Secure in Transmission and Secure behind the Network

A Review of Email Encryption Methods and How They Can Meet Your Company's Needs

By ZixCorp
www.zixcorp.com

zix

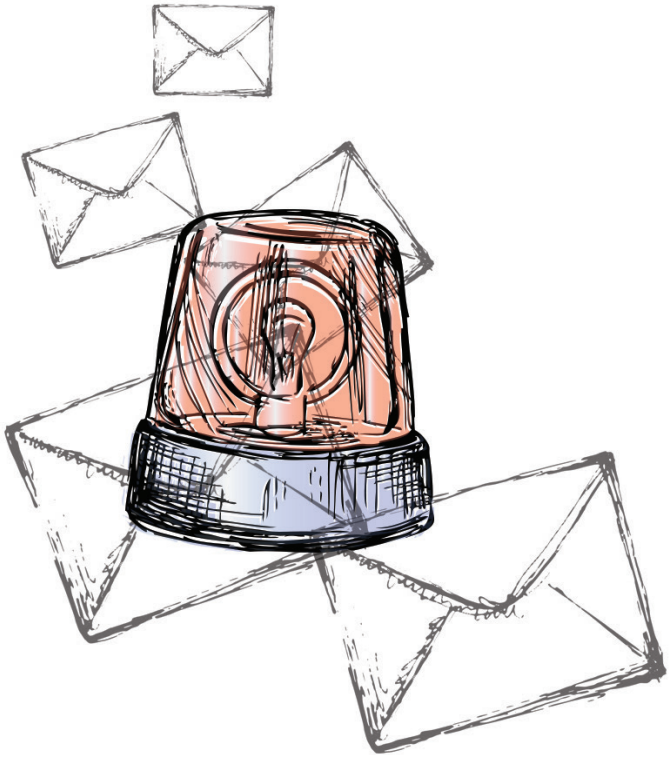
Life moves fast. Work, family and friends often keep us running from one commitment to the next. We take shortcuts to gain a little breathing room and forget a step when we're overwhelmed and falling behind. In a hustle to be early for an off-site meeting, you drive through a red light. Running late for a soccer game, you rush out of the house without locking the backdoor. That pace continues until you're suddenly jolted back to good habits. You see a car accident and drive a bit slower and safer. You hear about a burglary in your neighborhood and become adamant about locking your doors.

The lack of email security is yet another shortcut or forgotten step. While an email breach may not seem as dramatic as a car accident or a burglary, the Snowden revelations and Sony email breach were the jolts that made businesses and the public aware of email's vulnerability and the true sensitivity of this ubiquitous communication tool.

A SHIFT IN AWARENESS AND EXPECTATIONS

In the past, the only discussions people had about email were focused on the never-ending inbox and the amount of time wasted filtering through it. The Snowden revelations changed all that. Suddenly, every mainstream media outlet was covering email and its lack of security. Companies reconsidered how they sent intellectual property outside the office, and the public began asking about safe methods for exchanging personal data with their service providers. But like most jolts, the effect of the Snowden revelations wore off. Companies forgot about the risk of email amidst the flurry of business, and the public became distracted by everyday life.

However, we felt a jolt once again with the Sony email breach. While the public's interest and concern in the Sony breach and email security has momentarily faded, companies cannot ignore the revenue loss, reputational damages and liability associated with unsecure email. Companies can also



no longer excuse a lack of security by telling customers and business partners that they didn't know the risks of email if a breach occurs.

So how do you proactively protect email and your company?

STRONG AND STRONGER EMAIL ENCRYPTION

Encryption makes the contents of email, both the message text and any attachments, indecipherable to unauthorized individuals. Encryption can be used in transit, so that if an unauthorized individual outside the company intercepts an email while it moves across the Internet it cannot be read. Encryption can also be invoked to protect the message both in transit and within the company, so that even unauthorized individuals in the company network are unable to read the message. Both types of encryption offer varying benefits.

Encryption Behind the Network

End-to-end encryption safeguards email in the individual's email system. Anytime an email needs to be protected, the sender uses an encryption key to secure the email. For a recipient to view the email, a decryption key is required to open it. No matter if the email is stored in the Outbox or Inbox, it is always encrypted.

This level of security is appropriate for proprietary content, such as customer lists, intellectual property, earnings data and sensitive executive or board communication. It prevents curious employees from viewing emails that are not relevant to their role and malicious employees from gaining access to information that is valuable to the outside market.

Similarly, end-to-end encryption offers another layer of protection against malicious threats outside your company, known as advanced persistent threats. Despite even the greatest investment in network security and the most attentive IT department, there is no security barrier that is 100% fail proof to hackers attempting to gain access to the company network. Without a guarantee,

companies can use end-to-end encryption to prevent outside, unauthorized individuals from stealing content in the most sensitive emails if they break through network security.

With security a high priority, the use of end-to-end encryption for all emails may be tempting, but its drawbacks shine light on the need to leverage encryption in transit.

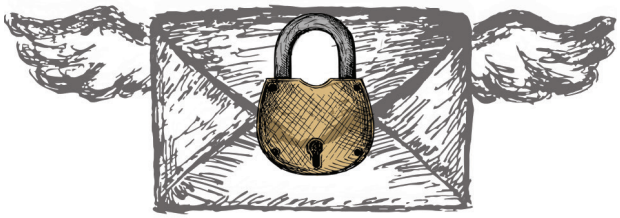
Encryption in Transit

The beauty of email is its ease of use. The exchange of communication and files is seamless with other companies and also with individuals. By forcing senders and receivers to use a key to encrypt and decrypt every message, the convenience of email is lost, and the wide spread adoption of email encryption is too cumbersome to succeed.

In using encryption in transit, your company can take advantage of innovative solutions that not only secure email if it's intercepted over the public Internet but do so without requiring any extra steps from employees, customers and partners. Encryption and decryption happen automatically, keeping business flowing and allowing your company to protect email as it travels outside your network.

Encryption in transit also assists companies in meeting regulatory obligations. If your company conducts business in the healthcare or financial industries, encryption in transit addresses the requirements outlined in the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). It also assists compliance with data privacy laws in several states, such as California, Nevada, Texas and Washington. Even if your company does not operate in a state that has passed privacy legislation, it may be obligated to comply with a state law for simply collecting personal data from a resident in such states as Massachusetts. Encryption in transit helps your company comply without adding a burden to employees and your recipients.

Encryption and decryption happen automatically keeping business flowing



Another benefit of encryption in transit is the convenience of maintaining security. While Target and other retail data breaches did not involve email, the vulnerability exploited in those breaches was the result of missed security patches. With all the responsibilities IT departments hold, it's difficult for patches to be completed in a timely fashion. Unlike end-to-end encryption which requires installation and maintenance on each desktop, solutions for encryption in transit are installed on the network and can offer automatic maintenance through a convenient software-as-a-service model.

BALANCING NEEDS WITH DIFFERENT SECURITY

Both encryption in transit and encryption behind the network protect email from unauthorized individuals viewing and misusing sensitive information. Whereas executive management or departments such as human resources and investor relations may need to secure email with valuable proprietary information at all times, other departments and employees who exchange sensitive information with business partners and customers may only need to protect email in transit. Recognizing the advantages of both encryption methods and how each can be used to meet company needs will enable you to protect email appropriately without unnecessary interference for your employees, customers and partners and your business.

ZixCorp is the leader in email encryption and provides both encryption methods to meet the varying needs of our customers. ZixMail offers encryption behind the network for most corporate email systems and Web-based email. With a single click, your employees can encrypt and decrypt emails and attachments, and your recipients can access secure messages through ZixMail on their desktop or through a secure web portal that can be accessed by anyone, anywhere on any device.

ZixGateway offers encryption in transit, and it is used and trusted by the nation's most influential institutions. With full content scanning of the subject line,

message body and attachments, ZixGateway can automatically encrypt, route, block or brand outbound email based on corporate policies. Through automation, ZixGateway removes risk associated with employee mistakes and relieves employees of the burden of deciding when to invoke encryption, enabling them to focus on their primary responsibilities.

ZixGateway also removes the hassle and stress for recipients. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email and replies are delivered securely and transparently. No extra steps or passwords are needed. Of the 1,000,000 messages encrypted by ZixCorp in a typical business day, 75 percent are exchanged transparently. And, just in case your recipient isn't a ZixGateway user, we use the Best Method of Delivery to deliver encrypted email in the easiest manner – whether that be ZixMail, transport layer security (TLS) or a secure web portal that can be accessed by anyone, anywhere on any device.

Regardless of whether you use ZixMail for encryption behind the network or ZixGateway for encryption in transit, you can be confident that the solution leverages innovative, industry-leading technology, is easy to use for senders and recipients and meets your needs in protecting proprietary company data and other sensitive information.

zixcorp

ZixCorp is a leader in email data protection. ZixCorp offers industry-leading email encryption, a unique email DLP solution and an innovative email BYOD solution to meet your company's data protection and compliance needs. ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government for easy to use secure email solutions. For more information, visit www.zixcorp.com.

Zix Corporation . 2711 N. Haskell Avenue . Suite 2300, LB 36 . Dallas, TX 75204 . 866 257 4949 . sales@zixcorp.com . www.zixcorp.com