

Liberating the inbox: How to make email safe and productive again

With spam levels breaking records every day, the quintessential business tool – email – has simultaneously become a major liability. With inboxes overrun with more and more unwanted email that threatens business productivity, regulatory compliance, and network security, organizations are having to look at what is being mailed in, out and around their network, at the gateway, at the mail server and at the endpoint. This paper focuses on the threat posed by unwanted emails that make it through to the inbox, explains the impact these threats have on organizations, and demonstrates what needs to be done in response to make email safe and productive.

Liberating the inbox:

How to make email safe and productive again

Email in a business

Email today presents a serious risk to security, business productivity, and compliance with government and industry regulations. As the use of email for legitimate business purposes continues to trend upward, so does its use as a tool for unwanted, illegitimate, and occasionally dangerous, business activity.

There are three predominant sources of risk that every organization faces: spam, information leakage, and compliance as it relates to email.

Spam

Spam currently ranks as the third-greatest threat to enterprise security, as Figure 1 shows.

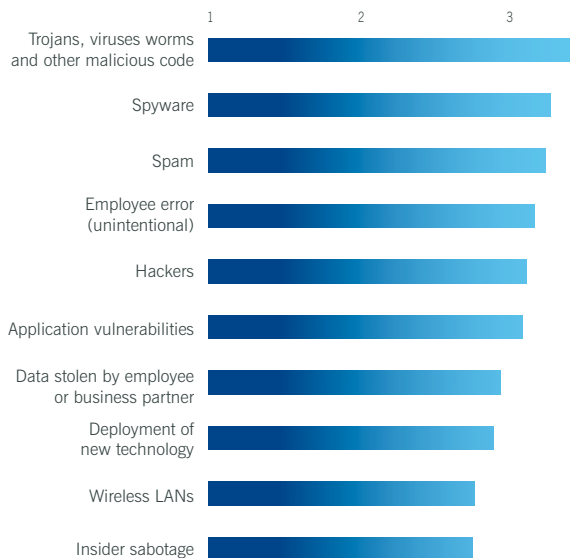


Figure 1: Top ten threats to enterprise security. Source: IDC¹

Professional spammers continue to clog up to 90 percent of unprotected mail stores and inboxes with unwanted emails that soak up bandwidth, upset end users with irritating or offensive content, and negatively impact employee productivity.

More recently, spammers have extended their role from the simply annoying to the outright criminal, using their emails as a beachhead for more malicious activity. As security vendors have become adept at blocking emails containing code which itself has a viral payload, spammers and malicious code writers have found more devious ways – such as the use of images and PDF attachments – to get spyware, zombie-creating Trojans, and other malware on to end-users' desktops.

Cybercriminals are increasingly spamming out emails offering, for example, a plug-in to view videos or pornography or even offering free bogus security applications. The emailed link in reality takes the duped user to an infected website from which a backdoor Trojan is downloaded. When the webpage loads, malware on the website infects the visiting computer, and is then used for a variety of criminal purposes, such as to steal data or to turn the computer into a spam-sending zombie.

Phishing attacks continue to lure unwary users to fake websites where they hand over confidential information, such as bank or credit card details.

The reason spam continues to flourish is because it works. It can take just one person to hand over their money or their financial details – wittingly or by having them stolen – for a campaign to be

successful. The vast amounts of money accrued by spammers who have been arrested and prosecuted is an indication of just how much money can be made, and the handful of cybercriminals who are caught is nothing compared to the huge numbers left undetected to carry on their campaigns.

In today's workplace, the task of blocking the wealth of malicious and productivity-hampering email, while allowing the free flow of legitimate business communication, is one of the biggest challenges IT departments face.

Information leakage

As well as heightening the risk of an organization's network becoming infected with malware, the growth in email has also led to an increased risk of information leakage.

Organizations are facing a growing number of leaks of confidential data, proprietary information, or intellectual property by their employees. As figure 1 shows, data stolen by an employee or a business partner ranks as the seventh-greatest threat to enterprise security and, according to analyst IDC, the most costly incidents are those that are deliberate, malicious action.¹

In today's organizations, most information is stored electronically and most is readily available to employees who can simply send it out of the company in an email. This might be deliberate, but can also be accidental, for example when the

“*Compliance is the state of being in accordance with established guidelines, specifications, or legislation – or being in the process of becoming so.*”

email client auto-completes a recipient name, but the one it finds first is not the one that the user intended.

Compliance

The third major issue for IT departments is that all their security measures must be carried out in the context of both internal acceptable use policies and external government and industry regulations, such as HIPAA and Sarbanes-Oxley.

Now key drivers in raising the issue of compliance, these regulations, which were originally issues of relevance only to large institutions in banking, healthcare and the like, are now of issue to all organizations. Breaching regulations, such as prematurely disclosing financial information ahead of a company's filing date, can be damaging and expensive to an organization.

Compliance is achieved by operating under a formal set of clearly defined guidelines that ensure adherence both to formal legislation and to accepted ethical standards and best practices. As the number of regulations grows, managing the compliance processes manually has become harder and automation is the way ahead.

Email security – a multi-layer issue

In the past, organizations viewed the problems of email almost solely as an inbound threat – spam and email-borne malware causing a nuisance, consuming bandwidth and storage space, and increasingly infecting endpoint computers. As described above, the situation now is much more complex, and the threats posed by email exist throughout the whole email infrastructure. As networks increase in size and complexity and email use grows, more points in the system become vulnerable. Inbound, outbound and

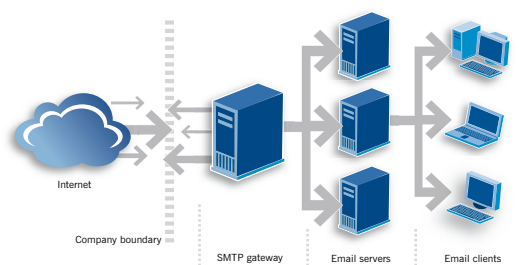


Figure 2: The email infrastructure's multiple vulnerable points

internal messaging are all vulnerable and need to be secured as part of an organization's overall network and data security.

Gateway security – inbound and outbound

The gateway remains the place where email protection “traditionally” sits, providing protection against threats such as spam and phishing attacks, viruses, denial of service attacks and directory harvest attacks. It is also at the gateway that offensive and other inappropriate inbound emails are blocked before they can reach the corporate servers.

Outbound emails containing confidential or sensitive information or emails that flout regulatory or corporate compliance rules can also be effectively stopped here. As a result outbound content monitoring and filtering is an increasingly strategic concern for IT administrators.

“Corporate users send and receive an average of 133 messages per day and this number is expected to reach 160 messages by 2009.”

Groupware security – internal

Internal threats are rapidly climbing the priority list of enterprise security threats and now account for three of the top 10 most serious threats facing corporations today – unintentional employee error, data stolen by an employee or business partner, and insider sabotage in figure 1.¹

The threats associated with inbound and outbound mail – malicious emails, inappropriate content, confidentiality and compliance breaches – all apply at the groupware level, with internal mail servers acting as the conduit for all traffic. In addition, malware can remain dormant in stored email attachments, posing a threat to the wider network long after they enter the organization.

Endpoint security – the last line of defense

An additional, and perennially significant threat, is that of malware entering the organization at the endpoint desktops, laptops, and notebooks via, for example, webmail or a USB memory stick can use the internal mail network to spread. Within the context of the email system, the endpoint is the final line of defense.

Making email safer

While most organizations have experienced dramatic growth in their email infrastructure, many have not seen a corresponding increase in email security – even though email is already the number one source of security threats for organizations.

Email protection has tended to be focused on the gateway, although, as figure 2 shows, there are in reality many points of vulnerability in an email system. This approach, as has been discussed, can leave a network exposed to a host of email-related threats that bypass the gateway defenses. The traditional gateway email hygiene model is, therefore, now incomplete.

The key to making email safer is to secure all the points of vulnerability – protecting all layers and ensuring that the gateway and groupware solutions integrate anti-virus, anti-spyware, anti-phishing and anti-spam protection and also provide the ability to filter email for dangerous, unwanted or confidential content. Maintaining up-to-date endpoint protection is vital to preventing infection via other means, as highlighted above.

At all points, it is essential to provide completely up-to-date, proactive protection against the full range of malware threats. Leading anti-virus and anti-spam engines automatically detect variants of spam campaigns or virus families, providing a more deterministic approach to protection.

There also needs to be a clear and transparent framework for behavior, setting down what is acceptable and what is not when it comes to using email. An explicit, organization-wide Acceptable Use Policy (AUP), accompanied by the ability to audit its use and enforce its rules is a simple first step in demonstrating the intention to meet regulations and goes a long way toward avoiding liability.

As an example, typical clauses might be:

- Don't forward or send email containing pornographic images
- Do limit attachment sizes to 5MB.

Best practice also dictates that intelligent encryption and archiving processes are put in place – the former to prevent eavesdropping by unintended email readers, and the latter to assist with audit and compliance matters such as e-discovery, when an organization is ordered by the court to provide records of email communication. Practices such as retaining log information, copying or archiving sensitive internal and external messages, and being able to intercept and re-route violating messages, give organizations visibility of and access to current and past traffic, and allow them to account for the email coming into, going out of and circulating around their email network.

The threats in email traffic

Inbound

- Spam
- Malware
- Phishing attacks
- Directory harvest
- Denial-of-service attacks
- Bandwidth drain

Outbound

- Information leakage
- Confidentiality breaches
- Regulatory requirements
- Inappropriate use/content,
- Legal disclaimers and branding
- Archiving
- Data encryption

Internal

- Inappropriate usage/content
- Confidentiality breaches, e.g. financial data
- Employee harassment
- Malware from webmail or USB memory sticks

Making email more productive

Just as there needs to be robust security to protect against malware, spam, denial-of-service attacks, directory harvesting, and so on, so there need to be capabilities in any solution that will let administrators enforce content filtering management and information leakage prevention policies. For example, security solutions should be able to automatically monitor email communications for keywords, strings such as Social Security numbers, and file types that might contain proprietary information.

There need also to be management features that lower the administrative overhead, giving administrators visibility and reporting capabilities that allow them proper control over the whole email infrastructure. This includes the ability to trace messages as they flow through the email infrastructure, and the ability to generate traffic and threat reports quickly and easily in order to paint a clear picture of what is passing through. This is particularly important in response to inquiries from senior management.

Summary

Since email is a mission-critical business tool, organizations have no choice about learning to

cope with its related security challenges, both external and internal. There are ways to make this easier in terms of impact on users, security administrators, and the organization as a whole. It IS possible to regain control of inboxes despite the changing nature of malware and spam, and it IS possible to do this efficiently. Approaching email from the point of view of the infrastructure will help identify where best to put in place checks and balances. For example, archiving is best left to the groupware level, because it is here that internal as well as inbound and outbound mail can be captured. Following the four basic principles for making email safe and productive – maintaining proactive, up-to-date protection against malware, phishing and spam, implementing an AUP, creating archiving and reporting processes, and monitoring and filtering content – will in the long run ensure an organization's system, and its users' inboxes, are freed from the tyranny of malware and spam.

The Sophos solution

Sophos Email Security and Control enables complete security and content management across the entire email infrastructure – from the gateway to the groupware server – eliminating known and unknown threats including spam, phishing and viruses other malware, and preventing information leakage and compliance violations. It enables safe, productive internal and external email communication with minimal administrative and end-user effort. It works with Sophos Endpoint Security and Control and Sophos Web Security and Control to provide consolidated protection across the email infrastructure and good compliance practices.

In addition, Sophos ZombieAlert™ Service can help organizations identify systems on their networks that have been infected and are sending spam. Sophos PhishAlert™ Service provides organizations with early awareness of phishing attacks that hijack their brand or identity.

Sources

- 1 Worldwide information protection and control (IPC) 2007-2011 forecast and analysis: securing the world's new currency., Doc #206750, May 2007. Brian E Burke, Rose Ryan. IDC.
- 2 Radicati Group, 2005

About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA, and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM