GFI White Paper

Email security in small and medium-sized businesses

No organization can afford to operate without an email security strategy. The risk landscape is constantly changing with new threats surfacing every day. This white paper looks at email security in small and medium businesses, the solutions available and what features SMBs cannot do without.

GFI®

Contents

Introduction 3

The changing risk landscape 3

Choosing a solution form factor 4

Key features of an SMB email gateway security solution 5

Conclusion 5

About GFI® 6

Introduction

In late 1971, a researcher from Bolt, Beranek and Newman (BBN) named Ray Tomlinson sent a text-based message between two computers sitting side by side in the company's Cambridge, Mass. headquarters. The machines were connected only by the ARPANET, the precursor to the Internet, which BBN built for the US Department of Defense.

This seemingly inconsequential moment changed communications forever – because Tomlinson had just sent the first-ever Internet-based email. Tomlinson developed email on his own, with no expressed need by customers or management. He and his team were simply charged with finding new ways to use the ARPANET, so he created email "because it seemed like a neat idea."

Forty years later, Tomlinson's "neat idea" has supplanted the telephone as the primary form of communication between and within many businesses. But the very qualities that have built email's success among legitimate users – low cost, ubiquity and ease of use – have also made it a powerful tool for criminals. Ask the average worker about email, and they are as likely to mention the "dark side" of email – spam, malware and phishing attacks – as they are the positive side. And ask the average security or compliance officer about email, and they are as likely to complain about outbound email threats – information leakage, compliance violations and legal liability from inappropriate content – as they are about inbound ones.

The security industry has provided large businesses with effective email security solutions for many years. This is due primarily to the heightened sensitivity large businesses have to email risk – particularly publicly traded and regulated ones. Email gateway security solutions have proven to be particularly effective, because they filter inbound and outbound email traffic at the email gateway, thus ensuring that only emails conforming to corporate policy are allowed in and out of the business. Because these solutions remove unwanted email before it reaches the email gateway, they also reduce bandwidth consumption in corporate networks.

Small- and mid-sized businesses (SMBs) historically have been less aggressive toward email security, due to lower perceived risk and a general lack of full-featured solutions suitable to SMB IT budgets and environments. Today, however, SMBs are under a constant assault of spam, viruses and other malware that can cause significant business harm – ranging from impaired productivity to lost business and brand damage. This has heightened the urgency for SMBs to develop effective strategies for email security. Fortunately, there are also email security solutions available today that provide many of the features large businesses have enjoyed for years, while delivering the ease-of-management and affordability required by the SMB market.

The changing risk landscape

News headlines frequently tout the proliferation of email-based spam and malware. Statistics vary depending on the source and state of malicious activity on the Internet, but at any given time anywhere from 60% to 97% of all email traffic is unwelcome. For SMBs, spam and viruses have traditionally been a nuisance and productivity hindrance, so deploying anti-spam and antivirus solutions that could block most of this traffic was "good enough."

More recently, however, the threat landscape has changed. Criminal organizations have evolved from targeting a select number of large businesses to targeting large numbers of businesses of all sizes. SMBs are particularly attractive to them, since they tend to have fewer defenses than their larger cousins. And they are targeting SMBs with a broader array of motivations and tools than ever before, including:

- Traditional spam attacks
- Malware attacks, where emails include malware as file attachments or links to malicious websites
- Phishing attacks, to trick recipients into visiting spoofed websites that request personal identity information or download malware onto the computer
- Spear phishing attacks, which are targeted attacks on specific "high value" people; these attacks are designed either to steal personal identity information or to gain control of their computers so they can be used to penetrate corporate networks

- Directory harvest attacks, where spammers unleash a wave of emails at an organization with common names in the email addresses, in an attempt to identify valid email addresses
- Denial of service attacks, which aim to shut down a company's ability to use email by bombarding email servers with a flood of messages.

The potential damage from these attacks extends beyond traditional "nuisance and productivity impairment." They can also cause more serious problems including data breaches, financial loss, compromised customer information, compliance violations and brand damage.

In many cases, malware is designed to provide criminal organizations with control over the infected computer. They may do this to steal personal identity information, to add the compromised machine to a spam botnet, or to use the computer to gain access to valuable data residing on a corporate network. For an SMB, this data could be in a customer or employee database, or on the networks of partners or customers to which the SMB has access.

Outbound email represents another set of risks for SMBs, including compliance violations, legal liability and general business damage from information leakage and inappropriate email. Many SMBs today do not monitor outbound email, nor do they have acceptable use policies in place, so they are virtually unprotected against these risks.

To combat modern email threats, SMBs need to deploy comprehensive and cost-effective email security solutions that can cleanse both inbound and outbound traffic, to reduce overall risk to the business.

Choosing a solution form factor

As mentioned earlier, comprehensive email gateway security solutions were once only viable for larger businesses, due to their expense, complexity and the risk/reward characteristics of the market. Today, however, there is a broad array of email gateway security solutions available to SMBs in a variety of form factors, including:

- **Software** – This is the traditional way to deploy email security. Software is deployed on-premise on hardware supplied by the SMB. The advantage of software is its configurability, and some businesses value the flexibility to choose their own hardware. However, this is the most management-intensive deployment model since SMB IT personnel must install and maintain the operating system as well as the security software.
- **Appliance** – In this form factor, the vendor provides a sealed appliance that comes preconfigured and optimized to run the email security solution. Appliances are easy to install and maintain, since they often update automatically. They can also provide excellent performance, since the hardware is optimized to run with the security software. They typically impose less management overhead than software, but the SMB must still provide the necessary infrastructure to ensure redundancy and availability.
- **Hosted service** – Also known as the "software as a service" or SaaS model, in this case the email security solution is hosted by a third party and available to the SMB on a subscription basis. The advantage of this model is that all infrastructure requirements – including ensuring redundancy, scalability and high availability – are the responsibility of the provider. Hosted services are ideal for smaller organizations with limited IT staff, because management is minimal and there are no on-premise hardware or software requirements. These solutions tend to be less configurable than software or appliances, and the most attractive aspect of the hosted model – that the solution is hosted and managed by a third party – can also be a drawback for businesses that do not want to have their email pass through a third party.

The optimal form factor will depend on the IT resources and business requirements of the SMB. For a small company with limited IT support, the hosted approach will be very attractive because it imposes the least management overhead. A financial services company, however, will most likely not want to send email to a third party and will want to use the appliance or software approach in order to maintain the entire architecture in-house.

Key features of an SMB email gateway security solution

Most email gateway security solutions will include anti-spam and antivirus engines. However, truly reducing email risk requires a number of additional features that address the full spectrum of threats posed by inbound and outbound email. Key features to consider when evaluating gateway solutions include:

- **Configurability** – Ease of use is important, but it should not come at the expense of configurability. The email security gateway solution should have enough configuration options so SMBs can customize the solution to their specific business requirements.
- **Multiple antivirus engines** – Defense-in-depth strategies were once only available to large businesses. Today, however, SMBs should seek similar capabilities. Because no antivirus engine is perfect, SMBs should adopt email gateway security solutions that use multiple such engines to improve overall anti-virus effectiveness.
- **Email exploit engine** – Antivirus engines block known malware. Email exploit engines block unknown malware. They do this by analyzing suspect code and determining whether or not it has the characteristics of malware. This is a critical capability for SMB email security solutions because it defends against "zero-day threats" – that is, malware that has not been seen before. This type of threat is increasingly common today and cyber criminals often engineer malware to be polymorphic, so it changes structure from machine to machine to evade detection by antivirus engines.
- **Anti-phishing engine** – These engines reveal the true domain names of spoofed websites promoted in phishing emails. This decreases the likelihood of the user falling prey to a phishing attack.
- **Intelligent spam filtering** – Anti-spam vendors are notorious for publicizing inflated effectiveness rates. For SMBs, it is important to focus not just on detection rates, but also on the corresponding false positive rate. These rates have a direct correlation – the higher the detection rate, the higher the false positive rate, and vice versa. Since a single false positive can be far more damaging than allowing multiple spam messages to enter the network, it is important to be able to configure the spam filter so it strikes the right balance to protect the business, while enabling fluid communication. The anti-spam engine should also be able to "learn" from user behavior so it does not impede the flow of business communication. For example, "Vicodin" and other painkillers are common in spam solicitations, but in health care organizations they are also the topic of legitimate email correspondence. A good anti-spam engine should be able to learn the difference between spam and legitimate emails in this type of situation so it does not bog down the business with excessive false positives. And finally, the anti-spam engine should be able to receive updates automatically from the vendor to keep pace with changing spam techniques. This way it will remain effective when new forms of spam appear, as we have seen in recent years with non-delivery-report, attachment or image-based spam.
- **Self-service spam quarantine** – Maintaining spam quarantines is a tedious, low-value activity for IT administrators. An effective SMB email gateway security solution will provide self-service quarantine administration, so end-users can review their own quarantines and unblock or delete messages themselves. This frees IT personnel to focus on more value-added activities, which is especially important for SMBs with limited IT resources.
- **Data loss prevention (DLP)** – As mentioned earlier, outbound email presents a broad array of risk to SMBs. Employees accidentally or intentionally leaking confidential or inappropriate information can lead to lost business, public embarrassment, compliance violations and even legal exposure. SMBs should look for DLP functionality in their email gateway security solution so they can mitigate these risks through a combination of attachment and content filtering.

Conclusion

While the email threat environment has never been more hostile for SMBs, there also has never been such a wide array of email gateway security solutions priced and configured for the SMB environment.

Choosing the right solution is a two-stage process. The first stage is to determine which form factor is right for you. If you are a small company with limited IT resources and your email traffic is not subject to regulatory or legal issues, then the hosted model is likely the best option. If you are a mid-sized business, or if you do have regulatory or legal issues to consider, then an appliance or software may be the best option.

The second stage is to consider the features you need. The email risk environment is much more complicated today than it was a few years ago, so simple anti-spam and antivirus functionality is not enough. This paper identifies a core set of features that any SMB can use as a checklist to ensure that their email gateway security solution truly mitigates email risk. And for SMBs, mitigating the risk of financial losses and brand damage is always a "neat idea."

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com