Email Security

Kunal Pandove
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

Amandeep Jindal
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

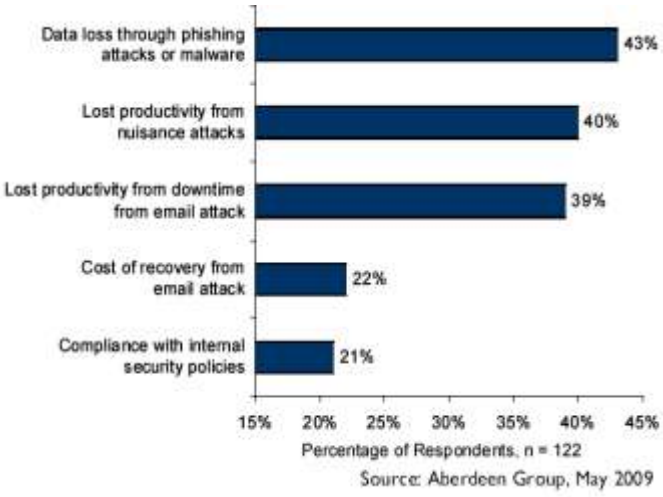
Rajinder Kumar
Research Associate
CSRC, PEC,
Sector 12, Chandigarh.

ABSTRACT
Organizations can't live without Email and it puts every organization at risk. As a global enabler of communications and collaboration, email simultaneously is the medium of choice for many hackers worldwide. Left unattended, email vulnerabilities can cripple an organization and devastate its brand. Solutions abound, but root causes malware laden spam, email with links to malicious web sites, phishing attempts, intentional and unintended data loss, botnet infestations – persist unabated, growing ever more clever and ever more resistant to detection. Organizations are driven to focus on email security by the need to protect themselves from the damages email attacks can cause.

1. VULNERABILITIES IN EMAIL SECURITY [1]
Email security must consider three fundamental dimensions of vulnerability:

- **Inbound email threats** such as spam, phishing attacks, malware, spyware, blended threats, scams, and spoofs.

Figure 1: Top Reasons Organizations Focus on Email Security



- **Outbound vulnerabilities and liabilities** including accidental data loss, intentional data leakage, botnet activity, and contaminated outbound mail. Outbound protection strategies must protect email in transit.
- **Risks associated with email within the organization** including inappropriate sharing of sensitive data and malware contamination. Organizations must protect email "at rest" – both the contents of user inboxes and folders as well as email archives.

2. BEST STRATEGIES
Organizations put their primary focus on:

- Protecting users from unwanted email and inbound email vulnerabilities
- Preventing the dissemination of spam or infected email from the organization
- Training employees in email best practices

Each of these areas of focus needs to be kept current. New and more sophisticated email threats arise continuously and must be dealt with by both keeping email protection capabilities at a state of the art level, and by keeping employees up-to-date with the latest forms of phishing and social engineering, email acceptable use policies, and pertinent regulations that apply to their email use.

Year over year, Best organizations are putting more focus on email security policies and are more often viewing outsourcing email security as a strategy to achieve their goals. Outsourcing email security goes by many names, such as Security in the Cloud, Managed Security Services, or Security- (or Software-) as-a-Service, to name the most common. Choosing to outsource email security as a top strategy is up more than 150%.

In considering email security strategy it's critical you pay attention to four important areas:

A. *Consider email security from all angles.*
First, you must address incoming email and the potential threats it may carry including contaminated mail carrying malware, phishing attacks, and pieces of a blended threat – innocuous seeming email that has a dangerous link inside. Second, you must address your outbound mail security, including protecting legitimate mail in transit, preventing both intentional and unintended data leakage, and making sure email from your organization is free from malware. In addition you must monitor for botnet activity, as it may originate from infected machines in your organization without your knowledge unless you're actively trying to detect it. Third, you must look at email internal to your organization – computers can get infected many ways and you don't want to spread contamination within your organization. Likewise, you don't want sensitive data leaked to someone within the organization who does not have legitimate access to it.

B. *Critical to your overall success is defining and enforcing email security policies*

These include explicit rules around handling sensitive data. You are responsible for your organization's sensitive data and virtually everyone has access to email. If you're not protecting your data vis-à-vis its inclusion in email messages or attachments, you're not protecting your data.

C. *Zero Hour Protection*

New email threats emerge perpetually. Labs work 24 / 7 to identify new threats and protect against them. You should avail yourself of these protections the instant they become available. It's no wonder that Best-in-Class organizations automatically respond to new threats to a much greater extent than the other classes, and most Best-in- Class organizations have protection in place for new threats within a few hours. Organizations that update their email protection on a scheduled basis rather than when the protection becomes available leave themselves needlessly vulnerable and, as our data indicates, suffer many more incidents of downtime and data loss.

D. *Encryption* [2]

Protecting email in transmission is critical to protecting sensitive data. Coupled with data loss solutions that either prevent unencrypted sensitive data from being sent or automatically encrypt sensitive data to protect it, organizations can take a big step in preventing data loss. Part of end-user training must be a reminder that email sent in the clear is like sending mail on a postcard – everyone who sees it can read it. Also, part of end-user training must be conveying the fact that technology exists that is actively looking at traffic to detect and collect sensitive data such as credit card numbers and social security numbers. Would-be villains don't need to know their victims – they simply prey on the unprotected.

3. REQUIREMENTS FOR SUCCESS[3]

In addition to having common performance levels, each organization also shared characteristics in five key categories:

(1) Process (the approaches they take to execute their daily operations)

(2) Organization (corporate focus and collaboration among stakeholders)

(3) Knowledge management (contextualizing data and exposing it to key stakeholders)

(4) Technology (the selection of appropriate tools and effective deployment of those tools)

(5) Performance management (the ability of the organization to measure its results to improve its business).

A. Process

Training end-users in safe email practice requires continuous re-enforcement and updating to keep users aware of the latest dupes designed with very sophisticated socially engineered tactics. This year, for example, end-users need to be alerted to the fact that newer phishing attacks are designed to look as if they are coming from someone within the organization itself. Some are addressed to colleagues with the recipient cc'd or bcc'd. Alerting end-users to known new threats can minimize the chances that they'll be conned into opening such mail.

B. Organization

Organizations need to create email abuse reports and they need omeone knowledgeable whose job includes reviewing the reports to detect attempted abuse as well as identify the target of such attempts. Creating the reports alone does nothing unless someone who knows what they mean reviews them regularly.

C. Knowledge Management

Creating email use reports is critical to designing and implementing appropriate email security policies. Understanding the organization's norm helps identify abnormal behaviors.

D. Technology

Organizations need to **scan incoming mail for all sorts of malware** – keep whatever you can outside. They need to scan all outgoing mail as well, because computers can get infected by visiting malicious sites, or introducing infections by way of contaminated files from a thumb drive, CD, or DVD. Don't risk contaminating others in the organization or damaging the organization's brand by sending out malware-laden email. Overall email security relies in part on endpoint security. Despite what everyone agrees is best practice, not all organizations insist on protecting their endpoints, and that's a mistake.

Beyond traditional anti-virus protection, organizations need to **explicitly work to deter phishing attacks,** the installation of spyware and key loggers, and work to thwart fraud. The escalation of attacks through email continues to rise unabated and you can expect this trend to perpetuate indefinitely. It's critical that organizations find ways to keep current in the email threat domain.

Policy is key to protecting the organization and its data. Email security policies can be refined over time, but begin by establishing and enforcing policy now.

Email attachments can be problematic on several fronts – they must be **scanned to ensure they don't contain malware, and they must be scanned to prevent inadvertent data loss.**

Many threats come in a form known as a **blended threat.** In a blended threat, innocuous looking email – email that is not obviously spam – contains a link that resolves to a malicious site. As new malicious sites arise at every moment, organizations need a **tight coupling between their email security and their web security.** Some anti-spam solutions actually check each link inside an email to determine if the sites where they point are legitimate.

Data loss tops the list of biggest concerns across all respondents, yet most organizations have yet to explicitly address data loss.

Identifying sensitive data and creating policies to protect it are critical to preventing data loss.

Highly sensitive data may call for special handling. Certain data may be so sensitive that you may want to keep it out of the traditional flow of email, period. Because traditional email follows well-defined protocols and paths for delivery, it's subject to attacks designed to exploit known vulnerabilities and common email use. Availing yourself a completely separate secure channel for communication might prove the safer course of action for information considered highly sensitive – government security data, patient healthcare data, and financial transactions.

E. Performance Management

Awareness and understanding of the email threats reaching the organization is critical to the continual refinement of email security policies and the bolstering of support where it's most needed

4. RECOMMENDED ACTIONS

Whether a company is trying to move its performance in email security from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements:

Steps to Success[6]

A. *Spam Filters*

A growing number of technology vendors are targeting spam with products that are designed to block and quarantine suspected spam. These offerings use sophisticated algorithms to scan each incoming message for signs that it may contain spam.

B. *Firewalls*

Spam firewalls offload message filtering from the email server, freeing up network resources and bandwidth. Spam-firewall appliances usually come preconfigured and can be set up in minutes. Maintenance is usually minimal.

C. *Anti-Malware Technologies*

Hardware- and software-based anti-malware products can block dangerous attachments from reaching employees' inboxes.

D. *Client Control*

Leading email clients, such as Microsoft Outlook and Outlook Express, as well as Mozilla Foundation's Thunderbird, offer built-in controls that are designed to minimize inbox spam.

E. *White Lists/Black Lists*

This feature is found in many spam filters and client controls. White lists of trusted email addresses allow messages to proceed to the user's inbox unimpeded by any filter or client settings. Black lists work in the opposite way, routinely blocking incoming email from known offenders.

F. *Don't send private messages with the company account.*

If you want to send personal messages from work (and you should probably try to minimize this), use a freebie account like Hotmail, Gmail, Yahoo!, or Excite, if your office permits it. The content of your emails is less visible to employers through these accounts, so the private messages you send will stay private.

G. *Use BCC if necessary*

. If you must send a group email to people who do not know each other, don't add their addresses to the form's CC field; this is one method spammers use to harvest email addresses. Instead, use BCC (Blind Carbon Copy) for their addresses, and put your own email in the form's "to" field

H. *Respond to group email appropriately.*

If someone has sent a group email that requires a response, but only to the sender or a couple of parties, don't copy everyone on your reply.

I. *Respect email laws and regulations.*

Some countries have very specific rules about bulk emailing. If you use email to promote your business, you need to know the laws for not only your country but probably wherever you are emailing to. It's a tall order, given the global village of the Internet, but its importance cannot be overstated.

J. *Use meaningful subject lines.*

Write something "meaningful" in the subject line, to give recipients a clue as to what your email is about. This is increasingly necessary to distinguish legit emails from spam. The latter's subject lines are are often deceptive.

K. *Enable spam filters.*

Most email clients, including freebie webmail types, have spam filtering that can be turned on or off. They are not 100% accurate, so you should make a habit of visually scanning your spam folder to ensure you haven't missed anything important. But that inconvenience is still worth leaving the filter on.

L. *Ditch your spammed out email account.*

If you have a freebie account that is loaded with incoming spam, save all your important contact info, backup desired emails, then ditch the email address. Get another one and then notify all your contacts. Don't forget to update any websites where your address is published.

M. *Use Text/ RTF format instead of DOC files.*

Microsoft's Word files (.doc format) are susceptible to some macro viruses. If you must send a document and cannot use one of the options above, copy your document to RTF (Rich Text Format) first, then email that as an attachment. Even if you don't have a virus on your computer, your colleague may. If they receive an RTF file, then there is less chance they will respond with a DOC file. (MS Word let's you work with RTF files as you would a DOC file.) It is also okay to send .txt (raw text), .pdf, and image files. Bad to send: any .EXE or other executable file. Possibly bad: .doc or .xls (Microsoft Excel spreadsheet) files.

N. *Train end-users in safe email practices.*

In an ideal world technology would thwart every attack and catch every data breach. However, as new attacks are being invented at every moment, keeping end-users aware of current threats minimizes the likelihood of their falling prey to the latest trap. Likewise, often it's uneducated users who send sensitive data inappropriately only because they don't know they shouldn't; implementing end-user training is imperative.

O. *Integrate email and web security.*

Because most of today's threats are blended threats – that is, threats that may begin with a seemingly innocuous email containing a URL that points to a malicious site – end-users need either email scanning that actually evaluates all embedded links, checking the sites to which they point, or they need tightly coupled web security that will prevent a link they click on in an email from resolving at a contaminated site. Ideally, they never have to see such mail in the first place.

P. *Implement anti-phishing, anti-spyware, anti-key logging, anti-fraud solutions.*

Increasingly sophisticated phishing attacks are of major concern, and data loss through these attacks is of primary concern to most respondents. Many of these threats can be detected and thwarted with appropriate solutions

Q. *Leverage the cloud.*

Using either a cloud-based solution or a hybrid solution that leverages the cloud, include cloud-based email security to ensure that spam and email threats that can be eliminated outside your network stay outside your network. Keeping known spam and infected mail outside lowers your risk and saves the potential costs of archiving unwanted mail.

R. *Scan outbound email attachments for sensitive data.*

Data in spreadsheets, word documents, PowerPoint presentations, and patient records, may well be data sensitive to the organization or protected by data privacy legislation. Without actively scanning outbound attachments, organizations leave themselves vulnerable to data leakage and regulatory sanction.

S. *Obtain data use reports.*

To protect their data, organizations need to classify their data and implement policies that limit access to sensitive data. To understand how data is being used within the organization requires data use reports. Email security policies that protect the organization while maintaining flexibility require knowledge of who has legitimate access to what data.

5. CONCLUSION

Protecting the organization and its data from the threats posed by email requires constant vigilance and enforcement – awareness of new threats as they emerge, an understanding of the organization's sensitive data and how to protect it, and an understanding that email is a mission-critical application that creates a backbone of communication within the organization and with customers, business partners, and prospects. Loss of the ability to send and receive email (email availability) can prove damaging if not disastrous depending on the length of outage and the business processes that rely on email. Deploying many elements of email security in the cloud is proving an ever more attractive option for many organizations.

6. REFERENCES

[1]http://www.aberdeen.com/Aberdeen-Library/5981/RA-email-security-phishing.aspx

[2]http://communication.howstuffworks.com/how-email-scams-work.htm

[3]http://www.bitpipe.com/data/detail?id=1256912322_366&type=RES&asrc=SS_SRCH

[4]http://www.bitpipe.com/data/detail?id=1239388805_506&type=RES&asrc=SS_SRCH

[5]http://www.windowsecurity.com/whitepapers/Email_security.html

[6]http://www.itsecurity.com/features/99-email-security-tips-112006/