Email threats are continuing to evolve and become much more dynamic and targeted in nature. As these threats keep growing, how will you ensure email security? This expert tip explores the best ways you can improve your enterprise email security today – beyond basic antivirus software and antispam filters that no longer provide sufficient protection.

Improving enterprise email security: Systems and tips
Karen Scarfone

Enterprise email security has changed a great deal since the days when all you needed was some antivirus software and a basic antispam filter.

The effectiveness of these older-generation email security controls has rapidly declined. Attackers now create painstakingly crafted messages for specific target recipients, oftentimes sending a message from the hacked email account of that person’s friend or relative. And emailed malware often exploits zero-day vulnerabilities that no antimalware system can stop. Needless to say, email threats have evolved and become much more dynamic and targeted in nature.

Securing the hulking on-premises email systems, such as Microsoft Exchange and IBM Lotus Domino, that most enterprises still rely on involves the deployment of many emerging network security technologies. This article provides several practical tips for technologies that can improve enterprise email security. These technologies are generally available both as add-ons to an organization’s email servers and as components of email security appliances that work closely with an organization’s email servers.

Email reputation management services
One of the most effective ways to screen incoming email messages for malicious content is to subscribe to email reputation management services.
These services collect information from organizations about the email they receive, including data on senders, subject lines, attachments and many other characteristics, for determining the likely intent of each sender. This information allows each organization to act accordingly, in terms of which email it allows through to recipients, based on the organization's security needs and the relative reputational scores of each email sender. The power of these services is their ability to detect patterns across many organizations, patterns that each organization individually would not be able to identify.

**Temporary quarantining**

A simple yet surprisingly effective technique for thwarting the latest email-borne attacks is to temporarily quarantine suspicious email messages. Many of today's threats, particularly those involving phishing, have incredibly short lifespans. It may only be a few hours from the time a phishing email is crafted and sent to when that threat is identified and the supporting malicious websites are taken down. Antiphishing technologies can't fully keep up with these fast-emerging threats, so it makes sense to employ capabilities that, upon detection of suspicious email content, temporarily delay delivery. Again, as with email reputation management services, the configuration of temporary quarantining depends on the organization's security needs, because erring on the side of caution may inadvertently delay benign emails from being delivered.

**Outbound email filtering**

Organizations should filter not only their incoming email messages, but also their outbound email. Often this can be done with technologies already in place. For instance, a data loss prevention (DLP) product can stop email from being sent that contain sensitive personally identifiable information (PII). Users could inadvertently send this email, or it could be sent maliciously by malware infecting users' computers. Many organizations also find it helpful to apply other email content security policies to outbound email, such as preventing email from being sent that contains profane language or that contains keywords indicating inappropriate content (e.g., "classified").
Policy-based email encryption

Policy-based email encryption involves applying encryption to select messages based on certain predefined criteria. For instance, companies can establish policies so that email sent by certain high-profile individuals, with specific words or groups of words in the subject line, or with various types of attachments will have their confidentiality protected through encryption. An organization may even choose to encrypt the content of all internal email, plus there are technologies that support email encryption for messages sent outside the organization (e.g., to business partners).

Ideally, the use of policy-based email encryption is transparent to users, protecting the confidentiality of their email without asking them to make the choice of whether to encrypt their communications on a message-by-message basis as some email encryption add-ons have done. This is increasingly important given the spread of bring-your-own-device usage in the enterprise. These devices often lack the security controls that organization-issued mobile devices contain. In environments where a mobile device management (MDM) product isn't in place, policy-based email encryption is a particularly important security add-on.

About the author:
Karen Scarfone is the principal consultant for Scarfone Cybersecurity in Clifton, Va., providing cybersecurity publication consulting services. Karen was formerly a senior computer scientist for the National Institute of Standards and Technology (NIST), and she has co-authored more than 50 NIST publications, including Special Publication 800-45 Version 2, Guidelines on Electronic Mail Security.
Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchCloudSecurity
- SearchSecurity
- SearchFinancialSecurity
- SearchMidmarketSecurity