Válido desde	01.06.202016
Válido hasta	01.10.2028
Próxima revisión:	01.10.2027
Persona(s) responsable(s)):	Olaf Petry, CISO
Confidencialidad	Pública

Información sobre protección de datos

Servicios de seguridad gestionados

Grupo Hornetsecurity

Información sobre protección de datos para los servicios ofrecidos

I. Introducción ... 3
1. Base ... 3
2. Información de contacto ... 3
II. Información general sobre el tratamiento de datos ... 6
1. Alcance del tratamiento de datos personales ... 6
2. Fundamento jurídico del tratamiento de datos personales ... 6
III. Tratamiento de datos para el funcionamiento de los *servicios* ... 7
1. Datos básicos ... 7
a. Datos maestros ... 7
b. Datos de configuración ... 7
2. 365 Permission Manager ... 8
3. 365 Total Backup ... 8
4. 365 Total Protection ... 9
5. 365 Total Protection Enterprise Backup ... 11
6. AI Cyber Assistant: AI Email Security Analyst ... 11
7. AI Cyber Assistant: AI Recipient Validation ... 11
8. AI Cyber Assistant: Conversational Agent ... 12
9. AI Cyber Assistant: Teams Protection ... 12
10. Inicio de sesión en el Panel de Control ... 13
11. Inicio de sesión en el correo web de Hornet.email ... 13
12. Hosted Exchange ... 14
13. IA, uso de la inteligencia artificial ... 14
a. Introducción ... 14
b. Finalidad del tratamiento ... 14

c. Datos recopilados por nosotros 15
d. Herramientas de IA, almacenamiento y conservación de datos 16
14. Security Awareness Service 17
15. Spam and Malware Protection 18
a. Opcional: Advanced Thread Protection (ATP) 19
b. Opcional: Secure Links (como parte de ATP) 19
c. Opcional: Email Encryption 19
d. Opcional: Archiving 20
e. Opcional: Continuity Service 21
f. Opcional: Signature and Disclaimer para correo electrónico 21
g. Opcional: E-Mail made in Germany 21
16. Test-Onboarding 22
17. VM Backup 22
18. Web Filter 23
19. Websafe, política de privacidad para terceros 23
IV. Posibilidad de oposición y eliminación 24
V. Derechos del interesado 24
a. Derecho de acceso (conforme al art. 15 del RGPD) 24
b. Derecho de rectificación (conforme al art. 16 del RGPD) 24
c. Derecho de supresión (conforme al art. 17 del RGPD) 24
d. Derecho a la limitación del tratamiento (conforme al art. 18 del RGPD) 24
e. Derecho a la portabilidad de los datos (conforme al art. 20 del RGPD) 24
VI. Destinatarios de los datos 25
VII. Transferencia de datos a terceros países 25

I. Introducción

1. Base

La base de una protección de datos eficaz es una información exhaustiva sobre la recogida, el tratamiento y el uso de sus datos («tratamiento de datos»). Por ello queremos informarle sobre lo siguiente:

- cuándo o en qué tipo de acciones tratamos datos,
- qué datos tratamos y por qué motivos,
- quién recibe los datos y
- qué derechos le asisten por el tratamiento de datos que realizamos.

Esta información sobre protección de datos se refiere únicamente al uso de datos personales en el contexto de los *servicios*. Siempre podrá descargar esta información sobre protección de datos en https://www.hornetsecurity.com/service-privacy-statement/.

2. Información de contacto

El cliente es siempre responsable del tratamiento de datos en el ámbito de los *servicios* en el sentido del Reglamento General de Protección de Datos (RGPD). Hornetsecurity actúa como responsable del tratamiento en el sentido del art. 28 del RGPD. Algunos de los servicios también son prestados por otras empresas del Grupo Hornetsecurity en calidad de subcontratistas:

	Encargado del tratamiento	Los servicios son prestados en régimen de subcontratación interna por
☐	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com	-/-
☒	Hornetsecurity Iberia S. L. Calle Vía de las Dos Castillas 33, Edificio 3 Ática 3 Planta Tercera D 28224 Pozuelo de Alarcón, Madrid España Teléfono: +34 91 368 77 33 Correo electrónico: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com

	Encargado del tratamiento	Los servicios son prestados en régimen de subcontratación interna por
☐	Hornetsecurity Argentina S.A. Belgrano 53 Piso, PB Dpto: B Tandil, Buenos Aires Argentina Tel.: +54 9 249 449 9296 Correo electrónico: info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com
☐	Hornetsecurity Ltd. 82 James Carter Road Mildenhall, Bury Saint Edmunds IP28 7DD Reino Unido Teléfono: +44 203 0869 833 Correo electrónico: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com
☐	Hornetsecurity Ltd BLK LS3, Level 1, Malta Life Sciences Park San Gwann Industrial Estate San Gwann, SGN 3000 Malta Teléfono: +44 203 0869 833 Correo electrónico: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 Estados Unidos Teléfono: +1 (412) 924-5300 Correo electrónico: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com
☐	Hornetsecurity Canada Inc. Suite 500, Park Place Building 666 Burrard Street, Vancouver, BC V6E 3P3 Canadá Teléfono: +1 (514) 527-3232 Correo electrónico: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com

	Encargado del tratamiento	Los servicios son prestados en régimen de subcontratación interna por
☐	IT-Seal GmbH IT-Seal GmbH Hilpertstr. 31. 64295 Darmstadt Alemania Teléfono: +49 (0) 6151 / 4938990 Correo electrónico: kontakt@it-seal.de	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 Correo electrónico: info@hornetsecurity.com

Hemos designado un responsable de la protección de datos. Puede ponerse en contacto con él escribiendo a
privacy@hornetsecurity.com

II. Información general sobre el tratamiento de datos

1. Alcance del tratamiento de datos personales

La prestación de los servicios requiere el tratamiento de diversos datos. Además, el alcance del tratamiento de datos depende del uso que usted haga de las funcionalidades de los servicios, por ejemplo, qué datos trata o hace tratar, o bien da su consentimiento para el tratamiento de datos.

Como parte del contrato celebrado con Hornetsecurity para el uso de los servicios, usted está obligado a facilitar los datos personales necesarios para el cumplimiento del contrato. La negativa a facilitar estos datos puede constituir un incumplimiento de sus obligaciones, por el cual puede estar obligado a prestar una indemnización por daños y perjuicios. No está obligado a facilitarnos datos personales. Sin embargo, si el suministro de estos datos es técnicamente obligatorio para el uso de nuestros servicios, una negativa significará que no podrá utilizar nuestros servicios.

Al utilizar los servicios, no está sujeto a la toma de decisiones automatizada en el sentido del art. 22 del RGPD.

2. Fundamento jurídico del tratamiento de datos personales

A continuación se presenta el fundamento jurídico del tratamiento de datos personales.

Motivo del tratamiento	Fundamento jurídico en el RGPD	Explicación
Cumplimiento del contrato o aplicación de medidas precontractuales	Art. 6, ap. 1, letra b)	El tratamiento solo se lleva a cabo en la medida necesaria para el ejercicio y cumplimiento de los derechos y obligaciones derivados del contrato. A menos que se indique expresamente lo contrario, solo tratamos datos en esta medida.
Interés legítimo	Art. 6, ap. 1, letra f)	El tratamiento se lleva a cabo en la medida en que tengamos un interés legítimo y no se manifiesten intereses superiores contrarios del interesado. El interés específico se explica en esta información sobre protección de datos como parte de la descripción del tratamiento.
Obligación legal	Art. 6, ap. 1, letra c)	El tratamiento tiene lugar en la medida en que es necesario para el cumplimiento de las obligaciones legales alemanas o europeas.

III. Tratamiento de datos para el funcionamiento de los *servicios*

Para que podamos prestarle los *servicios*, es necesario tratar determinados datos.

El fundamento jurídico del tratamiento de esta información y de los datos almacenados es la necesidad de cumplir la relación contractual existente. Por lo tanto, el periodo de almacenamiento se calcula principalmente por la duración de la relación contractual. No obstante, pueden aplicarse fundamentos jurídicos alternativos (como los periodos de conservación legales) una vez finalizado este periodo.

1. Datos básicos

La entidad del Grupo Hornetsecurity indicada en el apartado I, "Datos de contacto" (página 3), es la responsable del tratamiento de los datos maestros y de configuración.

a. Datos maestros

Los datos maestros del cliente (nombre, dirección, persona de contacto, número de teléfono, dirección de correo electrónico, departamento, cargo, servicios reservados, periodo de facturación, detalles de la cuenta) se registran para la administración de los servicios y se utilizan para cumplir los servicios acordados contractualmente. Los datos personales de los distintos usuarios (dirección de correo electrónico) se registran y se utilizan para cumplir los servicios acordados contractualmente.

El tratamiento de los datos de los distintos usuarios se realiza en el *hardware* propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

Los datos maestros del cliente son tratados por un subcontratista en sistemas de un tercer país (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, EE. UU) con el fin de mantener dichos datos. Los datos se transmiten sobre la base de cláusulas contractuales estándar.

El tratamiento de datos en el *software* CRM de Salesforce se lleva a cabo bajo responsabilidad conjunta de conformidad con el art. 26 del RGPD de las empresas mencionadas en el apartado I, "Información de contacto". Las partes afectadas pueden consultar el contenido principal de este acuerdo previa solicitud. El fundamento jurídico para ello es nuestro interés legítimo de conformidad con el art. 6, ap. 1, letra f) en conexión con el considerando 48 del RGPD para aumentar la eficiencia y minimizar los costes mediante la creación y el uso de estructuras administrativas conjuntas.

Además, partes de los datos maestros del cliente se transmiten a subcontratistas dentro de la UE a efectos de entrega y envío de facturas (por carta o correo electrónico) y se tratan en sus sistemas (PIN Mail AG, Alt-Moabit 91, 10559 Berlín, Alemania).

b. Datos de configuración

La configuración técnica del *servicio* contratado en cada caso se almacena en relación con la dirección de correo electrónico del usuario, la pertenencia a grupos de un usuario o el nombre de dominio del cliente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

Lo siguiente también se aplica a VM Backup y 365 Total Backup:

Para la validación de la licencia, los datos maestros necesarios para la identificación única (dirección de correo electrónico) se transfieren a los sistemas de Hornetsecurity Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malta, UE.

2. 365 Permission Manager

365 Permission Manager es una herramienta de *software* de Gobernanza, Riesgo y Cumplimiento (GRC) que permite a los usuarios ver de forma completa y entender sus permisos de archivos M365 en su propio *tenant* en la nube de Microsoft Azure para SharePoint Online, OneDrive for Business, Microsoft Teams y Microsoft 365 Groups.

El tratamiento automático de datos incluye la recuperación y el tratamiento de los metadatos de los objetos almacenados en el *tenant* de M365. Los objetos cuyos metadatos se recuperan son: archivos, carpetas, bibliotecas de documentos, sitios, usuarios y grupos. Los metadatos recuperados y tratados son los propietarios de los objetos (dirección de correo electrónico, nombre para mostrar), información sobre los objetos a los que se han concedido derechos de acceso (dirección de correo electrónico, nombre para mostrar, tanto de objetos dentro como fuera de la propia organización), así como las autorizaciones asignadas.

No es posible acceder al contenido de los objetos (contenido de los archivos).

Los metadatos recuperados y almacenados se eliminan en cuanto se elimina el objeto correspondiente en Microsoft Cloud o cuando se desactiva el servicio para el cliente en el Panel de Control.

Los metadatos recuperados se tratan en nuestro propio *hardware*, situado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

3. 365 Total Backup

365 Total Backup es una solución de copia de seguridad y restauración fiable, intuitiva y fácil de gestionar para buzones de correo de Microsoft 365, cuentas de empresa de OneDrive, bibliotecas de documentos de SharePoint, chats de Teams y *endpoints*.

365 Total Backup proporciona al cliente una configuración basada en políticas, una vista general y supervisión de los derechos, copias de seguridad y los objetos M365 de los que haya que realizar copias de seguridad a través de una consola *multitenant*. Todos los datos de las copias de seguridad se cifran con claves AES-256 personalizadas.

La gestión de los datos protegidos y cifrados es efectuada dentro del Grupo Hornetsecurity por Hornetsecurity Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malta ("Hornetsecurity Ltd.").

Los datos cifrados de la copia de seguridad se almacenan

Los datos cifrados de la copia de seguridad se almacenan según la configuración realizada por el cliente:

- en la nube de Hornetsecurity, entre otros lugares, en Alemania, Francia, Suiza, el Reino Unido, Canadá y Estados Unidos (Virginia y Georgia), proporcionada por Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover, Alemania.
- o, en el caso de instalaciones más antiguas (anteriores a febrero de 2022), en la nube de Microsoft Azure, zona de Europa Occidental, en régimen de «almacenamiento en frío», para lo cual Hornetsecurity Ltd. utiliza la plataforma de Microsoft Azure y sus servicios de cumplimiento normativo. La plataforma y los servicios de Azure para Europa Occidental cuentan con la certificación SOC 1 Tipo 2, SOC 2 Tipo 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS e HIPAA.

Durante el funcionamiento, la licencia de *software* utilizada se compara en línea con la licencia adquirida almacenada en los datos maestros. El contratista no transfiere ni trata los datos de los usuarios de los servicios.

4. 365 Total Protection

Con Spam and Malware Protection, los correos electrónicos entrantes del cliente se filtran en busca de contenido dañino (p. ej., virus), publicidad no deseada (p. ej., *spam*) y publicidad legítima (p. ej., boletines informativos) en los sistemas informáticos del contratista. Los correos electrónicos salientes también se filtran.

El tratamiento automático de datos incluye los metadatos de la transmisión del mensaje (dirección de correo electrónico del remitente y del destinatario, asunto del correo electrónico, fecha/hora de recepción y entrega del correo, direcciones IP de los servidores que participan en la comunicación, código y texto de error SMTP), el contenido de los correos electrónicos y la clasificación del correo electrónico (Clean, Spam, Virus, Infomail). Los metadatos de los mensajes se utilizan para que puedan visualizarse en el Panel de Control y se eliminan a los 14 meses como máximo. El propio correo se elimina después de entregarse o rebotarse correctamente.

El uso de Individual User Signatures, Company Disclaimer y 1-Click Intelligent Ads requiere el uso de un servicio de directorio por parte del cliente, que puede ser consultado por el contratista a través del protocolo LDAP. Además, los grupos del directorio de usuarios deben organizarse en el Panel de control. Los mensajes deben enviarse a través de los relés del contratista.

El tratamiento automático de datos incluye la dirección de correo electrónico del usuario, el nombre de grupo asignado en el servicio de directorio, otra información que pueda estar vinculada en el servicio de directorio, como la afiliación organizativa, el cargo, el número de teléfono, el número de fax y el contenido de la carpeta de correo que se asigna al grupo en el directorio por parte del cliente. Los datos personales extraídos del directorio se eliminarán una vez finalizado el uso del servicio. El mensaje tratado se elimina después de entregarse o rebotarse correctamente.

Cifrado global S/MIME y PGP: El contratista cifrará y firmará los correos electrónicos salientes y descifrará los correos electrónicos entrantes del cliente en sus propios sistemas informáti-

cos de conformidad con las políticas establecidas. Dependiendo de la configuración de las políticas, los correos electrónicos salientes se ponen a disposición del destinatario en el entorno protegido de Websafe.

El tratamiento automático de datos incluye la dirección de correo electrónico del remitente y del destinatario, la clave S/MIME o PGP privada y pública, el contenido del correo electrónico saliente a terceros (Websafe), la dirección de correo electrónico en claves públicas de terceros, el estado de cifrado y el contenido de los correos electrónicos. Los datos sobre el remitente, el destinatario y el estado de cifrado se utilizan para la visualización en el Panel de control y se eliminan a los 14 meses como máximo. El propio correo se elimina después de entregarse o rebotarse correctamente.

Archiving: El contratista archivará los correos electrónicos del cliente a prueba de auditorías en sus propios sistemas informáticos.

El tratamiento automático de datos incluye la dirección de correo electrónico del remitente y del destinatario, el asunto del correo electrónico, la fecha/hora de recepción del correo, las direcciones IP de los servidores que participan en la comunicación, el contenido de los correos electrónicos y, si procede, el nombre y el tipo de archivo adjunto.

Los datos de dirección del remitente y destinatario, el asunto del correo, la fecha/hora, y el nombre y tipo de archivo adjunto se utilizan para su visualización en el Panel de Control. Todos estos datos, incluido el propio mensaje, se almacenan durante un periodo de archivo específico del cliente más 1 año. Transcurrido este tiempo, se eliminan. La inhibición del borrado a petición del cliente puede aumentar el periodo de almacenamiento.

Advanced Thread Protection (ATP): protege el tráfico de correo electrónico del cliente frente a ataques selectivos e individuales, como el *spear phishing*, los ataques combinados, las amenazas persistentes avanzadas, el *ransomware* y el fraude CEO. Para reconocer los ataques, el contratista examina los correos electrónicos del cliente clasificados como sospechosos mediante técnicas avanzadas de filtrado.

Para ello, se trata automáticamente la metainformación sobre el contenido del correo electrónico y el tipo, el nombre y el contenido de los adjuntos-. La metainformación sobre el contenido del correo se utiliza para que pueda visualizarse en el Panel de Control y se elimina a los 14 meses como máximo. El correo se elimina del sistema ATP después de haberse analizado correctamente.

Contingency Covering: en caso de fallo del servidor de destino, el contratista proporcionará a cada usuario un buzón de correo electrónico con 10 GB de espacio de almacenamiento. Los usuarios autorizados pueden acceder a los correos electrónicos de este buzón a través de una interfaz de correo web o mediante IMAP y POP3.

El tratamiento automático de datos incluye los metadatos del mensaje (dirección de correo electrónico del remitente y del destinatario, fecha/hora de recepción del correo), el contenido del correo electrónico y los metadatos del correo web (nombre de usuario, dirección IP, duración de la conexión, volumen de recuperación, protocolo). Los metadatos de los mensajes, los

metadatos del correo web y los mensajes archivados se eliminan a los 14 meses como máximo. Los mensajes del buzón del correo web se borran como muy tarde cuando el cliente deja de utilizar el servicio.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*).

Para el uso del inicio de sesión único, la dirección de correo electrónico se transmite a Microsoft cuando el usuario inicia sesión.

No se transmite ningún otro dato a terceros ni estos acceden a los datos.

5. 365 Total Protection Enterprise Backup

Este servicio es una fusión de los servicios

- 365 Total Protection (sección III.4, a partir de la página 9) y
- 365 Total Backup (sección 3, a partir de la página 8).

Lea la información pertinente de las secciones indicadas.

6. AI Cyber Assistant: AI Email Security Analyst

AI Email Security Analyst informa a los usuarios finales de las medidas de precaución que deben tomar al gestionar el correo electrónico notificado. Además, esta función ofrece una explicación y una evaluación de los indicadores de legitimidad o malicia presentes en el mensaje.

Los administradores pueden utilizar AI Email Security Analyst en el seguimiento en tiempo real del correo electrónico, donde obtienen, bajo demanda, un análisis genérico, una evaluación de riesgos y una clasificación basada en IA del contenido de los correos. No se revela información detallada sobre el contenido de los correos electrónicos.

AI Email Security Analyst procesa datos mediante modelos de lenguaje grande (LLM) preentrenados, alojados en entornos encapsulados de MS Azure. Servidores de MS Azure en la región de EE. UU. para clientes de EE. UU. y Canadá, y servidores de MS Azure en la región de Europa para clientes de la UE y del resto del mundo.

Tras la evaluación, el contenido de los correos electrónicos no se almacena en el sistema de IA ni se utiliza con fines de entrenamiento. Los resultados de la evaluación, junto con los comentarios de los usuarios sobre el AI Email Security Analyst, pueden utilizarse para mejorar los algoritmos de detección.

El almacenamiento de los correos electrónicos se realiza en hardware propio, ubicado en centros de datos alquilados (colocación). No se cede la información a terceros. Aparte del contratista y de los representantes designados por el cliente, ningún tercero tiene acceso a los datos.

7. AI Cyber Assistant: AI Recipient Validation

AI Recipient Validation es una herramienta que permite a los usuarios finales de los *tenants* de M365 recibir una alerta en su cliente Outlook cuando un correo electrónico que envían podría estar mal dirigido (p. ej., si se ha añadido un destinatario incorrecto a un hilo de correo electrónico) o contener información confidencial (p. ej., números de tarjetas de crédito o datos personales). Los usuarios pueden aceptar los consejos o continuar sin realizar ningún cambio

en el correo electrónico. Las sugerencias del producto se actualizan en función del comportamiento del usuario.

El tratamiento automático de datos en la nube incluye el asunto del correo, remitente y destinatario (nombre en texto plano y dirección de correo en cada caso), tipo de correo (nuevo, respuesta, reenvío), hora de envío del correo, idioma configurado para el cliente de Outlook, todos los usuarios y grupos del *tenant*, número de destinatarios en listas de distribución, número de correos enviados, así como estadísticas de rendimiento del complemento de Outlook.

El tratamiento automático de datos en el cliente local de Outlook incluye el contenido del correo electrónico.

AI Recipient Validation no utiliza ni IA generativa ni modelos de lenguaje a gran escala (LLM). La evaluación se basa en una lógica de decisión basada en reglas, en forma de árbol de decisión. Los comentarios sobre si un destinatario ha sido confirmado como válido o no deseado en el contexto concreto del correo electrónico pueden utilizarse para ajustar esta lógica de decisión y, con ello, mejorar las evaluaciones futuras. En este proceso no se lleva a cabo ni el entrenamiento ni el ajuste fino de un LLM.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

8. AI Cyber Assistant: Conversational Agent

Se puede acceder al agente conversacional a través del panel de control y ofrece asistencia a los usuarios con nivel de socio y a aquellos con autorización para utilizar el agente. Proporciona respuestas a preguntas relacionadas con las ventas, la asistencia técnica y los indicadores de uso y rendimiento de los servicios.

El agente conversacional utiliza un modelo de lenguaje grande (LLM) preentrenado. Para responder a las consultas, el modelo tiene acceso a información interna seleccionada de ventas, marketing, técnica y de asistencia, así como, dentro del contexto de permisos del usuario, a metadatos relevantes de clientes y de uso procedentes del seguimiento en tiempo real del correo electrónico.

Los datos de entrada y salida se procesan como contexto en tiempo de ejecución y no se utilizan para el entrenamiento del LLM.

A efectos de control de calidad, se almacenan las últimas 50 entradas de usuario y salidas del LLM, con una duración máxima de 30 días.

Tenga en cuenta que las respuestas son generadas por IA y, en determinadas circunstancias, pueden no ser correctas.

El tratamiento de datos se lleva a cabo en nuestro propio hardware, ubicado en centros de datos alquilados (colocación). El tratamiento y el almacenamiento se realizan en Alemania. Para los usuarios de EE. UU., el tratamiento y el almacenamiento se realizan en EE. UU.

9. AI Cyber Assistant: Teams Protection

Teams Protection protege a los usuarios finales frente a mensajes comprometedores cuando intercambian mensajes en Microsoft Teams, analizando todos los mensajes que contienen

URL. Si se detecta una amenaza, el bot AI Cyber Assistant muestra un mensaje de advertencia en el historial del chat. Opcionalmente, se pueden eliminar los mensajes con URL potencialmente maliciosas. Teams Protection utiliza la base de datos y las tecnologías de detección de Secure Links de Hornetsecurity (parte de Advanced Threat Protection, página 19).

Los administradores obtienen en el panel de control una visión general de los chats en los que se han detectado URL maliciosas, con indicación de los interlocutores implicados y de la URL en cuestión. Se pueden bloquear las cuentas que difundan contenidos maliciosos.

Todos los mensajes de Teams se procesan en nuestros servidores, ubicados en nuestros propios centros de datos. Almacenamos las URL maliciosas detectadas y los participantes en la comunicación para advertir a nuestros clientes y mostrarles detalles sobre estas amenazas.

El tratamiento de los datos se lleva a cabo en nuestro propio hardware, ubicado en centros de datos alquilados (colocación). No se cede ningún dato a terceros. Aparte del contratista y de los representantes designados por el cliente, ningún tercero tiene acceso a los datos.

10. Inicio de sesión en el Panel de Control

Si ya es cliente de Hornetsecurity, puede acceder al Panel de Control de nuestra web, desde donde podrá utilizar y gestionar su servicio. Para conectarse, necesitará su nombre de usuario o dirección de correo electrónico y su contraseña. Por lo tanto, el periodo de almacenamiento se calcula principalmente por la duración de la relación contractual. No obstante, pueden aplicarse fundamentos jurídicos alternativos (como los periodos de conservación legales) una vez finalizado este periodo.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

El fundamento jurídico del tratamiento de esta información y de los datos almacenados es la necesidad de cumplir la relación contractual existente.

11. Inicio de sesión en el correo web de Hornet.email

Si ya es cliente de Hornetsecurity, puede acceder al Panel de Control de nuestra web, desde donde podrá utilizar y gestionar su servicio. Como cliente del correo web, puede conectarse a través de un enlace independiente a su buzón de correo. Para conectarse, necesitará su nombre de usuario o dirección de correo electrónico y su contraseña. Por lo tanto, el periodo de almacenamiento se calcula principalmente por la duración de la relación contractual. No obstante, pueden aplicarse fundamentos jurídicos alternativos (como los periodos de conservación legales) una vez finalizado este periodo.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

El fundamento jurídico del tratamiento de esta información y de los datos almacenados es la necesidad de cumplir la relación contractual existente.

12. Hosted Exchange

Además de la protección *antispam* y *antimalware*, el cliente puede reservar buzones de Hosted Exchange si no se va a utilizar un servidor de correo propio. Hosted Exchange le ofrece el funcionamiento seguro de un servidor Exchange gestionado profesionalmente en su dominio de correo con Active Sync, información de contactos compartida, calendarios en línea, colaboración en grupo y acceso desde diferentes clientes y plataformas de *hardware* sin ningún esfuerzo adicional.

El tratamiento automático de datos incluye los correos electrónicos recibidos y enviados, la dirección de correo electrónico del usuario, la pertenencia a grupos, la fecha de creación del buzón, las autorizaciones de/a otras cuentas internas del mismo dominio y los dispositivos móviles utilizados para acceder al buzón. Si se han introducido los siguientes datos, también se tratarán: empresa, cargo, departamento, número de empleado, supervisor, números de teléfono, dirección. Los datos se eliminarán a más tardar 90 días después de la cancelación del servicio.

Los correos electrónicos se transmiten a servidores de subcontratistas en la UE para su tratamiento y almacenamiento (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Alemania o Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Alemania).

El fundamento jurídico del tratamiento de esta información y de los datos almacenados es la necesidad de cumplir la relación contractual existente.

13. IA, uso de la inteligencia artificial

a. Introducción

Este documento explica nuestras prácticas con respecto a la recopilación, almacenamiento y tratamiento de metadatos de correo electrónico y temas latentes del contenido del correo electrónico para nuestros proyectos de aprendizaje automático e IA en Hornetsecurity. Nuestro enfoque da prioridad a la privacidad del usuario y se ajusta a las políticas vigentes sobre protección de datos. Aunque nuestro objetivo principal siguen siendo los metadatos de correo electrónico, la identificación de temas de correo electrónico proporciona información para perfeccionar los modelos de aprendizaje automático, en particular para la clasificación del correo electrónico, que es necesaria para servicios como los productos y funciones Targeted Fraud Forensics, Phishing Protection, AI Recipient Validation e Infomail-Filter.

b. Finalidad del tratamiento

Mejora continua de los modelos de clasificación de correos electrónicos

Perfeccionamos y mejoramos los algoritmos de aprendizaje automático utilizando datos de correo electrónico para garantizar la precisión y pertinencia de sus predicciones. Esto nos ayuda a distinguir eficazmente entre comunicación auténtica, *spam* y contenido malicioso.

Categorización del correo electrónico

Los metadatos de correo electrónico y los temas latentes se utilizan para clasificar los correos electrónicos en diferentes tipos, como «Publicidad» o «Phishing». Este enfoque está estrechamente relacionado con nuestro producto Infomail Filter, que permite a los usuarios poner en cuarentena los correos electrónicos no deseados.

Compartir información confidencial y filtraciones de datos

Para nuestros productos Targeted Fraud Forensics y AI Recipient Validation, es crucial predecir la probabilidad de que se transmita información confidencial a personas no autorizadas. Para ello, analizamos los metadatos de los correos electrónicos, los grafos sociales, p. ej., las conexiones entre remitentes y destinatarios, y los temas latentes para identificar posibles filtraciones de datos y amenazas a la seguridad.

Mejorar la facilidad de uso

Las acciones de los usuarios, como denunciar correos electrónicos no deseados o cambiar el contenido de los correos electrónicos basándose en sugerencias, influyen en la optimización de la facilidad de uso de los productos de Hornetsecurity. Esta optimización reduce los correos electrónicos no deseados y ofrece avisos y recomendaciones de actuación más pertinentes.

Protección de las cuentas y seguridad

Evaluar los datos de correo electrónico y analizar las tendencias para detectar anomalías o posibles amenazas a la seguridad, como campañas de *phishing* incipientes o cuentas de correo electrónico en riesgo, nos ayuda a proteger a nuestros usuarios y sus datos.

c. Datos recopilados por nosotros

Identificadores básicos:

- Dirección de correo electrónico del remitente
- Dirección(es) de correo electrónico del destinatario
- Direcciones IP, nombres de anfitrión y ASN (número de sistema autónomo, por sus siglas en inglés) de los servidores emisores

Datos temporales:

- Marca de tiempo de los envíos de correo electrónico
- Marca de tiempo para los comentarios de usuarios y administradores sobre correos electrónicos que hayan sido marcados como spam, infomail o inofensivos.

Características de los mensajes y estado de autenticación:

- Tamaño del mensaje
- Formato del mensaje (HTML, texto sin formato y otros detalles del tipo de contenido)
- La(s) suma(s) de comprobación del cuerpo y el encabezado del mensaje
- Detalles de autenticación y verificación (entradas para registros DKIM, DMARC, SPF)

Información sobre la interacción:

- Comentarios sobre el correo electrónico (p. ej., si se considera spam o inofensivo)
- Acciones de respuesta a los mensajes (p. ej., respuesta, reenvío, primer contacto)
- Acciones en respuesta a alertas y notificaciones (p. ej., decidir si se envía un correo electrónico después de que lo solicite AI Recipient Validation).
- Metadatos como el número de mensajes, palabras clave en el asunto y la distribución de las marcas de tiempo asociadas para destinatarios o listas de distribución específicos (AI Recipient Validation).

Metadatos de los archivos adjuntos:

- Número de anexos
- Tipos de archivo (por ejemplo, .pdf, .docx, .jpg)
- Tamaño de los archivos
- Nombres de archivos con datos personales anonimizados
- Suma(s) de comprobación del/de los archivo(s)

Enlaces y dominios:

- Enlaces en un correo electrónico o en archivos adjuntos con rutas URL y parámetros anonimizados
- Dominios de los enlaces extraídos y su información DNS (p. ej., registros A del DNS)

Datos de encabezado:

- Información de la sección de encabezado del correo electrónico, como:
- De
- Para
- Fecha
- Asunto con datos personales anonimizados
- ID del mensaje
- Datos del agente de usuario y del X-Mailer
- Líneas recibidas
- Resultados de la autenticación
- Encabezados de mensaje relacionados con el contenido (p. ej., "Content-Type")

Derivación del tema a partir del cuerpo del mensaje:

Para mejorar nuestros modelos de clasificación de correos electrónicos, extraemos el tema general del contenido del correo. El texto del mensaje se trata para reconocer una categoría o tema superior sin guardar detalles específicos ni delicados del propio texto del mensaje.

Ejemplo: un correo electrónico con detalles sobre una próxima venta de productos podría clasificarse generalmente como "Promoción" o "Evento de ventas".

d. Herramientas de IA, almacenamiento y conservación de datos

Todas las herramientas y modelos de IA se desarrollan internamente o se proporcionan a través de plataformas de confianza como Azure. Para el almacenamiento de IA, utilizamos tanto nuestra propia infraestructura como Large Language Models (LLM) alojados en Microsoft Azure para proporcionar funciones avanzadas de IA. Nuestros datos rápidos solo contienen los datos personales mínimos necesarios para prestar el servicio. Los datos nunca se almacenan ni se utilizan para el entrenamiento de modelos sin autorización explícita. Los LLM externos son entrenados sin nuestros datos por el proveedor del LLM.

La infraestructura de almacenamiento y procesamiento de IA se encuentra en el centro de datos de Hornetsecurity o en el entorno seguro en la nube de Azure. El acceso a los datos y modelos está estrictamente controlado y supervisado en virtud de la ley de protección de datos. No se permite el acceso a estos datos a terceros ni a personal no autorizado. Los modelos

de aprendizaje automático se proporcionan y utilizan exclusivamente a través de nuestra infraestructura segura o mediante conexiones seguras a los servicios de Azure. Cada transacción de datos entre los sistemas del cliente y nuestra API de IA/ML está protegida por sólidos procedimientos de cifrado de extremo a extremo. Esto garantiza la confidencialidad e integridad de los datos durante la transmisión.

Protocolos de almacenamiento y conservación

- Los datos se cifran en modo inactivo y durante la transmisión. Los procedimientos de cifrado se ajustan a las prácticas recomendadas del sector.
- Los datos se almacenan durante el tiempo que sea necesario para cumplir los fines de tratamiento indicados. Algunos archivos de registro pueden conservarse hasta 12 meses de conformidad con nuestra política de conservación de datos.
- Todos los demás datos almacenados para el funcionamiento o el cumplimiento de las funciones de un producto o servicio activo y de pago se conservan mientras sean necesarios.
- Los servicios dados de baja siguen entonces un procedimiento de desactivación.

Anonimización de la información personal identificable:

- Para garantizar la privacidad de los usuarios y cumplir las normas de protección de datos, los datos personales se anonimizan sistemáticamente antes de almacenarlos, en la medida de lo posible.
- La anonimización de la IIP (información de identificación personal, por sus siglas en inglés) es una medida adoptada para eliminar posibles sesgos en nuestros modelos de aprendizaje automático y garantizar que los modelos funcionen de forma objetiva.

14. Security Awareness Service

El Security Awareness Service registra los datos de los usuarios (nombre, departamento, dirección de correo electrónico, grupo asignado para la evaluación) mediante la importación de CSV, la comparación con MS365 o la sincronización LDAP. Los datos sirven para preparar una sesión formativa de concienciación (vídeos, cuestionarios, fichas informativas) y enviar a los usuarios simulaciones de correos electrónicos de phishing.

Los resultados de los ataques simulados se evalúan de forma estadística y se publican por grupo y por usuario. Si se activa el modo de privacidad, se excluye la posibilidad de realizar una evaluación personalizada. A partir de la información recopilada se forma un Employee Security Index (ESI®), o índice de seguridad de los empleados, que documenta el progreso realizado en relación con la concienciación y también permite una comparación directa con un grupo de usuarios con muy buena formación.

Para crear una simulación realista de situaciones de phishing también se utilizan como direcciones de remitente algunas direcciones de correo de la propia empresa en forma de remitentes falsos. Los usuarios pueden oponerse al uso de su dirección de correo electrónico para tales fines.

Para crear una simulación realista de correos de phishing de objetivo definido basados en OSINT (inteligencia de fuentes abiertas, por sus siglas en inglés) también se analizan datos personales y empresariales disponibles públicamente, como p. ej., información de portales de

evaluación empresarial como Kununu.com, o provenientes de redes sociales empresariales, como p. ej., Xing.com o LinkedIn.com. Además, en niveles de formación superiores se puede hacer referencia a correos electrónicos recibidos o enviados realmente con anterioridad que no tienen nada que ver con la simulación de phishing.

La información introducida por los usuarios en el contexto de los correos de *phishing* simulados (p. ej., datos de inicio de sesión en páginas de inicio de sesión generadas y falsificadas por nosotros) no se almacena ni se trata. Los documentos adjuntos que abran los usuarios en el contexto de los correos de *phishing* simulados (p. ej., documentos de Word o tablas de Excel) no contienen código malicioso.

Tratamiento de notificaciones sobre potenciales correos electrónicos de phishing en Outlook mediante la interfaz del complemento de Hornetsecurity:

- Si se trata de un correo de *phishing* simulado en el contexto del Security Awareness Service, el usuario recibirá una confirmación de la correcta notificación y ello se registrará estadísticamente.
- Si no se trata de un correo de *phishing* simulado y el cliente ha contratado también el servicio de filtro de spam y malware, el correo notificado se envía a nuestro laboratorio de seguridad para su posterior análisis.
- Si no se trata de un correo de *phishing* simulado y el cliente no ha contratado el servicio de filtro de spam y malware, el correo notificado se envía a un buzón de asistencia a elección del cliente.

Los datos de cliente necesarios para configurar el servicio y todas las evaluaciones estadísticas se eliminan a más tardar pasadas 4 semanas después de la finalización del contrato.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

15. Spam and Malware Protection

Con Spam and Malware Protection, los correos electrónicos entrantes del cliente se filtran en busca de contenido dañino (p. ej., virus), publicidad no deseada (p. ej., *spam*) y publicidad legítima (p. ej., boletines informativos) en los sistemas informáticos del contratista. Si el cliente lo desea, también se filtran los correos electrónicos salientes.

El tratamiento automático de datos incluye los metadatos de la transmisión del mensaje (dirección de correo electrónico del remitente y del destinatario, asunto del correo electrónico, fecha/hora de recepción y -entrega del correo, direcciones IP de los servidores que participan en la comunicación, código y texto de error SMTP), el contenido de los correos electrónicos y la clasificación del correo electrónico (Clean, Spam, Virus, Infomail). Los metadatos de los mensajes se utilizan para que puedan visualizarse en el Panel de Control y se eliminan a los 14 meses como máximo. El propio correo se elimina después de entregarse o rebotarse correctamente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*).

No se transmitirá a terceros ningún otro dato (encabezado del correo, remitente, destinatario, asunto, fecha, contenido del texto). Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

a. Opcional: Advanced Thread Protection (ATP)

ATP protege el tráfico de correo electrónico del cliente frente a ataques selectivos e individuales, como el *spear phishing*, los ataques combinados, las amenazas persistentes avanzadas, el *ransomware* y el fraude CEO. Para reconocer los ataques, el contratista examina los correos electrónicos del cliente clasificados como sospechosos mediante técnicas avanzadas de filtrado.

Para ello, se trata automáticamente la metainformación sobre el contenido del correo electrónico, así como el tipo, el -nombre y el -contenido de los archivos adjuntos. La metainformación sobre el contenido del correo se utiliza para que pueda visualizarse en el Panel de Control y se elimina a los 14 meses como máximo. El correo se elimina del sistema ATP después de haberse analizado correctamente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

b. Opcional: Secure Links (como parte de ATP)

Para aumentar la seguridad en el uso de nuestros servicios de correo electrónico, utilizamos la función «Enlaces seguros». Con ella, los enlaces contenidos en los correos electrónicos entrantes se reescriben técnicamente y, al acceder a ellos, se comprueban primero a través de una infraestructura de seguridad.

En el marco de esta comprobación, se analizan automáticamente la dirección de destino y los contenidos web a los que se puede acceder a través de ella en busca de indicios de phishing, software malicioso u otras características relevantes para la seguridad. Para ello se utilizan procedimientos basados en reglas, así como técnicas de aprendizaje automático y aprendizaje profundo. No se lleva a cabo ningún procesamiento del contenido de los correos electrónicos mediante modelos de lenguaje a gran escala (Large Language Models) ni IA generativa.

El análisis de seguridad se limita a la URL a la que se accede y a los recursos web a los que se puede acceder a través de ella. El contenido del correo electrónico, la información del remitente y del destinatario, así como los archivos adjuntos, no se utilizan para el entrenamiento, el ajuste fino ni el desarrollo posterior de los modelos de detección empleados.

En la medida en que una URL o la propia página web a la que se accede contenga datos personales, estos pueden ser tratados técnicamente en el marco de la comprobación de seguridad. Estos datos no se utilizan con fines de entrenamiento ni para la optimización de los modelos de detección subyacentes.

c. Opcional: Email Encryption

El contratista solicitará y gestionará certificados S/MIME, cifrará y firmará los correos electrónicos salientes y descifrará los correos electrónicos entrantes del cliente en sus propios siste-

mas informáticos de conformidad con las políticas establecidas. Dependiendo de la configuración de las políticas, los correos electrónicos salientes se ponen a disposición del destinatario en el entorno protegido de Websafe.

El tratamiento automático de datos incluye la dirección de correo electrónico del remitente y del destinatario, la clave S/MIME o PGP privada y pública, el contenido de correos electrónicos salientes a terceros (Websafe), la dirección de correo electrónico en claves públicas de terceros, el estado de cifrado y el contenido del correo electrónico. Los datos sobre el remitente, el destinatario y el estado de cifrado se utilizan para la visualización en el Panel de control y se eliminan a los 14 meses como máximo. El propio correo se elimina después de entregarse o rebotarse correctamente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*).

Para solicitar certificados S/MIME, la dirección de correo electrónico y el nombre y apellidos del solicitante del certificado se transmiten a un subcontratista en la UE para su tratamiento (InterNetX GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg, Alemania).

Para la autenticación de dos factores (2FA) del destinatario de Websafe, el número de teléfono móvil del destinatario se transmite a un subcontratista (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, EE. UU.) para su tratamiento si se da el consentimiento. La transferencia tiene lugar basándose en cláusulas contractuales estándar. Allí, el número de teléfono móvil se elimina inmediatamente después de completar el proceso en Twilio. El contratista conserva el número de teléfono móvil mientras exista el buzón del destinatario.

No se transmitirán a terceros más datos que los especificados para la solicitud del certificado S/MIME y la generación de una clave 2FA. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

d. Opcional: Archiving

El contratista archivará los correos electrónicos del cliente a prueba de auditorías en sus propios sistemas informáticos.

El tratamiento automático de datos incluye la dirección de correo electrónico del remitente y del destinatario, el asunto del correo electrónico, la fecha/hora de recepción del correo, las direcciones IP de los servidores que participan en la comunicación, el contenido de los correos electrónicos y, si procede, el nombre y el tipo de archivo adjunto.

Los datos de dirección del remitente y destinatario, el asunto del correo, la fecha/hora, y el nombre y tipo de archivo adjunto se utilizan para su visualización en el Panel de Control. Todos estos datos, incluido el propio mensaje, se almacenan durante un periodo de archivo específico del cliente más 1 año. Transcurrido este tiempo, se eliminan. La inhibición del borrado a petición del cliente puede aumentar el periodo de almacenamiento.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

e. Opcional: Continuity Service

El contratista proporciona los correos electrónicos entrantes y salientes del cliente en el archivo durante un periodo de 3 meses, siempre que estos correos se enruten a través de los servidores de Hornetsecurity.

El contratista también proporcionará a cada usuario un buzón de correo electrónico con 10 GB de espacio de almacenamiento. Los usuarios autorizados pueden acceder a los correos electrónicos de este buzón a través de una interfaz de correo web o mediante IMAP y POP3.

El tratamiento automático de datos incluye los metadatos del mensaje (dirección de correo electrónico del remitente y del destinatario, fecha/hora de recepción del correo), el contenido del correo electrónico y los metadatos del correo web (nombre de usuario, dirección IP, duración de la conexión, volumen de recuperación, protocolo). Los metadatos de los mensajes, los metadatos del correo web y los mensajes archivados se eliminan a los 14 meses como máximo. Los mensajes del buzón del correo web se borran como muy tarde cuando el cliente deja de utilizar el servicio.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

f. Opcional: Signature and Disclaimer para correo electrónico

El uso de Signature and Disclaimer requiere el uso de un servicio de directorio por parte del cliente, que puede ser consultado por el contratista a través del protocolo LDAP. Además, los grupos del directorio de usuarios deben organizarse en el Panel de control. Los mensajes deben enviarse a través de los relés del contratista.

El tratamiento automático de datos incluye la dirección de correo electrónico del usuario, el nombre de grupo asignado en el servicio de directorio y otra información que pueda estar vinculada en el servicio de directorio, como la afiliación organizativa, el cargo, el número de teléfono, el número de fax y el contenido de la carpeta de correo que se asigna al grupo en el directorio por parte del cliente. Los datos personales extraídos del directorio se eliminarán una vez finalizado el uso del servicio. El mensaje tratado se elimina después de entregarse o rebotarse correctamente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

g. Opcional: E-Mail made in Germany

El contratista hace posible que la infraestructura de correo electrónico del cliente se conecte a la red E-Mail made in Germany (EmiG) y para ello realiza la implementación necesaria en el servidor de correo para cumplir los requisitos de cifrado de transferencia continua de correos electrónicos en la red EmiG.

El tratamiento automático de datos incluye los metadatos de la transmisión del mensaje (dirección de correo electrónico del remitente y del destinatario, asunto del correo electrónico,

fecha/hora del correo entrante, direcciones IP de los servidores que participan en la comunicación, estado de cifrado) y el contenido de los correos electrónicos. Los metadatos de transmisión de mensajes se utilizan para su visualización en el Panel de Control y se eliminan a los 14 meses como máximo. El propio correo se elimina después de entregarse o rebotarse correctamente.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

16. Test-Onboarding

Para probar el funcionamiento de los servicios, puede registrarse directamente a través de nuestro sitio web. Para ello necesitamos diversa información sobre usted, sobre el dominio, el servidor y el usuario para los que se requiere el servicio, así como el servicio deseado. Los campos obligatorios están identificados correspondientemente. El resto de la información se facilita voluntariamente. Por lo tanto, el periodo de almacenamiento se calcula principalmente por la duración de la relación contractual. No obstante, pueden aplicarse fundamentos jurídicos alternativos (como los periodos de conservación legales) una vez finalizado este periodo.

Los datos maestros del cliente son tratados por un subcontratista en sistemas de un tercer país (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, EE. UU) con el fin de mantener dichos datos. Los datos se transmiten sobre la base de cláusulas contractuales estándar.

A este respecto, el fundamento jurídico del tratamiento es la aplicación de medidas precontractuales o la necesidad para el cumplimiento del contrato.

17. VM Backup

VM Backup es una solución de copia de seguridad y recuperación fiable, intuitiva y fácil de gestionar para servidores virtualizados en entornos Hyper-V y VMware, así como para servidores físicos de Microsoft.

VM Backup permite al cliente realizar copias de seguridad en las ubicaciones especificadas por el cliente en los intervalos de tiempo especificados por el cliente. El cifrado de las copias de seguridad está garantizado por claves de cifrado AES-256 (contraseña) configuradas por el cliente. Todas las copias externas están cifradas con AES-256. El cifrado es opcional para las copias de seguridad *in situ* (primarias) y también es compatible.

En el caso de las copias externas, los datos se almacenan opcionalmente en un almacenamiento en la nube alquilado por el cliente a terceros proveedores (Microsoft Azure Blob Storage, Wasabi Cloud Object Storage, Amazon S3 o BackBlaze Cloud Storage). El cliente actúa como contratante en relación con los terceros proveedores.

Durante el funcionamiento, la licencia de *software* utilizada se compara en línea con la licencia adquirida almacenada en los datos maestros. El contratista no transfiere ni trata los datos de los usuarios de los servicios.

18. Web Filter

Las llamadas http/https y ftp salientes del cliente se enrutan a través del servidor *proxy* del contratista. El tráfico de datos se comprueba en busca de contenidos potencialmente dañinos y, de ser necesario, se filtra.

El tratamiento automático de datos incluye la fecha y la hora de llamada a una dirección web, la dirección IP de llamada, la URL de llamada, la categoría clasificada del objeto de llamada, la entidad autentificada: bien la dirección de correo electrónico, posiblemente seudonimizada, bien la dirección IP o el nombre del servicio de directorio y la ruta del objeto o la cadena del conector del filtro web (sAM AccountName, ID del dominio, nombre del ordenador, IP del ordenador, programa de llamada). Estos datos (URL sin ruta) se utilizan para la visualización en el Panel de Control y se eliminan a los 14 meses como máximo.

El tratamiento de los datos se realiza en el hardware propio ubicado en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte del contratista y los representantes designados del cliente, ningún tercero tiene acceso a los datos.

El fundamento jurídico del tratamiento de esta información y de los datos almacenados es la necesidad de cumplir la relación contractual existente.

19. Websafe, política de privacidad para terceros

Para que podamos prestarle este servicio, es necesario tratar determinados datos. El tratamiento de esta información y de los datos almacenados es necesario para el cumplimiento de la relación contractual existente con nuestros clientes. Este es el fundamento jurídico del tratamiento. Al utilizar el servicio Websafe, usted no está sujeto a la toma de decisiones automatizada en el sentido del art. 22 del RGPD.

El tratamiento automático de los datos incluye los metadatos del mensaje (dirección de correo electrónico del remitente y del destinatario, fecha/hora de recepción del correo electrónico), el contenido del correo electrónico, los metadatos de Websafe (nombre de usuario, su dirección IP, duración de la conexión, volumen de recuperación, protocolo) y, si procede, el número de su teléfono móvil. Sus correos electrónicos se almacenan en Websafe durante 3 meses. Transcurrido ese tiempo, se eliminan. Su cuenta de Websafe existirá mientras reciba correos electrónicos en ella. Si deja de recibir correos electrónicos, su cuenta de Websafe se eliminará automáticamente transcurridos 12 meses desde la última vez que recibió un correo electrónico. Todos sus datos personales (y, en particular, su número de teléfono) se eliminarán de nuestros servidores.

Para completar el registro, tenemos que enviar un PIN a su dispositivo móvil. También puede ponerse en contacto con el remitente de su correo electrónico para que le reenvíe el PIN de otra forma. El proveedor del servicio Websafe no cobra ninguna tarifa por utilizar el servicio Websafe y enviar mensajes SMS.

El subcontratista para el envío de los SMS a su dispositivo móvil es la empresa Twilio Inc, 375 Beale Street, Suite 300, San Francisco, California 94105, EE. UU. El número de teléfono móvil se transmite basándose en las cláusulas contractuales estándar de la UE. El número de teléfono móvil se eliminará inmediatamente después de su uso con Twilio.

El tratamiento de datos de los metadatos de los mensajes, los metadatos de Websafe y los mensajes del buzón de Websafe tiene lugar en nuestro propio *hardware*, que se encuentra en centros de datos alquilados (*colocation*). Los datos no se transmiten a terceros. Aparte de Hornetsecurity GmbH, ningún tercero tiene acceso a estos datos.

IV. Posibilidad de oposición y eliminación

En la medida en que el tratamiento de datos se base en su consentimiento o en nuestro interés legítimo, usted tiene derecho a oponerse al tratamiento o a revocar el consentimiento otorgado en cualquier momento. Su oposición o revocación solo tendrá efecto para el futuro. Puede ponerse en contacto con datenschutz@hornetsecurity.com en cualquier momento para ejercer su derecho de oposición o revocación. Aunque se oponga al tratamiento basado en nuestro interés legítimo, podremos continuar el tratamiento si podemos demostrar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre sus intereses, derechos y libertades.

V. Derechos del interesado

Si se tratan datos relativos a su persona, usted será el interesado a efectos del art. 4, ap. 1 del RGPD. Como interesado, usted tiene los siguientes derechos en relación con sus datos personales. Para ejercer estos derechos, puede ponerse en contacto con nosotros utilizando los datos de contacto indicados anteriormente.

a. Derecho de acceso (conforme al art. 15 del RGPD)

Tiene derecho a acceder a sus datos personales procesados por nosotros. Esto incluye la información obligatoria establecida en el art. 15 del RGPD.

b. Derecho de rectificación (conforme al art. 16 del RGPD)

Tiene derecho a solicitar la rectificación inmediata de los datos personales erróneos y a que se completen los datos personales incorrectos.

c. Derecho de supresión (conforme al art. 17 del RGPD)

Tiene derecho a solicitar la supresión de sus datos personales si se aplica uno de los motivos enumerados en el art. 17 del RGPD, en particular si ya no existe ningún fundamento jurídico para el tratamiento.

d. Derecho a la limitación del tratamiento (conforme al art. 18 del RGPD)

Tiene derecho a solicitar la limitación del tratamiento de sus datos personales si se aplica uno de los motivos enumerados en el art. 18 del RGPD, en particular a petición suya en lugar de la supresión de los datos.

e. Derecho a la portabilidad de los datos (conforme al art. 20 del RGPD)

Usted tiene derecho a recibir todos los datos personales que hayamos almacenado sobre usted en un formato estructurado, de uso común y lectura mecánica, y a transmitir estos datos a otro responsable del tratamiento sin impedimentos por parte del responsable al que se hayan facilitado los datos personales.

Derecho a presentar una reclamación ante la autoridad de control competente (art. 77 del RGPD)

De conformidad con el art. 77 del RGPD, tiene derecho a presentar una reclamación ante la autoridad de control competente en su caso.

VI. Destinatarios de los datos

Una parte del tratamiento de sus datos personales en el marco de los *servicios* también es realizada por encargados del tratamiento, que realizan estas funciones exclusivamente sobre la base de un acuerdo de tratamiento de conformidad con el art. 28, ap. 3 del RGPD.

VII. Transferencia de datos a terceros países

Los datos personales que recopilemos de usted en el curso de la prestación de los *servicios* no se transferirán a terceros países fuera del Espacio Económico Europeo.

Para enviar mensajes de texto de autenticación de dos factores, utilizamos el proveedor Twilio, con sede en EE. UU. (por lo tanto, en un tercer país), de conformidad con el art. 44 del RGPD. Twilio participa en el DPF (Data Privacy Framework) de la UE y EE. UU. y trabaja de acuerdo con cláusulas contractuales estándar, lo que garantiza un nivel adecuado de protección de datos.

Para gestionar sus datos contractuales, utilizamos el proveedor Salesforce, que tiene su sede en EE. UU. (por lo tanto, en un tercer país), de conformidad con el art. 44 del RGPD. Salesforce participa en el DPF (Data Privacy Framework) de la UE y EE. UU. y trabaja de acuerdo con cláusulas contractuales estándar certificadas, lo que garantiza un nivel adecuado de protección de datos.

Para gestionar su firma electrónica de contratos, utilizamos el proveedor Docusign, que tiene su sede en EE. UU. (por tanto, en un tercer país), de conformidad con el art. 44 del RGPD. Docusign trabaja conforme a cláusulas contractuales estándar certificadas, lo que garantiza un nivel adecuado de protección de datos.