HORNETSECURITY®

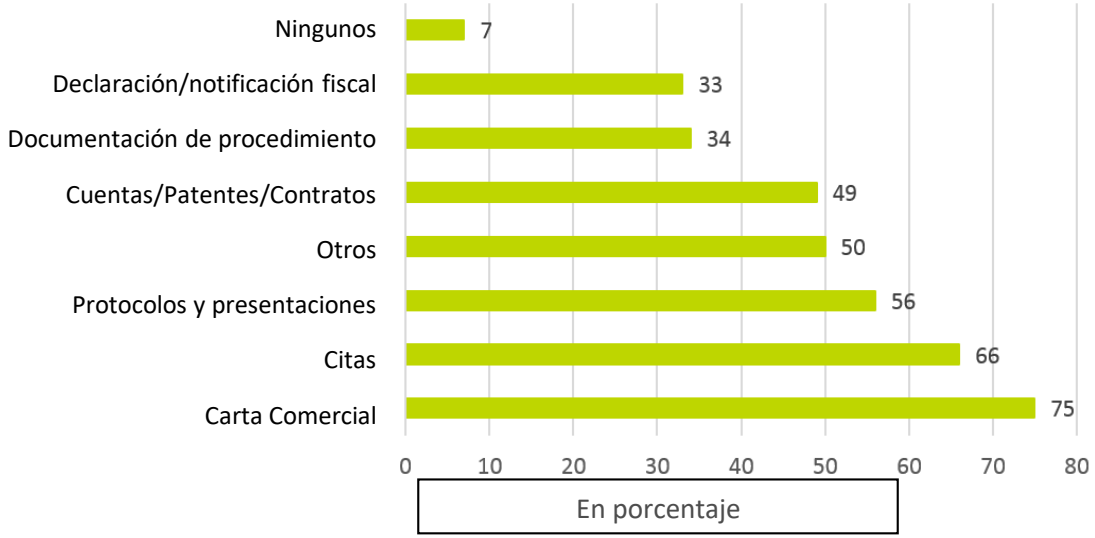
Cifrado de Correo de Hornetsecurity

Extensión y límites de utilización

- El cifrado de correo se puede comparar con https en el internet
- El uso de correo electrónico es, generalmente sin cifrado
- ¿Porqué no se usa el cifrado? Porque es:
  - Difícil de configurar
  - Propenso a fallar, sobre todo con sistemas de destino
  - Poco conocimiento del *Know-How* del área
  - Ignorancia / falsa confianza

Problema Seguridad de correo

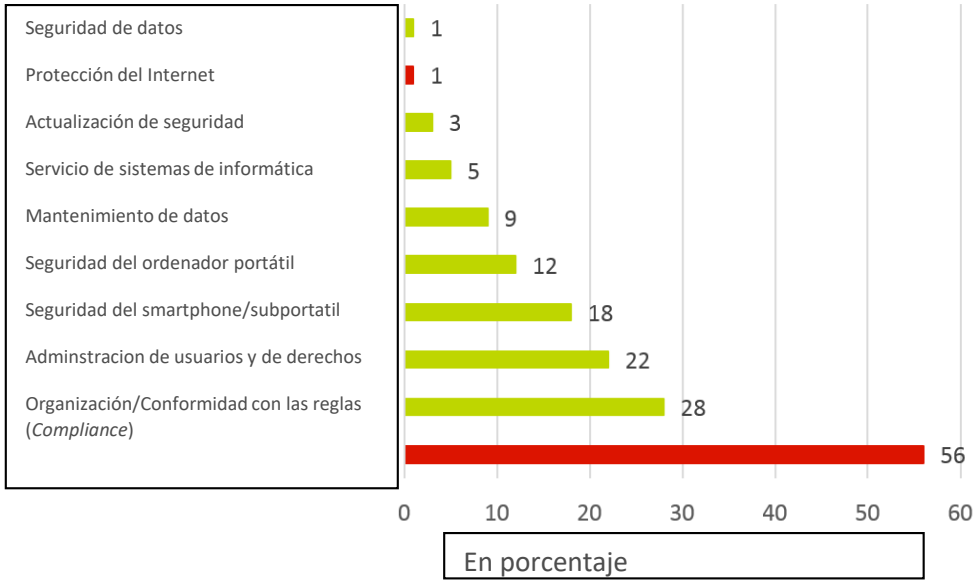
- ¿Cuáles son las informaciones confidenciales/relevantes que se envían por correo electronico y son importantes para el negocio?



Origen: Deutschland sicher im Netz e.V. – Leitfaden Verschlüsselung von E-Mails, 2012

La discrepancia de seguridad de Internet frente a la seguridad de correo electrónico

¿Qué medidas de protección NO toman las empresas medianas?



Fuente: Deutschland sicher im Netz e.V. – Studie zur Sicherheitslage im Mittelstand, 2013

La seguridad de Internet y del correo electrónico se confunden a menudo, pero son muy diferentes.

Ventajas de Cifrado de Correo

- Confidencialidad: Informaciones que necesitan ser protegidas están seguras (Otros no pueden leer los correos electrónicos, protección contra piratería de datos)
- Integridad: No se puede cambiar el contenido de los correos electrónicos
- Autenticidad: El remitente y el destinatario son conocidos
- Protección de datos: La protección de datos se cumple
- Las condiciones se llevan a cabo en común acuerdo con el socio: por ejemplo la protección de informaciones confidenciales cuando un negocio empieza

El cifrado – ¿Cómo funciona?

- Se necesitan dos llaves: 1 privada, 1 pública
- El método se puede comparar con un buzón

  "Todo el mundo puede echar una carta, pero solo el que tiene la llave la puede abrir"
- La función es de 2 caminos

  "La ida es fácil, pero solo se puede volver con la llave adecuada"

El cifrado – ¿Cómo funciona?

- Cada llave (pública o privada) puede cifrar
  - Cada par de llaves esta adjudicado al otro
  - Solo estas dos llaves funcionan juntas
- La llave privada cifra
  - Solo la llave pública que le corresponde puede descifrar con éxito
- La llave pública descifra
  - Sólo la llave pública correspondiente puede descifrar con éxito

El cifrado – ¿Cómo funciona?

La llave privada cifra

- Sólo la llave pública correspondiente puede descifrar con éxito
- Se sabe de quien es la llave privada correspondiente, por eso el remitente es conocido (autenticidad del remitente)
- El contenido no fue cambiando por parte de terceras personas después de el cifrado (integridad del contenido)

El cifrado – ¿Cómo funciona?

La llave pública cifra

- Solamente la llave pública correspondiente puede descifrar con éxito
  - Después de que la noticia haya sido cifrada, sólo puede ser descifrada y leída por una persona (confidencialidad del contenido)

El cifrado – ¿Cómo funciona?

Cifrado y descifrado

Remitente:

E-Mail original + Frimar (Llave privada del remitente) + Codificar (Llave pública del destinatario) = E-Mail codificado y firmado

Destinario:

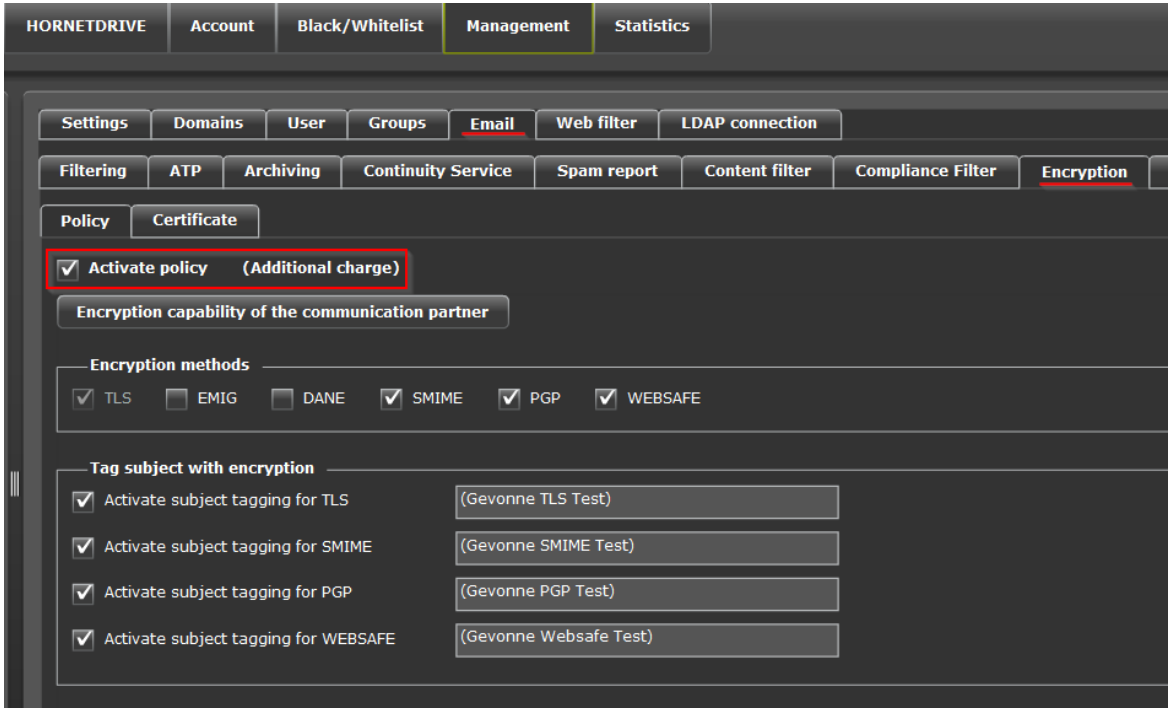
E-Mail cifrado y firmado + Descifrar (Llave privada del destinatario) + Comprobar la firma (Llave pública del remitente) = E-Mail original descifrado y controlado

Comparación S/MIME y PGP

Característica	S/MIME	PGP
Cifrado del contenido	Sí	Sí
Firma de noticias	Sí	Sí
Llave autentificacion	Central (PKI/Root CA)	Decentral (intercambio directo)
Esfuerzo de administración	Más bien poco	Más bien alto
Costos de la llave	Sí	Más bien poco
Asistencia por clientes de correo	Sí (integrado)	No (solo por Add-On)
Costos para aplicación local	alto	Muy alto
Costos para el servicio del Gateway	poco	poco

Cifrado de Correo de Hornetsecurity

- ¡Un clic es suficiente!



Cifrado de Correo de Hornetsecurity

Compliance, transparencia y control

Resumen del trafico de correo electrónico cifrado, cuidado central de reglas y directivas.

Uso fácil

Ningún esfuerzo de administración por parte del usuario.

Protección contra piratería

Una solución fuerte de cifrado de correo protege el correo electrónico comercial.

Simple administración

Una manera muy fácil de establecer el cifrado de correo electrónico y administrarlo.

Cifrado de Correo de Hornetsecurity

Compliance, transparencia y control

- Protección de datos
- Rastreo de E-Mail
- Directivas claras de cifrado para toda la compañía

Cifrado de Correo de Hornetsecurity

Uso fácil

- Cifrado automático
- Descifrado automático
- Control del cifrado por palabra clave en el asunto (sujeto)

Cifrado de Correo de Hornetsecurity

Protección contra piratería

- Certificados personalizados de E-Mail para cada usuario
- *Websafe*
- Uso de diferentes tecnologías de cifrados y protocolos
  - S/MIME
  - PGP
  - TLS incluido *Perfect Forward Secrecy*

Cifrado de Correo de Hornetsecurity

Simple Adminstración

- Test de validez del cifrado de los intermediarios
- Manejo de certificados de usuarios en el panel de control
- Adaptación individual de directivas para el cifrado en planos de dominio: grupos y usuarios
- Nivel alto de automatización– no hace falta administrar los certificados
- Vigilancia y soporte 24/7
- Escabilidad completa
- Actualización automática