



KPMG ANALYSIS

Companies Scrambling to Automate E-Mail Encryption

May 18, 2007

By Dave Pelland, Managing Editor, Technology Insider

With accidental data disclosure and e-mail theft becoming rampant, companies are installing content-inspection and encryption software into their networks to protect messages before they leave the building.

Automated encryption software typically examines the source and content of outgoing messages and applies policies that specify which messages get encrypted, using factors such as an e-mail's sender or its subject.

"The kind of publicity associated with information breaches is leading to a lot of interest in encrypting any piece of information that's going out of a firm," says Chip Hay, vice president of marketing for security software provider Code Green Networks. "Companies are looking across the board to avoid information leaks."

Depending on the information and an organization's policies, some messages can be blocked entirely from leaving the firm.

"There's growing interest in policy-based encryption methods [in which] users don't have to keep corporate policies in their heads," Hay says. "Companies want to take that burden off employees and put it in a place where encryption can be automated, and where audit trail records can be kept of everything that's encrypted."

For instance, regulatory requirements may mandate companies to encrypt messages containing customer financial or health data. A company could also automatically encrypt communications being sent by corporate officers or its financial and legal departments.

"With the growth of regulatory compliance demands, organizations want to take [encryption] decisions out of end-users' hands," says Gretchen Hellman, director of product marketing and compliance for Voltage Security. "They don't want to trust the end user to [be forced to] recognize documents having sensitive information that needs to be encrypted. People just forget."

The need to encrypt e-mail is gaining momentum as companies secure channels that allow information to leave their networks, following several incidents in which messages containing personally identifiable information were sent to the wrong recipients.

Last November, Jefferson College in Missouri disclosed that financial data about 143 students was accidentally sent campus wide, and Virginia Commonwealth and the University of Virginia also reported student Social Security numbers were disclosed improperly in e-mail messages or attachments.

Gateway-based encryption systems examine outgoing messages for sensitive information such as credit card or Social Security numbers, or trade secrets such as intellectual property, project code names or software source code.

MORE...

Attachment Spam May Emerge as Malware Vector

AUGUST 8 PDF attachments are the latest effort to evade corporate spam filters, and may foreshadow the use of e-mail attachments as a way to deliver malware.

Selected Technology Company Earnings

JULY 31 Technology and media companies generally reported earnings growth in the second quarter.

Transfer Pricing Risk Hitting Boardroom Agendas

JULY 25 Technology companies face a major challenge in transfer pricing risk as national governments seek new sources of tax revenue.

Product Placement Takes Its Role on the Global Stage

JULY 18 The head of a television studio talks about how product placements are expanding across the globe.

Data Protection Gets Policy, Tech Backing

JULY 11 The focus of enterprise security is shifting to data protection and stronger policies for accessing and storing information.

IT Governance Is a Matter of Information Over Technology

JULY 5 A language barrier between audit committee members and technology officers can severely complicate IT risk oversight.

For Better Security, Web Browsers Go Green

JUNE 26 The latest generation of Web browser certificates could help reduce phishing attacks against banks, retailers and other companies.

"You can set a policy that says any e-mails outbound from someone in the legal department have to be encrypted," says Paul Henry, vice president of strategic accounts for security software provider Secure Computing.

Until a couple of years ago, e-mail encryption depended on desktop software and would require users to encrypt messages manually.

Today, the technology has evolved so that companies can integrate content inspection and encryption software with its e-mail gateway. "The encryption is fully transparent to the users," Henry says. "Users don't have to make encryption decisions -- the content analysis and encryption is done automatically for them."

In some instances, companies are also encrypting internal e-mails, as well as using encryption to guard against disclosure of customer information that could require the company notify to consumers under state data-breach disclosure laws.

Of course, encrypted messages are meaningless if recipients can't open them. Typically, business partners will integrate software into their employees' e-mail programs so messages can be decrypted automatically, such as insurance companies using encryption to communicate with agents and brokers.

But if someone without integrated decryption software is sent an encrypted e-mail, it will generally have an HTML overlay containing instructions on how to authenticate their address and access the message.

Integrating content-inspection software into outgoing e-mail messages can also identify and block sensitive information, such as financial data, that shouldn't be sent in the first place, Hay says. For example, employees attempting to send information that would violate a policy may receive a message explaining how sensitive information should be handled.

"Most information leaks [stem from] accidents or poorly designed business processes," Hay says. "They're not malicious attempts to steal information."

"By automating ways to educate employees, companies are expecting to see the number of incidents go down as employees get smarter about what they're doing."

As encryption software becomes more common for corporate e-mail, software providers say it could also make inroads with companies that want to communicate electronically with customers.

"Companies couldn't send encrypted messages to consumers before, because receiving them was not so easy," says Voltage's Hellman. "We anticipate that e-mail encryption and anti-phishing methods will help enable better customer service and electronic statement delivery."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5

POOR

EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

Submit

© 2007 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative. All rights reserved.

[KPMG Online Privacy Statement and Disclaimer](#)