Volume : 3 | Issue : 3 | March 2014 • ISSN No 2277 - 8160

Research Paper

Computer Science

A Preventive Measure to Secure Your Email on Cloud

Ms.Komal saxena Asst. Professor

Mr. Anjan Saxena Senior Software Engineer, Tele Apps

ABSTRACT

Email is the basic communication tool being used today. Be it in home or in an organisation. It is more prevalent in the workplace. The reasons for its evolvement as a communication tool are its sheer speed and cost effectiveness. With internet access and so heavy email usage in modern business practices, the security implications are bigger than ever. With this comes the ease of giving attention to data protection and storage laws. It is the responsibility of an organisation to provide security to the sensitive data in email from various customers, suppliers and staff. It is important to ensure that inbound, outbound and stored email is kept safe and secure. [1] Email security threat does not discriminate between the type of organisation.[2] Organisation need to make sure that they are armed with the best security solutions available. The Widespread use of email has provided hackers and crackers with an easy way to distribute the harmful contents to the internal network.[3] There various email threats that can hamper a network like information leakage, malware attack, phishing etc. There are various different approaches that can be taken to ensure email security. These approaches include placement of security on-site within the confines of the business network or move the security off-site completely. In this paper, we are going to talk about how email security can be improved by incorporating cloud based solutions.

KEYWORDS : Email Security, Email threats, cloud solution, spyware, malware, and virus

1. INTRODUCTION

With the advent of technology, the messaging environment is getting more complex day by day. An organization is being swamped with the unwanted email, malicious code, spyware, employee breaches of confidence, and so many removable media devices entering and exiting the boundary of an organization. Organization requires a way to lock and secure their communication system from all these threat. Managing Email security is an excellent way for an enterprise to re-establish control over their environment.[4]

It is getting difficult for enterprises to stay one step ahead of new attacks, new complexities, new regulations, and new demands on their systems. Email systems are the centre of the electronic threats being introduced in an enterprise network. Apart from virus, spam and spyware being brought through email, releasing of confidential information through email has being increasing. New regulations, while not focusing specifically on email systems, increasingly impact decisions on email and email policies. This requires enterprises to secure and harden their email systems as much as possible[4]

2. Threats to Email System

2.1 Information Leakage

With the widespread usage of email as communication tool within an organization, there is a great risk of crucial data being stolen from within the organization. Email contains sensitive data of an organization that can be stolen and used illegally. [3]

Employee use email to share sensitive data was officially intended to remain within the organisation. Various studies have been done and shown that how employee used email to send out confidential corporate information. Employee indulge in these illegal activity because of being disgruntled and revengeful or they fail to realize the the potentially harmful impact of such a practice and its harm to the organisation.[3]

2.2 Attachment of Malicious and offensive Content

Email is being sent by staff containing offensive material like racist, sexist etc that can make an organization vulnerable from a legal point of view. There has been various laws being made against these type of practice. For example, under British Law, employers are held responsible for emails written by employees in the course of their employment, whether or not the employer consented to the mail.[3]

Emails are also being sent with malicious attachments. These attachments are generally the viruses. Melissa and LoveLetter were among the first viruses to illustrate the problem with email attachments and trust. They made use of the trust that exists between friends and colleagues. [3]

Email is also triggered with known exploits that uses the flaw in software to disseminate the virus. Nimda worm was one of the virus that took the internet by surprise, circumventing many email security tools and breaking into servers and corporate networks. It took the advantage of flaw in Internet Explorer and Outlook Express by running automatically on computers having a vulnerable version of Internet Explorer and Outlook Express.

Emails are made vulnerable to attack by embedding scripts into an HTML mail. Virus based HTML scripts run automatically when the malicious mail is opened. They do not rely on attachments; therefore, the attachment filters found antivirus software are useless against providing security.[3]

2.3Not enough security by Antivirus Software and Firewall[3]

Installing a firewall is a wise step by an organization in order to protect their intranet, but is not enough. Organization gets false sense of security upon installing a firewall. Firewalls can prevent an unauthorised user to access the network but does not check the content of mail being sent and received by those authorised to use the system. Email systems can easily surpass this level of security.

Same as firewall, antivirus software are not enough for providing efficient secure email management. Antivirus software cannot protect against all email viruses and attacks. It is difficult for the antivirus vendors to update their signature in time against the deadly viruses that are distributed via email in a matter of hours.

2.4Growing use of Social Media

Social networking tools are exploding in popularity and hence are leading to active targeting. In a report by Websense, it reported that 10% of links posted on Facebook are either spam or malicious. One of the fundamental problems with social media is that organizations allow the use of social media, often doing nothing to protect the organization from its threats than considering it to be legitimate for use in their organization.[5]

3 EMAIL SECURITY SOLUTIONS

3.1 Email Security Checklist[2]

For an email secure infrastructure, there is a need to select a solution that meets the security needs of today and tomorrow. For this you need to manage an email security checklist. Whatever solution is choosen, it is required to check for this following security components an email security solution should address.

1. Spam Filtering: Inbound and outbound attacks can be stopped

with minimum 99% of effectiveness.

2. Antivirus Protection: Choosing an antivirus that deliver stellar defence against viruses, Trojans, spyware and other malicious threats.
3. Global Attachment Filtering: Built-in and customizable support for filtering varied attachment types
4. Global Disclaimers: Easy creation of rules for global disclaimers for outbound emails.
5. Rapid Deployment: Solution should be able to be up and run instantly, delivering immediate results.
6. System Compatibility: Solution should be easily integerated with any email infrastructure and/ or operating system.

3.2 A proactive approach to solution

A proactive approach towards email security management involves the content checking of all inbound and outbound email at server level, before distribution to your users. Using this way, all potential harmful content is removed fro an infected or dubious email , and only then it is forwarded to the user.

By installing a comprehensive email content checking and antivirus gateway on their mail server, companies can protect themselves against the potential damage and lost work time that the current and future viruses may cause.[3]

3.3 On-Premise email security solution

There are various on-premise solution available that helps in effective email security management. Hosting your own email server inside the business is still the most popular way of maintaining email services in the workplace. Most common on-premise email hosting solution being used is in the form of an on-site email server, either in form of an integrated small business server package or as a standalone server solution, such as Microsoft Exchange.[1]

3.4 Cloud based email security solution

With more organization moving their email to the cloud, or simply wishing to keep their email security at arm's length where a third-party specialist can maintain and update the solution, the cloud-based email security service is growing in popularity.

Cloud-based email security works as a buffer between the mail server and the wider Internet. All inbound and outbound email is received at the security service before being passed to the mail server, whether that server is also in the same cloud, a different cloud, or even back on the premises. Doing this ensures that the content is virus-free and confirms with content policy before it is released for sending or for downloading to a client PC.[1]

4. CONCLUSION

There are many advantages to cloud-based solutions, especially for small or medium-sized organization where IT resources are limited. Cloud-based solutions are faster and less expensive to implement as no new infrastructure is required. Bandwidth can be saved, since spam and malware are blocked in the cloud. It provides a unique combination of zero-hour, virtualization-based, and traditional signature-bases antivirus engines. It provides email continuity as email can be continued to send and receive even if the email server is down. With so many benefits in the short and long term for the organizations, cloud-based solutions are effective solutions for email security management.

REFERENCES

[1] Email security: Hosted or on-premise? Choosing the correct option(s);GFI White Paper | [2] Email Security: The performance, protection and choice SMBs deserve; GFI White Paper | [3] Protecting your network against email threats; GFI White Paper | [4] Meeting Email Security Head On: Dell Secure Exchange Services | [5] Messaging and Web Security Best Practices for 2011 and Beyond. An Osterman Research White Paper |