Enterprise E-mail Security Best Practice Guidelines

Dr. Steve Arnold
Practice Director, IT Strategy & Information Security
UW E-Business Consortium
University of Wisconsin-Madison
slarnold@wisc.edu
608-890-1291

January 2009

EXECUTIVE SUMMARY

E-mail is the lifeblood of modern business communications.

It forms the foundation of unified messaging (with facsimile and voice mail) and unified communications (unified messaging plus voice, instant messaging, presence, and conferencing). It's required internally to achieve the minimum levels of productivity to compete effectively in the marketplace, and is essential externally to communicate with customers and suppliers.

E-mail is also a potential source of liabilities. E-mail is subject to threats that can be terminal to careers, organizations, and in certain sensitive contexts, such as military operations and espionage, even human lives.

E-mail presents a security challenge. It accepts invalidated, rich-media data, and even programs, from anonymous sources anywhere on the Internet for processing on virtually any desktop, laptop, and handheld computer. It is used ubiquitously for organizational and personal communication, including informal personal correspondence and bulk data transfer.

Users of e-mail expect reliable, near-real-time delivery, even though the Simple Mail Transfer Protocol (SMTP) and its extensions are only architected for best-effort service. The challenge of meeting user expectations is compounded by the fragmented responsibility for the diverse systems and networks that make up the Internet. The cost of high-profile e-mail security incidents, whether they involve sending or receiving malware or sensitive personal information, can easily reach levels attracting board room attention.

It is the objective of this Best Practice Report to briefly explain 10 e-mail security measures with the highest leverage to improve e-mail security and which are often incompletely implemented or inadvertently neglected. The report also provides a self-assessment checklist for periodic review of your e-mail security practices.

SCOPE OF THIS REPORT

This Best Practice Report discusses *enterprise* electronic mail security, that is, the security of organizational e-mail. Consumer e-mail will not be considered here, as it is generally less valuable, subject to different threats and environmental constraints, and far fewer resources are available for its security.

This report is primarily concerned with e-mail systems maintained internally. All organizations should apply all of these best practices. However, if your organization is using hosted e-mail and/or infrastructure services, the service provider(s) should follow those best security practices applying to infrastructure they provide.

INTENDED AUDIENCE

This report is targeted at IT executives, information security professionals, and individuals (postmasters) responsible for managing the company's e-mail system.

TABLE OF CONTENTS