White paper

E-mail security

Introduction

This white paper provides useful background information on e-mail security issues. It will help you examine the security threats facing your corporate e-mail system and determine what kind of e-mail security solution your company needs.

The following topics are covered:

Corporate e-mail: A mission-critical application

E-mail-related threats to network security
- Spam
- Information leaks
- Interception and tampering
- Offensive contents
- Viruses
- Delivery failure

Protecting corporate e-mail systems against security breaches
- Security policy
- Security software
- Eliminating spam
- Preventing information leaks
- Encryption
- Content control
- Combating viruses
- Reporting & archiving

A powerful solution that arms your mail server
- Mail essentials for Exchange/SMTP
- GFI FAX & VOICE

Corporate e-mail – a mission-critical application

E-mail use for business purposes is fast on the rise as companies increasingly recognize electronic messaging as an efficient means of communication that is quicker and cheaper than more traditional methods.

Thousands share the enthusiastic view expressed by Mike Elgan, *Windows Magazine* editor, in the 18 June 1999 issue of his popular weekly newsletter: “We take e-mail for granted, but it is a truly wonderful medium. It's flexible, automatable, asynchronous and fast.”

At the moment, the average white-collar worker sends and receives about 30 e-mails a day, the Institute for the Future has found. Forrester Research predicts that customer contacts by e-mail will grow by more than 250% over the next three years. In 1996, only 15% of the US population used e-mail, but this figure is expected to reach 50% by the year 2001 – or sooner. By 2000, e-mail users are expected to number 107 million and explode to 6.9 trillion messages a year, *Windows Magazine* reported in October 1997.

This irreversible eruption in e-mail use has revolutionized the way business is conducted. However, as Wayne Rash, managing editor technology at *InternetWeek*, pointed out in an article dated 5 May 1999: “E-mail, as simple as it seems to most of us, has grown to be a complex, critical application.”

Perhaps the complexity of this prime communications medium can best be seen when considering how to make one’s corporate messaging system more secure.

E-mail-related threats to network security

A variety of different elements weaken your corporate e-mail system and while some are widely known – such as e-mail viruses – others tend to be ignored – like information leaks by internal users.

E-mails carrying offensive messages or confidential corporate information can create immense inconvenience and expense for a company that has not equipped its mail server with the appropriate tools. The same goes for spammers who use the e-mail system at work to send thousands of unsolicited e-mail messages. And what about the vast damage and time-loss caused by e-mail viruses, which seem to make ever more frequent appearances these days?

Some companies lull themselves into a false sense of security upon installing a firewall. This is a wise step to protect their intranet, but it is not enough: Firewalls prevent network access by unauthorized users. But they do not check the content of mail being sent and received by those authorized to use the system, for instance. More targeted measures are needed to counteract this and other security loopholes in a corporate network.

The threat of spam

About 90 per cent of e-mail users receive spam – or unsolicited commercial mail – at least once a week, a recent survey conducted by the Gartner Group shows. The research results, issued in June 1999, revealed that almost half those surveyed were spanned six or more times a week. The study surveyed 13,000 e-mail users.

Although US Congress and state legislatures are seeking to ban spam, and the Federal Trade Commission sues spammers whose junk mail deceives consumers, unwanted mail is on the increase.

As well as consuming bandwidth and slowing down e-mail systems, spam is a frustrating time-waster, forcing employees to sift through and delete mounds of junk mail. It also proves irritating and offensive to recipients who feel their privacy has been invaded. However, there is a third aspect to spam: it constitutes a security hazard.

Spammers can use a corporate mail server to send out their unsolicited messages, often bringing trouble upon the unwitting organization. Virgin Net recently underwent such an experience when one of its subscribers apparently used its network to send out 250,000 junk messages. As a result of this individual's actions, Virgin Net was put onto the Real-time Blackhole List (RBL), an undesirable listing which leads other ISPs to reject mail coming from that company.

The threat of information leaks

Organizations often fail to acknowledge that there is a greater risk of crucial data being stolen from within the company rather than from outside.

Various studies have shown how employees use e-mail to send out confidential corporate information. Be it because they are disgruntled and revengeful, or because they fail to realize the potentially harmful impact of such a practice,

employees use e-mail to share sensitive data that was officially intended to remain in-house.

FBI statistics, for example, reveal that among Fortune 500 companies, most data thefts in 1998 were by internal users. Again, research results carried in *PC Week* in March 1999 report that, out of 800 workers surveyed, 21-31% admitted to sending confidential information – like financial or product data – to recipients outside the company by e-mail. Ten per cent of those surveyed disclosed that they had received e-mail containing company-confidential information.

The threat of e-mail interception and tampering

Unsecured e-mail can fall prey to malicious software tools such as sniffers, which automatically lie in wait for interesting information relayed through their system as e-mails are transferred from sender to recipient.

Unknown to e-mail senders, sniffers are placed in the path of all e-mail messages going through a computer. The individual who has planted this device receives copies of all the messages passing through and is then in a position to read – and store – those deemed interesting or profitable. The person in question might look out for credit card numbers, e-mail addresses, passwords, personalities or competitors.

Some indulge in this pastime simply for the voyeuristic thrill of accessing messages addressed to others. The situation is more worrying when the intentions behind sniffers are injurious, stemming from a desire to spy on competitors, enemies, the wealthy, or whatever.

Apart from scanning and intercepting mail traffic, it is also possible for unauthorized people to tamper with e-mails so that the message reaching the recipient is not the one originally sent by its author.

Data on e-mail tampering – or the unauthorized altering of an original message – is revealing. A 1998 survey sponsored by the US Senate found that 12.6% of Fortune 1000 companies reported evidence of e-mail tampering. Security experts believe the actual incidence of tampering is even higher – a reasonable supposition, considering that over 200 million e-mail messages are sent daily.

The threat of e-mails containing offensive messages

E-mails carrying sensitive information, or unsolicited mail messages sent out by corporate users are not the only problem a company has to tackle with regard to employees' e-mail use. E-mails sent by staff containing racist, sexist or other offensive material could prove equally troublesome, not to mention embarrassing – and expensive!

This factor hit the headlines during the much-publicized antitrust case against Microsoft Corp., when the US government presented as evidence the contents of e-mails written by top Microsoft executives describing plans to topple competitors. On a similar note, Chevron recently had to pay $2.2 million to settle a lawsuit resulting from an e-mail message bearing sexist contents.

Under British law, employers are held responsible for e-mails written by employees in the course of their employment, whether or not the employer consented to the mail. The insurance company Norwich Union was asked to pay $450,000 in an out-of-court settlement as a result of e-mailed comments relating to competition.

Besides, offensive e-mails can cause considerable damage to the work environment simply by generating an unpleasant, hostile or unprofessional atmosphere.

The threat of viruses

Viruses are a major e-mail security hazard that companies simply cannot afford to ignore. Over 11,000 different computer viruses exist to date and some 300 new ones are created each month. Their effects range from negligible to bothersome to destructive.

The extent of the problem is so great that today many companies have even begun to prohibit the use of e-mail attachments, as this is where viruses are often embedded. Unless forewarned, users are generally unaware that they have received a virus until they open the infected attachment. By this time, it is too late: the virus is activated and starts to take over, completely infecting the hard drive and the messaging network.

The danger of viruses transmitted through macros, another common form of virus transmission, is that they allow the user to continue working and sharing documents. This way, the virus spreads faster, infecting more and more users. One such macro virus, known as Melissa, reared its ugly head on March 26, 1999. Melissa forced organizations the world over – among them Microsoft and

Intel – to suspend all e-mail transactions. This may well have been an effective response to the new viral onslaught, when timely action was taken – but it also signified incalculable productivity loss, despite stemming data loss. As a result, Melissa left a huge dent in corporate coffers: "It is responsible for millions of dollars worth of damage", an April 1999 issue of *InfoWorld* reported.

Other fiercely destructive viruses followed fast on Melissa's trail, such as the Chernobyl (CIH) virus and the Explore Worm, both of which wipe out files, resulting in data loss. Again, companies like Microsoft, Intel, Boeing and Forrester Research were reported in the press as having shut down their mail servers when hit by the Explore Worm outbreak in June 1999. And, as if all this were not enough, anti-virus researchers predict that more damaging e-mail viruses are yet to come.

The threat of delivery failure

Another security feature worth having is the facility to ensure e-mail delivery, particularly now that e-mail is used for critical business messages, such as proposals, product information, orders, and so on. Confirmation of delivery is an essential tool to set the sender’s mind at rest that each message sent has been received by the intended recipient.

Also, through the tracking and archiving of e-mail messages, companies can keep a record of their e-mail messaging.

Protecting corporate e-mail systems against security breaches

Corporate security policy

The security menaces are many, but effective solutions do exist. The first step to enhance security recommended by cyber-security consultants is the formulation of a corporate e-mail policy document. This is used to inform all members of the organization which messaging practices are deemed unacceptable.

Without being overly restrictive, such documents should provide guidelines and procedures to be followed by employees in their use of e-mail at the workplace. Examples of the kinds of e-mail messages that could prove detrimental to the organization should be supplied. The overriding point to be emphasized is that by adopting this policy, the company and its staff stand to gain by benefiting from messaging security that is as watertight as possible.

Next, the organization must acquire new security tools to help enforce these regulations, informing all users that this measure is being taken.

Security software

Corporations may choose from a selection of e-mail security packages. Some solutions are created to tackle a particular menace alone while others contain a convenient bundle of tools to deal with the various hazards. It is up to each organization to select the software that best suits their needs.

As always, price is bound to be one of the determining factors in making the right choice. Another essential characteristic to seek is a product that is as transparent to the user as possible. A package that installs on the existing corporate e-mail system and is easy to use means that a company can enjoy the security benefits offered immediately upon installation. This section examines the different e-mail security features available on the market, either separately or as part of a solution.

Eliminating spam

An efficient anti-spam tool will pick up words and phrases that usually appear in unsolicited commercial e-mails and block the unwanted message from entering the system. While preventing inconvenience to recipients, this saves the corporation time that employees would otherwise have wasted reading and deleting junk mail – paid work time that could be better applied.

Advanced anti-spam features include the detection of incorrect ‘From’ headers and addresses in the e-mail body, typical spam practices, as well as the facility to be programmed to block e-mails containing any phrases the company chooses. Another essential ingredient is the ability to prevent spammers from using the corporate system to send out vast quantities of mail, a practice known as mail relaying.

Also effective against spam is a quarantining feature that deters e-mail messages with dubious content from going through. This feature acts as a kind of clearinghouse, allowing an authorized person to approve the filtered messages before they are sent or received.

Preventing information leaks

A content checking tool is a must to prevent users from sending out confidential or sensitive corporate information via e-mail. This tool automatically scans the contents of each message being mailed.

To be effectual, this tool should link to a quarantining feature that isolates e-mails with suspect content and prevents them from being sent unless an authorized person within the organization has approved the message.

Equally essential is the automatic addition of disclaimers stating that the message sent is intended solely for the addressee. This tool should include the option of being programmable to include a company message such as a slogan, apart from the legal disclaimer.

Stopping interception and tampering

The right encryption technology, such as PGP or S/MIME guarantees secure messaging*.

Encryption technology is based on cyptographic keys that consist of a binary sequence of 1s and 0s. The PGP standard is 128-bit cryptology, a code emerging as the new digital standard that is considered "uncrackable", according to a *Washington Post* article dated May 1998.

The encryption system is based on paired keys and algorithms that encrypt messages with one key (the public key) and permit decryption with a different key to which it is paired – the private key.

Users can freely make known and publish their public key so that anyone wishing to contact them securely by e-mail can use it to encrypt their message. The public key transforms the message into a string of garbled, undecipherable text that can only be decoded with the user's private key.

The reader's private key then decrypts the information that was sent after being encoded by the public key. The user alone can access his/her private key by means of a password.

Content control

Likewise, a content screening tool is necessary to prevent corporate users from sending or receiving offensive, profane or inappropriate e-mails, such as racist

or sexist messages, bawdy jokes, pornographic material or other undesirable content.

This should be coupled with a tried and tested quarantining feature that bars e-mails with suspect content from being sent or received unless an authorized person within the organization has approved the message first.

To reinforce this preventive approach, companies should invest in a tool that automatically adds a legal disclaimer to the end of every message sent out by the organization. A professional disclaimer feature will additionally allow companies to tag a corporate message to each mail as well as the legal statement.

Combating viruses

A reliable virus scanner screens all incoming and outbound messages and attachments for e-mail viruses and worms.

Of course, it is not enough for a package to detect a virus. A good security tool must be able to block the infected documents or clean them before the e-mail reaches the addressee. Additionally, the anti-virus solution should notify the recipient and/or network administrator of the e-mail-borne virus. This way, viruses are stopped in their tracks before they do any harm and senders can be alerted that their systems are infected.

Anti-spam tools may also be used in the battle against e-mail viruses as they can be programmed to entrap and isolate certain viruses on the basis of key words. This is a particularly potent method when the organization has received an advance warning about a new virus.

An e-mail security package should ideally offer customers a choice of anti-virus technologies. This way, users are not tied down to one anti-virus vendor if it falls behind in virus detection.

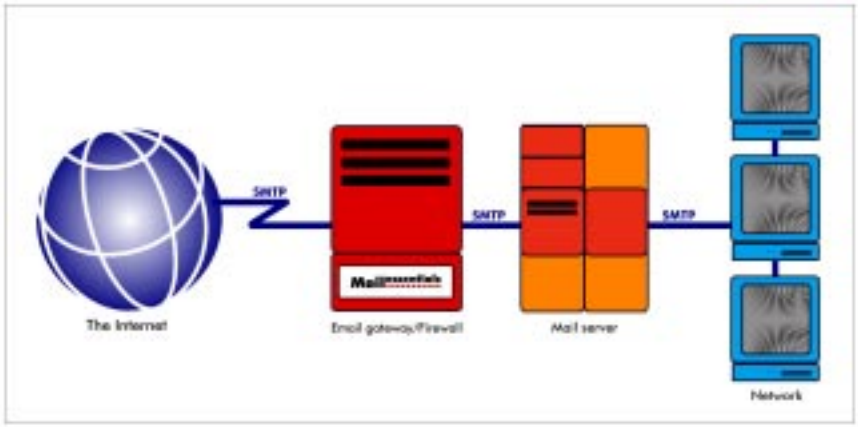
Reporting & archiving

A worthwhile e-mail security software package will allow organizations to track e-mail usage and monitor communications, enabling users to ascertain when each individual message has been sent and confirm whether it has been received.

A powerful solution that arms your mail server

Mail essentials for Exchange/SMTP

Mail essentials for Exchange/SMTP is the ideal solution for those seeking to enhance their corporate mail security.



Mail essentials operates as a gateway between the mail server and the Internet.

Mail essentials adds powerful e-mail security and management features to existing mail servers, such as:

- Content checking for offensive or confidential information - Blocks undesirable e-mail before it is sent or received.

- Quarantining of e-mail - Allows managers to approve the sending or receiving of e-mails with certain content or attachments.

- Encryption – Ensures secure incoming mail by enoding it through PGP, while automatically informing senders of the public key though the product's disclaimer function.*

- Disclaimers - Automatically includes a company-wide message to each e-mail that is sent out.

- Virus checking of all incoming and outbound mail, using technology by anti-virus leaders such as Norton, McAfee and F-PROT.

- E-mail management - Allows companies to track e-mail usage and communications (for example, to know when an e-mail was sent and received by another party). In addition, it facilitates the compiling of reports on e-mail usage.

- Automatic compression of all outbound mail to save on bandwidth.

- Personalized auto-replies with tracking numbers - Enables companies to confirm to customers that their e-mail was received. Tracking numbers give customers and employees an easy point of reference.

- Advanced anti-spam measures - Picks up on typical spam practices such as incorrect From headers and addresses in the e-mail body, and prevents spammers from using a company's mail server to relay their mail.

- POP3 downloader with built-in dial-up and support for multiple POP3 servers.

- Archiving of e-mail to any ODBC database - Allows companies to keep a complete record of all e-mail communications and provides the possibility to periodically check e-mail content.

- Transparent operation for user and administrator.

Mail essentials operates as a gateway between the mail server and the Internet. Therefore its implementation is completely transparent to the user. For the administrator, there is little or no additional user administration.

An evaluation version can be downloaded from: **http://www.gficomms.com**.

The Small Business version of this package means that it is well suited to small enterprises as well as larger organizations. Pricing of Mail essentials starts at $149 for the Small Business Version. An added bonus is the fact that GFI has issued the Mail essentials anti-spam feature as freeware.

**For more information on e-mail encryption, please refer to GFI's white paper on the topic, due soon.*

GFI is shortly issuing a white paper on managing a corporate e-mail system.

GFI FAX & VOICE

GFI FAX & VOICE is the leading supplier of Windows NT based communications software. Founded in 1992, GFI FAX & VOICE is a global company with offices in the US, Germany, France, Australia, Malta and the UK.

Leading the way through innovation and engineering excellence

In 1995, GFI FAX & VOICE was one of the first companies to launch a Windows NT based fax server: FAXmaker. Soon after, in 1996, GFI FAX & VOICE again proved its cutting edge status by developing one of the first Exchange fax connectors, FAXmaker for Exchange. During this year, GFI FAX & VOICE partnered with Microsoft Asia to allow Microsoft to penetrate a market that required fax as part of the Exchange server solution. In 1997 alone, GFI FAX & VOICE shipped 20,000 fax servers, proving FAXmaker to be one of the most popular fax server platforms for Windows NT.

GFI FAX & VOICE is also leading the way in e-mail management and automation. Launched in 1997, Emailrobot for Exchange/SMTP was one of the first applications designed to help companies handle the fast increasing e-mail overload. Emailflow develops on this product's strengths, adding more winning features to this corporate tool.

GFI FAX & VOICE is a privately held company, and employs 55 people. The company has been named one of 1999's fastest growing software companies for Windows by Microsoft Corp. and CMP Media.

Corporate clients

GFI FAX & VOICE's customer list includes: Microsoft, Digital, Honeywell, Siemens, Matshushita, Ericsson, OKI, Olivetti, Triumph Adler, Berliner Investment Bank, Bayersdorff A.G., PTT Telecom, Norwegian Telecom, Swiss Telecom, Cumbria Police Force, London Fire Brigade, UK Police departments, German financial institutions, Giorgio Armani, Benetton and many more.

USA & Canada
GFI FAX & VOICE USA
105 Towerview Ct.
Cary, NC 27513
Tel:1 (888) 2-GFIFAX:
Tel: (919) 388-3373; Fax: (919) 388-5621
Email: sales@gfifax.com

United Kingdom
GFI FAX & VOICE
5 Princeton Mews
167/169 London Road
Kingston-Upon-Thames
Surrey KT2 6PT
Tel: (020) 85460640; Fax: (020) 85460741
info@gfifax.co.uk

Central Europe
(Germany, Austria & Switzerland)
GFI FAX & VOICE Gmbh.
Palmaille 59, 22767 Hamburg, Germany
Tel: 040-306810-0; Fax: 040-306810-10
Email: info@gfigmbh.de

France
GFI FAX & VOICE France S.A.R.L.
30, avenue Charles Flahault,
34090 Montpellier
Tel: +33 (4) 99.61.40.17
Fax: +33 (4) 99.61.40.18
E-mail: ventes@gfifrance.com

Australia
GFI Australia (Fax & Communications) P/L
26 Stirling Street
Thebarton, SA 5031
Sales FreeCall: 1800-CALL-GFI
Tel:+61-8-8351-9780; Fax:+61-8-8351-7997
Email: sales@gficomms.com.au

GFI FAX & VOICE Ltd.
'Communications House'
Mediterranean Street, SGN 07
St Julians, Malta
Tel: +356-382 418; Fax: +356-382 419
Email: sales@gfifax.com