Global Information Assurance Certification Paper

The need for Content Security

Hidayath Ullah Khan
January 15 2001

Many organizations are increasingly using Internet for sharing of information and conducting on-line business in the form of e-Commerce and Web-Commerce. This has resulted in the development and widespread use of technologies such as Java, ActiveX, XML etc. which provide many new additional features and functionality, and yet at the same time, expose the Internet users to many new, and increasingly serious security threats. Some of these threats are hidden within the data content of the Internet traffic stream, making them harder to get detected using conventional anti-virus software solutions. These threats can potentially cause a lot of damage to the corporate network as well as other resources.

This paper briefly examines the different situations in an organization that underline the need for implementing Content Security and also highlights the various Content Filtering Tools available for Email, FTP & Web Browsing.

Why Content Security?

"Content Security" is needed to counter three primary issues affecting an organization:

1.0 Security Threats
2.0 Productivity Problems
3.0 Legal Issues

1.0 Security Threats:

Threats to computer systems have increased dramatically over the past few years. According to FBI, around 62% of the companies experienced security breaches during the year 2000 in USA alone. More and more companies are deploying firewalls to protect their resources in the false assumption that firewalls provide complete security. But the threats have not decreased. The reason for this is that traditional hacking has been augmented by new classes of attacks like:

- Information Leakage
- Inappropriate Content
- Vandals and Viruses

1.0.1 Information Leakage:

Just as the email and web connectivity can make an employee productive, nothing can stop him from transmitting company sensitive confidential information to untrustworthy sources at the speed of the wire. The leaked information can cause

huge losses for the company or might tarnish the image of the company in the business markets. Unless some kind of content filtering is not enabled to check the contents of the outgoing mail and web traffic, these kind of attacks will go unnoticed.

1.0.2 Inappropriate Content:

Valuable time and network bandwidth is quite often, wasted by accessing unproductive sites. Additionally, there are thousands of web sites, which hold a collection of hacker tools and exploits that can be easily downloaded by disgruntled employees to launch an internal attack. Unless some form of content filter has not been deployed to check the contents of downloads for malicious tools, these sorts of attacks are hard to prevent.

1.0.3 Vandals and Viruses:

Vandals also known as "mobile code or active content" are the new kinds of threat that cannot be detected using conventional anti-virus software solutions. Unlike a virus, which require a user to execute a program in order to cause damage, vandals are auto-executable applications, which get executed whenever a user views a web page. Vandals are far more dangerous and lethal than their virus counterparts. The danger with vandals is that it runs automatically with full rights and privileges and can take any action on a PC. Thus, active content has become a useful technology used by hackers to break into PCs.

RFC 1135 states: A "virus" is a piece of code that inserts itself into a host, including operating systems, to propagate. It cannot run independently. It requires that its host program be activated.

Currently, there are thousands of known viruses classified in to many different categories depending upon the kind of the damage they are capable of inflicting. Every other day, we learn about hackers letting loose their viruses on the Internet in order to cause maximum damage. As a matter of fact, Internet is acting like a catalyst for the lightening speed at which viruses are spreading into organizations. The rate at which the ILOVEYOUVIRUS spread to different parts of the globe in such a short time proves the case in point.

1.1 The Point of Entry:

According to a recent study conducted by ICSA on the number of companies that experienced security breaches, it was found out that in a majority of the cases viruses entered these organizations through their Internet gateways. In other words, the **POE** "Point of Entry" for viruses has now shifted to Internet gateways, instead of the earlier methods, like users bringing in infected floppies, or users, downloading programs through attached modems etc.

Once a virus enters an organization through the Internet Gateways or firewalls, it will by-pass the server based anti-virus protection mechanism since users download files directly to their desktops. And if a virus travels within an email

attachment, the rate at which desktops get infected is very high because the mails get forwarded to one another. The system administrator's face a daunting task of "putting out fires", as viruses flow in via e-mail and Internet down loads. To stop this nuisance from re-occurring quite often, viruses have to be stopped at their "Point of Entry" (the firewalls or perimeter routers) in to the corporate network.

1.2 Firewalls are not enough –

Though firewalls are tremendous tools for protecting the network from unauthorized access, however, they still lack an inherent mechanism to inspect the content of data coming from or going to the Internet. Moreover, Firewalls do not protect from attacks of Java and ActiveX vandals. Therefore, the solution is to integrate the virus and vandal protection in to the firewall itself.

1.3 The Vandals:

In contrast to viruses, which require a user to execute a program in order to cause damage, vandals AKA "mobile code" or "active content", are auto-executable applications that get executed whenever a user views a web page. They do not replicate or modify and infect files but rather cause instant damage. Unlike viruses, the complete destructive payload will be already delivered by the time the vandals are identified and removed. Usually the vandals are harder to detect and typically operate in a Hit-N-Run fashion.

Vandals are found in executables, Java, Active X, JavaScript, Visual Basic Script, cookies and plug-ins.

1.4 Types of Vandal attacks –

- **Denial of Service:**

  Vandals in this category render a system completely useless by crippling it or eating up all the resources or by just shutting the system down.

- **Password Theft**:

  Vandals in this category steal a user's password and transmit it over the Internet to be later used to masquerade as the original user.

- **Modem Hijacking:**

  Vandals in this category can hijack a modem and redirect it to an another number in order to incur huge bills.
  Recently, AT&T were ordered to pay a 2.8$ million as compensation to its consumers, who received hefty telephone bills as a result of modem

hijacking. It so happened, that when some unsuspecting users were surfing the web, they were enticed in to visiting a web site, which promised free pornographic pictures. In order to view the pictures, the users were asked to download a plugin which silently disconnected their modem from the main ISP, switched off the modem's speakers and reconnected them back to an another ISP which had huge calling rates.

1.7 Vandals Vs Viruses

Vandals	Viruses
Auto-executable applications	Require the user to manually run the program
Do not replicate themselves	Replicate themselves
Hit and Run	Remain on the system
Very hard to detect using conventional anti-virus solutions	Can be scanned and cleaned
Found in Java applets, ActiveX content, plug-ins	Found in infected floppy disks, email attachments, word, excel macros

Anti-virus software is adequate at catching viruses that are defined in their databases. However, if a new Trojan horse or Internet worm attacks a user's PC, they will not be protected by anti-virus software. When a new virus is released it takes hours for anti-virus companies to formulate a patch and distribute it to customers. This "lag" time allows thousands of PCs to be infected and harmed.

This is where Content Security comes in to picture. The solution is to integrate firewall with a Content Filtering Gateway to be used as a first line of defense in combination with reactive anti-virus products to protect against brand new malicious code attacks. Content Filtering Gateway identifies and analyzes code as it enters the network. All characteristics of the code are examined for security violations on the fly. Any code that violates the corporate security parameters is logged and blocked at the gateway, while end users are notified with an onscreen alert.

1.8 Different Content Filtering tools available:

- eSafe Protect Gateway
- MimeSweeper
- Finjan Surfin Gate

For implementation details of MimeSweeper, please refer to the Dwight Daily's article on content filtering
URL: http://www.sans.org/infosecFAQ/stopgap.htm

1.9 Content Security benefits:

- Ability to proactively blocks viruses and vandals at their point of entry in to the network
- Blocks email based on keyword content, sender address, or other parameters
- Additional layer of Security

The other reasons for Content Security –

2.0 Business productivity in an organization is affected by:

- Casual Surfing
- Bandwidth wastage

Most organizations are currently not immune to the above mentioned risks as Internet is being heavily used by the companies for email, web browsing, ftp etc. External business partners and nomadic employees access corporate applications over the Internet making it one of the most critical resources of an organization. Bandwidth hungry applications also chew up a lot of valuable Internet bandwidth.

Therefore, it is very essential for an organization to analyze the type of traffic crossing its Internet gateways and determine how much of it are business related and how much is not. Clearly, the solution is not just to buy more bandwidth but to deploy some kind of screening system to help ensure productivity and conserve the valuable bandwidth.

Here is an example that shows how much a company stands to loose on account of casual surfing:

- **A 1000 user company**
- **100 People Surf**
- **Casual Surfing takes place for 0.5 hour per day**
- **Average Salary is $10 per hour**
- **$10/hr x .5 x 100 x 220 days =**
- **$110,000 in lost productivity / year for 100 users**

3.0 Legal Issues:

- It is easy for people to use an organization's Internet connection for crimes. Recently, a child pornography racket was unearthed at a medical center in UK.

- Organization can be held liable: Florida library threatened with "hostile workplace" lawsuit.

Different types of Web Filters:

- Client Solutions &
- Server Solutions

Client Solutions:

- Filtering software has to be installed on each desktop
- Requires lot of admin time to administer
- Can be easily disabled by the user
- Examples: The Library Channel; Net Nanny

Server Solutions:

- Server based products offer higher levels of security and eliminates the need for placing software on desktops.
- Centralized administration
- Examples: Bess, WebSENSE, X-Stop

How do Web Filters work?

- Filters limit access to information using either a keyword or database method.
- Keyword method is the most basic method of filtering. It blocks objectionable material by looking for specified keywords.
- It can be very inaccurate and can block info that contains some legal word combinations.
- Database systems are composed of IP addresses and URLs. They are more accurate than keyword blocking, but need to be updated regularly in order to be effective.

Benefits of Web Content Filters:

Web Content Filters maximize employee productivity and conserve network bandwidth by helping channel employees to Internet sites that are related to their

work. And by controlling access to inappropriate or objectionable sites, Web Content Filters also help in reducing the risk of corporate liability.

Conclusion:

Companies conducting on-line business over the Internet are exposed to a wide variety of auto-executing code that can be used maliciously. Corporate employees are exposed to these risks everyday by simply browsing the Web to perform research, buy products or to communicate with business partners and associates.

Security is vital for an organization's success. For any organization to be successful, email and Internet access needs to work effectively. Content Security provides an additional layer of security in conjunction with firewalls, VPN, IDS etc to protect against the constantly evolving Internet attacks.

References:

1. "Content Security Resource Center"
   URL: http://www.esafe.com/home/csrt/index.asp

2. "MIMEsweeper: Content Security"
   URL: http://www.re-soft.com/product/mimeswep.htm

3. "Malicious Code Research Center".
   URL: http://www.finjan.com/mcrc/

4. Daily, Dwight. "The Stopgap Measure: Content Filtering". 15 September 2001
   URL: http://www.sans.org/infosecFAQ/stopgap.htm

5. Zeltser, Lenny. "The Evolution of Malicious Agents". May 2, 2000
   URL: http://www.sans.org/infosecFAQ/agents.htm

6. "Internet filtering software by websense"
   URL: http://www.websense.com

7. VIBERT, ROBERT. "The Next War"
   URL: http://www.infosecuritymag.com/sep2000/logoff.htm

8. Stone, Martin. "Cybercrime Growing Harder To Prosecute". January 21, 2000
   URL: http://www.ecommercetimes.com/news/articles2000/000121-nb1.shtml