SOPHOS

¿Quién husmea en su correo electrónico?

Características deseables en una puerta de enlace de correo electrónico segura

Por **Chris McCormack**, Director sénior de marketing de productos

Desde que se supo que el gobierno estadounidense recopila cantidades ingentes de datos de comunicaciones electrónicas, la noción de privacidad online ha sufrido un duro golpe. No obstante, la pérdida de datos corporativos confidenciales no es meramente una cuestión de espionaje gubernamental o corporativo. El correo electrónico plantea el mayor riesgo de exposición accidental de datos, pérdida de privacidad o incumplimiento con las leyes de protección de datos. En este monográfico le ayudaremos a entender las amenazas actuales a la seguridad del correo electrónico. Le explicaremos los obstáculos para cumplir con la legislación vigente y le mostraremos las razones por las que necesita una puerta de enlace de correo electrónico segura que le ofrezca algo más que cifrado.

Un monográfico de Sophos noviembre de 2014

Su correo electrónico es un libro abierto

Casi todo el tráfico de correo electrónico atraviesa puntos públicos de Internet sin cifrar en formato de texto plano. Es como enviar una postal por correo. Cualquier persona que tropiece con él, ya sea de forma maliciosa o por coincidencia, podrá leer el contenido completo sin que usted lo sepa nunca.

Se preguntará a quién podría interesar leer su correo electrónico. ¿Qué tal su proveedor de acceso a Internet o de correo electrónico? A Google sin duda le interesa. En un juzgado Google confirmó recientemente que los usuarios de Gmail no pueden tener "ninguna expectativa razonable" de privacidad o confidencialidad.[1]En su moción para desestimar una demanda colectiva de mayo de 2013 contra la empresa del buscador, Google declaró:

> "Todos los usuarios de correo electrónico deben necesariamente esperar que sus correos electrónicos sean tratados de forma automática. Al igual que a un remitente de una carta a un compañero de empresa no puede sorprenderle que el asistente del destinatario abra la carta, la gente que usa soluciones de correo electrónico basadas en web no puede pretender que sus correos electrónicos no sean procesados por el proveedor de correo electrónico del recipiente en el transcurso de la entrega. De hecho, una persona no puede tener la legítima expectativa de privacidad con respecto a la información que entregue voluntariamente a terceros."[2]

Esta es una "sorprendente admisión", según el grupo de defensa del consumidor Watchdog, que recomienda que las personas preocupadas por la privacidad de su correo electrónico no usen Gmail.[3] Lamentablemente, esa no es ninguna solución. Es tan práctico como pedirle a la gente que no use el correo electrónico de forma alguna. Incluso si no utiliza Gmail, sin duda tiene que escribirse con clientes, socios u otras personas que lo hacen.

Puede que también haya escuchado hablar de PRISM, el programa masivo de minería de datos y vigilancia clandestina gestionado por la Agencia de seguridad nacional (NSA) estadounidense durante los últimos años. La NSA ha recopilado y almacenado incalculables cantidades de mensajes remitidos a través de Google y otros proveedores de acceso a Internet, así como de servicios de correo electrónico como Hotmail y Yahoo.

Pero los riesgos con el correo electrónico no se limitan a que Google o la NSA los analicen de manera intencionada. ¿Cuántas veces "respondió a todos" accidentalmente al querer enviar un correo electrónico a un solo destinatario? O envió un correo electrónico accidentalmente a una persona equivocada gracias a la función de autocompletar en su programa de correo electrónico? Este tipo de cosas suceden todo el tiempo. Y las consecuencias de enviar información confidencial a la persona equivocada podría ser devastadora; desde reconocer públicamente una fuga, a multas, pérdida de confianza, daños a la reputación, y cosas peores.

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

Suplantación de identidad y otras técnicas de phishing

Además hay otra serie de ataques de correo electrónico que debería tener en cuenta, como el phishing y sus derivados. Phishing es el acto de intentar adquirir información como nombres de usuario, contraseñas o información de la tarjeta de crédito mediante un correo que simula provenir de una fuente de confianza.

El phishing suele tener éxito al ser una técnica basada en la suplantación de direcciones de correo electrónico (spoofing) en la que los atacantes utilizan direcciones en el campo "de" que imitan direcciones de correo electrónico de cuentas legítimas de, por ejemplo, un banco, o incluso que parecen provenir del dominio de su propia empresa (como si el remitente fuera alguien del departamento de TI).

La última tendencia es concentrarse en determinados individuos o grupos dentro de organizaciones de forma más personal y astuta, lo que se conoce como "spearphishing". El "spearphishing" es una táctica común de las campañas de amenaza avanzadas persistentes (APTs por sus siglas en inglés) cuyo objetivo es acceder a la red de una entidad y obtener información confidencial.

Casi para terminar también tenemos los clásicos correos electrónicos de spam. Gracias a su filtro anti-spam existente, probablemente no vea la mayoría de ellos y si los encuentra, podrá identificar fácilmente el clásico correo electrónico de un príncipe nigeriano.

Pero la gente aún puede sucumbir a ciertos engaños y acabar abriendo archivos adjuntos maliciosos. Los investigadores han determinado que el spam que parece provenir de redes sociales como Facebook es más efectivo. [4]

Los spammers cada día innovan más y utilizan técnicas como el spam distribuido a fin de evitar los filtros anti-spam. Es lo que se conoce en inglés como "snowshoe spamming" y que básicamente consiste en distribuir los correos a través de una ingente cantidad de direcciones IP. Esto dificulta que los filtros anti-spam puedan detectar todos los correos, mejorando las posibilidades de que uno llegue a la bandeja de entrada del usuario.

Cumplimiento con las regulaciones gubernamentales

Asegurar la información confidencial de los clientes, socios y empleados no es solo una mejor práctica, sino que a menudo es requerido por la ley. El cumplimiento con las regulaciones vigentes es una prioridad para las empresas en sectores como los de la salud, servicios financieros y gubernamentales. E incluso si usted no trabaja en una de ellas, debe tener en cuenta las leyes de protección de datos que puedan afectar a sus clientes.

Hay una serie de regulaciones en casi todas las regiones del mundo que enumeran los requisitos a cumplir en caso de una fuga de datos. En los Estados Unidos está la GLBA que rige a las instituciones financieras, la PCI DSS para la seguridad de las tarjetas de pago, la HIPAA y HITECH para el sector sanitario, así como otras muchas regulaciones estatales que se han de tener en cuenta. Y si está en otra jurisdicción, hay regulaciones similares allí también. La Normativa de protección de datos de la UE que entrará en vigor en 2015 incluye numerosos requisitos que se habrán de cumplir.

Lo que todas tienen en común son los requisitos para el cifrado de la información personal que se almacena o transmite por vía electrónica (por correo electrónico o de otra manera). Estas leyes suelen determinar sanciones o multas en caso de que no se cumplan las mismas o ante casos de fugas o acceso indebido a los datos.

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

Tres pasos muy sencillos para cumplir con las normas:

1. Comience definiendo una política y educando a los usuarios

Proporcione a sus empleados y partes interesadas una política documentada que explique los elementos claves de su estrategia de prevención de pérdida de datos. Céntrese en los tipos de datos que necesita proteger, sus razones para protegerlos, las consecuencias de no hacerlo y los procedimientos a seguir para asegurarse de que estén protegidos.

2. Implante tecnologías de protección de datos de correo electrónico

La política que implante y las habilidades de sus usuarios deberán estar respaldadas por una solución tecnológica eficaz, transparente y sencilla. Necesita una solución que le brinde protección frente a la pérdida de datos de forma accidental y que proteja los datos sensibles que deben salir de su empresa. Una pasarela de correo electrónico segura basada en una política de cifrado es un elemento esencial de cualquier solución de protección de datos efectiva.

3. Comience con lo básico y amplíela a lo largo del tiempo

La protección de datos puede llegar a ser fácilmente abrumadora, por lo que es importante dar prioridad a sus necesidades de protección de datos. Comience con la fuente más probable de fugas: el correo electrónico. Asegúrese de que dispone de las políticas necesarias para proteger los datos más importantes de clientes, empleados, socios, tales como números de tarjetas de crédito, números de seguridad social u otros datos de tipo PII o HIPAA. Una vez que esas políticas están funcionando sin problemas debe ampliar su aplicación.

¿Qué es lo que le está deteniendo?

Con toda esta motivación para asegurar su correo electrónico y disponer de una solución de cifrado, ¿qué le está impidiendo implantarla?

La complejidad: La mayoría de soluciones de cifrado de correo electrónico son difíciles de encontrar, desplegar y administrar. Necesita una inversión significativa para evaluar e implementar una infraestructura que tiene un gran impacto en toda la empresa. Su vida sería mucho más sencilla si hubiera una solución que su proveedor de seguridad existente pudiera implantar, una que no requiriera un gran despliegue ni personal especializado que la gestionara.

Costes: La mayoría de soluciones de cifrado de correo electrónico son caras al principio, además de suponer una serie de costes continuados derivados de su gestión y mantenimiento. ¿No sería ideal si hubiera una solución de seguridad de correo electrónico que ofreciera cifrado y prevención de pérdidas de datos dentro de su presupuesto actual contra el spam?

Experiencia de usuario: La mayoría de las soluciones de cifrado de correo electrónico perjudican el flujo de trabajo del usuario. Básicamente porque requieren la intervención del usuario para cifrar correos electrónicos sensibles, lo que puede inducir a errores. O los usuarios necesitan utilizar flujos diferentes para acceder a correos cifrados, lo que reduce su productividad y aumenta la resistencia a su adopción. Una solución mejor se ejecuta de forma transparente en el trasfondo y cifra de forma automática los correos electrónicos siguiendo políticas de prevención de pérdida de datos, sin impactar de forma alguna en los usuarios o requerir nuevo software cliente.

Características deseables en una puerta de enlace de correo electrónico segura

A continuación le presentamos una lista detallada con las características deseables en una solución de puerta de enlace de correo electrónico segura para protección de datos.

Simplicidad y facilidad de administración

- Busque una solución de puerta de enlace de correo electrónico segura que combine anti-spam, prevención de pérdidas de datos y el cifrado de correo electrónico de acuerdo con políticas sencillas en un solo producto y de un solo proveedor, y todo gestionado desde una única consola.
- Debería seleccionar una solución que definiera de antemano los datos sensibles de manera que sea fácil implantar políticas de prevención de pérdida de datos en cuanto se comience a usar.
- Asegúrese de que las políticas de cifrado del correo electrónico sean lo suficientemente sencillas como para que cualquier persona en su empresa pueda crear fácilmente nuevas políticas o afinar las mismas, sin necesidad de tener que pasar por cursos de formación o leer documentación.
- Seleccione una solución que no requiera la tediosa y compleja tarea de gestionar claves.

Fantástica experiencia de usuario

- Una solución de cifrado de correo electrónico debería escanear automáticamente tanto los correos electrónicos como sus archivos adjuntos en busca de datos sensibles y cifrarlos antes de que salgan de la organización (de forma automática y transparente, sin forzar a los usuarios a marcar aquellos mensajes que requieran de cifrado para que así no se les olvide).
- Elija una solución de cifrado de correo electrónico que no interfiera con los remitentes o destinatarios. Debería permitir a los usuarios enviar correos electrónicos como siempre han hecho, utilizando su cliente de correo electrónico preferido en su equipo de sobremesa, portátil, dispositivo móvil o bien vía web.
- Su solución de cifrado de correo electrónico no debería requerir un software especial o necesitar que los receptores tuvieran que abrir un portal web determinado a fin de poder ver un correo cifrado.

Asequible

- Lo ideal sería encontrar una solución de cifrado de correo y de prevención de pérdidas de datos que encajara con su presupuesto actual anti-spam.
- Seleccione una solución que sea fácil de evaluar e implementar, que no requiera formación y que se pueda desplegar sobre su solución anti-spam, software o hardware actual y sin necesidad de añadir nada especial.

¿Quién husmea en su correo electrónico?

Prevención de pérdida de datos y cifrado SPX de Sophos

Con nuestra innovadora tecnología de cifrado de datos SPX (con patente en curso) y las políticas de prevención de pérdidas de datos integradas con las diferentes tipologías de datos sensibles pre-definidas, Sophos tiene la respuesta para sus necesidades de protección de datos.

Es fácil de implementar, integra anti-spam, cifrado de correo electrónico y prevención de pérdida de datos en un solo producto que no requiere la instalación de ningún software cliente especial.

Permite un fácil manejo de todo desde una única consola intuitiva que no necesita administrar claves de cifrado o certificados, así como cuenta con un elegante asistente de creación de políticas de prevención de pérdidas de datos que tendrá funcionando en minutos.

Nuestro motor de políticas de prevención de pérdidas de datos incorpora de forma pre-definida cientos de tipologías de datos sensibles a fin de que pueda implementar la política que necesita con tan solo instalarlo. Podrá además crear sus propias políticas de forma personalizada.

Es totalmente transparente para los usuarios y les permite usar su cliente de correo electrónico preferido (incluyendo el de sus dispositivos móviles). Y es además asequible, dado que todas estas funciones vienen incluidas en Sophos Email Appliance y Sophos UTM Email Protection por prácticamente lo que ahora paga únicamente por su solución anti-spam.

Pruebe Sophos Email Protection con cifrado SPX

Ventas en el Reino Unido e internacionales
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Australia y Nueva Zelanda
Línea gratuita: 1 866 866 2802
Correo electrónico: nasales@sophos.com

Oxford (Reino Unido) | Boston (EE. UU.)

SOPHOS

11.14.wpna.simple