Interested in learning more about security?

SANS Institute InfoSec Reading Room

Beyond Email: Defending Against Malicious Code in a Healthcare Setting

This paper takes an in-depth look at defending healthcare organizations from malicious code, from the perspective that effective protection requires a multilevel defense that includes polices and procedures, user education, physical security, system configuration and maintenance, password management, anti-virus software, and adequate backups, and the support of the entire organization.

Beyond Email: Defending Against Malicious Code in a Healthcare Setting

Dianne Belt
SANS Security Essentials (GSEC) Practical Assignment
v.1.2f (August 2001)

Introduction

Regular audits by regulatory agencies, such as the Joint Committee on Accreditation of Healthcare Organizations and the Food and Drug Administration, have historically forced the healthcare industry to look critically at how it protects the integrity, confidentiality, and availability of health data, whether automated or on paper. However, the increasing automation of healthcare information management, including the use of the Internet, has made this task more challenging in recent years. Breaches of patient privacy disclosed by the media have focused increasing public and governmental scrutiny on the security, or lack thereof, of computerized healthcare data. These concerns led to the inclusion of a mandate for electronic data security standards in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and a proposed Security Rule was published in 1998. As we work to implement the pending HIPAA Security Rule, one of the issues on which we must focus increasing attention is the protection of our systems from malicious code.

The Threat

For purposes of this discussion, a computer 'virus' is a piece of executable code, be it a virus, Trojan horse, logic bomb, worm, or other code type, designed to damage a computer or the information it contains or prevent the computer from being used in its normal manner. In this paper the terms 'virus' and 'malicious code' are used interchangeably.

Malicious code can come from a variety of sources. Examples of such sources are: data or program files downloaded via FTP, the Internet, or other mechanisms; infected diskettes or compact disks; files received via electronic mail; and worms that exploit various system vulnerabilities. The disgruntled insider, who has physical access to a computer or network, may also introduce it.

The individual who creates malicious code may do so for a variety of reasons. Some act out of spite. Others do it for sport, bragging rights, or notoriety. Some claim to have a political agenda, such as cyber-terrorists and those who say they do it simply to point out vulnerabilities.

In the past, virus writers have been stereotyped as 'script-kiddies', misguided juveniles who created and released malicious code without thinking through the consequences of their actions. However, in recent years, we have been forced to abandon this stereotype. According to Computer Associates, the mid-1990s saw the emergence of two additional types of virus writer, the "professional" and the "unintentional". Professional virus writers fully understand what they are doing when they create and release malicious code. On the other hand, unintentional virus writers are often "experienced computer users who over-extend themselves" and "unwittingly alter a known (macro) virus detected within their company while 'researching' it" with macro development tools that are readily available in Microsoft Word or Excel. The new variant then can, and sometimes does, spread through their company and beyond.[2]

Regardless of why malicious code is created, or by whom, it disrupts the efficient operation of an organization, wasting both time and money. Also, if an organization's computer system is brought down, the implications to patient care may be critical. Malicious code may also allow

unauthorized access to individual medical records or other sensitive information and may modify, even destroy, critical patient data. For this reason, the healthcare industry's defense against malicious code clearly falls under HIPAA regulation and must be comprehensively addressed.

Effectively defending against malicious code requires a multilevel strategy that includes the following:

1. Written policies and procedures.
2. User awareness and education.
3. Physical security.
4. Product selection, configuration, and maintenance.
5. Password management.
6. Anti-virus software for servers, clients, and electronic mail.
7. Adequate system backups.

Nor can this defense be strictly an Information Technology problem. A strong defense requires support and assistance from the entire organization, including enterprise-wide management, Human Resources, and individual computer users.

Policies and Procedures

The only way to truly secure a computer is to power it off, disconnect it from any network, put it in a locked room, and never let anyone near it. Obviously, this is impractical. A computer cannot be protected from malicious code without enlisting the support of those who will use it.

But before you can begin to educate your users, you must clearly define what is expected of them. The first step in this process is a written, and preferably enforceable, general system usage policy. If the policy is to be enforceable, it must have the support of enterprise-wide management and Human Resources, as it is they, rather than Information Technology, who must perform the appropriate disciplinary actions for policy violation.

A medium-sized healthcare organization can easily have thousands of users, and the level of education, professionalism, computer sophistication, and organizational commitment of these users may vary widely. Many users, such as physicians, volunteers, students, contractors, and temporary workers, may not be employees of the organization. Some, such as medical transcriptionists working from home or physicians dialing-in from their offices, may use PCs that are not owned by the organization. Effective policies and procedures must address these diverse circumstances.

The general system usage policy should address all aspects of usage by non-Information Technology personnel and should clearly define the rules and procedures for appropriate system usage. For example, if such personnel are not to perform Internet downloads under any circumstances, the policy should state this. If Internet downloads are allowed under certain circumstances, these circumstances should be clearly defined with relevant examples. Additionally, there should be written procedures for safely performing such downloads, either in the general system usage policy or elsewhere if more appropriate. Depending on the organization, the general system usage policy may address the following issues:

1. Data ownership.

2. User expectations for privacy while using the system, including Internet and email usage.

3. Expectations for patient, corporate, and computer system confidentiality, including any confidentiality agreements that users will be required to sign.

4. General procedures for software acquisition.

5. General expectations concerning software downloads, installation, configuration, and /or execution.

6. General expectations concerning hardware maintenance and/or configuration.

7. Expectations concerning the acquisition, maintenance, and/or usage of desktop anti-virus software. This should include any remote PCs not owned by the organization, such as those of physicians' office or employees working from home.

8. Expectations concerning the acquisition, maintenance, and/or usage of firewalls on remote PCs not owned by the organization.

9. Expectations concerning the protection of the organization's computer network from other persons who may have access to a remote PC, such as family members or roommates of employees working from home.

10. Standards for system IDs, password selection, and password maintenance.

11. Expectations concerning electronic mail usage and email attachments.

12. Expectations concerning Internet usage.

13. Expectations for personal usage of the system.

14. Procedures for unattended personal computers, especially in public areas.

15. Procedures for incident notification.

16. Proper disposal of used magnetic media, such as diskettes, tapes, compact disks, or hard drives.

17. Consequences of policy violation for both employees and non-employees.

User Awareness and Education

User computer security awareness and education must be a continuous process in a healthcare organization, if not in all companies. New employees must be trained and older ones reminded on a regular basis.

One effective way to train new employees is to work with Human Resources so that Information Technology has a role in new employee orientation. The general system usage policy discussed above can be the basis for an IT presentation. While there may not be time during orientation to discuss the entire policy in detail, the most important parts can be covered; and the employees can each be given a copy of the policy for future reference. If several members of the IT staff rotate responsibly for the presentation, it may be helpful to work from a prepared script. This assures that everyone presents consistent information.

Use this opportunity to explain to the new users why it is important for them to follow the policy, and try to include some interesting examples of things that happened when the policy was violated. For example, discuss the seemingly 'innocent' Internet utility that caused the patient order entry system not to run on the nursing station PCs on which it was installed. Give specific suggestions, such as how to compose a strong password that can be remembered without writing it down. Try to keep the presentation positive, and let the new employees know that they each have an important role to play in protecting the integrity, confidentiality, and availability of patient data.

Also, don't forget those non-employees. If physicians, volunteers, students, contractors, or temporary workers are not included in the regular new employee orientation, ask Human Resources if it might be feasible to include them. If this is not possible, work within the organization as needed to assure they receive the same information as new employees.

An internal web site is one way to do computer security awareness training for current employees. Include links to the general system usage policy and to any other policies or procedures that should be distributed enterprise-wide. Other useful links might be: virus information and current virus alerts; virus hoaxes; tips on protecting a home computer or choosing a secure password; and articles on social engineering or other computer security topics.

Electronic mail is another way to distribute information, such as virus alerts or reminders about email attachments. A link within the email to your internal web page does double duty, reminding users of the existence of the web page.

If new employees are required to sign confidentiality and/or access agreements, consider having current employees re-sign these agreements at each annual performance review. This will

require the support of upper-level management, but it is yet another reinforcement of the organization's computer security awareness program.

Physical Security

Limiting physical access has traditionally been a key part of protecting computer systems from malicious behavior. This aspect of computer security is particularly important in healthcare organizations, which frequently are public buildings at least parts of which are open 24 x 7. In a typical hospital, for example, almost all parts of the facility are accessible to non-employees throughout the day and night. Areas of particular importance to Information Technology are:

1. The IT Data Center.

2. Critical IT offices.

3. Networked computers in areas accessible to patients, visitors, or members of the general public, such as front lobbies, nursing stations, or at the bedside.

Access to the IT Data Center should be controlled by a written policy detailing who is routinely authorized to enter the area and who may grant such authorization in ad hoc situations. All access to the Data Center should be logged and/or video recorded. Critical offices should be locked when not staffed by appropriate personnel. Some organizations control entry to the Data Center and other critical areas through the use of a two-factor authentication method, such as a card reader or biometric device plus a PIN number.

Networked computers in public areas should be logged off or placed into a password-protected screen saver mode before being left unattended. Also, password-protected screen savers, where available, should be configured to start automatically after a few minutes of inactivity.

A close working relationship with Protective Services can help Information Technology increase overall security awareness within the organization. Employees who are trained to ask, "May I help you?," to someone who looks out of place, can play a significant role in protecting an organization's computer resources from malicious behavior.

Product Selection, Configuration, and Maintenance

All proposals for new software purchases should be subjected to a technical review process prior to approval. The purpose of this review is to assure that the proposed software meets security standards and is compatible with software already in use within the organization. Security issues should be considered when choosing between products. For example, some organizations choose to use an email product other than Microsoft Outlook, because of Outlook's propensity to be exploited by virus writers. This is not meant to imply that other products are less vulnerable than Outlook, merely that these vulnerabilities are less widely exploited at the present time.

Once operational, all products, including operating systems, applications, file servers, and other network hardware components, must be kept current as patches are made available by the

appropriate vendor. A network-based vulnerability scanner, such as Saint or ISS Security Scanner, should be used on a regular basis to check for any unpatched, known holes. Network statistics should be monitored on a regular basis to look for abrupt or unusual changes in file size or system usage trends.

Avoid doing blind, default installs of operating systems and applications. Installing only the modules for which there is legitimate business need and disabling any unnecessary functionality can significantly reduce the potential vulnerability of the system. Configure operating systems and applications to reduce the risk of virus infections. For example, Trend Micro recommends the following configuration for Windows and related Microsoft applications:[11]

1. Disable Windows Scripting Host functionality in the Windows Setup program.

2. Do not hide file extensions of known file types in Windows Explorer.

3. Set Internet Explorer security to at least "medium".

4. Prompt user to save email attachments to disk before opening.

5. Enable macro-virus warnings in Microsoft Office products.

6. Prompt user before saving changes to the Microsoft Word global template.

Please see the Trend Micro Safe Computing Guide referenced at the end of this article for more information, including detailed instructions for implementing the above items.

Password Management

Good password management procedures are an important tool in defending against malicious code. All user accounts should have a corresponding password, and default vendor passwords on new software should be promptly changed. Teach users the importance of a strong password and how to compose a strong password that can be remembered without the need to write it down. Configure operating systems and applications to force strong passwords, and periodic password changes, whenever possible. With appropriate written authorization, a password-cracking tool, such as L0phtCrack, can also be used to enforce strong passwords.

To guard against social engineering, system and/or application access should be assigned only upon the approval of appropriate management personnel; and all system and/or application access should be standardized by job title or function. Beware of social engineering at the Help Desk as well, by establishing procedures whereby users requesting password resets can be unequivocally identified before the reset is performed.

The number of simultaneous logons permitted for an individual user should be restricted to what is needed for the user's job performance. Allowing users to logon to more than one workstation simultaneously increases the risk that a logged in workstation will be left unattended. Don't create unnecessary vulnerabilities by giving users unnecessary functionality.

All system and application access should be promptly deactivated whenever a user is terminated or resigns. Information Technology should work with management and/or Human Resources as needed to assure that appropriate personnel are notified in a timely manner. Mechanisms should also be put into place for the prompt notification of IT when a non-employee no longer needs access.

Anti-virus Software for Electronic Mail

Electronic mail scanning software should be utilized on both the Internet email gateway and the internal mail server(s). Products such as those offered by Symantec and Trend Micro can scan in-coming, out-going, and internal messages for known virus signatures in real-time. Infected files are cured or quarantined as appropriate. Signature files can be updated automatically via the Internet, and content filtering for email attachments, spam, chain letters, and email hoaxes is also available.

Attachment blocking is an invaluable tool in defending an organization against new email viruses. For example, all email attachments with .EXE or .VBS extensions can be stripped off incoming messages and placed in a quarantine area. Most non-Information Technology users have no business need to receive such files via email, so the impact upon the average user is minimal. Information Technology and other users with legitimate need, and appropriate authorization, can send compressed or renamed files to avoid the filter. Alternatively, the Security or Email administrator can retrieve any blocked attachments for which there is a business need from the quarantine area.

When large numbers of attachments must be blocked within a short period of time, such as during an outbreak of a new Microsoft Outlook Visual Basic virus, running attachment blocking on both the mail gateway and the internal mail server helps prevent infected attachments from slipping through due to overload. As a nice little extra, attachment blocking can also be used to block MP3 and other nuisance files that unnecessarily consume system resources.

Unfortunately, anti-virus software and attachment blocking on the mail gateway and the internal mail server are no protection when a user accesses external email from a web browser, such as with Hotmail or Yahoo. The general system usage policy should prohibit users from utilizing web-based email software while at work. The policy can be reinforced with HTTP content filtering.

Anti-virus Software for File Servers and Clients

File server and client anti-virus products, such as those offered by McAfee, Symantec, and Computer Associates, scan for known virus signatures and generally cure infected files. Both real-time and scheduled scanning are available, but real-time scanning should be used whenever possible. Virus signature and engine updates should be implemented on all servers and clients as soon as they become available.

A network application launcher, such as Novell ZENWorks, can be used to automate the virus signature file update on the clients. ZENWorks can be used to create a network application

object for the client anti-virus software. The application object can then be distributed over the network to the client desktops, eliminating the need to visit each PC. The distribution can be transparent to the user, if desired.

A written policy should govern the implementation and configuration of anti-virus software on all servers, and conversely on all clients, and a uniform configuration standard should be applied. For example, the policy should define the file types that must be scanned, at a minimum, by all file servers and the action(s) to be taken when an infected file is found. If scheduled rather than real-time scans are permitted under certain circumstances, these circumstances should be defined in the policy, along with how scheduled scans must be configured and how often they must be performed. Regular audits should be performed to ensure that all servers conform to the policy and are running up-to-date anti-virus software.

Anti-virus software should also be installed, running, and up-to-date on all privately owned PCs used by remote users or those who transfer files between work and home, whether via diskette or email. If it is the responsibility of the equipment owner to install and maintain up-to-date anti-virus software, this must be clearly stated in the policy governing such users.

All users should be trained in how to perform ad hoc virus scanning of CDs, diskettes, local hard drives, and files downloaded from remote sites – if such downloads are permitted. A written policy and procedure for such scans, detailing when and how they are to be performed, should be in place.

System Backups

When all efforts to defend a computer system against malicious code fail, the only recourse may be to restore the affected data from backup; and yet, inadequate or non-existent backups are one of the more common system vulnerabilities. An organization may diligently perform daily backups, but never test these backups to verify that they actually work. It may have excellent backup policies and procedures, but non-existent or inadequate policies and procedures for restoring critical systems. The time to discover these errors is not after malicious code has damaged the system or the information it contains.

In order to assure that system backups are adequate, all mission critical systems must be identified and a risk analysis performed for each system. The SANS (System Administration, Networking, and Security) Institute recommends that the following issues be addressed when performing this analysis:[7]

1. Are adequate backup policies and procedures in place for each critical system?

2. Is the backup interval acceptable?

3. Is the system being backed up according to the procedure?

4. Has the backup media been verified to assure that the data is being backed up accurately?

5. Is the backup media securely stored and protected from physical damage both while in-house and off-site?

6. Are copies of the operating system and any restoration utilities stored off-site, including any necessary license keys?

7. Have restoration procedures been validated and tested?

Good standard operating procedure requires that backups be performed at least daily. The SANS Institute recommends that, at minimum, a full backup be performed weekly with daily incremental backups. At least monthly, the backup media should be verified, by doing a restore to a test server, to assure that the data is being backed up accurately.

Volume retention is another critical factor to consider when designing backup procedures. The volume retention period must be longer than the window of vulnerability for the affected data. For example, most organizations backup financial data at the end of each month. However, it may take another 2 – 4 weeks for the accounting staff to verify that the books balanced at month end, and errors may be discovered during this reconciliation process. This means that if a computer virus damaged the data in early January, the damage may not be discovered until the end of February. If the tape containing the monthly backup performed January 1 has already been overwritten, it will be impossible to return the system to its state as of the end of December, when the books were last known to have reconciled accurately.

Conclusion

Effectively protecting a healthcare organization from malicious code is not just anti-virus software and email scanning. Nor is it only the responsibility of Information Technology. It requires a multilevel defense that includes polices and procedures, user education, physical security, system configuration and maintenance, password management, anti-virus software, and adequate backups, and that has the support of the entire organization. Just as everyone in a healthcare organization has an important role to play in providing high quality care and good customer service to patients and their families, so must we all do our part to protect our organization's computer resources, and the information they contain, from malicious code.

References

1. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure Computer Science and Telecommunications Board, and the Commission on Physical Sciences, Mathematics, and Applications National Research Council. *For the Record: Protecting Electronic Health Information.* "Chapter 4: Technical Approaches to Protecting Electronic Health Information." Washington, D.C: National Academy Press, 1997. http://books.nap.edu/books/0309056977/html/82.html#pagetop

2. Computer Associates International, Inc. *Choosing Antivirus Software.* October 17, 2001. http://www3.ca.com/Solutions/Collateral.asp?ID=910&PID=128

3. Gue, D'Arcy Guerin, Executive Vice President, Phoenix Health Systems. *The HIPAA Security Rule (NPRM): Overview.* HIPAAdvisory. http://www.hipaadvisory.com/regs/securityoverview.htm

4. Harper, Chris, and Cooper, Gary. *Defending Against the New Virus Threats.* Secure Enterprise Computing Seminar Series. October 12, 2001.

5. Hjort, Beth, RHIA. "Measuring Up - Information Security: It Takes a Community," *Journal of American Health Information Management Association*, January, 2001. http://www.ahima.org/search/index.html (search on computer virus)

6. Martin, Jay. *A Practical Guide to Enterprise Antivirus and Malware Prevention*. SANS Information Security Reading Room. August 17, 2001. http://www.sans.org/infosecFAQ/malicious/guide.htm

7. SANS/FBI Twenty Most Critical Internet Security Vulnerabilities http://www.sans.org/top20.htm

8. Sardinas Jr., Joseph L., PhD, and Muldoon, Jeannine D., PhD, RN. "Are You Vulnerable to Hackers? How to Protect Patient Information," *Journal of American Health Information Management Association*, November/December, 2001. http://www.ahima.org/search/index.html (search on computer virus)

9. Symantec Corporation. "Understanding Symantec's Anti-virus Strategy for Internet Gateways," *The Symantec Enterprise Papers*, Volume XXX. http://www.symantec.com/avcenter/reference/wpnavieg.pdf

10. Thrower, Woody, Burnett, Stan, and Wahlquist, Gary. "Prevent Current and Future E-mail Worms," *Symantec Security Response*, May 12, 2000. http://www.symantec.com/avcenter/security/Content/2000_05_12.html

11. Trend Micro, Inc. *Trend Micro Safe Computing Guide*. http://www.antivirus.com/vinfo/safe_computing/

12. Trend Micro Enterprise Solution – Gateway Protection http://www.antivirus.com/products/internet_gateway.htm

13. Trend Micro Enterprise Solution – Email Server Protection http://www.antivirus.com/products/email-groupware.htm

Last Updated: March 19th, 2018

Upcoming SANS Training

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

SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Boston Spring 2018	OnlineMAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced