Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 1

The Email Threat

John Richmond

Contents

Abstract

Electronic messaging has become the lifeblood of many businesses. It has become the major tool for business communications. With this reliance on email businesses need to understand the security issues that revolve around electronic messaging.

This paper will provide a detailed look at securing the network from the threat posed by E-mail. It will consider the exploits and threats that exist, and then it will look at how to protect email systems against potential security breaches.

Introduction

Implementing network security is like trying to chase a moving target. Companies can, and do spend vast sums of money every year trying to solve problems as they occur. Many experienced the misery that the Sobig and Love Bug viruses caused, and the fire fighting exercises which ensued. For many years companies relied on updated desktop virus definitions to protect themselves, however these days are long gone. Securing a network is not a one off piece of work but more of an evolving challenge. With regards to this paper it is important to note that most companies in today's market place would find it inconceivable not to have a fire wall configured and in place, but would still overlook the single biggest source of their problems, which is email.

Email has become more popular than postal mail in the UK, with the number of emails being sent and received from household s exceeding letters by nearly 300 million. Britain also leads Europe in email usage, sending more than 170 million more emails than the French, and 185 million more than the Germans per month. This is according to Net Value, who tracked email usage in Ger many, France, Denmark, Spain and the UK during December 2001 and January 2002.

Forrester Research has predicted that Email conversations will cut through inbox clutter and temper growth to 939 billion emails by 2006 , and that marketing companies will spen d $6.8 billion on e mail services by 2006.

So we can see that there has, and will continue to be extraordinary growth in the way businesses use email. However to many users email is simple tools to meet an end, when in fact it is has beco me a multifaceted, complex and critical business tool.

The complexity of this prime communications tool can best be seen when considering how to make the corporate messaging system more secure.

Network Security and the Email Threat

There is an array of diverse elements that can weaken and cripple an organisations e-mail system. Some of the issues are well known and documented, while others are not, or even worse tend to be ignored When an emails payload carries offensive or confidential data this can cause inconvenienc e and expense to a company or organization that has not considered the vulnerabilities of email and equipped them with the correct tools to defend and neutralise such attacks. This also applies to spammers who utilise email systems to generate thousands o f u nsolicited emails, and to the menace that are email viruses, which can cause tremendous expense and downtime to companies.

Many companies install a firewall of some description and then start to believe the job is done and they are secure. While this is a good starting point it is only a starting point, more targeted measures need to be applied to the corporate network to close the email security loopholes

- **Threat of mail server compromise**

The greatest fear for many administrators is that their Mail Server will become compromised or corrupt beyond repair. For the purpose of this paper we will look at Microsoft Exchange server. There are some key areas that can be exploited with the Exchange server; these are Network port scans, IIS, server enumerati on, share pilfering and LDAP enumeration.
TCP/UDP scanning is a typical way for an attacker to build up a map of the network. The Exchange server by default has 30 listening ports open.
It's basically the same old story that if you allow anonymous or nul l sessions to be established, an attacker can glean a ton of useful configuration and user information from your system.
Exchange 2000 sets shares by default to allow Everyone, or Authenticated Users with Read access. Of particular interest is the Exchang e message tracking system. If this is turned on, then tracked messages will be stored in this shared folder using a name scheme of %COMPUTERNAME%.log. In this folder the System Attendant will keep track of who is sending e-mail to whom. This file contai ns principal names and e-mail addresses, which can be useful to an attacker searching for clues .
Exchange Server 2000 requires that IIS be installed with the Web Service, SMTP service, and NNTP service. These services provide necessary components. The S MTP service is dependent only upon the IIS Admin service.
It is the Web Service that is the questionable aspect. Many people cannot decide whether or not Exchange server depends on the Web Service to be running, and so leave the service running.

- **The threat from Spam**

Currently about 90 per cent of e-mail users receive spam at least once a week, a recent survey conducted by the Gartner Group shows. Currently 68% of US Internet users say that they find unsolicited e-mail useless and bothersome, and two thirds of US Internet users support legislation to prevent the widespread use of unsolicited e-mail as a marketing tool.
Although in Europe the European Commission are reviewing a call to ban spam, unwanted mail is on the increase.
Spam can and does consume bandwidth and slows down e-mail systems, spam mail is a drain on resource, forcing employees to filter through and delete the unsolicited junk mail, causing them to become unproductive to the business. Unsolicited commercial communications cost UK business £5,000,000,000 per year (source: Novell). It also proves irritating, offensive and upsetting to recipients who feel their privacy has been invaded. 10% of unsolicited e-mail is pornographic. (Source: Computing Services and Software Association). However, there is another aspect to spam, which is often overlooked: it constitutes a security hazard.
It is possible for spammers to use a corporate mail server to send out their unsolicited messages / marketing, without the organization knowing this happening, and can in itself lead to sanctions against the organization. One such organization, which was hit by spammers in this way, was Virgin Net. The effect on Virgin was three fold; Virgin Net was placed on the Real time Black hole List, it cost the company 40 management hours of investigation and Virgin Net received much negative publicity.

- **The threat of e-mail interception, tampering and spoofing**

Email has become a simple way for businesses to communicate with, that many do not know or care about the mechanics of how it works.
What many people within organisations to do not appreciate is that while email may well be secure on the internal network once it leaves the corporate network and heads onto the Internet it is not secure in anyway. Email can be easily read and changed before it reaches the recipient.
There are numerous software tools such as sniffers, which automatically lie in wait for interesting information relayed through their system as e-mails are transferred from sender to recipient.
Unknown to e-mail senders, sniffers are placed in the path of all e-mail messages going through a computer. The messages are then intercepted, and copies taken. Many of these operations are highly sophisticated and are generally motivated by financial gain. Some of the criteria, which these people may watch for, are credit card numbers, bank details, passwords and email addresses.
Whilst scanning and intercepting mail is one thing, there has been an upsurge in the tampering of email so that the recipient does not receive the email originally sent.
A threat, which has become more prevalent in the last few years, is that of email spoofing. This involves the emails sent to people purporting to be from

a legitimate organisation when they are really from s bog us source. The mails will attempt to obtain personal data from the recipient, usually financial data. In November and December 2002 online auction site Ebay was hit twice with fraudulent email schemes. Other companies to have suffered in recent years are Amazon.com and America Online.
Experts believe the actual incidence of tampering higher than reported, this in part being organizations reluctance to divulge this information for fear of crippling negative publicity.

- **Threat from information leaks**

It is well documented that organizations often fail to acknowledge that there is a greater risk of critical data being stolen from within the company rather than from outside.
Various studies have shown how employees use e-mail to send out confidential corporate information. The reasons for this are varied, some because they are disgruntled and revengeful, or simply because of ignorance, and so fail to understand the impact their actions may have.
The Information Security Breaches Survey 2002, sponsored by the UK's Department of Trade and Industry, found that in small companies, insiders caused 32 percent of the worst security incidents. In large companies this figure climbed to 48 percent.
Research has shown that up to 21-31% of employees admit to sending confidential or restricted information to recipients outside the company by e-mail. On the reverse of this up to ten per cent of those questioned admitted to receiving mail containing company confidential information.

- **The threat of e-mails containing offensive messages**

Over the last few years there has been an explosion in the E-mails sent by staff containing racist, sexist or other offensive material could prove equally troublesome, not to mention embarrassing – and expensive.
British law holds employers responsible for e-mails written by employees in the course of their employment, whether or not the employer consented to the mail. The insurance company Norwich Union was asked to pay £210,000 in an out-of-court settlement as a result of e-mailed comments relating to competition. In addition there have been several high profile cases in recent years where employees have taken their employers to court over obscene, malicious or racist emails.
Besides, offensive e-mails can cause considerable damage to the work environment simply by generating an unpleasant, hostile or unprofessional atmosphere.

- **Non-Delivery threat**

As email has become an integral part of business life it use has also become critical. Email is now used for proposals, orders, confirmations, p roduct documentation, etc. In this context it is essential that confirmation of delivery is recorded and tracked to ensure that the intended recipient receives the email. This therefore calls for the need for a secure mechanism for tracking, archiving an d retrieving email messages.

- **Virus threat**

One of today's major email security hazards is the virus. This threat is one that companies cannot afford to ignore. There are to date over 20,000 viruses in existence, while there are estimated 500 new ones eve ry month.

The effects of such email borne viruses should not be underestimated; the effects can be insignificant to totally destructive.
In May 2000 the Love Bug was unleashed on the world. It is estimated that 30,000 businesses in the UK were affected in the first 48 hours of the virus becoming active. The Love Bug virus was a worm, which was spread by email, and was very destructive in its nature, completely infecting the hard drive of computers and then infecting the messaging networks. The cost to businesses has been put at hundreds of millions of dollars worldwide.

Securing the e-mail system

- **Email Security Policy**

So the threats, which email pose to an organization, are many, however there are solutions to all these threats.
One of the firs t steps to combating against the treat is the formulation of an email policy. This policy should be incorporated in to a much wider corporate security policy.
The purpose of the email policy document is to educate the users on the best security practices when using email. If used correc tly the document should provide guidelines and proce dures that are to be followed in the use of email in the corporate workplace.
Without being overly restrictive, such documents should provide guidelines and procedures t o be followed by employees in their use of e -mail at the workplace. The critical message that should be emphasised to employees is that the policy is there to benefit them and the organization by making email messaging secure.
However the email policy wil l not work alone. To help enforce the policy and nullify the email threat an organisation should use security tools to enforce and regulate the email threat. There are numerous software applications

available to organizations that deal with the email threats discussed earlier. It is the organization that should evaluate the products and find the one which best fits its purpose.

We will now consider what email solutions exist in the marketplace.

- **Spam Elimination**

To eliminate spam in an organisation it should employ the use of an anti-spam tool. The anti-spam product should meet the following characteristics. An efficient anti-spam tool should cover the following areas:
It should have accurate spam identification. The product should be able to keep the spam email out, while letting legitimate email though. The key is to keep the number of false-positives to a minimum.
The product should be able to be tailored. This means the product should allow organizations to create and amend policies based on their own Spam definitions. Not all companies define Spam as being the same thing, and so have differing policies regarding Spam.
Anti Spam counteractive measures. The product should have the ability to apply different actions to spam depending on the type and classification. Again organizations have differing policies to spam email and as such the product should be able to tailor to these needs.

- **Stopping interception and tampering**

In order to stop interception and safeguard against tampering with their emails on the Internet an organisation should look to encryption technology, such as PGP, S/MIME or SSL, to guarantee secure email messaging.
PGP (Pretty Good Privacy) is the most common form of encryption technology in use on the Internet. PGP is 128-bit encryption. It uses "Public Key Cryptography." Each user generates a "Public Key" and a "Private Key." The public key is public. It is given out, put on public key servers, and included in the signature. When a mail message is then sent, it is encrypted using public key. When the mail message is received, the private key is used to decrypt it. There is no way to determine the private key from the public. The private key can also be used to digitally "sign" a message with or without encrypting it. The recipient can use the public key to verify the email message.
One point to note with using encrypted email is that virus checking programs cannot scan encrypted mail and their attachments. Therefore it is good practice to have a workstation virus-checking program that watches for viruses as applications and files are opened.

- **Preventing information leaks**

One way to prevent information leaks from within the organization is to employ the use of an email content checking product.
Email content scanning products check inbound and, in this case more importantly on outbound messages. The products scan for confidential data, location filtering and prohibited content.
They search for keywords and phrases, profanities, banned file types, oversize data packets , and malicious code. The products can be set to quarantine email messages and generate alerts for administrators.
With the continuing move towards public -key infrastructure (PKI) and e -commerce, the products should also be able to perform content analysi s on encrypted or signed email.

- **Content Scanning**

A content screening tool is necessary to prevent corporate users from sending or receiving offensive, profane or inappropriate e -mails, such as racist or sexist messages, pornographic material, certain fi le types and other undesirable content. The tool should be flexible to allow the organisation to manipulate what is scanned and to what depth.
The content screening product should al so sc an for viruses within emails and attachments.
In addition the produc t should have quarantine features to enable suspect emails to be placed in a secure area and be prevented from being received or sent. In this way an emails content can be reviewed by an authoritative body within the organisation and then released if deem ed suitable
Organizations should also look to utilise tools which that automatically add a legal disclaimer to the end of every message sent out by the organization.

- **Reporting**

Email management and reporting tools will allow organizations to track e -mail usage, monitor communications, track individual emails, and track high email domains. This will allow the organisation to enforce the email policy within the organisation.
Content archiving tools help reduces the ongoing cost of email storage, brings control to mailbox management, optimises the backup/recovery cycle and ensures that valuable information can be retrieved quickly and efficiently for compliance and knowledge management use.

- **Virus Protection**

Virus protection forms part of an organizations defence. It should not be the only defence but should work in unison with the other products and policies in place to safeguard against the email threat.
The virus scanner should be used to scan all incoming and outgoing mail to the organisation. They should be able to detect the various types of virus: boot, file (files containing executables or code), macros, script or worm.
The product should also be able to clean the virus, block the virus, quarantine it and raise alerts not only to administrators but also to recipients to warn of the email borne virus.
Another feature is the definitions update procedure. With the rise in email viruses it is important that the package allows for automatic updates for up to the minute protection.
Content checking tools may also be used in the battle against e-mail viruses. Many of the content checking tools can be configured to scan for certain signatures, phrases or attachments which can then be trapped and isolated before delivering their harmful payload. This method is of extreme use when organisations are warned of a new email virus threat but do not have the latest definitions to combat the new virus.

Conclusion

So we can see that there are many threats posed to the network security by the use of email messaging systems. Organisations can no longer ignore this threat, as email has become the communication lifeblood for many. It has been shown that there are ways to combat against these threats and secure the network from the threat of email.

Reference:

1. Desmond, Paul. “Time to Get Tough About Email Security.” 12 May 2003
URL:
http://itmanagement.earthweb.com/columns/secugud/article.php/2205041
2. Hinton, Craig. “Email Security.” SC Magazine. February 2003.
URL:
http://www.scmagazine.com/scmagazine/2003_02/test_01/index.html
3. “Enterprise Secure Email Requirements.” February 2003
URL:
www.agorics.com/Library/CriticalRequirements.pdf
4. Roscoe, Trefor. “The Love Bug Bi tes.” July 2000
URL:
http://www.shef.ac.uk/uni/projects/wrp/virustut.html
5. KPMG
URL:
http://www.kpmg.com/about/press.asp?cid=469%20
6. Microsoft
URL:
http://www.microsoft.com/exchange/techinfo/security/bestconfig.asp
7. Festa, Paul. “Identity thieves strike Ebay. ” November 2002
URL:
http://news.zdnet.co.uk/internet/0,39020369,2126405,00.htm
8. Computing Services and Software Association
URL:
http://www.sototo.com/coa/138.htm
9. Novell
URL:
http://www.novell.com/offices/emea/uk/news/press/index.html
10. Kangas, Erik. “The C ase For Secure Email.” 2002
URL:
http://luxsci.com/extranet/arti c les/email-security.html

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor