E-mail Security: An Overview of Threats and Safeguards

By Kevin Stine and Matthew Scholl

Not everyone in the organization needs to know how to secure the e-mail service, but anyone who handles patient information must understand e-mail's vulnerabilities and recognize when a system is secure enough to transmit sensitive information.

E-mail messages are generally sent over untrusted networks-external networks that are outside the organization's security boundary. When these messages lack appropriate security safeguards, they are like postcards that can be read, copied, and modified at any point along these paths.

Securing an e-mail system is the responsibility of an organization's IT department and e-mail administrator. However, anyone responsible for the confidentiality, integrity, and availability of the information sent via e-mail should be aware of the threats facing e-mail systems and understand the basic techniques for securing these systems.

The E-mail System in a Nutshell

An e-mail system is made up of two primary components that reside in an organization's IT infrastructure: mail clients and mail servers.

Users read, compose, send, and store their e-mail using mail clients. Mail is formatted and sent from the mail client via the network infrastructure to a mail server. The mail server is the computer that delivers, forwards, and stores e-mail messages. All components-the mail servers, the mail clients, and the infrastructure that connects and supports them-must be protected.

Voluntary industry standards (e.g., SMTP, ESMTP, POP, IMAP) for formatting, processing, transmitting, delivering, and displaying e-mail ensure interoperability among the many different mail client and server solutions.

E-mail security relies on principles of good planning and management that provide for the security of both the e-mail system and the IT infrastructure. With proper planning, system management, and continuous monitoring, organizations can implement and maintain effective security.

Common Threats

Because e-mail is widely deployed, well understood, and used to communicate with untrusted, external organizations, it is frequently the target of attacks. Attackers can exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access to resources. Common threats to e-mail systems include the following:

Malware. Increasingly, attackers are taking advantage of e-mail to deliver a variety of attacks to organizations through the use of malware, or "malicious software," that include viruses, worms, Trojan horses, and spyware. These attacks, if successful, may give the malicious entity control over workstations and servers, which can then be exploited to change privileges, gain access to sensitive information, monitor users' activities, and perform other malicious actions.

Spam and phishing. Unsolicited commercial e-mail, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. Such messages can disrupt user productivity, utilize IT resources excessively, and be used as a distribution mechanism for malware. Related to spam is phishing, which refers to the use of deceptive computer-based means to trick individuals into responding to the e-mail and disclosing sensitive information. Compromised e-mail systems are often used to deliver spam messages and conduct phishing attacks using an otherwise trusted e-mail address.

Social engineering. Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization's users or get users to perform actions that further an attack. A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

Entities with malicious intent. Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on a mail server. For example, once the mail server is compromised, an attacker could retrieve users' passwords, which may grant the attacker access to other hosts on the organization's network.

Unintentional acts by authorized users. Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action.

Security Safeguards

Management, operational, and technical safeguards are necessary to ensure that the confidentiality, integrity, and availability needs of the mail system, its supporting environment, and the data handled by it are addressed.

The National Institute of Standards and Technology is a nonregulatory agency within the Department of Commerce. Its Information Technology Laboratory recommends that organizations employ the following guidelines in planning, implementing, and maintaining secure e-mail systems.

Implement Management Controls

Management security controls-such as organization-wide information security policies and procedures, risk assessments, configuration management and change control, and contingency planning-are essential to the effective operation and maintenance of a secure e-mail system and the supporting network infrastructure. Additionally, organizations should implement and deliver security awareness and training, because many attacks rely either partially or wholly on social engineering techniques to manipulate users.

Carefully Plan the System Implementation

The most critical aspect of deploying a secure e-mail system is careful planning before installation, configuration, and deployment. As is often said, security should be considered from the initial planning stage, at the beginning of the system development life cycle, to maximize security and minimize costs.

Secure the Mail Server Application

Organizations should install the minimal mail server services required and eliminate any known vulnerabilities through patches, configurations, or upgrades. If the installation program installs unnecessary applications, services, or scripts, these should be removed immediately after the installation process is complete.

Securing the mail server application generally includes patching and upgrading the mail server; configuring the mail server user authentication and access and resource controls; configuring, protecting, and analyzing log files; and periodically testing the security of the mail server application.

Secure the Mail Client

In many respects, the client side of e-mail represents a greater risk to security than the mail server. Providing an appropriate level of security for the mail client requires carefully considering and addressing numerous issues.

Securely installing, configuring, and using mail client applications generally includes patching and upgrading the mail client applications; configuring the mail client security features (e.g., disable automatic opening of messages); enabling antivirus, antispam, and antiphishing features; configuring mailbox authentication and access; and securing the client's host operating system.

Secure the Transmission

Most standard e-mail protocols send, by default, user authentication data and e-mail content in the clear; that is, unencrypted. Sending data in the clear may allow an attacker to easily compromise a user account or intercept and alter unencrypted e-mails. At a minimum, most organizations should encrypt the user authentication session even if they do not encrypt the actual e-mail data.

A related control to protect the confidentiality and integrity of the message is to deploy a secure e-mail solution such as leveraging PKI technology to encrypt and sign the message. Digital rights management and data leakage prevention systems can be used to prevent the accidental leakage and exfiltration of sensitive information.

Secure the Supporting Operating Environment

While the mail server and mail clients are the two primary components of an e-mail system, the supporting network infrastructure is essential to its secure operations. Many times, the network infrastructure, including such components as firewalls, routers, and intrusion detection and prevention systems, will provide the first layer of defense between untrusted networks and a mail server.

Is Encryption a Requirement?

The HIPAA security rule requires covered entities to *consider* data encryption, but it does not require them to implement it. A covered entity can comply with the security rule if it safeguards protected health information using a comparable method.

HIPAA did not make encryption a requirement in part because the technology was harder to come by at the time the security rule was written. As encryption becomes easier to deploy, covered entities may have a harder time justifying a decision not to use it.

Provisions within the American Recovery and Reinvestment Act do modify the HIPAA privacy and security rules, but they do not add requirements that healthcare providers must encrypt their protected health information. However, two sections of ARRA could lead organizations to consider encrypting e-mail messages:

- **Meaningful use incentive program.** To meet the objectives of this voluntary program, participants must provide patients with electronic copies of their health information. One possible way to deliver this information is e-mail. Providers that consider sending sensitive patient information via e-mail must secure it appropr-iately, and some type of encryption would be logical.
- **Breach notification.** The rule provides a safe harbor for covered entities that encrypt sensitive data. Organizations that experience the loss, theft, or unauthorized access of unencrypted protected health information (in any format) must notify the victims and the Department of Health and Human Services; if the information is encrypted, the organization may be exempt.

-Editors

Maintaining a Secure Mail System

Maintaining the security of a mail system is an ongoing process, requiring constant effort, resources, and vigilance, and usually involves the following actions:

Configure, Protect, and Analyze Log Files

Log files are often an organization's only record of suspicious behavior. Enabling logging mechanisms allows the organization to use collected data to detect both failed and successful intrusions, initiate alert notifications when further investigation is

needed, and assist in system recovery and post-event investigations.

Organizations require both procedures and tools to process and analyze the log files and review alert notifications.

Back up Data Frequently

One of the most important functions of a mail server administrator is maintaining the integrity of the data on the mail server. This is important because mail servers are often one of the most vital and exposed servers on an organization's network.

The mail administrator should back up the mail server on a regular basis to reduce downtime in the event of a mail service outage and support compliance with regulations on the backup and archiving of data and information, including those found in e-mail.

Protect against Malware

Organizations require malware scanning and spam filtering capabilities at the mail client and the mail system levels. Organizations should also conduct awareness and training activities for users, including telecommuters, so that users are better prepared to recognize malicious mail messages and attachments and handle them appropriately.

Perform Periodic Security Testing

Periodic security testing of the mail system confirms that protective measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the operational mail system. Organizations should consider using a combination of techniques, including vulnerability scanning, to assess the mail system and its supporting environment.

NIST offers additional information on mail system security and on general information security technologies and methodologies through its NIST Computer Security Resource Center at http://csrc.nist.gov.

Reference

Tracy, Miles, Wayne Jansen, Karen Scarfone, and Jason Butterfield. "Guidelines on Electronic Mail Security." NIST Special Publication 800-45 version 2. February 2007. Available online at http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf.

Kevin Stine (kevin.stine@nist.gov) is information security specialist and Matthew Scholl is group manager at the National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, Security Management and Assurance.

Article citation:
Stine, Kevin; Scholl, Matthew. "E-mail Security: An Overview of Threats and Safeguards" *Journal of AHIMA* 81, no.4 (April 2010): 28-30.