WHITE PAPER

Ensuring Email Security

The benefits of using a perimeter-based managed service

720.895.5700 : INFO@MXLOGIC.COM : WWW.MXLOGIC.COM

Executive Overview

With unsolicited email costing businesses millions in wasted employee resources and productivity, and acting as the carrier for a host of potential security woes, spam and blended email threats are among the biggest problems facing enterprises today. Not only have spam and viruses taken their toll on business networks, but fraud and phishing scams, designed to hijack financial and personal consumer information from the Internet, have become so prevalent and damaging that government regulations now require financial and healthcare industries to integrate high levels of online security to protect transactions and keep confidential information secure. And, the growing concern to keep business email safe is putting extreme pressure on IT managers and business leaders to seek out and implement email defense solutions that are effective and economical.

There are hundreds of anti-spam and anti-virus companies in the market selling products and services designed to defend against unwanted email – solutions in the form of software, appliances and managed services. Managed filtering services, along with being convenient and economical, are also extremely effective in keeping threats outside the network. Most managed email defense services are designed to block email threats before they can harm the internal network – filtering email outside the enterprise network and removing or blocking viruses, spam, and unwanted content before they can pass through the enterprise firewall and harm the internal messaging system and network.

While there are some who still express concerns around the security and confidentiality of email traffic being filtered by a managed service provider, more and more organizations are turning to these providers for network protection. In fact, all types of enterprises use managed services to filter email, from the Fortune 500 to small, five to ten person companies.

This white paper will review the fundamentals of email security, including filtering methods, and demonstrate how businesses can increase network security using a managed service specifically designed to filter email threats at the network perimeter.

All types of enterprises use managed services to filter email, from the Fortune 500 to small, five to ten person companies.

This white paper will review the fundamentals of email security, including filtering methods, and demonstrate how businesses can increase network security using a managed service specifically designed to filter email threats at the network perimeter.

Email: The Basics

While it is one of the Internet's oldest applications and has become the foundation of the majority of today's business communications, most users don't understand the fundamentals of email. Virtually all email account holders know how to send, open, receive, and reply to messages, but few really understand the journey an email message must take before it reaches its final destination, which is likely why so few people understand the potential risks involved in communicating via email. In order to gain insight into the security of email filtering solutions, it's important to review how email travels through the Internet.

Fundamentally, sending an email message is like sending a postcard through regular U.S. mail.

Sending email

Fundamentally, sending an email message is like sending a postcard through regular U.S. mail. An email message, like a postcard, must first be composed using a Mail User Agent (MUA) like Microsoft® Outlook. The MUA will then send the email via a Message Transfer Agent (MTA) like Microsoft® Exchange - a program that usually resides on email servers and transfers email messages between other MTAs. All MTAs rely on the Simple Mail Transport Protocol (SMTP). The SMTP, as a protocol, provides the rules that enable email servers to locate each other across the Internet, and then transmit messages between them.

Sorting the email

In the same way that postal mail is sorted first by ZIP code, email messages are sorted by domain. Each domain name maps to a unique Web address, called an Internet Protocol (IP) address, which is a string of numbers that servers use to route messages. These relationships are stored in the Domain Name Registry. When the SMTP server receives a message, it compares the domain to the registry to determine what IP address to send the message to. Once it determines the proper server, the SMTP server sends the email message on its way.

Delivering the email

Depending on the location of the destination server, the original SMTP server may not actually make the final delivery – often with messages being handed off several times to other servers along the way. The originating server identifies the domain and passes the message to another server. This process is repeated until the correct server is finally reached. The server that finally receives the email is generally a post office protocol (POP) server. Once a message reaches

the appropriate domain server, it is funneled into the correct POP account and stored until the user logs in and checks for mail. At this time, the email program connects to the ISP's POP server and retrieves the email in the account. The entire journey, with its numerous hops and alternative routes, may take only a matter of seconds.

Email Vulnerability and Security

From a security standpoint, a postcard can be read by anyone on its way through the postal system before its delivery to the intended recipient. Whether the postcard is read by a postal worker, someone receiving it by accident, or someone who has intercepted the mail, the act requires considerable effort and criminal intent. And, if someone were trying to read a specific postcard, they would have to search through millions or even billions of pieces of mail to find it.

An email message is very similar to the traditional, open-faced postcard. On its journey from sender to recipient, email traverses the public Internet and can be read by anyone who has the right technology and messaging knowledge – and who knows exactly what email messages they are seeking.

Interception is possible

With SMTP, an open-recipient based protocol, the receiving MTA has no choice but to accept all email sent to it. Because the SMTP looks for the easiest delivery path, emails are subject to queuing on unknown MTAs – traveling on unspecified routes to their final destination with interception possible at any point along the way.

It is the inherent vulnerability of SMTP gateways that makes networks so susceptible to email-borne threats. With this process, all SMTP-compliant emails, malicious or not, are generally guaranteed to be accepted, unless protective measures have been put in place.

Protection at the network

With 578 million email users in the world, network security organizations are developing solutions to keep business networks protected from the insecurity of email. Today, there are three main ways to deploy email security inside an enterprise. A business can purchase software and install it on its servers or desktops, buy an appliance and install it at the network, or integrate a managed service at the network perimeter and route all email through it. The managed

It is the inherent vulnerability of SMTP gateways that makes networks so susceptible to email-borne threats.

service is becoming the most viable solution, especially with the shifting tactics used by spammers. Because it intervenes directly in the constant flow of email traffic, a managed service can filter out email-borne threats before they reach the business network.

There is, however, a means of combining a number of these solutions into one coordinated spam-fighting solution controlled by a single interface. Only as a managed service can multiple spam control solutions be incorporated into a unified spam control system using a single interface. MX Logic® has created exactly this sort of solution in its Stacked Classification Framework®.

Optimal managed services work without a business having to make any infrastructure changes.

Managed Services: Protecting the Network

Most managed services are built around perimeter protection – filtering email outside the enterprise network and removing or blocking viruses, spam, and unwanted content before they can pass through the enterprise firewall and harm a business' internal messaging system and network.

MX record redirection

Optimal managed services work without a business having to make any infrastructure changes. Most managed service providers require that the business customer simply redirect its MX record to their servers. MX records are entries in a domain name database that identify the mail server responsible for handling email for that domain. In other words, the MX record is like an organization's primary postal address, to which all of its mail is sent. All email would then flow into the managed service's servers and be scanned and filtered before being sent on, or quarantined according to set policies.

Using the same MX record redirection, some managed email defense providers also have the capability to complete outbound filtering to ensure that email messages being sent from the corporate network are appropriate and free of viruses and worms.

Quarantining is possible

With MX Logic's managed service, customers can choose to have any messages, which are identified as spam or infected with viruses, stored in a safe, external quarantine area, accessible only by messaging administrators. A managed service that provides the option to quarantine suspect messages

helps businesses reduce network bandwidth utilization and unnecessary storage capacity by maintaining the quarantine outside the business network.

For the majority of small and medium-sized businesses, adopting a managed service solution offers the easiest, most cost-effective protection when compared to installing and maintaining software and appliance products directly on their own servers or desktops. In addition, the centralized nature of a managed service supports real-time systems updates, which allows for more rapid protection against new forms of spam, viruses and worms.

Proxy-based Filtering Reduces Risk

Managed email protection and security service companies leverage two methods for filtering email: the 'proxy-based' method and the 'store-and-forward' method. While both methods utilize the domain's MX record for filtering, they differ greatly with respect to email delivery performance, domain-level vulnerability, and network security. In general, the proxy-based method does not disturb the normal flow of email nor increase the risk of message loss, while the store-and-forward method does alter the normal flow of email and increase the level of risk.

The proxy-based method does not disturb the normal flow of email nor increase the risk of message loss.

Real-time message filtering

Typically, the proxy-based method only results in sub-second message latency because it does not accept and store the messages in order to filter them. Instead, this proxy filtering process acts as a conduit between the email sender and recipient – filtering the message in-stream, real-time as it passes from the sender to the recipient. Because messages are never stored during the in-line filtering process, emails filtered using this method experience sub-second delivery – avoiding the latency issues from high-traffic and overburdened queues commonly experienced with the store-and-forward method.

No risk of delivery failure

The proxy-based filtering approach removes the risk of delivery failure due to 'network islanding.' Network islanding is the term used when the destination server identifies a message as undeliverable and the message becomes stranded between the originating server and its destination. Unlike the store-and-forward method, proxy-based filtering removes this risk by never accepting responsibility for the delivery of legitimate message traffic. If disaster strikes at the destination message server, the email will bounce back to the sender normally as mandated by the SMTP and delivered when the receiving email server is back online.

MX Logic: Our Managed Service

It should now be evident that, although email is inherently vulnerable to risk, using a managed email defense service is the key to strengthening network security. In fact, MX Logic's managed Email Defense Service was designed to provide comprehensive filtering and security while still ensuring its customers retain complete control over their email. On average, a single email experiences 7 to 10 hops, the number of routers through which it is sent, as it travels from sender to recipient. MX Logic is just one more hop in the journey. But adding this extra hop introduces no additional insecurity to the process of sending or receiving email. In fact, while MX Logic acts like any other router in the transmission process, it actually adds layers of security to the email.

Employing a managed service to filter email typically requires nothing more complex than an MX record redirection.

A secure MX record

As described earlier, employing a managed service to filter email typically requires nothing more complex than an MX record redirection. This holds true for businesses using MX Logic's managed Email Defense Service. To benefit from perimeter-based filtering, the corporate MX record must be changed so that a client's email is routed through MX Logic's filters before entering the business network.

By redirecting its MX record to point to MX Logic only, an organization adds additional security to its internal network because now all email and email-borne threats are directed to MX Logic first. By 'delisting' or hiding its MX record from the public Internet, less information is available about the company, its corporate network, and its employees – resulting in the significantly reduced potential for email infiltration by spammers and hackers.

The business is ultimately in control

When MX Logic is an organization's sole MX record, unsolicited email cannot be sent directly to that company or that company's employees. Additionally, using a unique MX Record masking technique, MX Logic offers added protection from denial of service attacks, directory and dictionary harvest attacks, mail bombs, and channel flooding.

Remember, however, that MX Logic never controls a customer's MX record – that's entirely up to the client organization. At any time, an organization can remove MX Logic as the primary MX record and switch back to its own.

MX Logic: A Secure Architecture

With more background about the managed service and MX Logic's perimeter-based filtering, some may question the security of email as it travels through the filtering process. Recognizing this as a legitimate business concern, MX Logic architected its email defense solutions to make unauthorized email viewing or alteration virtually impossible – even for MX Logic.

Proxy-based filtering streams the messages

Earlier, proxy-based filtering was described as the optimum filtering process and is used by leading managed service providers. MX Logic is one provider that is committed to increasing security and privacy by employing the proxy-based, real-time filtering method. With this method, MX Logic neither stores nor acknowledges receipt of an email message. Instead, MX Logic acts as a proxy, recognizing inbound email traffic with the SMTP and immediately opening a connection to the customer's email server. Messages are then passed through MX Logic's automated filtering layers as they are streamed into the enterprise.

MX Logic scans and filters most emails in a matter of milliseconds - providing additional assurance that email never resides on its servers long enough to be read. The only time MX Logic stores messages on behalf of its clients is when they have configured their filtering policies so that messages containing viruses, spam, or unwanted content are quarantined. Those suspect messages, however, are safely segmented with message headers stored separately from the text of the message. With this tactic, even if a particular header were somehow accessed, it would be exceptionally difficult to locate the corresponding body text of that message.

Store-and-forward has risks

Other managed service providers that use a store-and-forward architecture first accept email, store it on their servers, scan it, and finally send it on. If those providers ever experience outages, the messages they are storing will be lost. But because MX Logic never stores legitimate messages, if it were to experience an outage or failure all messages being sent through MX Logic simply "return" to the sending MTA to be resent at a later time. Or, if the client maintains a secondary MX record, email would be routed directly to the secondary domain.

MX Logic code of conduct

MX Logic employees do not have access to any client email. In fact, its operations employees have defined roles that limit any single individuals'

Because MX Logic never stores legitimate messages, if it were to experience an outage or failure all messages being sent through MX Logic simply "return" to the sending MTA to be resent at a later time.

access to all components of the Email Defense Service. MX Logic's Terms and Conditions specifically state that "Email messages are processed electronically, and are not reviewed by [MX Logic's] personnel. The Company recognizes that user-specific information and the content of the emails sent to or from [the enterprise] shall be deemed confidential information." In other words, our team will not read, alter, copy, redistribute, or otherwise interfere with or observe a client's email, unless requested to do so.

With MX Logic's service, now small businesses can afford the best protection.

Around-the-clock threat monitoring and protection

Most organizations, with the exception of large enterprise organizations, do not have a dedicated team of email threat specialists who monitor the global state of email around-the-clock and provide updates in real time. With MX Logic's service, however, even small businesses can afford the best protection. The MX Logic Threat Center is a sophisticated streaming data environment that monitors the global state of email for spam, viruses, worms and other email threats 24 hours a day, seven days a week.

Our Threat Center employs a dynamic defense by continuously incorporating information from its sensor network into its database and rewriting and updating its filtering rules to protect against the latest threats. In addition, with the managed service, MX Logic customers can choose to integrate a disaster recovery feature, which protects a business from message loss in the event of a customer network outage. This support, coupled with MX Logic's threat communication process that provides early notification of destructive email to the business community, is a feature unmatched by most on-premise solutions.

Industry-leading processing centers and availability

By utilizing leading technology and redundant message processing centers, MX Logic provides 99.99 percent service availability, although historically MX Logic's network availability has been 100 percent – levels expected from an industry leader. Our data centers provide immediate disaster recovery and high availability, and the MX Logic Network Operations Center (NOC) provides 24x7x365 operational support and automated monitoring of all service components.

Internal passwords are changed often, access to servers is highly restricted and open only to authorized personnel, firewalls restrict IP access, and all message traffic is load-balanced to ensure optimum message throughput. Our production facilities provide for carrier-grade infrastructure and our architecture design lends itself to a low-cost and highly distributed "pod" environment. Network and application monitoring provides remote operations personnel visibility into suspect or trouble alerts and alarms. Servers running MX Logic's Email Defense Service are inaccessible via the public Internet. Overall, ours is a redundant, diverse, and secure service.

Messaging Security Experts

Since the early 1990s, the founders of MX Logic have been committed to finding solutions that minimize the increasing risks associated with email and increase the security and privacy of messaging as a whole. In fact, these industry experts introduced the first web-based email service to the Internet in 1995 and in 1996 released the first commercial-managed messaging service, which they grew to over 30 million customers supporting 60 million messages a day. They established MX Logic in April 2002 and later that year launched its flagship Email Defense Service, designed to protect businesses of all sizes against email attacks including spam, viruses, worms, unwanted content and email flooding.

MX Logic's focus on innovation led to the launch of several industry-firsts, including being the first managed service provider to leverage Bayesian Statistical Classification, provide spam beacon blocking, offer quarantine management via email, and provide corporate-level quarantine release reports. With three levels of defense to choose from and around-the-clock protection at every level, businesses, service providers and channel partners can easily and proactively manage email security at the network perimeter.

Email-based threats are innumerable and constant: spamming continues unabated, new computer viruses are constantly released, and each workday brings new waves of emails with unwanted content and attachments.

Summary

The Internet is, by definition, a global network connecting millions of computers with more than 100 countries linked into exchanges of data, news and opinions. Its structure and design is intended for public use – making secure and private electronic messaging nearly impossible. Internet service providers, and the many routers through which email passes en route to its destination, create any number of opportunities for exposure and risk.

Using MX Logic's services, an organization's email traffic experiences one additional hop on the Internet journey. Flowing through this additional router, however, does not pose increased security risks to email. In fact, with MX Logic's architecture, the business email network is actually protected by additional layers of security. Businesses can also feel confident that email messages traveling into MX Logic are kept safe and confidential because MX Logic never stores email, unless an organization requests suspect messages (e.g. viruses, spam, etc.) be quarantined. Filtering usually takes less than a second, so messages experience no functional latency and stream too quickly to be read or viewed in the process. And, MX Logic's Email Defense Service enables users to activate, configure, and control the service – an inherent part of fostering business email security.

Email-based threats are innumerable and constant: spamming continues unabated, new computer viruses are constantly released, and each workday brings new waves of emails with unwanted content and attachments. Successfully protecting the business email network requires constant diligence and extensive resources. MX Logic takes on this burden for businesses of all sizes. Businesses can take the pressure off their team by incorporating MX Logic's managed Email Defense Service and allowing MX Logic's key Internet messaging innovators to keep their messaging network safe and secure.

About MX Logic

MX Logic is a leading provider of managed email and Web security services that deliver enterprise-grade performance without enterprise-level complexity and cost. Our easy-to-use, award-winning services reduce risk and liability, lower overall IT costs, and increase productivity. MX Logic services are available through our industry-leading partner network. For more information, visit www.mxlogic.com.

More information:
MX Logic Sales Team
9781 S. Meridian Blvd. Suite 400
Englewood, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com