Global Information Assurance Certification Paper

Frank Zipfel

SANS Security Essentials GSEC Practical Assignment v. 1.3

11 March 2002

Understanding the Virus Threat and Developing Effective Anti-Virus Policy

Summary

According to recent ICSA statistics, your company was over 99% likely to be confronted with the threat of a virus infection in the year 2000, over 50% of which could be classified as a virus disaster. Was your company prepared to deal with this threat?

This paper focuses on providing the reader with an overview of the current virus landscape and aids in developing best practice anti-virus policies. After presenting the threat, we'll introduce you to today's most popular anti-virus tools. Using your knowledge of the threat and of the solutions will help you manage the risk of infection, ensuring confidentiality, integrity, and availability of computer systems and data and minimize the cost of reactive management in case your proactive measures fail.

Introduction

Computer Economics, a California-based research advisor, published 2001 figures that place the worldwide cost of malicious code attacks at an estimated $13.2 billion. The majority offenders were Love Bug at $8.75 billion, code Red at $2.62 billion, SirCam at $1.15 billion, and Nimda at $635 million. (Find the Cost of (Virus) Freedom)

Although the exact figures are contested, one cannot argue that the financial damage caused by virus activity is substantial and on the rise. (Lies, damned lies and anti-virus statistics)

CERT/CC reports an increase of over 50% in the number of viruses from 2000 to 2001. (CERT/CC Statistics 1988-2001) SARC corroborates this by identifying an estimated 60,000 known viruses to date versus some 30,000 at the end of 2000. (Am I Protected?) ICSA writes that infections were up 20% in 2000 versus the previous year, with 99.67% of companies surveyed experiencing at least one virus encounter and 51% claiming at least one virus disaster during the twelve month period preceding the survey. According to ICSA's survey, the rate of infection per 1000 PC's has doubled every year since 1996. (Computer Virus Prevalence 2000)

Malicious code has existed in theory or in the lab since the 1960's. Only with the proliferation of personal computers in the 1980's have we seen the rapid development and dissemination of virus code in the wild. Bootsector and file infector viruses were the norm in the 1980's and early 1990's, spread mostly via sharing of floppy disk or BBS downloads. The 1990's and 2000's saw an explosion of file-infector, macro, and other scripting language viruses brought on by a combination of the rapidly developing Internet and overly complex and unsecured operating systems and applications.

Definition of a Virus

A computer virus is a self-replicating program that without the user's knowledge or intervention attaches itself to or replaces an executable file, a data file that can contain embedded executable code, or system areas or executables. At best, this type of malicious software (malware) simply utilizes computer or network resources; at worst it intentionally compromises the computer system's confidentiality, data integrity, or availability.

While trojans and worms are generally regarded to fall under the broader umbrella of malicious code, we will include them in our discussion as either a delivery vector over a network in the case of worms, or a payload in the case of Trojans. A worm may contain viral code, in which case we will consider it a vector to the virus. Similarly, certain trojans may be hidden within a worm, thus fitting the description of self-replicating and malicious.

A computer virus consists of three distinct parts, a vector, a replicator/infector, and a payload. A vector is

the method by which a virus propagates. Boot sector viruses, for example, alter or replace the boot sector of bootable devices. Thus, by starting from an infected device, the virus is loaded into computer memory and becomes active. According to statistics published by leading anti-virus (AV) researchers the most popular vector in use today is via e-mail attachment. A close second delivery mechanism is worms infecting unpatched or misconfigured web servers, Microsoft Internet Information Server in particular, and a distant third is unprotected shares on MS Windows boxes. To be sure, many other types affecting all operating systems exist, but these lead by shear number and are a good representation of what is out there.

The replication code of a virus can be classified by infection condition. Infector code relies on a set of rules or conditions to propagate itself to other files on the infected system or to other systems across a network. Example conditions include replicating after a predetermined number of infections, or over a given period of time, spreading on a certain date, or in response to the presence of a certain file or files. There is a further distinction between "slow" and "fast" infectors, the purpose of which is to spread slowly to avoid detection or to spread as quickly as possible to maximize number of infected systems. Notice that the goal of both is the same, but the philosophy on how to best spread varies.

Finally, a virus contains a payload. This military term denotes that portion of the virus we typically think of as causing damage to a computer system. Types of payloads abound, but the most noteworthy and most prolific include: damaging, destroying, or altering executable or data files, thus leading to system instability or availability, breached confidentiality, or compromised data integrity.

For a more comprehensive definition of virus types, including stealth, polymorphic, and armored viruses, please refer to the alt.comp.virus and virus-L/comp.virus FAQ's. ([alt.comp.virus] FAQ Part 1/4) (VIRUS-L/comp.virus FAQ v2.00)

Proactive Anti-Virus Strategies

As in all areas of computer security, the object is to minimize risk. We can define risk as threat X opportunity.

Because we generally have little control over the threats, we will concentrate mainly on reducing opportunity. It is unrealistic to expect to eliminate all risk of infection, but we stand a good chance of mitigating our exposure to risk with the right policies and procedures.

On the extreme end, we would simply disconnect our computer from all external means of program or data transferal, including LAN and WAN, and floppy disk/drive access. To prevent infection from within, we might remove any tools that could be used to program a virus on our system, such as editors or compilers or macro language interpreters. The open extreme would be total access with no controls. Clearly, we seek to find the appropriate middle as defined by your system's or data's value.

The goal then of the IT professional is to implement a plan that will ensure a computer system's and data's availability to legitimate users, the data's integrity, and the system's and data's confidentiality. An anti-virus policy must be an integral part of the general "Defense in Depth" computer security policies. Defense in depth implies a layered approach to achieving the above goals by blocking many possible paths, usually in order of priority, thus increasing your odds of success. AV policies are most effective as part of a comprehensive security policy, which might include Firewalls, IDS, and redundant systems.

How do we allocate resources to virus prevention? We must first determine the cost of an infection versus the value of our systems/data. This is the business case for AV policy. Assigning value to your system or data can be tricky. Two proposed quantitative metrics are the Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE) formulas. SLE determines the loss caused by a single incident. It is defined as: SLE = Asset Value X Exposure Factor. Say for example that one worker, who is paid $20 per hour, can not use her workstation due to a virus infection, and a consultant, who is paid $100 per hour, spends three hours sanitizing and repairing the damage caused by the virus. According to our formula, the worker has incurred 3 X $20 = $60 + the consulting fees of 3 X $100, to give us a SLE of $360. Note that this doesn't take into account more subtle factors, such as potential value that could have been added by the worker to the company during that business day, and the company's better use of the $300 consultation fee

towards improvements versus incident response, or perhaps that missed deadline that has other serious consequences.

The ALE then is simply the SLE X number of yearly occurrences. Imagine a widespread infection using the above scenario, or a recurrence several times per year. It is easy to see why prevention and planning are worthy investments.

Another method of assigning risk is through qualitative analysis. By assigning a high, medium, or low risk, you prioritize areas of need. This method is probably more appropriate as a birds-eye view approach to target the hot-spots most quickly.

It's fairly easy to make a business case for virus protection after-the-fact. It is important that the IT professional makes clear the importance and ultimate cost-savings of a proactive approach.

Protection Methodologies

In order to protect our systems from attack, we need to implement methods that lower the opportunity for infection. All proactive measures we will examine rely on the ability to either close a vector of infection, e.g. firewall ACL's and software updates, or identifying and blocking the virus threat if an infection vector is successful, e.g. antivirus software.

Looking back on our earlier statistics, the biggest virus threat vector we currently face is via e-mail attachment. Most viruses propagated via e-mail initially require user interaction to run and become active. Various methods of deception are used, including forging e-mail headers to appear as if they originate from trusted sources, i.e. Melissa virus, or by appearing to contain urgent or humorous information or software, i.e. VBS.Stages. The unsuspecting user runs the malware attachment which often grabs e-mail addresses from various programs and mails itself out and the cycle begins anew.

Firewalls

A firewall is software or hardware that acts like a traffic cop allowing or disallowing access from one computer or network to another based upon a set of predetermined rules, also known as an Access Control List or ACL.

A hardware router utilizing Name Address Translation (NAT) is an example of a simple firewall. Worms scanning for vulnerabilities from the internet may hit upon your router, but unless you allow traffic to pass through to your internal network for a given service, such as Web-hosting, you have essentially blocked the threat. These routers work on the packet level and are not capable of distinguishing safe versus unsafe packet content. Today's sophisticated routers offer much more granularity of control in the creation of in-and-outbound ACLs and many are beginning to offer Stateful Pocket Inspection, a type of heuristics based analysis of traffic that might indicate a possible attack and take steps to prevent it.

Personal firewalls that can be deployed on individual workstations are gaining in popularity. A few examples on Windows platforms are Norton Internet Security or Zonealarm. Both are application layer firewalls that come with a predefined set of traffic filtering rules that can be customized as needed. Both essentially start with a "deny all" policy and ask you which application should be allowed to interact over your network. Uniquely useful at a user level is the ability to allow specific outbound traffic. If you are not sure if a particular application should be accessing the net, maybe it is time to research what exactly it might be doing. This is a wonderful way for the user to become aware of and protect themselves and others against spy-, ad-, or malware that may be compromising their system.

Anti-Virus (AV) Software

Regardless of manufacturer type or OS platform, AV software works on a similar basis. Once installed, AV software monitors all read and write attempts from any device, i.e. hard drive or network, calculating a file signature that it compares against a built-in database of known virus signatures. Most AV software also has some heuristics built in that checks against possible virus activity for un-catalogued viruses.

The main weakness then of AV software is the constant race to identify and protect against new viruses. The consumer must keep the AV signatures up-to-date in order to stay optimally protected. Most modern scanners offer a subscription system and utilities to automatically check for

and download new signatures. If a virus is detected, AV software attempts to reverse the damage and eliminate it. This is not always possible, as is the case when files are replaced or overwritten.

There are three major categories of AV software, centrally managed, e.g. McAffee Sonicwall AV option, Norton AV for Enterprise, and individual workstation solutions, e.g. Norton AV, PC Cillan, and more recently, Web-based scanners such as PandaSoftware Online scanner.

In almost all cases, the centrally managed solution is preferable. The main advantages are central deployment, uniform policy enforcement, the ability to push-out updates, and the usually lower cost of per-seat volume licensing.

Software Updates/Settings

We've already mentioned the importance of keeping our AV software current through frequent update downloads. The last tool we'll be discussing is application and operating system updates. New infection vectors that utilize some weakness in our OS or applications are constantly being discovered. The recent holes discovered in Windows XP UPnP, automatic execution of executable attachments in Outlook, scripting exploits that automatically download and install malware via Internet Explorer, or the ever-popular ISAPI and directory traversal weaknesses that have given Microsoft IIS a black-eye, all serve as undeniable examples of the importance of patching your OS and applications.

Fortunately, most vendors are diligent in offering such updates; but again, unless they are applied, you remain vulnerable. Microsoft offers an online automated update service that customizes a list of recommendations based on your OS and patch history. Generally, you want to apply all critical hot patches and service releases as they become available. More recently, Microsoft has released tools that automatically notify the user of updates. Future tools promise to automatically download and install updates in the background. How much you trust your software vendors with the type of control over your system is another topic. I know many who would say the medicine, although sometimes bitter, is preferable to the illness.

I'd also like to refer the reader to the many excellent articles on securing default installations. Symantec, for

example, speaks about turning off the embedded scripting features in MS Outlook programs. (Prevent E-Mail Worms) Microsoft is renewing its commitment to secure computing and many relevant articles can be found on their security websites. (Microsoft.com)

Creating a Corporate AV Policy

We've discussed the threat and have given concrete examples of how to deal with it. Policy, now the final tool in our arsenal, ties the previous information together and gives us a framework to operate in.

To reiterate, the point of this entire exercise is to protect the confidentiality, integrity, and availability of our resources. We therefore, need to identify the assets, identify the threat, and then create proactive and reactive strategies to minimize risk and deal with incidents.

Our proactive strategies aim to minimize risks, develop contingency plans, create and assign responsibilities to an incident response team. Reactive strategies assess damage, implement the contingency plan, repair the damage, and document the incident so that our policies can be re-examined and constantly improved. This is an ongoing and dynamic process.

Christopher Benson of Inobits Consulting (Pty) Ltd. Offers an excellent flowchart outlining this process in his paper entitled Security Strategies. (Security Strategies) Note that the outline works for many types of threats and can therefore be used to generate a comprehensive security policy.

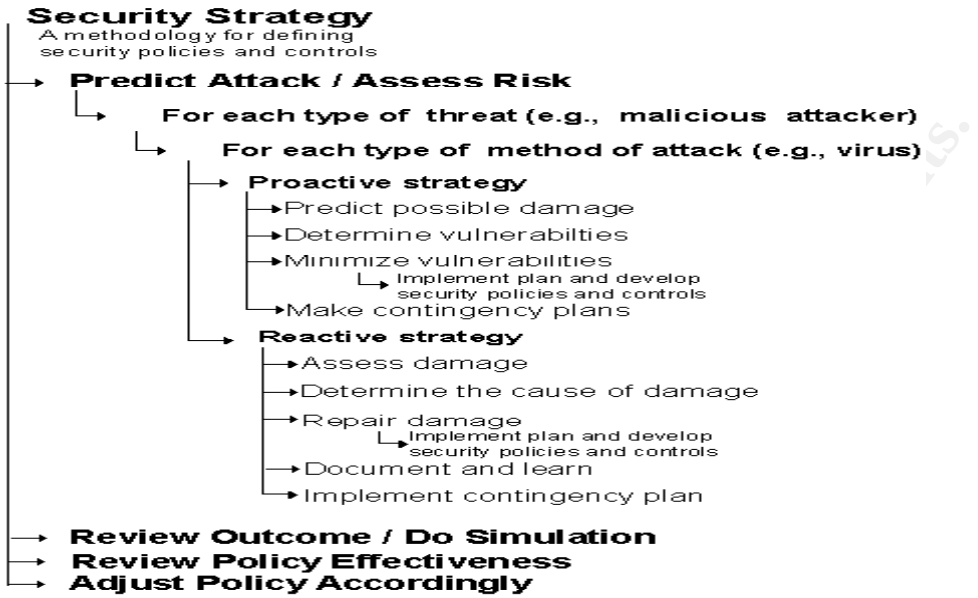

Figure 1 – Security Strategy Flow Chart

Using the above flowchart, let's step through an example scenario. We'll use the e-mail virus attachment since it is the most prevalent.

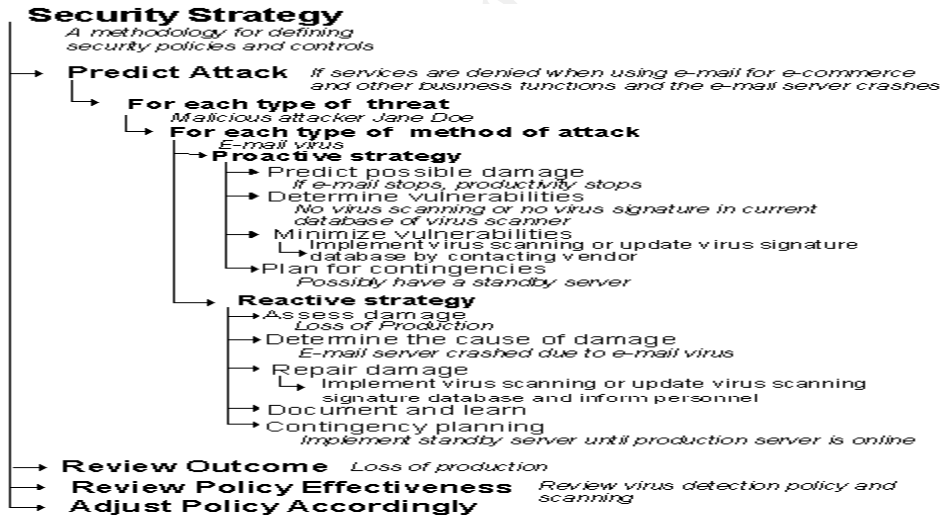

Figure 2 – Security Strategy Flow Chart Example – E-Mail Virus

First, we predict the threat. In this case a denial of service (DoS) of our e-mail server. Specific to this example, the DoS is determined to be caused by a virus using

an e-mail attachment as a vector. Next, we begin our proactive strategy. We try to predict the damage. Here, a DoS hampers productivity by stopping us from communicating with the outside world via e-mail. The identified vulnerabilities leading to the possible incident are no virus scanning at all or no signature for a particular virus in the AV database. In order to minimize the risk, we implement AV scanning or updating of the current AV virus signature database. We also recommend a backup e-mail server for contingency purposes. If our proactive strategy fails us, we define our reactive options. The incident handling process consists of damage assessment. Again, in our scenario, it would be the loss of productivity, possibly using an SLE formula. We determine the extent of the damage to our e-mail server brought on by the virus. Our proposed solution is to scan and eradicate the virus using AV software. We will apprise the relevant company employees of the situation. We fully document the incident, and attempt to strengthen our policy based upon what we have learned. We also place our backup server online until the original server has been repaired. The last section of the flowchart reiterates the concept of learning from the past to improve our chances in the future. What have we learned through this incident? How can we improve our security posture to prevent similar attack in the future? What revisions do we need to make to our policies to mitigate reoccurrence? Using this outline, we can establish a long and wide-ranging set of policies to deal with any threat we can conceive of.

Several sources make sample AV policies available online. These may offer additional ideas or serve as templates to create your own. (Symantec Corporation)(TruSecure Anti-Virus Policy Guide Version 3.6.0)(Emm)

Future Threats

New vulnerabilities continue to be discovered in current technologies. What risks do newer technologies such as wireless network access bring? Let's examine three fledgling technologies that may offer the newest infection vectors of today and tomorrow. The wireless Ethernet standard 802.11b has exploded into the home and business markets during the past two years. Poorly configured access

points are an easy infection vector to what are essentially open networks. Any standard network aware virus poses a threat. Bluetooth, a competing standard of inter-device wireless communication and networking, poses similar risks. (Potential Threats to WAP Enabled Devices)

How much amplified is the threat of virus infection on PDA's when you take into consideration that they are the perfect infection vector into many internal, secured networks. A cross-platform virus whose infection vector is a PDA running Palm OS being synced with Microsoft Outlook on a desktop computer running Microsoft Windows XP is not that far fetched. (Does Your Business have the Security to Handle the Threat?)

Handheld devices, such as Palm computers or digital cellular telephones using proprietary and Wireless Access Protocols and scripting (WAP and WAPScript) have already seen pseudo virus attacks that corrupt data and cause denial of service conditions. (Virus Protection Coming for Wireless Users) (Malicious Threats to Personal Digital Assistants)

Insecurities in computer systems that are inherently networked, like the earlier mentioned WAP phones, may lead to unprecedented short infection times. Although currently limited in the opportunity or potential threat they currently pose, once more powerful devices incorporating recent WAP extensions that allow JAVA and JAVA script become available, powerful mobile viruses will become a reality. (Does Your Business have the Security to Handle the Threat?) Imagine a virus being released into the wild on one cell phone, then that phone using the built-in phonebook to call and spread itself, or perhaps tumbling through all known cell numbers for a given carrier. How long would it take to infect all active phones?

Another growing threat is posed by peer-to-peer networks. The concept of P2P networks is as old as networking itself. Recently, the use of software that allows hundreds or thousands of people to share files, i.e. mp3s, divx, software, has blossomed. Examples of such networks by popularity are Napster, Kazaa, Morpheus, Gnutella, and FreeNet.

Eric Chien of Symantec makes an interesting point that not only can malware easily be propagated, but the usually publicly known protocols could be misused to spread communication of malware. Due to the ability of P2P software

to bypass traditional firewalls by opening connections from within the private network they could be ideal vectors for trojan or virus delivery or even provide a path for automatic virus code updates. (Malicious Threats of Peer-to-Peer Networking)

Conclusion

Virus control is an integral component in your comprehensive toolbox against the many threats to your system. The adage "Forewarned is Forearmed" appropriately applies to the area of AV policy creation. By understanding the virus threat and identifying weaknesses in your own system, you can design appropriate pro-and reactive counter-measures which will preserve the integrity, availability, and confidentiality of your resources. Using the given flowchart, identify and create policy and contingency plans that will aid you in managing the risk of a virus infection.

Works Cited

[alt.comp.virus] FAQ Part 1/4. Ed. David Harley, et al. 29 February 2000. www.faqs.org. 11 Mar. 2002 <http://www.faqs.org/faqs/computer-virus/alt-faq/part1/>.

Am I Protected? Symantec. 11 Mar. 2002 <http://www.sarc.com/>.

CERT/CC Statistics 1988-2001. 10 January 2002. Carnegie Mellon Software Engineering Institute. 11 Mar. 2002 <http://www.cert.org/stats/cert_stats.html>.

Computer Virus Prevalence 2000. ICSA. 11 Mar. 2002 <http://www3.icsa.net/portal/regdownload.shtml?URL=http://www.trusecure.com/html/tspub/pdf/vps20001.pdf>.

Does Your Business have the Security to Handle the Threat? Ed. Doug Campbell. Mar. 12, 2002. Mbusinessdaily. 19 Mar. 2002 <http://www.mbizcentral.com/magazine/story/archive/december-2000/virus>.

Emm, David. "Guidelines for an Anti-Virus Policy." (1996): .

Find the Cost of (Virus) Freedom. Ed. Michelle Delio. 14 January 2002. Wired News. 11 Mar. 2002 <http://www.wired.com/news/infostructure/0,1377,49681,00.html>.

IT Developments and Trends that Affect Your Business . 17

Jan. 2002. Computer Economics. 11 Mar. 2002 <http://www.computereconomics.com/cei/02/eflash/011702.html>.

Lies, damned lies and anti-virus statistics. Ed. John Leyden. 16 Jan. 2002. www.theregister.com. 11 Mar. 2002 <http://www.theregister.co.uk/content/56/23707.html>.

"Lower IT Costs Through Better Anti-Virus Management." Symantec (1999): . 11 Mar. 2002 <http://www.sarc.com/avcenter/reference/nvxwp2b.pdf>.

Malicious Threats of Peer-to-Peer Networking. Ed. Eric Chien. Dec. 2001. SARC. 11 Mar. 2002 <http://www.sarc.com/avcenter/reference/p2pnetworking.pdf>.

Malicious Threats to Personal Digital Assistants. Ed. Eric Chien. Oct. 2002. SARC. 11 Mar. 2002 <http://www.sarc.com/avcenter/reference/malicious.threats.to.pdas.pdf>.

Microsoft.com. Microsoft. 11 Mar. 2002 <http://www.microsoft.com/security>.

Potential Threats to WAP Enabled Devices. Ed. Eric Chien. Nov 2000. SARC. 11 Mar. 2002 <http://www.sarc.com/avcenter/reference/threats.to.wap.devices.pdf>.)

Prevent E-Mail Worms. Ed. Woody Thrower, et. al. 12 May 2000. Symantec. 11 Mar. 2002

<http://www.sarc.com/avcenter/security/Content/2000_05_12.html>.

Security Strategies. Ed. Christopher Benson. Microsoft. 11 Mar. 2002 <http://www.microsoft.com/technet/security/bestprac/secstrat.asp?frame=true>.

TruSecure Anti-Virus Policy Guide Version 3.6.0. 1 Oct. 2002. TruSecure Corporation. 11 Mar. 2002 <http://www3.icsa.net/portal/regdownload.shtml?LOC=1&URL=avpg360.pdf&ECDE=W0002>.

Virus Protection Coming for Wireless Users. Ed. Bruno Giussani. 19 Oct. 2000. CNN.com. 11 Mar. 2002 <http://www1.cnn.com/2000/TECH/computing/10/19/wireless.virus.help.idg/index.html>.

VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00. Ed. Nick FitzGerald. 9 Oct. 1995. www.faqs.org. 11 Mar. 2002 <http://www.faqs.org/faqs/computer-virus/faq/>.