SOPHOS

Who's Snooping on Your Email?

What to look for in a secure email gateway

By **Chris McCormack**, Senior Product Marketing Manager

Since revelations that the U.S. government is collecting massive amounts of data from electronic communications, the notion of online privacy has taken a big hit. Yet the loss of sensitive corporate data is not merely a question of government snooping or corporate espionage. Email poses the highest risk for accidental data exposure, breaches of privacy, or non-compliance with data protection regulations. In this whitepaper we'll help you navigate today's threats to email security. We'll explain the obstacles to compliance and show you why you need a secure email gateway that offers more than just encryption.

A Sophos Whitepaper September 2013

Your email is an open book

Almost all email traffic traverses the public Internet unencrypted in plain text format. It's like sending a postcard in the mail. Anyone that stumbles across it, either maliciously or coincidentally, can read the full content without you ever knowing.

You might be wondering who could be interested in reading your email. What about your ISP or online mail service provider? Google is definitely interested. In a recent court filing, Google acknowledged that Gmail users have no "reasonable expectation" of privacy or confidentiality.[1] In its motion to dismiss a May 2013 class action lawsuit against it, Google stated:

> "All users of email must necessarily expect that their emails will be subject to automated processing. Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their emails are processed by the recipient's [email provider] in the course of delivery. Indeed, a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[2]

That's a "stunning admission," according to the Consumer Watchdog advocacy group, which recommends that people concerned with email privacy shouldn't use Gmail.[3] Unfortunately, that's no solution. It's about as practical as recommending people not use email at all. Even if you don't use Gmail, undoubtedly you have to correspond with customers, partners, or other stakeholders that do.

You might also have heard of PRISM, a clandestine mass electronic surveillance data-mining program run by the U.S. National Security Agency (NSA) for the last several years. The NSA collected and stored untold amounts of messaging traffic from Google, ISPs, and other online mail services like Hotmail and Yahoo.

But the risks with email are not limited to intentional snooping by the likes of Google or the NSA. How many times have you accidentally "replied-all" to an email intended for one recipient? Or accidentally sent an email to the wrong individual thanks to auto-complete in your email client? This happens all the time. And the consequences of sending sensitive information to the wrong person could be devastating, ranging from publicly acknowledging a leak, to fines, loss of trust, reputation damage, and worse.

1 http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

2 http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm

3 http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care

Spoofing, spearphishing and snowshoe spam

Then there's the latest email attacks to consider, such as phishing, which continue to evolve. Phishing is the act of attempting to acquire information such as usernames, passwords or credit card details by masquerading as a trustworthy email.

Phishing is often successful because of a technique known as email address spoofing, where the attackers use addresses in the "from" field that mimic legitimate accounts such as a bank, or even one using your company's domain name to make the email appear to come from an internal sender like your IT department.

The latest trend is to target specific individuals or groups within organizations in a more personal and devious manner—now called spearphishing. Spearphishing is a common tactic of Advanced Persistent Threat campaigns, which aim to gain entry to the target organization's network and obtain confidential information.

Last but not least, there's good old-fashioned email spam. Thanks to your existing anti-spam filter, you're probably not seeing most of it and you can easily identify the odd email from Nigerian princes that gets through.

But people are still susceptible to certain kinds of trickery and can be fooled into opening malicious attachments. Researchers have found that spam appearing to come from a social media site like Facebook is more effective.[4]

Spammers are getting more innovative, using techniques like snowshoe spamming to evade anti-spam filters. Snowshoe spamming, as the name implies, spreads the load out across an enormous number of IP addresses. That makes it difficult for anti-spam filters to catch it all, improving the chances that one might get through to a user's inbox.

Compliance with government regulations

Securing sensitive information for customers, partners, and employees isn't just a best practice—it's often the law. Compliance with regulations is a priority for organizations in healthcare, financial services and government. And even if you're not, you need to consider data protection laws that might affect your customers.

There are a number of regulator acts in nearly every region that dictate compliance and disclosure requirements in the event of a data leak. In the U.S., there's the GLBA governing financial institutions, PCI DSS for payment card security, HIPAA and HITECH for the healthcare sector, and numerous state regulations to consider. And if you're in another jurisdiction, there are similar regulations there too.

What they all have in common are requirements for the encryption of personal information that is either stored or transmitted electronically (via email or otherwise). These laws typically define penalties or fines for non-compliance and disclosure requirements in the event of a leak or breach.

4 "Evolving spammers using bogus social media email to fool users," BizReport, August 28, 2013, http://www.bizreport.com/2013/08/evolving-spammers-using-bogus-social-media-email-to-fool-use.html

Three simple steps to compliance:

1. Start with defining a policy and educating users

Provide your employees and stakeholders with a documented policy that explains the key elements of your data loss prevention strategy. Focus on the types of data you need to protect, your motivations for protecting it, the consequences if you don't, and the procedures to follow to ensure it's protected.

2. Deploy email data protection technology

Your users and policy must be supported by effective, transparent technology. You need a solution to protect from accidental loss and to secure sensitive data that must leave the organization. A secure email gateway with policy-based encryption is an essential element of any effective data protection compliance solution.

3. Start with the essentials, expand over time

Data protection can easily become overwhelming, which is why it's important to prioritize your data protection needs. Start with the most likely source of leaks: email. Make sure you've got the necessary policies in place to protect your most sensitive client, employee, or partner data first—such as credit card numbers, social security numbers and other PII or HIPAA data. Once those policies are running smoothly you should consider broadening your implementation.

What's holding you back?

With all this motivation to secure your email and have an encryption solution in place, what's holding you back?

Complexity: Most email encryption solutions are difficult to source, deploy and manage. You need a significant investment to evaluate and deploy infrastructure that has such wide-reaching impact on the entire company. It would make your life a lot simpler if there was a solution you could drop in place from your existing security vendor—one that doesn't require a big deployment project and specialized staff to manage.

Cost: Most email encryption solutions are expensive in up-front dollars, plus ongoing costs of managing and maintaining the solution. Wouldn't it be ideal if there was an email security solution that offered encryption and DLP within your existing anti-spam budget?

User experience: Most email encryption solutions are disruptive to end-user workflow. They require explicit activity on the part of users to encrypt sensitive email, inviting mistakes. Or users need to deal with encrypted email outside of their normal email workflow, reducing productivity and increasing resistance to adoption. A better solution runs transparently in the background, automatically encrypting email based on DLP polices, without impacting users or requiring new client software.

What to look for in a secure email gateway

Here is a checklist of features to look for in an effective secure email gateway solution for data protection.

Simplicity and ease of management

- Look for a secure email gateway solution that combines anti-spam, DLP, and simple policy-based email encryption in a single product from a single vendor, managed from a single console
- Your selected solution should include pre-defined sensitive data types so it's easy to build DLP policies out of the box
- Ensure the email encryption policies are simple enough that anyone on your staff can easily create new policies or fine-tune existing policies without training or documentation
- Select a solution that doesn't require tedious and complex key management

Great user experience

- An effective email encryption solution should automatically scan both email and attachments for sensitive data types, and encrypt it before it leaves the organization—automatically and transparently, without forcing users to flag emails for encryption (in case they forget)
- Choose an email encryption solution that doesn't disrupt senders or recipients. It should allow users to send email as they always have, using their preferred email client on their desktop, laptop, mobile device, or online
- Your email encryption solution should not require special software or launching a web portal for recipients to view encrypted email

Affordability

- Ideally, select a solution that provides DLP and email encryption within your existing anti-spam budget
- Select a solution that's easy to evaluate and implement—without special hardware, software, or training on top of your existing anti-spam solution

Sophos SPX Encryption and Data Loss Prevention

With our innovative, patent-pending SPX encryption and integrated DLP policy with pre-packaged sensitive data types, Sophos has the answer for your data protection needs.

It's simple to deploy, integrating anti-spam, email encryption and data loss prevention into a single appliance with no special client software to install.

It's easy to manage everything from a single intuitive console with no encryption keys or certificates to manage and an elegant DLP wizard that will have you up and running in minutes.

Our DLP engine comes with hundreds of pre-packaged sensitive data types so you can create effective DLP polices right out of the box. You can easily create your own custom types too.

It's completely transparent to users, allowing them to use their preferred email client (including their mobile device). And it's affordable—with all these features included in our Sophos Email Appliance for about what you're paying for anti-spam alone (available in our UTM Email Protection version 9.2, out in late 2013).

Free Trial at Sophos.com

Try a Sophos Email Appliance

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

09.13.wpna.simple

SOPHOS