

...EL CUMPLIMIENTO DE NORMATIVAS DE EMAIL

Los directores de sistemas y gerentes informáticos de sectores tan regulados como el sanitario o el financiero, o de empresas grandes que cotizan en Bolsa son muy conscientes de qué es necesario para el cumplimiento de las normativas de email. En empresas más pequeñas o privadas y sectores no regulados, el cumplimiento de estas normativas no suele estar claro, y la aparente complejidad y las serias consecuencias de su incumplimiento pueden resultar sobrecogedoras.

La preocupación no tiene justificación alguna. La mayoría de empresas utilizan un conjunto formal de pautas claramente definidas que garantizan la adherencia tanto a las leyes formales como a los estándares éticos y prácticas aceptadas. Estas pautas deberían establecer también el tratamiento de desviaciones, accidentales o de cualquier otro tipo. La ausencia de estas pautas hace que la respuesta positiva y eficaz a auditorías o, lo que es peor, a investigaciones legales resulte extremadamente difícil.

El presente documento analiza el cumplimiento de normativas en lo relacionado con el correo electrónico, ofreciendo pautas simples y claras para la administración de las infraestructuras de correo electrónico*.

DEFINICIÓN

"Cumplir las normativas" significa estar en concordancia con las pautas, especificaciones o leyes establecidas, o encontrarse en proceso de estarlo.

1 Establecer reglas claras sobre el uso del correo electrónico

El correo electrónico es la herramienta fundamental de comunicación, tanto interna como externa, en la vida diaria de las empresas. El correo electrónico puede contener hasta un 80% de los registros empresariales y por eso es esencial establecer reglas para su utilización.

El punto de partida es la definición de un marco de comportamiento claro y transparente que establezca qué usos son aceptables y cuáles no. Una política de uso aceptable explícita, a nivel empresarial, cuyo uso pueda auditarse y con reglas aplicables, supone un primer paso sencillo para manifestar la intención de cumplir normativas y un gran avance a la hora de evitar responsabilidades legales. Como ejemplo, cláusulas habituales podrían ser:

- no enviar o reenviar mensajes de correo electrónico que contengan imágenes pornográficas
- limitar el tamaño de los archivos adjuntos a 5MB.

Una vez creada la política de uso aceptable, asegúrese de que sus prácticas cumplen la amplia gama de leyes locales, regionales, nacionales e internacionales que afectan a las comunicaciones por correo electrónico.

Existe una gran variedad de ejemplos en Internet.

2 Evitar la pérdida de datos a través del correo electrónico

Los datos que residen en los sistemas son información empresarial de valor que debe protegerse con cuidado contra la revelación accidental o deliberada de información confidencial a terceros fuera o, en ocasiones, dentro de la empresa. La política de uso aceptable cubre algunos de los procesos, pero tanto empleados nuevos como aquellos que dejen la empresa, distraídos o disgustados, pueden poner en peligro la seguridad de los datos.

Es fundamental crear un mecanismo automatizado y administrado de forma central para evitar la pérdida de datos, independientemente de las intenciones de los trabajadores. Dicha solución debería:

- bloquear mensajes por el tipo de archivo adjunto
- escanear mensajes según palabras clave
- añadir exenciones de responsabilidad y letreros al correo en todas las direcciones
- cifrar mensajes para que sólo pueda leerlos el destinatario que se pretende
- evitar el abuso del sistema de correo por parte de usuarios desconocidos o maliciosos.

3 Mantener la transparencia y el acceso al tráfico anterior y actual

Asegúrese de que conoce y puede dar cuenta de los mensajes de correo electrónico entrantes, salientes y que circulan por su empresa. Es su responsabilidad:

- Conservar un historial accesible de las comunicaciones por email relevantes, con información de registros que muestren quién envió qué a quién y cuándo.
- Copiar o archivar mensajes delicados, tanto internos como externos.
- Poder interceptar mensajes que no cumplan las normativas y redirigirlos a los responsables de aplicarlas, para evitar incidentes y poner soluciones en práctica.

Es importante darse cuenta de que no todos los mensajes contienen datos delicados, por lo que no es necesario archivarlos o cifrarlos todos. Según su competencia, existen también límites en el tiempo que deben conservarse las copias de las comunicaciones por email.

De hecho, los costes del almacenamiento y acceso a grandes volúmenes de correo electrónico hacen que sea necesaria una actitud determinista a la hora de decidir qué debe archivarse o cifrarse, y por cuánto tiempo.

4 Eliminar spam, pesca de información y programas maliciosos

El correo electrónico es uno de los medios principales de entrada de programas maliciosos en ordenadores y sistemas. Las campañas de spam cambian muy rápidamente para intentar burlar la detección, utilizando gran variedad de medios, como troyanos de registro de pulsaciones del teclado o enlaces a sitios web maliciosos, con la finalidad de robar información empresarial confidencial y personal.

Es necesario estar seguro y poder demostrar que la infraestructura de correo está protegida contra programas maliciosos, virus, programas espía y otras amenazas para la integridad del sistema y de los datos. Para ello, es necesaria una solución que bloquee programas maliciosos, spam, ataques de denegación de servicio y recopilación de direcciones de email.

El bloqueo de las amenazas en el perímetro de los servidores de correo internos y estaciones elimina la mayor parte del riesgo externo asociado con la pérdida de datos. La política de uso aceptable contribuirá en gran medida a evitar el riesgo interno restante.

SEGÚN LOS ANALISTAS

"Puesto que las estrategias de mensajería deben combinar el bloqueo de programas maliciosos con el filtrado de contenido, el cumplimiento de normativas, medios de prueba de fuentes electrónicas y archivos, es necesario un conjunto de productos que reduzcan la carga administrativa, que satisfagan las necesidades del cliente y que minimicen las interrupciones provocadas por vulnerabilidades nuevas o cambios en las normativas."

Christian Christiansen, Vicepresidente de Servicios y Productos de Seguridad, IDC

Sophos Email Security and Control ofrece una gama de soluciones de hardware y software para proteger la infraestructura de correo al completo contra amenazas y permitir el cumplimiento de los requisitos normativos. Funciona en conjunción con Sophos Endpoint Security and Control y Sophos Web Security and Control para ofrecer una protección completa de la red que permita prácticas de cumplimiento adecuadas. Para más información sobre estos productos y cómo probarlos, visite esp.sophos.com.

Sophos es un líder mundial en seguridad y control de sistemas informáticos. Ofrecemos protección completa para empresas, educación y gobiernos: defensa contra programas malintencionados, intrusión, programas espía, aplicaciones no deseadas, spam y abuso de políticas internas, además de control de acceso a la red (NAC). Nuestros productos, caracterizados por su gran precisión y facilidad de uso, protegen a más de 100 millones de usuarios en más de 150 países. Con más de 20 años de experiencia y una red global de centros de análisis de amenazas, respondemos rápidamente ante amenazas emergentes y mantenemos el más alto nivel de satisfacción del cliente. Sophos es una empresa global con sede central en Oxford, GB.

Boston, EE.UU. • Mainz, Alemania • Milán, Italia • Oxford, GB • París, Francia
Singapur • Sydney, Australia • Vancouver, Canadá • Yokohama, Japón

© Copyright 2007. Sophos Plc. Todos los derechos reservados. Otras marcas registradas por sus propietarios.

**Exención de responsabilidades: el presente documento no pretende sustituir otra orientación legal profesional o problemas de cumplimiento de normativas que puedan afectar a su empresa. Para determinar sus necesidades, es aconsejable que pida ayuda a expertos reconocidos en materia de cumplimiento de normativas.*