Determine cause of action - Not all viruses are created equal. The strategy

and countermeasures need to be commensurate with the threat and are based upon the assessment. If the incident is an isolated case, the AV Team will handle by it by themselves (such as with Magistr). If it looks as if an outbreak is occurring, the following procedures will be followed:

1. AV Team notifies management - Important to give them a heads up in case drastic measures need to be taken.

2. AV Team notifies Machine Service Bureau - The MSB has oversight over the areas that the AV Team needs to work with and can muster up additional resources if necessary.

3. AV Team notifies Corporate Communications - CC calls an emergency meeting to be held at a predetermined location. Parties are notified via pager and attendance is mandatory.

The following groups are represented:

AV Team - Develop a containment / eradication game plan.
Email Group - Decide if filters need to be applied.
Help Desk - What indicators to watch for? What kinds of questions to ask potentially infected users? What to tell curious employees?
Network Transport - Need to block any ports? What traffic to watch for?
Upper Management Rep - Keeps management in the loop.
Application Development - Starts working on in-house patches, scripts, dat files. Has beaten the vendor on several occasions.
Corporate Communications - Determines if company-wide warnings need to go out (usually through the intranet). For the Magistr virus the following message was displayed on the intranet home page:

```
W32/Magistr@MM virus:
    The messages sent by this worm contain various subject headings,
   body text and attachments. The body of the message is derived
   from the contents of other files on the victim's computer. It may
   send more than one attachment and may include non-.EXE or non-
   viral files along with an infectious .EXE file.
    The I/S Division has taken several actions to prevent the
   circulation of W32/Magistr. Specifically, a filter has been put
   in place to help deter e-mails with the virus from entering the
   Company's e-mail system.
    Employees need to use caution to avoid opening any unfamiliar e-
   mail attachments, particularly those ending with .SCR,.PIF,.COM
   or .EXE. If you have opened an unfamiliar attachment please
   contact the I/S Help Desk immediately.
```

4. AV Team notifies external parties - Get dialogue going with the AV vendor (this is currently the only external party notified by ABC Corp). They probably have already received calls pertaining to this virus and may have some immediate containment advice. Also, it is important to get a timeline from them

as to when a fix will be ready if it is a new virus or strain (usually two to six hours).

With the Magistr incident, the fixes were in place for those machines with the latest version of AV software for some time before the machines in my group got infected, its just that not all of the machines in ABC Corp had that latest version installed.

Develop Containment / Eradication Game plan - The game plan is your basic feedback loop in the classic PDSA style (Plan, Do, Study, Act). The various stages of the loop are repeated, as necessary, until the problem has been eliminated.

Devise Strategy
\/
Execute Countermeasures
\/ /\
Communicate w/ team to monitor progress
\/
Virus Contained & Eradicated
\/
Implement Changes

Containment

For our purposes, containment refers to execution of actions designed to prevent any further damage from the virus. The intent is to put into practice the plan developed at the emergency meeting.

1. Backup the System - Particularly when dealing with an intrusion, an incident handler will want to immediately create two image backups of the offending system. These will capture everything on the drive, including deleted files, page files and file metadata. One of the backups should be sealed as evidence and the other used for the investigation.

For ABC Corp's virus fighting efforts, however, they have decided that backups are not a necessary part of the containment procedure. As they see it, their emphasis is on cleaning up the infection, not on criminal prosecution or traceback. During an outbreak, there may be hundreds of infected hosts. An attempt to back up all of them would be very time consuming and costly. While they will make every effort to save the machine's data, if they are dealing with a virus with a destructive payload, it is up to the users to follow a regular backup schedule so that in the event that data is lost, the system can be rebuilt from the user's most recent clean backup.

ABC Corp displays the following on the security website of the company intranet:

```
An ounce of prevention...Your best bet is to always maintain backup
copies of files you just can't do without. That way, if your computer
does get infected and crash beyond repair, you will have copies of
your important documents.
```

2. Remove host/system from network? - This is a very difficult decision, especially during active intrusions.

This may apply for virus containment in the event that one of ABC Corp's hosts is attempting to propagate its infection to others and the countermeasures for that particular virus have yet to be developed and applied. Once the fixes have been implemented, the host will be returned to the network and monitored to see if it is still behaving badly.

3. Continue to consult with system owners - It is important for the incident handlers to keep the system owners apprised of the status of cleanup, for the well-being of the system owners as well as for the purpose of trying to gather information relating to possible causes of the infection.

At ABC Corp, incident handlers keep lines of communication open with system owners, usually speaking with them directly as the cleanup ensues. They are careful not to use condescending or accusatory tones or to try to find fault with the user's actions.

4. Verify AV defenses - The handler should quickly determine whether or not the machine in question is properly patched, has the latest version of AV software installed and has the most current AV signature files on it. Assuming the case that these measures should have prevented the infection and are present, the handler needs to find out quickly why they didn't work. If the machine isn't up to date, the handler will need to find out why not.

Eradication

This phase goes hand in hand with containment, with the end result hopefully being the complete removal of the virus from all machines within the network. It is also very important to prevent reinfection via the same channel, or you may end up going through the whole ordeal again.

1. Improve defenses - Since it is obvious that the protection level was inadequate prior to the infection, it is imperative that the defensive position be enhanced.

The AV Team cooperates with the other areas involved to upgrade the defenses at several points, including filtering at the firewall, routers, and servers and updating AV signatures and login scan scripts at the workstation level.

For Magistr, I personally went around to all of the machines in my group and made sure that they were upgraded to the latest version of our AV software and ran scans on all of them, which showed no other infections. Also, the managers of the other groups in my building were alerted so that they could do the same with their staff's machines. At the company-wide level, executable email attachments were blocked for a week.

2. Perform a vulnerability analysis - This involves using a network vulnerability analysis tool to make sure that the defenses have been improved throughout the network.

For ABC Corp, this involves running a full AV scan on all of the servers and workstations with the most current version of AV software and the latest signature files.

3. Remove the cause of the incident - This is pretty much self-explanatory. For virus infections, it entails installing the signature files and scripts that eradicate the virus and running them.

At ABC Corp, this step is combined with (2) above to detect and remove the virus.

For our Magistr example, we already had a pretty good idea that the machine was infected, and we also knew that it was running an outdated version of the AV software, so we skipped a lot of the preceding steps. Instead, the first thing that we did was to install the AV update and run a full system scan. We spend a lot of money for this software, so we may as well let it do the dirty work when we can. Well, we got our money's worth this time. As the scan ran, it displayed the name of each infected file it came across. The list was flying by faster than closed captioning for an auctioneer. When the scan finally finished, the AV handler searched through the AV scan report for the names of infected files created by Magistr. He then used the Find utility to locate any of these files on the hard drive and Regedit to locate any references to these infected files in the registry. He deleted any occurrences that he came across. After explaining to me that the virus had some sneaky anti-debugging routines, he had me shut of the computer directly with the power switch in order to thwart them. With this, my journey into the world of virus fighting was over.

4. When the box is too far gone - Even with the incident handlers' best efforts, sometimes a machine has sustained too much damage from a destructive payload or the infection is too extensive to eradicate. If this is the case, the system must be reformatted and restored from the most recent clean backup.

At ABC Corp, there is an emphasis on urging users to make regular backups of their important data. This will protect them to some degree from a host of potential problems not limited to viruses (such as hardware or software failures), which may lead to data corruption or loss.

There was a concern that the infected machine I identified might be subject to

a reformat and reinstall because of the extent of the infection. However, the AV software, once upgraded, and the actions of the AV Team member seemed to have sufficiently eradicated the problem.

Recovery

Once the AV Team is confident that an outbreak has been eliminated, it is time to return the network to fully operational, uninfected status.

1. Validate the system - This step is simply a confirmation that the virus has been completely removed and the system has been returned to its normal operating status. It is important that the system owners sign off on this.
The AV Team will work with the system owners to verify that everything appears to be functioning as it was pre-infection.

2. Monitor the system - While things may seem to be back to normal for the users, the incident handlers' duties aren't quite finished. They need to monitor the system for signs that it is, in fact, still infected or has become reinfected.
The AV Team can monitor virus-like activity on many fronts. They can watch traffic directly to and from the machine, use scheduled scripts and scans to watch for infected code and observe activity to and from specific ports and addresses.
The infected machines in my group were monitored but no further signs of the Magistr virus were discovered. The users were instructed to watch out for any abnormal activity and report it immediately to the Help Desk, but at the time of this writing there hadn't been any need to do so.

Follow-up

As the final phase of the incident response cycle, follow-up gives all of the involved parties a chance to identify lessons learned that may improve future incident handling efforts.

1. Develop a final report - This should be started immediately after the incident is closed by the primary that handled its resolution. All involved parties should review the draft. While an attempt should be made to achieve consensus, in the case of strong dissent it should also be noted in the report.
The AV Team only uses final reports for what they consider serious cases. It has been some time since they have had a case that merited developing a final report.
With Magistr, since the rate of infection was so slight (less than a dozen machines), the AV Team decided that it didn't warrant a final report, a lessons

learned meeting or the need to send recommendations for change to management.

2. Lessons learned meeting - This is a get together of the people involved with handling the incident. It is an opportunity to review which of the policies and procedures worked well during the incident and which may need improvement for future incidents.

The AV Team does not hold lessons learned meetings, although the handlers communicate to each other informally about which things worked and which didn't.

3. Send recommended changes to management/implement them - This is an opportunity for incident handlers to relay to management ideas on how to improve responses. Recommendations should include cost estimates, implementation schedules, and the risks associated with making the proposed changes along with the potential risks if the company fails to make the changes.

The AV Team keeps a running dialogue with management and does not restrict making recommendations only to those times after an incident occurs. The policies and procedures of the AV Team are dynamic and improvements are continually being considered and implemented. One example of this occurred while I was writing this paper. The vast majority of viruses are introduced into ABC Corp by users accessing internet-based email, which bypasses the front-end smtp AV scanning of the network. The AV Team had been getting mixed results when instructing users to stop doing this, so instead of implementing some draconian measures they instead went ahead and purchased a hardware solution that will scan all internet-based email and close off this infection vector.

Executive Summary

Recently, the so-called Magistr virus has been making its way around the Internet. We are pleased to report that while this particular virus had the potential to be very costly to an organization of our size, the effect here at ABC Corp has been minimal. We have documented less than a dozen cases of infection within the company, which is virtually insignificant considering we have over 24,000 machines. Of the infected machines, none suffered serious data loss. Multi-layered hardware and software defenses, the dedication of the AV Team and intelligent user behavior have combined to prevent this very dangerous virus from being anything more than an inconvenience to ABC Corp. With our continued commitment to upgrading our technological defenses and educating our users, we intend on reducing our infection rates even further.

Conclusion

I have to say that my first-hand glimpse into the inner workings of the anti-virus efforts at ABC Corp has been both informative and educational. After learning all of the theory in the GCIH course, it was interesting to see how things were done "in the real world". Frankly, I was surprised how closely the policies and procedures of the AV Team correlated with those outlined in the Incident Handling Guide, since they were developed completely independently of each other. I think it serves as validation for both parties. For ABC Corp, it shows that they have a solid anti-virus program. For SANS, it highlights the relevancy of the subject matter of the course and it proves that the best practices, as described in the Incident Handling Guide, really are borne out of the experiences of real-world security practitioners.

References

The SANS Institute. Computer Security Incident Handling Step-by-Step. version 1.5.
May 1998.

Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook.
New Riders Publishing. 1999.

Symantec Anti-Virus Center (SARC) - Magistr.
URL -
http://www.symantec.com/avcenter/venc/data/w32.magistr.24876@mm.html

McAfee Virus Information Library - Magistr.
URL - http://vil.mcafee.com/dispVirus.asp?virus_k=99040&

Sophos Virus Info - Magistr.
URL - http://www.sophos.com/virusinfo/analyses/w32mag.html

F-Secure Virus Descriptions - Magistr.
URL - http://www.f-secure.com/v-descs/magistr.shtml