Email Filtering and Anti-Spam Software – The Way Forward

Contents

Today's IT services

The last 20 years have seen a large growth in outsourcing of IT services by corporations. Outsourcing IT services allows the business to focus on its core business. Areas such as Email, Database Management and System Administration are examples of IT services that may be outsourced.

The fastest growing area in recent years has become cloud based services. Cloud based services have been around for some time. Early forms of cloud based services include Yahoo and Gmail Email accounts, both being Web-based Email applications running in the cloud.

Cloud services have evolved and have become increasingly sophisticated. One particular example is Software as a Service (SaaS). SaaS has been made possible by virtualisation of servers, combined with high network throughput. This has meant a change in the IT services market.

The growth of cloud services is not without issues. For example, Amazon Web Services allows a user to create cloud services (including virtual servers) for free, provided usage does not exceed a threshold each month. The free services can be a boon for small businesses that only need a service for a short period of time. However, there is a downside. The cloud based services are open to abuse; indeed, Amazon Web Services was recently reported to have the highest percentage of malware hosting virtual servers[1].

Malware – an Evolving Threat

Malware is short for Malicious Software. It is designed for many purposes; the most common is to hijack a computer in order to obtain user information, such as login names and passwords. Other forms of Malware are Ransomware, Trojans, Computer Viruses and Worms. Malware is often spread via Email attachments.

The problem with Malware is that it too is becoming more evolved. A recent Malware called PoweLiks appears to have been around since 2012; however, it was first identified in 2014[2]. The Poweliks malware is particularly clever, as it resides in the system registry and can survive reboots.

Another recent form of malware known as "Backoff" can infect Point of Sale terminals. Backoff can collect credit/debit cards numbers and transfer the details to criminals for use. At the time of writing Backoff has compromised 1000 businesses in the United States[3].

Phishing

Phishing uses various means to attempt to steal user login identities and passwords. The methods used vary, but in general an Email crafted to look like it is from an organisation (banks are a favourite) is sent to a user. The Email may either contain a link to a bogus site, or it may contain an attachment that may either be malware, or contains malware.

[1] http://www.spamfighter.com/News-19098-Amazon-Top-Malware-Hosting-ISP-Solutionary.htm
[2] https://blog.gdatasoftware.com/blog/article/poweliks-the-persistent-malware-without-a-file.html
[3] http://arstechnica.com/security/2014/08/point-of-sale-malware-has-now-infected-over-1000-companies-in-us/

There is an indication that phishing attempts are becoming more sophisticated. One example of this is a scam recently reported by Help Net Security. The technique used was to send an SMS to Android phone users, warning them that their device had a virus. The SMS was crafted to look like it was from Kaspersky Labs.

The Email contained an attachment, which the Email text informed the user would resolve the virus issue. However, the attachment in fact was a piece of malware called SandroRAT[4]. SandroRAT is a much evolved form of malware that is capable of updating itself. It can also download other malware. Worse, it can intercept incoming calls.

Defence against phishing has in the past relied heavily on AV solutions. Whilst this is still an effective method (and should be considered as part of a defence in depth strategy[5]) it must be remembered that new threats often take time for the AV vendors to catch up with. The problems faced by AV vendors are that they must first analyse the threat, and then devise a solution and test the solution. This takes times.

Malware Propagation

The spread of Malware via Email cannot be trivialised. Nor is it easy to defend against threats by means of staff training. As an example, a user may receive training to identify Email borne threats. This works out well most of the time. However, a scenario outlined below shows how easy it is even for an employee trained to recognise the threat to open a Malware infected Email.

Scenario

A user receives an Email containing malware. Whilst they open that Email, they also have another genuine Email open. The user flicks between screens. The genuine Email also has a link. Whilst flicking between screens, the phone rings. Distracted, the user accidentally clicks the wrong Email link. This may mean (in some cases) that the business network now is infested with a worm, or the user's machine has a key logger installed.

When the above scenario is considered from a business perspective, there are several possibilities. One is that the user's PC is the only PC infected. This may be easy to resolve, however, it may mean that the user's PC has to be rebuilt from a backup. This could mean the user can't work for one day.

A second possibility is that a server becomes infected. Impact may vary from just one or two users to a company-wide outage. In addition to the lost time spent restoring the server, other aspects may come into play, including damage to the company brand.

Threats are Widespread and Increasing

The level of threats spread by Emails is growing.

[4] http://www.net-security.org/malware_news.php?id=2830

[5] Defence in depth is a defence strategy consisting of layered defences against threats. An example might be to have Email filtering as the first line of defence, anti-virus as the second line.

Spam remains an issue. It is estimated that around 70-97% of all Email is spam. A proportion of spam is likely to contain Email borne threats.

The Australian Competition and Consumer Commission (ACCC) released its yearly report in June 2014[6]. Below are some of the findings.

1. 91,000 Australians victimized in scams during 2013 with 14% of these victims suffering financial losses of more than AU$89 million.

2. 40% of the 91,000 were hit via Internet and Email scams.

3. Phishing Scams and Identify Theft have risen by 73% in a single year striking more than 15,000 Australians in the year 2013.

4. Annual scams report of 2013 showed dating and romance scams moved to number one position in terms of financial losses amounting to $25,247,418.

The ACCC report indicates that Phishing, Spam, and other Email attacks are on the rise. The statistics quoted in the report show that Email borne attacks represent a significant potential cost to your business.

Traditional Security

Traditional security against Email threats involves using Antivirus programs. These programs utilise a Database of threats, and will scan Emails on arrival to check that they do not contain any malware.

This model is still a perfectly acceptable model; however, it should form a part of the defence against Email threats. The main defence should be to prevent the Emails from arriving in the user's Inbox to in the first place.

Email threats can take substantial amount of time for IT staff to resolve. A new virus outbreak means that patches have to be downloaded to Email servers, and potentially to end user PCs, laptops and other mobile devices. Further, patches may not be immediately available. This may mean that some servers inadvertently become infected with malware and have to be rebuilt. The cost of removing or rebuilding servers that have become infected with Malware is high.

The threats from malware are increasing. One way to prevent them is to construct a "defence in depth" strategy. In this type of strategy, the Antivirus software is one part of the defence. The main part of the defence occurs before the Email is even delivered to the user's Inbox, and comprises an Email filtering solution.

Domain Blocking

Domain blocking is a method of defence. In this method, the filter checks the domain of the Email against a domain blacklist. This can be an effective anti-spam measure. A drawback is

[6] http://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2013

that it does rely on the domain name being added in time to the blacklist. As domain names are often added quickly and taken down just as quickly, it is not always effective.

Recent research by Blue Coat indicates that 470 million sites exist for 24 hours. Of these sites, 22% are malicious[7]. This makes the job of keeping track of malicious domains difficult, if not impossible.

Email Filtering

Email Filtering is the scanning of Email to identify threats and to filter out spam. Email filtering is a necessary Anti-Spam measure. Email Filtering can work on a few different layers. AV software does some filtering in order to block out known Email threats.

More sophisticated methods of Email filtering use various analytics to determine whether an Email is valid or is likely to contain malware. Bayes filtering is one method used. Other methods include Whitelists and Blacklists.

MailShark

Small businesses may not have the budget for dedicated IT staff, or they may have a small number of IT staff, who may not have the time to be "fighting fires". The benefit that **MailShark** offers is that Business Owners or IT personnel do not have to maintain the security of Inbound and Outbound Email to their Email servers.

Further to this, Email servers can cost money to ensure that patching is up to date for the latest Email borne threats. Email threats frequently wreak havoc before patches are released.

How MailShark Works

MailShark uses the best Email filtering techniques available today. MailShark also provides an easy to use Web-based interface that provides a complete view of Email.

Some of the techniques used by MailShark are Whitelists & Blacklists, RBL lookups, Message Content Filtering, Bayes Filtering, Checksums and Optical Character Recognition.

When an Email is sent to a user, it first goes to **MailShark**. **MailShark** then checks the Email before forwarding it to the user's mail server. This process is shown in Figure 1.

[7] http://www.net-security.org/secworld.php?id=17297

Figure 1

Messages flagged as spam will be quarantined. Quarantine Reports are generated periodically and a web interface is available for users to check for quarantined messages. Management of Whitelists and Blacklists is also done via the web interface.

Benefits of MailShark

Using MailShark can bring a number of benefits to an organisation. The main beneficiaries are the business itself, IT personnel and the end users.

Lower Costs

Business benefits by lower overall costs. Depending on the solution, these costs may be simply from not having Email outages caused by Malware. If the business moves to a 100% cloud based Email service, then the cost of maintaining servers and licenses is reduced. Conversely, if the business continues to use in-house Email servers, there are still likely to be savings due to reduced Email outages.

Overall, the benefits of moving to a Cloud based, Anti-Spam Email Filtering solution are cost-effective in the long term. Even if the business does use a hybrid model where Anti-Virus is deployed on local servers, there are still benefits. This type of defence in depth strategy can ensure the safety of a business.

Less Time Wasted

IT personnel can be freed up from having to resolve issues caused by malware propagation. The end users are less likely to experience Email issues, and therefore can be more productive.

Technical Support

MailShark has highly skilled technical support available 24/7. The majority of the support team are from mission critical, enterprise environment work backgrounds. They understand the need to resolve critical issues quickly.

Other Benefits

MailShark Safeguards your business if your local MS Exchange or SMTP Mail Server is down or offline.

All Emails passing through **MailShark** are stored for up to 90 days to ensure no loss of business Emails occur.

Once your MS Exchange or SMTP Email Server is back online, **MailShark** delivers your Emails to your server automatically - no user intervention required.

MailShark also provides Port redirection. If your ISP blocks port 25 or you wish to avoid Denial of Service attacks to your mail server, **MailShark** will accept your Inbound Email and re-direct it to your server listening on another port (other than port 25).

Contact Us

MailShark Corporation

Suite 2-3, 262 Macquarie Street Liverpool NSW 2170

PO Box 357

Hoxton Park, NSW 2171

Web: http://www.mailshark.com.au/

Email: info@mailshark.com.au