2006

The Implementation of E-mail content management in a large corporation

Michael Hansen
Edith Cowan University

Craig Valli
Edith Cowan University

DOI: 10.4225/75/57b65aeb3476c
Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

The Implementation of E-mail content management in a large corporation.

Michael Hansen & Craig Valli
Edith Cowan University, Australia
mhansen2@student.ecu.edu.au
c.valli@ecu.edu.au

Abstract

It is a well known fact that while E-mail is a valuable tool to any business that it has also become the main cause in the distribution of viruses, worms and other malware. Further to this is the real threat of spyware that can affect performance on computers, phishing schemes that can cheat employees into giving up valuable information, such as passwords, using social engineering and the time-consuming and costly effect of spam to a corporate network. This paper will analyse and show the effect of a successful implementation of E-mail filtering software in a large corporation, together with some of the major findings discovered so far.

Keywords - SurfControl, spam, content management, filtering.

INTRODUCTION

Webopedia defines electronic mail, or email, as the transmission of messages over a communication network. Most companies make extensive use of emails in their day-to-day work, because it is fast, flexible and reliable. However, this usage may also come at a cost as email messages are often the vehicle used to transport malicious software (malware), spyware or spam. These nasties will at a minimum use bandwidth and valuable employee time, but also have the potential to affect performance or availability of company resources. For this reason, most large corporations will introduce a number of security initiatives, such as spam filtering, anti-virus software etc. This paper will describe the implementation of an email content management system, called SurfControl in a large corporation and reveal some of the findings discovered since this software package was implemented.

The company that is used in this paper is a medium to large organization with approximately 3,000 employees and a number of offices throughout the state.

There are a number of processes that were considered before the implementation of an email content management software package, such as

- What are we attempting to protect the company against
- Are the policies and work processes in place
- What are the legal requirements
- What are the costs compared to the risks
- What are the maintenance costs

These points will be covered in greater detail in the following sections.

EMAIL THREATS

These next sections cover some of the threats that are typically delivered or sent via email. It is important to understand what we are attempting to protect against before attempting to introduce and install security measures, so here are short descriptions of the threats delivered via email.

Spyware

Wikipedia defines spyware as software that subverts the computers operation for the benefit of a third party, meaning that it normally is designed to exploit infected computers for commercial gain. Spyware originally started as advertisements (adware) and web monitoring for marketing purposes, but it has since developed to the more serious and sinister key-loggers. Key-loggers record keystrokes and can be used to steal personal information, such as credit card numbers and passwords. Another typical behavior of an infected computer is a substantial loss of performance and reliability, causing the system to crash and hang.

Spam

Spam is generally known as unwanted and unsolicited email, however it is also more appropriately known as junk mail. The biggest issue with spam is the time wasted by employees reading these messages, and also the amount of network bandwidth wasted by the exorbitant amount of messages received. Another threat is that spam can be used to carry viruses or other malicious code. IDC (2004) estimates, that the number of spam being sent on an average day is 17 billion in 2004, that the average time spent by email users is 10 minutes per day looking at these messages and that these figures are growing rapidly to the degree that Murphy and Zwieback (2005) estimates that 80% of all email traffic worldwide is spam.

Phishing

Webopedia defines phishing as the scam used to get users to reveal private information that can then be used for identity theft. This is often achieved by emailing the user claiming to be from a legitimate business, such as a bank or Ebay, and asking the user to visit the Web site to update their personal information, for example password and credit card numbers. The web sites are naturally bogus, but made to look as the actual and legitimate business, and used to capture the users information. This scam is becoming more and more common, and it can be very hard to detect for a common user.

Malicious Software

Malicious code or malware is typically rogue programs intended to infect and cause damage to a computer. Pfleeger (2003, p 111-112) defines the various types of malware as

- Viruses – a program that infects by attaching itself to a healthy program. They spread manually by being copied or forwarded by an individual, and normally carry a payload with destructive instructions, such as deleting files
- Trojan Horse – a program that in addition to its primary use, has a second, non-obvious and malicious effect
- Logic Bomb – a kind of malware that s triggered by a specified condition, such as a date/time or an event
- Worm – is a program that spreads copies of itself through a network. The difference between a worm and a virus is that the worm self-replicates, meaning that it spreads copies of itself without manually intervention

Social Engineering

Some of the latest techniques used by hackers are a combination of the above threats, but could be classified as social engineering. This is typically done by addressing emails directly to the user with a legitimate sounding content, thereby fooling the user into opening an attachment that contains the malware.

Inappropriate Material

This threat can be either to company reputation, or cause discrimination or harassment. The company must be seen to take reasonable action to prevent inappropriate material been sent over the network. Content filtering can, according to Wakefield (2004), stop spam, scan attachments for inappropriate language, block dangerous attachments, quarantine questionable messages or embedded images and also log and notify managers about potential breaches. This can save the company massive amounts in litigation and lawsuits, and likewise prevent employee misuse of company resources for personal benefits.

POLICIES AND PROCEDURES

Policies and procedures

Pipkin (2000, p 96) states that policies are the primary building block in every information security design in defining the responsibilities of the organization, the individual and management. Policies specify what must or must not be done, whereas procedures define how the policies are implemented in greater detail.

This is a very important step that should be completed before attempting to implement content filtering. Following are some of the important parts listed in the email policy used within this organization

Illegal Use

E-mail users must not use the company's e-mail system to infringe the copyright or other intellectual property rights of third parties, to distribute or store, defamatory, fraudulent, harassing or obscene messages and files, or otherwise to engage in any illegal or wrongful conduct. This includes the use of insulting, sexist, racist, obscene or suggestive electronic mail.

External emails (incoming and outgoing)

Users must be aware that all emails are subject to content rules and are scanned to check for conformance. This includes, but is not limited to, categories included in 'illegal use' above.

Legal Requirements

Another important part of the equation is the legal requirement. The Australian Government (2003) has given the following requirements to companies sending emails as part of the daily business process – the Spam Act 2003. The Act carries a substantial penalty of up to 1.1 million dollars. The main points of interest in the act are:

Unsolicited commercial electronic messages (Spam) must not be sent.

Commercial electronic messages must include information about the individual or organization who authorized the sending of the message.

Commercial electronic messages must contain a functional unsubscribe facility

Other legal requirements are the Western Australian Censorship Laws, which according to WAIA (2001) prohibits any person from transmitting objectionable material using a computer service. Furthermore the Australian Human Rights and Equal Opportunity Commission (2005) states that managers responsible for monitoring work environments and ensuring acceptable standards of conduct are observed, especially that a workplace is free from discrimination and harassment. These responsibilities are specified in state and federal laws.

Procedures

Pipkin (2000, p.97) states that procedures are definitions of how to implement the policies to a specific technology. Procedures are detailed instructions, manuals and standards. However, this paper will not examine the specifics of the procedures in detail, but just mentioned some to clarify what is actually needed.

The first procedure should cover the software and the maintenance requirements of the software, such as installing patches and receiving signature updates. This procedure should also cover the monitoring of logs and reports. Procedures should also exist to describe in detail the steps needed to discipline or terminate employees misusing the system.

Other procedures needed are to describe how the user is informed about illegal usage and how to possibly release a quarantined email. The following is an example of the message used within this company to inform the user of an email that was filtered.

```
This message has been isolated after activating a rule in the company's filter.

Date: 25/08/2005
Triggered Rule : Executables
Sender: sender@company.com.au
Subject: FW: Test message

If you believe this message is a legitimate business related e-mail, you may contact the
Response Centre or REPLY WITH HISTORY to this email and the quarantined message will
be reviewed for possible release.
```

This email illustrates how a user is informed about a breach with enough information about the email to reveal if the message is still required. The message also specifies how to release the original email should this be required. The response centre will have specific procedures regarding quarantining and releasing of emails after checking the content thoroughly for malware etc.

Training and Education

Training and education is vitally important. A good example of this is the social engineering example mentioned earlier. The only way to protect against that is through training and education. This organization hands out the policies to all new starters and holds an information session to ensure that everybody is made aware of their responsibilities. This is naturally both a legal and employee satisfaction requirement.

BUSINESS CASE

Non-tangibles

The business case that was put before senior management outlined the benefits that email content management would have to the organization. This second section shows some of cost benefits, but this section deals with the more non-tangible issues. The main points were, according to Hancock (2005):

- Increased protection from Legal Liability (already covered)
- Enforcement of the Email policy
- Increased Virus Protection – this will be covered later
- Increased productivity
- Increase management reporting and content management – increased logging facilities to generate reports enabling decision making
- Reduction of Objectionable Material

Audit

A pilot project was created to examine email content and to test various software packages. This project revealed that up to 40% of all email was in breach of existing policies. It also directly lead to one person being terminated and others being suspended without pay. Another interesting, but not surprising fact, was that the amount of spam and objectionable emails were increasing drastically. But the most serious issue was an external complaint from a customer, stating that a grossly offensive email had been received from an employee using the corporate email account. This last complaint could easily have resulted in legal action, court costs and more importantly have dented the reputation of the company.

Some other interesting statistics are that within the trial month (single month), the audit showed, according to Hancock (2005):

- 30,000 picture files with titles such as why women cannot fix cars and Viagra overdose

- 240 movie files
- 1780 PowerPoint files titles such as Bodypainting and Best Sick notes

Cost Benefit

As we all know then managers are mostly interested in the bottom line, so the business case naturally included a proper cost benefit and risk analysis. The major points were an estimate that showed that even if 2 out of the 3 thousand employees only spent five minutes per day reading spam, deleting or forwarding non-work related material then the cost in lost time would be over $50,000 per month. Remember that IDC (2004) estimated that users spent 10 minutes a day on such emails and this figure was rising, so this cost is not unreasonable.

Another substantial cost was the rising cost of disk space to store email on the server, and upgrade to the server itself to handle the increasing amount of storage and traffic. There was also the unnecessary use of bandwidth for these often large email attachments, so altogether it was an fairly easy decision to introduce the software package.

SOFTWARE

Software package

IDC (2004) gives the following guidelines to choose the appropriate software for content management:

- Effectiveness over time, as the number of spam rises, the number reaching the users inbox should fall.
- Easy administration – minimize the time of IT staff to maintain and keep solution up-to-date
- Flexibility

In this case the company chose SurfControl, mainly because of the reasons listed above, i.e. the products ease-of-use, very low maintenance expense and effectiveness shown during the pilot project. SurfControl is obviously a proprietary product with an initial purchase price and yearly software maintenance costs. This paper is however meant as a general email content management solution rather than a sales pitch for a specific product. There are a number of other products available including open source solutions, like SpamAssassin. The decision on what software to use is the dependant on circumstances within the company, and is considered to be out of-scope for this paper.

Rules

The rules that are specified are fairly standard no matter what software package has been chosen. These rules will scan the message and attempt to determine the legality of an email. If the email is deemed to be illegal (in respect to company policy), then it will be quarantined and the user will be sent another email to that effect. Each email can be analyzed to determine why they failed the control, and they can be manually released at the request of the end-user, but only when the user is absolutely certain that this message is work-related and benign.

Rules typically install with a set of defaults depending on the product and can then be tailored to the organizations needs. The established rules within this organization are as follows, according to Hancock (2005):

- No executables – this also provides an additional virus protection. A number of executables contained viruses, but this was not recognized by the anti-virus software at that stage. But after updating the virus signature files and re-examining the email content it was determined to contain viruses
- No encrypted emails – this even includes password protected attachments. If the organization allowed personal encryption without knowledge of keys, then it would be unable to check the content of the email
- No inappropriate URLs – this is a list that is updated daily be the vendor

- No video and audio formats – the company policy specifies that these formats are not used and accepted, so …
- Anti-Spam agent – this is also update daily be the vendor and contains a dictionary management tool with illegal words. This product has a variety of different dictionaries depending on the content filter, but some of them are: adult, gambling, violence and hatred and SPAM

This last component will also cater for word misspellings, which are typically attempted by spammers to cheat these filters. A good example of this is the number of different Viagra spellings. The way the anti-spam agent works is that every email with a value of less than 100 points are passed through to the recipient without a problem. Illegal words in the dictionary are then rated depending on severity. As an example, then word "bestiality" is worth 100 points in the adult dictionary, meaning that any email containing this word will be automatically quarantined. However the word "sex" is worth 40 points, meaning that a sender can have sex twice, but a third time will mean quarantine (so to speak).

It is worth noting that the package does no longer contain a list of email addresses belonging to known spammers. This is because spammers harvest legitimate email address and use them to spoof the from-address, which renders so-called white or black-lists less effective, according to Cerf (2005).

Implementation

The implementation of the software package was done in small groups of 50-100 people at a time. This was done to minimize impact and to work with the various business groups in tailoring and perfecting the settings. Another important part in the implementation strategy was to communicate how the system and procedures works and to re-emphasize the policies.

OUTCOMES OF THE IMPLEMENTATION

Statistics

The following tables and graphs show some of the more important results that the introduction of the email content management system has had within the organization over the past year. These figures are courtesy of Hancock (2005).

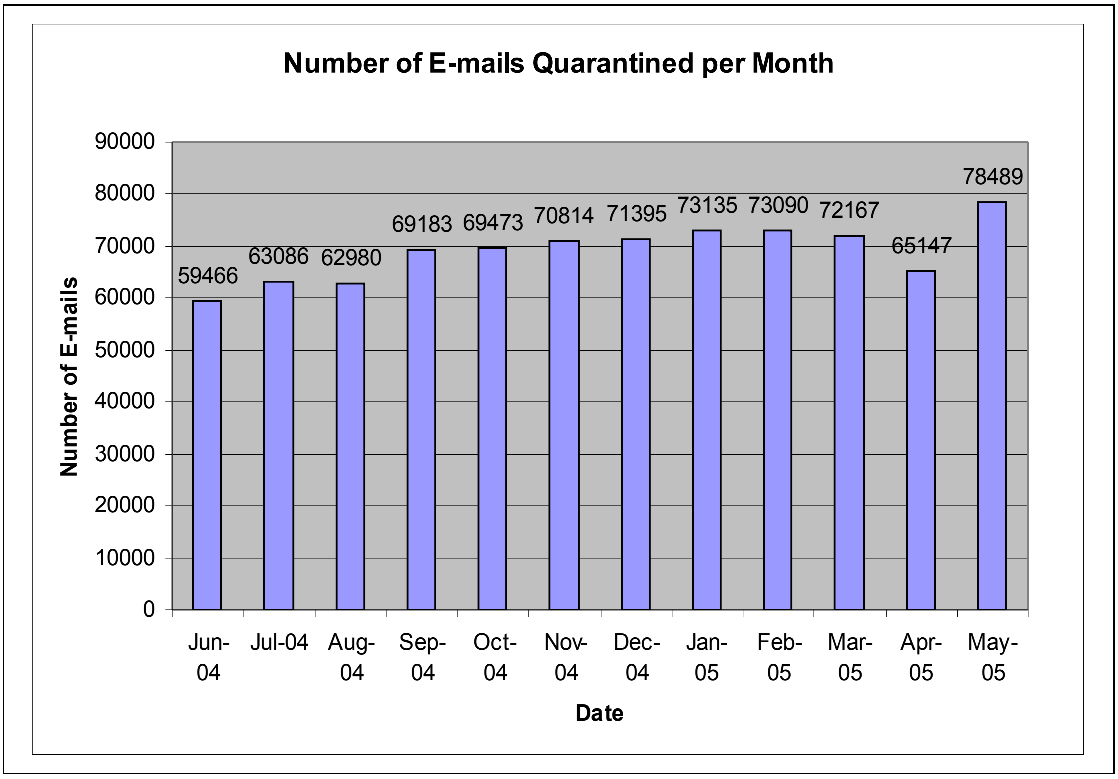
The first figures shows the number of emails sent, received and the number of emails that violated the email policy.

Email statistics for May 2005

Internet email received	Internet email sent	% of email received that contained malware, SPAM or prohibited content
325,316	164,379	28 %

This basically shows that more than 1 in 4 emails received contained prohibited content. Another tests traced an incoming email containing a rather large video file (before this was stopped and quarantined). It showed the email entering the organization, and within 5 minutes being forwarded a number of times to friends and family both outside and within the organization. This naturally affects both bandwidth and employee productivity.

The following graph shows the number of emails quarantined per month over the last year.



The figures show the increased number of emails, which is probably not that surprising, but can certainly be used to justify the introduction of a spam filtering package into any organization.

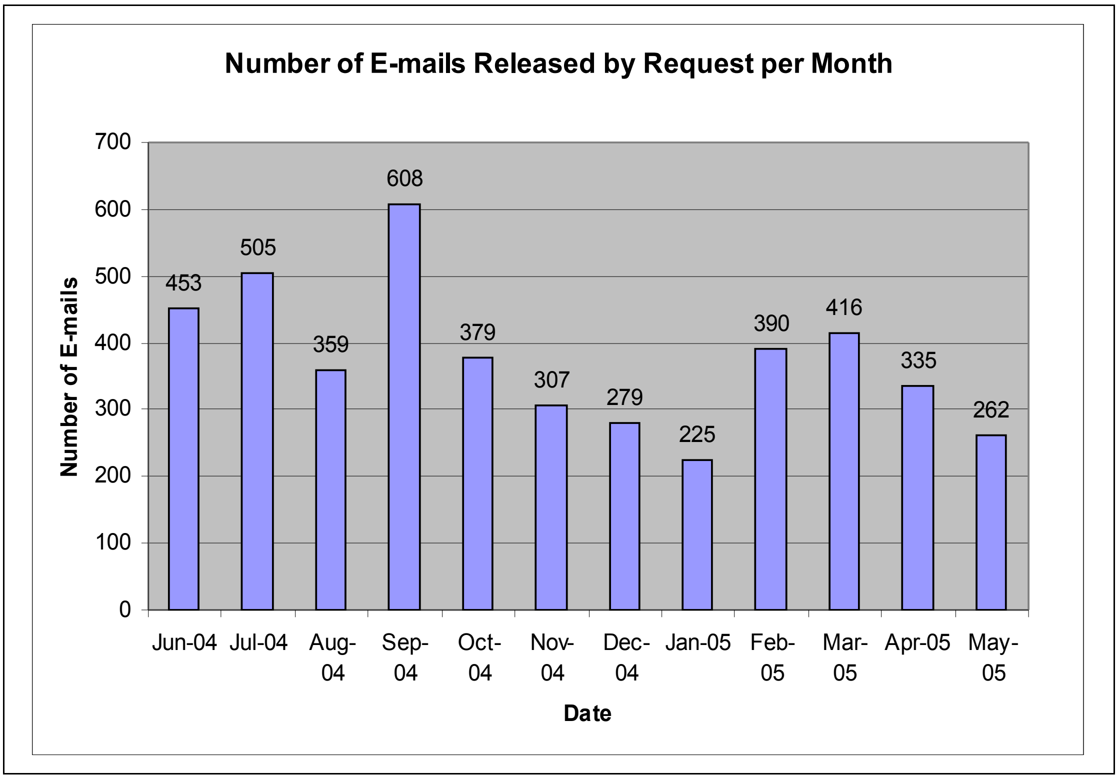
The following figures show the number of emails quarantined and the number that the user has requested being released, because the content was actually work-related.

Content Management Statistics for May 2005

E-mails Quarantined by the Content Management System	Emails requested for Release and Authorised	% of Emails Quarantined and Released
78,789	262	0.33 %

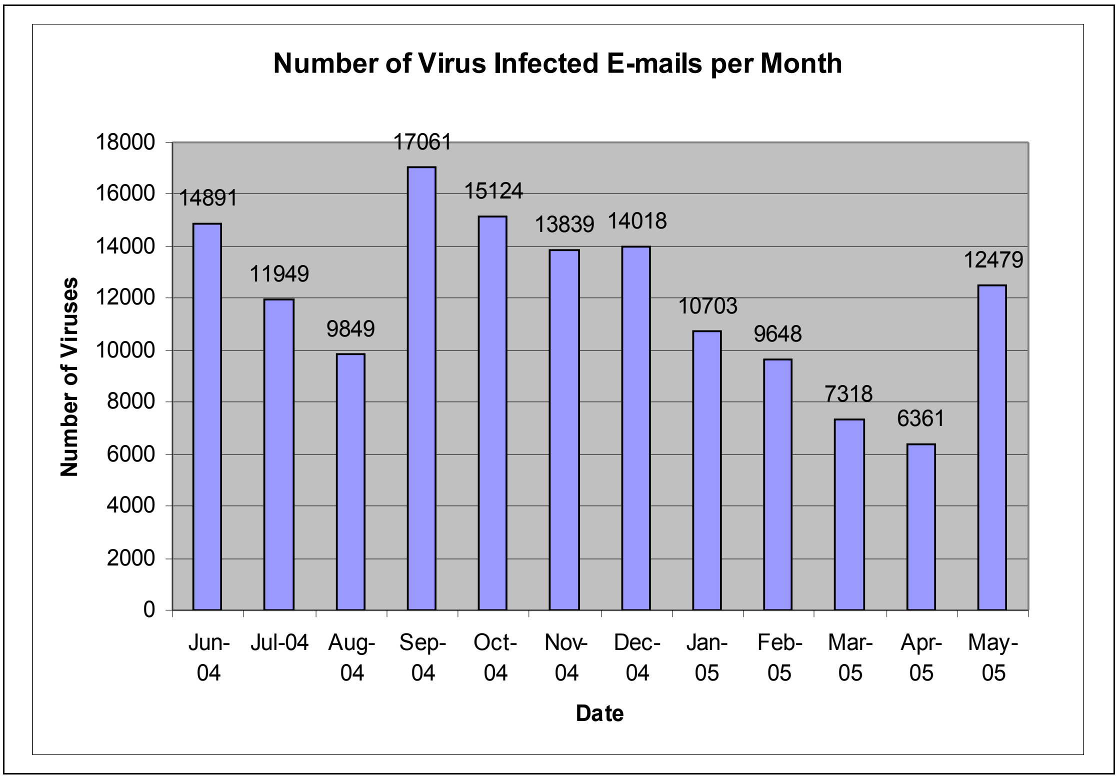
This is obviously a very low number, which also proves that the filtering is working reasonable well with regards to false positives. Gaudin (2003) reports that false positives have the very serious potential of damaging business by not letting legitimate mail through to the employee and that up to 70% of people have not gotten expected email. However, in this organization the user is shown the email header information, like sender, cc and subject line, plus the rules violated, and it is possible to recover and restore the email, so this problem is not considered to be of significance.

The following graph shows the number of emails released by request per month over the last year.



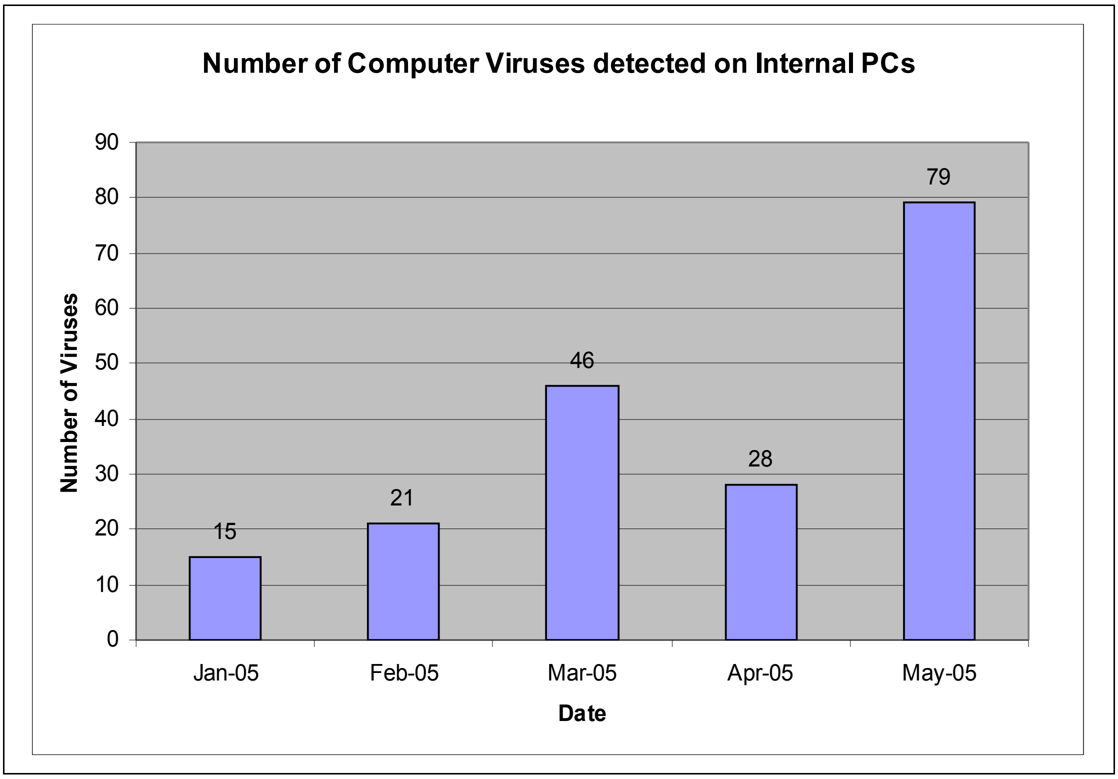
This shows that the number of emails released is falling. The main reason for this is that the process and policy has been tightened up recently, meaning that call centre staff who is normally responsible for releasing these emails are more selective in the process.

The next two graphs show the number of viruses within emails that have been intercepted per month over the past year.



The virus detection is not a direct result of the spam filtering package, but rather of the anti-virus software on the email gateway, however it illustrates how important email content management really is. One virus has the potential to cause sever destruction and outages in the entire network, so imagine what damage 12479 viruses could do in one month !

The last graph shows the number of viruses that has been detected on individual computers. This is not really a part of this paper, but it has been included to show that other countermeasures are also needed to stop viruses entering the network. Most of these viruses entered computers via q personal CD, floppy or USB drive. All computers within the network has the latest anti-virus software installed with signature updates happening daily which manages to minimize the potential damage.



PROBLEM AREAS

Encryption

One of the biggest concerns with the current setup is the lack of encryption. Not only is all emails sent and received in plaintext, it is also directly specifies in the policy that the use of encryption is not allowed. Calsoft (n.d) states that the decision should not be whether to supply email encryption, but rather how, or as Pfleeger (2003, p.474) puts it, you would not put sensitive information on a postcard.

The major threats to email content are, according to Pfleeger (2003, p.474):

- Message confidentiality – meaning that the message is not exposed during transmission. This can be solved by using an encryption algorithm
- Message integrity – that the receiver sees what is sent. Solved via encryption and hash routines that calculate a checksum and includes this in the digital signature
- Sender authenticity – that the sender is who he says he is. Solved by the use of digital signatures
- Non-repudiation – the sender can not deny having sent the message. This is also verified by the use of digital signatures.

This paper will not enter into the intricacies of introducing email encryption and the use of digital signatures into a large organization, but it should be looked at closely and rectified as soon as possible.

Some of the more concrete problems discovered in the beginning was the forward with history feature included in most email packages. This means that the content of a previously received email is included when a reply is sent and it also means that most emails very quickly grow to a substantial size, but also that the 100 points available as part of the anti-spam agent can be used up by previously sent emails. A procedure has now been put in place to reduce this feature as much as possible for the sake of disk space on the email server and limit the spam filtering effect.

Some of the other problems discovered early were email reports produced by programs on the mainframe or servers, and sent to the users via email. Because of the sheer size of some of these emails and for example often innocent customer names, then these reports would be considered as spam. This was solved by excluding emails sent internally via batch processing.

Other oddities included users with the names of Mr. Winner and Mrs. Gamble, which would get most of their email guarantied because of their unfortunate names. This illustrates the need for a slow and steady implementation plan, which includes training and education.

CONCLUSION

This paper has described a successful implementation of email content filtering in a large organization. The figures clearly show the importance of such a software package to both secure the company reputation and fulfill its legal requirements. In this case it has even saved the company money that it would otherwise have had to spend on hardware upgrades to the mail server. The savings in wasted time otherwise spent by employees easily makes up for the cost of this proprietary software package.

Spam is here to stay, and it will most likely increase dramatically over the next few years. Malicious code will become harder to detect, which is all the more reason for companies to spend time and effort on security upgrades.

But what will the future hold? Probably more of the same, but also newer threats on newer platforms, such as mobile phones, laptops and palmtops. Cerf (2005) defines spim as spam via instant messaging (IM), which has already occurred and which will become main-stream sooner rather than later.

REFERENCES

Australian Government (2003), Spam Act 2003: An Overview for Business. Retrieved September 4, 2005 from http://www.dcita.gov.au/__data/assets/pdf_file/20453/Spam-overview4business.pdf

Australian Human Rights and Equal Opportunity Commission (2005), Information for Employers. Retrieved September 10, 2005 from http://www.hreoc.gov.au/info_for_employers/index.html

Burke, B.E. (2005), The Evolution of Content Filtering: Multiple Layers of Threat Protection. Retrieved August 30, 2005 from http://www.surfcontrol.com/uploadedfiles/general/white_papers/Evolution_of_Content.pdf

Calsoft (n.d), E-mail security. Retrieved September 11, 2005 from http://www.calsoft.co.in/whitepapers/emailsecurity.html

Cerf, V.G. (2005), Spam, Spim and Spit. Retrieved September 10, 2005 from http://0-proquest.umi.com.library.ecu.edu.au/pqdweb?index=0&did=845179211&SrchMode=1&sid=2&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1126338057&clientId=7582

Gaudin, S. (2003), False Positives: Spam's casualty of War costing billions. Retrieved September 11, 2005 from http://itmanagement.earthweb.com/secu/article.php/2245991

Hancock, T. (2005), Email Content Management. Internal presentation.

International Data Corp (2004). IDC Study: The True Cost of Spam and the Value of Antispam Solutions, 2004. Retrieved August 30, 2005 from htp://www.surfcontrol.com/uploadedfiles/general/white_papers/IDC_Spam_Study.pdf

Pipkin, D.L. (2000), Information Security. New Jersey: Prentice Hall.

Pfleeger, C.P. (2003), Security in Computing. New Jersey: Prentice Hall.

Murphy, J. & Zwieback, D. (2005), Managing Emerging Security Threats. Retrieved August 30, 2005 from http://www.surfcontrol.com/uploadedfiles/Mnging_Security_Threats.pdf

SurfControl (2005), SurfControl E-mail Filter. Retrieved September 10, 2005 from http://www.surfcontrol.com/uploadedfiles/SEF_datasheet.pdf

WAIA (2001), Censorship Act 1996(Excerpt). Retrieved September 10, 2005 from http://www.waia.asn.au/Documents/CensorshipAct96.html

Wakefield, R.L. (2004), Computer Monitoring and Surveillance. Retrieved September 4, 2005 from http://0-proquest.umi.com.library.ecu.edu.au/pqdweb?did=663573171&sid=2&Fmt=4&clientId=7582&RQT=309&VName=PQD

Webopedia (n.d). Online dictionary found at http://www.webopedia.com/

Wikipedia (2005), Spyware. Retrieved September 4, 2005 from http://en.wikipedia.org/wiki/Spyware#History_and_development

COPYRIGHT