

The need of email Content Security

Vasilis Paliouras*
Space Hellas, S.A.

Abstract

This paper addresses the security implications and business impact of a messaging system extending the role of content security from hostile code filtering to defending against unauthorized transfer of information. In addition, hidden or indirect consequences are discussed as well as some countermeasures and controls to minimize the corresponding security risks.

Introduction

The Internet and specifically the utilization of the email service have raised two conflicting issues. On the one hand, it improves business communication, information sharing, market effectiveness and productivity but on the other hand it can become the platform for security breaches with known or unknown undesirable consequences ranging from a crippled or hacked corporate network to a ruined reputation and costly litigation. Thus, the need to filter and control email messages for viral, offensive or confidential content has never been more evident.

All Internet Email content people receive, read, and send carries a risk. The security threats having business impact are not confined to the boundaries of viruses, Trojans or generally viral code. Stopping email abuse and misuse is a two-dimension problem: controlling inbound and outbound traffic of malicious and hostile code and filtering inappropriate email content. What 'inappropriate' means depends on what kind of organization or business is and on the security policy that has to be enforced.

Risks

The most recent Klez worm which is still spreading as well as Melissa, Anna Kournikova or Love Letter worms, have crippled email systems and corporate networks in minutes. Those incidents have proven that antivirus software by its own cannot prevent such security breaches. This is caused primarily because antivirus vendors cannot react instantly and develop antidotes and because no user intervention is required to help further spreading.

Unwanted junk mail or spam and unsolicited commercial e-mail can quickly fill up inboxes and be an excessive burden to e-mail resources in addition to waste of

time of cleaning up or 'taking a look' just for fun. Generally, it is not a trivial task to completely stop spam despite attempts to categorize it, keeping track of it or legislate against it. Employees should be informed and discouraged from posting or using their work e-mail addresses for Internet shopping or general use.

Email abuse, when uncontrolled growth of e-mails intended for entertainment is allowed, can result to wasted time and system resources. Just imagine a simple joke as an email attachment which results to a long series of forwards and replies, each bearing a copy of the previous messages, how severely will cut down on an employee's productivity, as well as affecting a group as a whole and how easily will add up to a huge number of wasted working hours.

It is well known that an organization may be held liable for the illegal actions of its employees if they were carried out in the course of their employment. So, if employees send and receive offensive or illegal content, their organization may accept legal charges. In addition, broadcasted emails, which are considered humiliating or harassing, will create a hostile work environment and affect morale. Illegal material such as child pornography, transmitted through email system can lead to litigation, have network assets seized in an investigation, and do damage to reputation. Furthermore, defamation through email is another issue that has to be considered because an affected company can sue the employee who sent the defaming content as well as his or her employer.

Most organizations hold a vast amount of sensitive information in a variety of forms, from paper to electronic records. This sensitive information can be personnel data or customer data varying from shopping habits to criminal records. The unauthorized release of this information could present huge problems, ranging from a loss of reputation to brand damage and even to court actions. Industrial espionage is another serious danger if an employee intentionally discloses by email some confidential material resulting the loss of the competitive advantage and in some cases completely ruining the business.

Countermeasures

A business can protect itself and its employees from all of the risks associated with email by enforcing the right sort of policies and procedures. Firstly, it has to be defined what 'appropriate' content is for the business, characterizing all the rest as 'inappropriate' and secondly to apply email content analysing and filtering controls.

Content filters provide an excellent line of defense, implementing policies translated into rules, by blocking dangerous attachments and inappropriate content. There are some key elements that an email content filtering solution should address to be more effective and reliable. The most important feature is to be able to delve into the file content analysing and understanding the data that an

email can contain. It has to disassemble and recursively break down all the different formats and forms that a message can have, so as not to be possible to be fooled. In this way, reliable attachment control or stripping of specific formats can be safely accomplished, avoiding potential viral code with unknown viruses and disallowing illegal or unnecessary emails entering or leaving the network.

Advanced text analysis is necessary to prevent users from sending sexually explicit text and racial epithets or sensitive information to unauthorized parties. Lexical analysis is one way to cut down leak of confidential information as most of these files include special words or phrases. Furthermore, keyword searching and inspection can substantially reduce spam and unsolicited email. Moreover, advanced image analysis (where image removal is not acceptable in everyday work) is needed in order to prevent pornographic content distribution. These kinds of analysis should be customizable and granular, taking into account false positives, allowing the examination of attachments including those that are compressed (zipped files) or embedded to other attachments or carriers.

Email content filtering is not a panacea without countermeasures to complement its weaknesses and limitations. Any kind of advanced email filtering you may enforce will turn out to be useless if you let employees use Web mail like Hotmail or Yahoo, circumventing the security policy. Steganography, is a new vehicle to bypass the filtering controls because it is very difficult to inspect, trace and determine whether a confidential document is hidden within a picture or movie, for example, or not.

Conclusion

Email content filtering is the most reliable way to enforce e-mail procedures and policies mitigating the risk of employee abuse of e-mail services, breach of confidentiality, virus infection and possible liability resulting from that abuse. If you really want to control what is entering or leaving the corporate network, content security should be enforced in every tunnel to and from the Internet.

* Vasilis Paliouras received the MEng degree in Electrical and Computer Engineering from the Aristotle's University of Thessaloniki in Greece in 1997 and the MSc degree in Information Security from Royal Holloway College, University of London, UK in 1998. Since 2001, he has been working as a Security Analyst for Space Hellas S.A.