Top 10 Best Practices in Secure Messaging

Much of corporate email doesn't require special handling. But for that which does, secure messaging technologies enable the use of best practices that help assure compliance and protection of intellectual property in a corporate user and customer-friendly way. Some of these secure messaging best practices are:

1. Content Filtering Implement corporate messaging policies and practices that ensure compliance with the wide range of laws, regulations, and industry practices that affect your company. Compliance begins with detection of sensitive content using an intelligent content filtering solution. Scan message headers, subjects, bodies and attachments of all kinds to detect sensitive information, and information that becomes sensitive when present with other associated information.

2. Policy-Based Message Routing Once you can analyze message content reliably, the next step is to act on what's learned — automatically. Allow it, block it, quarantine it, or direct the message to its destination using the most appropriate of several secure delivery mechanisms. Construct policies that take actions consistent with your corporate messaging policies to protect sensitive content, preferably with a powerful and easy-to-use user interface.

3. Multiple Secure Delivery Mechanisms Several different technologies can be employed to deliver messages securely. Between individuals, traditional S/MIME or PGP encryption and digital signing offers a secure means of delivery but can involve complex key management. Between business partners, S/MIME or TLS encryption between email gateways protects confidentiality over the public Internet. Messages can be delivered securely to anyone using "pull" web delivery mechanism consisting of a notification email with a web link to the message stored securely on the messaging server. Security policies should choose from simple recipient self-registration, or more secure pre-defined accounts. And finally, a "push" delivery mechanism can attach a securely encrypted version of the message to the notification email, openable only by the recipient with the correct password.

4. End-User Self Registration When consistent with your corporate security policies, enabling web delivery recipients to self-register on receipt of first secure message can simplify operations for everyone, including your IT staff and for the end-user. All subsequent interactions with the system should then require end-user authentication.

5. Self-Service Password Management A large portion of help-desk requests deal with forgotten passwords. This overhead should be eliminated by smart and secure end-user self service. End-users should be able to change their passwords with no assistance required from the help-desk, yet ensure that no new avenues of attack are opened.

6. Message Delivery Tracking Senders should be made fully aware of the delivery status of their secure messages, and administrators should be able to comply with auditing requirements.

7. Message Recall Whether a message has become quickly obsolete, or you simply made a mistake and hit "Send" too soon, the option to recall a message can prevent embarrassment and misunderstanding.

8. DMZ Component The messaging server should sit behind the corporate firewall, and a secure relay component in the DMZ should protect the messaging server from potential attack.

9. Corporate Branding For secure delivery mechanisms that touch customers, the extra detail of including your logo in the notification messages adds to confidence and consistently builds your brand.

10. FIPS 140-2 Certified Cryptography The Federal government by directive, and many industries such as financial and health care as a best practice, require the use of FIPS 140-2 validated cryptography in their IT equipment. FIPS-approved cryptography helps assure proper selection and implementation of cryptographic algorithms that form the basis for secure communication.

axway
business. in motion.