Controlling Outbound E-mail

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

OK, so you have good protection against inbound e-mail carrying viruses, worms, phishing attacks, scams and unwanted content in general. But what about controlling the enormous potential for data leakage and damage to your organization’s reputation represented by outbound e-mail?

In my last column, I mentioned some of the factors to consider in controlling inbound e-mail and principles of performance management for any system. Today I’m pointing to a white paper from Osterman Research commissioned by Permessa Corporation in 2007 and entitled, “Why Your Organization Needs to Focus on Outbound Content.”

The authors point out that about half as many mid-sized and large organizations have outbound e-mail controls as have inbound e-mail controls. Losing control over confidential information, they note, can cost organizations enormous sums in public relations costs and penalties for violating regulations and laws pertaining to personally identifiable information. Uncontrolled e-mail is a channel for data leakage of intellectual property such as trade secrets or strategically important competitive information. Circulation of offensive e-mails within the organization can have serious consequences; the authors cite cases in which “Chevron Oil settled a sexual harassment lawsuit for $2.2 million after four women received offensive email from a fellow employee. Morgan Stanley settled a $60 million lawsuit filed by two employees after they received racist jokes sent through the company’s email system.”

Permessa provides a number of data sheets on several software products for controlling outbound e-mail. For example, their “Email CONTROL! Enforcer” and “Email CONTROL! Premium” products run on IBM Lotus/Notes Domino e-mail systems; “Email CONTROL! Enterprise for Microsoft Exchange” runs on Microsoft Exchange e-mail systems.

For more information about outbound e-mail control, see Andrew Wolff’s excellent overview published in 2006. For a collection of my own columns looking at e-mail policies, see my white paper, “Using E-mail Safely and Well.”

[Disclaimer: I have no financial or other relations to any of the organizations named in this article.]

***

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.
Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.