WHITEPAPER: Encryption and risk management

Encryption and risk management

Encryption of selected emails is a key part of risk management. Managing that risk effectively starts with a rules-based, policy-driven approach to encryption, which is imposed automatically and deployed as a cloud-based service for the greatest ease of use and hosted in a secure data centre.

Symantec.cloud

Encryption and risk management

Contents

Introduction

When a company executive sends a sensitive memo with details of an upcoming merger in an interoffice envelope over to the CFO for approval, how do you know that the mail clerk didn't take a look inside and is busy selling that information to the competition? Of course, you don't.

Email is a lot faster and more efficient than paper envelopes; and it is easy to get lulled into a false sense of security. It starts on your desktop and ends up on the recipient's desktop, so how could anybody else get hold of it? There are hundreds of ways. Emails are snooped, hacked, altered and stolen every day. Most email is sent 'in the clear' and, with the right tools and a little knowledge, reading somebody else's email is as easy as opening up a paper envelope.
A simple wax seal on a paper envelope has historically been an elegant way to ensure against spying, but in the age of the internet, a digital equivalent is needed. Encryption is the most secure approach to guaranteeing the security of an email in transit, but before it will be adopted, it needs to be better understood. End-users are often resistant to using encryption because of its perceived complexity. Most office workers, when asked to send an encrypted email, don't have a clue as to where to start, and conjure images of smoke-filled Cold War-era spy rooms with agents painstakingly translating encoded messages by hand, a single letter at a time.

In reality, encryption is much easier than it sounds (at least for senders and recipients), but the perception of difficulty remains. Getting end-users to comply is problematic and, even when their compliance is successfully enlisted, there is a subjective element involved. What needs to be encrypted, and what can be sent in the clear? With each end-user left to his or her own devices to interpret security need for each email, the result is inconsistent even in the best of circumstances.

Encryption: who needs it?

Legislative mandates, an increasingly open and far-reaching topic, and competitive threats all create an environment of risk, specifically with regard to data theft, identity theft and industrial espionage. Encryption plays a major role in risk management.

The first element of risk management is determining a level of 'acceptable risk', and then providing mitigating policies and technologies to address unacceptable risks. That somebody would intercept an email inviting co-workers to go to a club after work is more than likely an acceptable risk, and encryption would be unnecessary for such emails. Sending personnel information to your payroll provider? The consequences of loss may be devastating.

The problem, however, lies in deciding what gets encrypted and what does not. In most cases, it's an obvious decision, but it is a process that would be prone to error, were it left to each individual to decide. The decision about which email should be encrypted and which should not is best left to policy-driven technological solutions, rather than individuals. This is the role of Symantec MessageLabs Email Encryption.cloud, part of the Symantec.cloud product suite, which imposes an automatic policy engine to make the encryption decisions for you.

Why don't people encrypt email?

The perception of complexity may be the first roadblock to implementation of encryption technology for email transmission, but the second roadblock is the perception that you just don't need it.

- In 60% of businesses, over 20% of staff work away from the office for more than one day a week.
- In 74% of businesses, employees access three or more applications remotely.
- 85% of businesses expect their mobile workforce to increase.

Legislation in both the US and the UK has imposed strict requirements for data protection. Think you don't need to worry because you don't fall under the jurisdiction of those laws? Think again. In the UK, the Data Protection Act applies to all businesses, and requires companies to take technology-based measures to ensure that email is not seen by unauthorised users.

In the US, tighter controls over HIPAA laws (which govern security of healthcare information) require not only those in the healthcare industry to comply, but everyone who comes in contact with the healthcare industry as well. If you have a client that is a hospital or a healthcare provider in the US, it's very likely that you'll fall under HIPAA's jurisdiction, even if all you're doing is selling them office supplies.

Security managers still face major obstacles in getting end-users to embrace encrypted email. The benefits are obvious – email is more secure, and there is less likelihood that the contents of the email will be seen by somebody who is not authorised to see it. Many of the primary hurdles faced by those security managers are easily overcome. Let's look at a few of the misconceptions of encrypted email, and how they are addressed by Symantec MessageLabs Policy Based Encryption.cloud.

1. "I don't need it." Not every email needs to be encrypted, and front-line employees and clerical staff may fail to see the need for it. Certainly, some individuals within the company may not need it, while others may need it only for selected emails containing certain types of information or which are directed to specific recipients. Symantec.clouds's policy-driven engine decides, based on predetermined rules and internal policy, when encryption is needed and then applies it automatically.
2. "It's too time-consuming." End-users incorrectly believe that encryption requires several extra steps on their part. Sending an email is easy, and they want to keep it that way. Policy Based Encryption.cloud lets users send encrypted messages without any extra steps.
3. "I don't know how." End-users may be resistant to email encryption simply because they are unfamiliar with it. Once deployed, however, sending encrypted emails is largely automatic, and no more difficult than sending a regular clear-text email.
4. "Recipients won't be able to readily decrypt messages." This is another variation of the 'Cold War spy room' misconception – in reality, recipients are able to receive, decrypt and read their messages very easily. Policy Based Encryption.cloud provides both a 'push' and 'pull' method for receiving email. The push method makes the encrypted email accessible directly from the recipient's inbox, while the pull method sends a notification to the recipient, who then retrieves it from a secure URL.
5. "Encrypted email is vulnerable to viruses." This may be true in many cases, as traditional anti-virus software and malware protection systems are not able to scan encrypted text. Policy Based Encryption.cloud, however, enforces the same strong protection against email viruses as is available with clear-text email, through integration with Symantec MessageLabs Email and Web Safeguard.cloud.

The solution: policy-based encryption

Criminals, spies and data thieves have to wade through a lot of very mundane text before they find that valuable pearl they've been looking for. In fact, most emails are very ordinary, and in no need of protection, so in most cases there is no need to impose encryption on those transmissions. But other emails that may contain personal data such as payroll information, financial records or strategic corporate documents should be encrypted.

The problem lies in telling the difference. The decision on whether or not to encrypt is based on two things: internal company policy, and external security and data protection legislation (such as the Data Protection Act in the UK, or

[3]http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html

HIPAA and Sarbanes-Oxley in the US). Policy and compliance are management issues, not meant to be decided or imposed by front-line users, and so it would be a critical mistake to leave the decision on whether to encrypt or not up to those individuals. Rather, the best approach is to create a high-level internal policy, which dictates what types of email should be encrypted, and which creates a set of rules. Said rules would, for example, dictate that emails containing certain types of information be encrypted, or that emails sent to specific recipients, or emails sent from specific employees or departments, should be encrypted.

Enforcing policy is often difficult at best, and is therefore better done on a rules-based, automated basis. This approach takes the guesswork out of the process, and imposes a level of uniformity that is essential to compliance efforts.

The business case: Symantec MessageLabs Policy Based Encryption.cloud

The incidence of data leakage via email is clearly evident, and poses a significant risk. Loss of corporate information, as well as the risk of compromising personal information that must, by legislative mandate, be kept private, requires encryption. When imposing encryption in an email environment, there are several areas that must be addressed, most notably:

1. Anti-virus protection must be maintained with encrypted email transmissions
2. Encryption needs to be easy to use for both end-users that are sending and receiving encrypted emails
3. Encryption must be rules-based and policy-driven, with a system for imposing its use uniformly

Symantec.cloud addresses all three requirements. Because it integrates handily with other Symantec MessageLabs services such as anti-spam.cloud, anti-virus.cloud, content control.cloud and archiving.cloud, users can still be assured of virus-free and malware-free email. End-users need not do anything, and no technical training is required to use email encryption. On the recipient side, encrypted email can be sent to any user. Receiving an encrypted email can be done easily, either by downloading a free software application that integrates with the email client, or by going to a secure URL to retrieve the email. Lastly, Symantec.cloud imposes a rules-based, policy-driven system that automatically makes encryption decisions based on recipient, sender or content.

On the management side, even large corporations often lack security specialists in the IT department, and the implementation and maintenance of encryption must also be simple. This is best approached through a cloud-based system. Symantec.cloud solutions are hosted through their 14 secure data centres (all monitored 24/7), thereby not requiring users to deploy dedicated encryption servers on site. Not only does the hosted approach reduce capital expenditure, it also improves security overall. Hosted data centres typically conform to a much higher set of standards, and Symantec.cloud is no exception.

Find out more about Symantec MessageLabs Policy Based Encryption.cloud - call us today or visit www.symanteccloud.com

Office Locations

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester GL3 4AB
United Kingdom
Main +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone +44(0)800917 7733

DACH
Wappenhalle,
Konrad-Zuse-Platz 2-5,
81829 München,
Deutschland
Tel +49(0)89 94320 120
Support +44(0)870 8503014

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Main +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Freephone +44(0)800 917 7733

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +45 88 71 22 22

BELGIUM/LUXEMBURG
Symantec Belgium
Astrid Business Centre
Is. Meyskensstraat 224
1780 Wemmel
Belgium
Tel +32 2 257 13 00
Fax +32 2 257 13 01

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-Free +1 866 460 0000

CANADA
170 University Avenue
Toronto ON M5H 3B3
Canada
Toll-Free +1 866 460 0000

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: +852 6902 1130

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: +800 120 4415

AUSTRALIA
Level 14
207 Kent Street
Sydney NSW 2000
Australia
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1800 088 099

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku
Tokyo 107-0052
Japan
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: +531 121917

About Symantec.cloud

More than 31,000 organisations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud's MessageLabs services to administer, monitor and protect their information resources more effectively. Organisations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on 14 data centers around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.

For specific country offices and contact numbers, please visit our website:
www.symanteccloud.com

World Headquarters
MessageLabs
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
+44 (0) 1452 627 627