Gültig von:	01.06.2016
Gültig bis:	01.10.2028
Nächste Prüfung:	01.10.2027
Verantwortliche Person(en):	Olaf Petry, CISO
Vertraulichkeit:	Öffentlich

Datenschutzhinweise

Managed Security Services

Hornetsecurity Group

Datenschutzhinweise für die angebotenen Dienste

I. Einleitung 3
1. Grundlage 3
2. Kontaktinformationen 3
II. Allgemeines zur Datenverarbeitung 5
1. Umfang der Verarbeitung personenbezogener Daten 5
2. Rechtsgrundlage für die Verarbeitung personenbezogener Daten 5
III. Datenverarbeitung für den Betrieb der *Dienste* 6
1. Grundlegende Daten 6
a. Stammdaten 6
b. Konfigurationsdaten 6
2. 365 Permission Manager 7
3. 365 Total Backup 7
4. 365 Total Protection 8
5. 365 Total Protection Enterprise Backup 10
6. AI Cyber Assistant: AI Email Security Analyst 10
7. AI Cyber Assistant: AI Recipient Validation 10
8. AI Cyber Assistant: Conversational Agent 11
9. AI Cyber Assistant: Teams Protection 11
10. Control Panel, Anmeldung am 12
11. Hornet.email Webmail, Anmeldung an 12
12. Hosted Exchange 12
13. KI, Einsatz von Künstlicher Intelligenz 13
a. Einleitung 13
b. Zweck der Verarbeitung 13

c. Von uns gesammelte Daten 14
d. KI-Werkzeuge, Datenspeicherung und Aufbewahrung 15
14. Security Awareness Service 16
15. Spam and Malware Protection 17
a. Optional: Advanced Thread Protection (ATP) 18
b. Optional: Secure Links (als Bestandteil von ATP) 18
c. Optional: Email Encryption 18
d. Optional: Archiving 19
e. Optional: Continuity Service 19
f. Optional: E-Mail-Signature and Disclaimer 20
g. Optional: E-Mail made in Germany 20
16. Test-Onboarding 21
17. VM Backup 21
18. Web Filter 21
19. Websafe, Datenschutzerklärung für Dritte 22
IV. Widerspruchs- und Beseitigungsmöglichkeit 23
V. Betroffenenrechte 23
a. Recht auf Auskunft nach Art. 15 DSGVO 23
b. Recht auf Berichtigung nach Art. 16 DSGVO 23
c. Recht auf Löschung nach Art. 17 DSGVO 23
d. Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO 23
e. Recht auf Datenübertragbarkeit nach Art. 20 DSGVO 23
f. Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, Art. 77 DSGVO 23
VI. Empfänger von Daten 24
VII. Datenübermittlung in Drittländer 24

I. Einleitung

1. Grundlage

Grundlage eines effektiven Datenschutzes ist die umfassende Information über die Erhebung, Verarbeitung und Nutzung Ihrer Daten ("Datenverarbeitung"). Daher möchten wir Sie informieren,

- wann bzw. bei welchen Aktionen wir Daten verarbeiten,
- welche Daten wir aus welchen Gründen verarbeiten,
- wer Daten erhält,
- welche Rechte Sie wegen der Datenverarbeitung durch uns haben.

Diese Datenschutzhinweise beziehen sich nur auf die Nutzung personenbezogener Daten im Rahmen der *Dienste*. Diese Datenschutzhinweise können Sie dauerhaft und jederzeit herunterladen über die Adresse https://www.hornetsecurity.com/service-privacy-statement/

2. Kontaktinformationen

Verantwortlicher für die Datenverarbeitung im Rahmen der *Dienste* im Sinne der Datenschutz-Grundverordnung (DSGVO) ist stets der Kunde. Hornetsecurity wird als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig. Die Leistungserbringung erfolgt teilweise auch durch andere Hornetsecurity-Konzernunternehmen als Unterauftragnehmer:

	Auftragsverarbeiter	Die Leistungserbringung erfolgt im inneren Unterauftragsverhältnis durch
☒	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Deutschland Telefon: +49 511 515 464-0 E-Mail: 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 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Argentina S.A. Belgrano 53 Piso, PB Dpto: B Tandil, Buenos Aires Argentina Tel: +54 9 249 449 9296 E-mail: info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com

	Auftragsverarbeiter	Die Leistungserbringung erfolgt im inneren Unterauftragsverhältnis durch
☐	Hornetsecurity Ltd. 82 James Carter Road Mildenhall, Bury Saint Edmunds IP28 7DD United Kingdom Fon: +44 203 0869 833 Email: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Ltd BLK LS3, Level 1, Malta Life Sciences Park San Gwann Industrial Estate San Gwann, SGN 3000 Malta Fon: +44 203 0869 833 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 United States Fon: +1 (412) 924-5300 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Canada Inc. Suite 500, Park Place Building 666 Burrard Street, Vancouver, BC V6E 3P3 Canada Fon: +1 (514) 527-3232 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	IT-Seal GmbH IT-Seal GmbH Hilpertstr. 31 64295 Darmstadt Deutschland Tel.: +49 (0) 6151 / 4938990 E-Mail: kontakt@it-seal.de	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com

Wir haben zudem einen Datenschutzbeauftragten bestellt. Diesen erreichen Sie unter: datenschutz@hornetsecurity.com.

II. Allgemeines zur Datenverarbeitung

1. Umfang der Verarbeitung personenbezogener Daten

Die Bereitstellung der Dienste macht die Verarbeitung verschiedener Daten erforderlich. Darüber hinaus richtet sich der Umfang der Datenverarbeitung nach Ihrer Nutzung der Funktionalitäten der Dienste, beispielsweise welche Daten Sie dort verarbeiten bzw. verarbeiten lassen oder in die Datenverarbeitung einwilligen.

Im Rahmen des mit Hornetsecurity geschlossenen Vertrags über die Nutzung der Dienste sind Sie verpflichtet, diejenigen personenbezogenen Daten bereitzustellen, die für die Vertragserfüllung erforderlich sind. Die Weigerung, diese Daten bereitzustellen, kann eine Pflichtverletzung darstellen, aus der Sie zum Schadensersatz verpflichtet sein können. Sie sind nicht verpflichtet, uns personenbezogene Daten bereitzustellen. Soweit die Bereitstellung dieser Daten aber technisch zwingend mit der Nutzung unserer Dienste verbunden ist, führt eine Weigerung dazu, dass Sie unsere Dienste nicht nutzen können.

Bei der Nutzung der Dienste unterliegen Sie keiner automatisierten Entscheidungsfindung im Sinne von Art. 22 DSGVO.

2. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten werden nachfolgend dargestellt.

Verarbeitungsgrund	Rechtsgrundlage in der DSGVO	Erläuterung
Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen	Art. 6 Abs. 1 b)	Eine Verarbeitung erfolgt nur in dem Umfang, der für die Wahrnehmung und Erfüllung der Rechte und Pflichten aus dem Vertrag erforderlich ist. Soweit nicht ausdrücklich anders dargestellt, erfolgt die Datenverarbeitung durch uns nur in diesem Umfang.
Berechtigtes Interesse	Art. 6 Abs. 1 f)	Eine Verarbeitung erfolgt, soweit wir ein berechtigtes Interesse haben und keine entgegenstehenden überwiegenden Interessen des Betroffenen ersichtlich sind. Das konkrete Interesse wird in dieser Datenschutzhinweise im Rahmen der Verarbeitungsdarstellung erläutert.
Rechtliche Pflicht	Art. 6 Abs. 1 c)	Eine Verarbeitung erfolgt, soweit dies zur Erfüllung deutscher oder europäischer gesetzlicher Pflichten erforderlich ist.

III. Datenverarbeitung für den Betrieb der *Dienste*

Damit wir Ihnen die *Dienste* bereitstellen können, ist es erforderlich, bestimmte Daten zu verarbeiten.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

1. Grundlegende Daten

Verantwortlicher für die Verarbeitung der Stamm- und Konfigurationsdaten ist die Entität aus der Hornetsecurity Gruppe, die unter I, "Kontaktdaten" (Seite 3), markiert ist

a. Stammdaten

Die Stammdaten des Auftraggebers (Name, Anschrift, Ansprechpartner, Telefonnummer, E-Mail-Adresse, Abteilung, Position, gebuchte Dienste, Abrechnungszeitraum, Kontoverbindung) werden zur Verwaltung der Dienste erfasst und zur Erfüllung der vertraglich vereinbarten Leistungen verwendet. Persönliche Daten von Mitbenutzern (E-Mail-Adresse) werden erfasst und zur Erfüllung der vertraglich vereinbarten Leistungen verwendet.

Die Datenverarbeitung von Mitbenutzerdaten erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Datenverarbeitung der Stammdaten des Auftraggebers werden zum Zweck der Kundenstammpflege an Unterauftragnehmer auf Systemen in einem Drittland verarbeitet (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). Die Übermittlung der Daten erfolgt auf Grundlage von Standardvertragsklauseln.

Die Datenverarbeitung in der CRM-Software von Salesforce erfolgt in gemeinsamer Verantwortung gem. Art. 26 DSGVO der unter I, „Kontaktinformationen" genannten Unternehmen. Betroffene können die wesentlichen Inhalte dieser Vereinbarung auf Anfrage einsehen. Rechtsgrundlage hierfür ist unser berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f) i. V. m. Erw. 48 DSGVO an der Effizienzsteigerung und Kostenminimierung durch die Schaffung und Nutzung gemeinsamer Verwaltungsstrukturen.

Des Weiteren werden Teile der Stammdaten des Auftraggebers zum Zwecke der Rechnungszustellung und des -versands (per Brief oder E-Mail) an Unterauftragnehmer innerhalb der EU übermittelt und auf deren Systemen verarbeitet (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Germany).

b. Konfigurationsdaten

Die technische Konfiguration des jeweils gebuchten *Dienstes* wird in Verbindung mit der E-Mail-Adresse des Nutzers, der Gruppenzugehörigkeit eines Benutzers oder dem Domainnamen des Kunden gespeichert.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Für VM Backup und 365 Total Backup gilt außerdem:

Für die Validierung der Lizenz werden die zur eindeutigen Identifikation erforderlichen Stammdaten (E-Mailadresse) an die Systeme der Hornetsecurity Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malta, EU, übertragen.

2. 365 Permission Manager

365 Permission Manager ist ein Software-Tool für Governance, Risk & Compliance (GRC), mit dem Benutzer einen vollständigen Überblick und ein Verständnis ihrer M365-Dateiberechtigungen im eigenen Tenant in der Microsoft Azure Cloud für SharePoint Online, OneDrive for Business, Microsoft Teams und Microsoft 365 Groups erhalten.

Die automatische Datenverarbeitung umfasst den Abruf und die Verarbeitung der Metadaten der im M365 Tenant gespeicherten Objekte. Objekte, deren Metadaten abgerufen werden, sind: Dateien, Ordner, Dokumentenbibliotheken, Sites, Benutzer, Gruppen. Abgerufene und verarbeitete Metadaten sind die Besitzer der Objekte (Mailadresse, Anzeigename), Informationen zu den Objekten, denen Zugriffsrechte erteilt wurden (Mailadresse, Anzeigename, sowohl von Objekten innerhalb als auch außerhalb der eigenen Organisation), sowie die zugeordneten Berechtigungen.

Ein Zugriff auf die Inhalte der Objekte (Dateiinhalte) ist nicht möglich.

Die Löschung der abgerufenen und gespeicherten Metadaten erfolgt, sobald das entsprechende Objekt in der Microsoft Cloud gelöscht wird oder wenn der Dienst für den Kunden im Control Panel deaktiviert wird.

Die Verarbeitung der abgerufenen Metadaten erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3. 365 Total Backup

365 Total Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Sicherungs- und Wiederherstellungslösung für Microsoft 365 Mailboxen, OneDrive—Konten für Unternehmen, SharePoint-Dokumentbibliotheken, Teams-Chats und Endpoints.

365 Total Backup ermöglicht dem Kunden über eine Multi-Tenant-Konsole eine richtlinienbasierte Konfiguration, Übersicht und Überwachung von Rechten, Sicherungen und zu sichernden M365 Objekten Alle Backup-Daten sind mit kundenindividuellen AES-256-Schlüsseln verschlüsselt.

Die Datenverwaltung der gesicherten und verschlüsselten Daten erfolgt in der Hornetsecurity Gruppe konzernintern durch Hornetsecurity Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malta ("Hornetsecurity Ltd.").

Die verschlüsselten Sicherungsdaten werden aufgrund der durch den Kunden getätigten Konfiguration gespeichert:

- in der Hornetsecurity-Cloud, unter anderem in Deutschland, Frankreich, der Schweiz, Großbritannien, Kanada und den Vereinigten Staaten (Virginia und Georgia), bereitgestellt von der Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover,
- oder bei älteren Installationen (vor Februar 2022) in der Microsoft Azure Cloud, Zone Westeuropa – als „Cold Storage", wobei Hornetsecurity Ltd. die Microsoft Azure-Plattform und Compliance-Dienste nutzt. Die Azure Westeuropa Cloud Plattform und Services sind zertifiziert nach SOC 1 Type 2, SOC 2 Type 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS and HIPAA.

Während des Betriebs wird die eingesetzte Softwarelizenz online mit der in den Stammdaten hinterlegten erworbenen Lizenz abgeglichen. Eine Übertragung an oder Verarbeitung der Nutzdaten der Dienste durch den Auftragnehmer erfolgt nicht.

4. 365 Total Protection

Bei Spam and Malware Protection werden eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf den IT-Systemen des Auftragnehmers gefiltert. Es werden auch ausgehende E-Mails gefiltert.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs und der -zustellung, IP-Adressen der an der Kommunikation beteiligten Server, SMTP-Errorcode und -text), Inhalt von E-Mails und die Klassifikation der Mail (Clean, Spam, Virus, Infomail). Die Nachrichten-Metadaten werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Für die Nutzung von Individual User Signatures, Company Disclaimer und 1-Click Intelligent Ads wird der Einsatz eines Verzeichnisdienstes auf Seiten des Auftraggebers vorausgesetzt, der vom Auftragnehmer über das LDAP-Protokoll abgefragt werden kann. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein. Die Nachrichten müssen über die Relays des Auftragnehmers versendet werden.

Die automatische Datenverarbeitung umfasst die Mailadresse des Nutzers, zugeordneter Gruppenname im Verzeichnisdienst, weitere ggf. im Verzeichnisdienst verknüpfte Informationen wie Organisationszugehörigkeit, Position, Telefonnummer, Faxnummer und Mailfooter-Inhalte, die auf Seiten des Auftraggebers der Gruppe im Verzeichnis zugeordnet sind. Die personenbezogenen Daten, die dem Verzeichnis entnommen werden, werden nach Beendigung der Dienstnutzung gelöscht. Die verarbeitete Nachricht wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Global S/MIME & PGP Encryption: Der Auftragnehmer verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien. Je nach Einstellung der Richtlinien werden ausgehende E-Mails im geschützten Websafe für den Empfänger bereitgestellt.

Die automatische Datenverarbeitung umfasst die E-Mail-Adresse des Absenders und Empfängers, privater und öffentlicher S/MIME bzw. PGP-Schlüssel, ausgehende E-Mailinhalte an Dritte (Websafe), Mailadresse in Public Keys von Dritten, Status der Verschlüsselung und Inhalte von E-Mails. Die Daten Absender, Empfänger und Verschlüsselungsstatus werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Archiving: Der Auftragnehmer archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen.

Die automatische Datenverarbeitung umfasst die Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs, IP-Adressen der an der Kommunikation beteiligten Server, den Inhalt von E-Mails und ggf. Name und Typ des Anhangs.

Die Daten Absender- und Empfängeradresse, Mailbetreff, Datum/Uhrzeit, Anhangsname und -typ werden zur Anzeige im Control Panel verwendet. Alle diese Daten inkl. der Nachricht selber werden nach kundenspezifischer Archivdauer zzgl. 1 Jahr gespeichert und danach gelöscht. Eine Löschhemmung auf Kundenwunsch kann die Speicherdauer erhöhen.

Advanced Thread Protection (ATP): schützt den E-Mail-Verkehr des Auftraggebers vor gezielten und individuellen Angriffen, wie Spear-Phishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud. Zur Erkennung von Angriffen werden durch den Auftragnehmer als verdächtig eingestufte E-Mails des Auftraggebers durch erweiterte Filtertechniken untersucht.

Hierzu werden Metainformationen zum Mailinhalt sowie der Mailanhangstyp, -name und -inhalt automatisch verarbeitet. Die Metainformationen zum Mailinhalt werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail wird nach erfolgreicher Analyse aus dem ATP-System gelöscht.

Contingency Covering: Der Auftragnehmer stellt im Falle des Ausfalls des Zielservers je Benutzer ein E-Mail Postfach mit 10 GB Speicherplatz zur Verfügung. Auf E-Mails in diesem Postfach können autorisierte Benutzer über ein Webmail-Interface oder per IMAP und POP3 zugreifen.

Die automatische Datenverarbeitung umfasst Metadaten der Nachricht (die Mailadresse des Absenders und Empfängers, Datum/Uhrzeit des Maileingangs), Mailinhalte sowie Webmail-Metadaten (Anmeldename, IP-Adresse, Verbindungsdauer, Abrufvolumen, Protokoll). Nachrichten-Metadaten, Webmail-Metadaten und archivierte Nachrichten werden nach spätestens 14 Monaten gelöscht. Nachrichten im Webmail-Postfach werden spätestens gelöscht, wenn der Kunde den Dienst nicht mehr nutzt.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist.

Für die Nutzung von Single-Sign-On wird bei der Anmeldung des Nutzers die E-Mail-Adresse an Microsoft weitergegeben.

Eine Weitergabe anderer Daten an Dritte erfolgt nicht, Zugriff auf die Daten durch Dritte erfolgt ebenfalls nicht.

5. 365 Total Protection Enterprise Backup

Dieser Dienst ist ein Zusammenschluss der Dienste

- 365 Total Protection (Seite 8) und
- 365 Total Backup (Seite 7).

Bitte lesen Sie dort die entsprechenden Informationen.

6. AI Cyber Assistant: AI Email Security Analyst

AI Email Security Analyst teilt Endbenutzern mit, welche Vorsichtsmaßnahmen sie im Umgang mit der gemeldeten E-Mail treffen sollten. Zudem liefert das Feature eine Erklärung und Bewertung legitimer oder bösartiger Indikatoren innerhalb der Nachricht.

Administratoren können AI Email Security Analyst im E-Mail Live Tracking verwenden, wo sie auf Abruf eine generische Analyse, Risikoeinschätzung und KI-gestützte Klassifizierung der Mailinhalte erhalten. Es werden keine Detailinformationen der E-Mail-Inhalte bekanntgegeben.

Der AI Email Security Analyst verarbeitet Daten über vortrainierte LLMs, die in gekapselten MS Azure-Umgebungen gehostet werden. MS Azure-Server in der Region USA für Kunden aus den USA und Kanada, MS Azure-Server in der Region Europa für Kunden aus der EU und dem Rest der Welt.

Die E-Mail-Inhalte werden nach der Bewertung weder im KI-System gespeichert noch zu Trainingszwecken verwendet. Die Ausgabe der Bewertung in Verbindung mit dem Nutzer-Feedback des AI Email Security Analyst können dazu verwendet werden, die Erkennungsalgorithmen zu verbessern.

Die Speicherung der E-Mails erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

7. AI Cyber Assistant: AI Recipient Validation

AI Recipient Validation ist ein Tool, mit dem Endbenutzer von M365-Tenants in ihrem Outlook-Client gewarnt werden können, wenn eine von ihnen gesendete E-Mail möglicherweise fehlgeleitet ist (z. Bsp. wenn ein falscher Empfänger in einen E-Mail-Thread aufgenommen wurde) oder sensible Informationen enthält (z. B. Kreditkartennummern oder personenbezogene Daten). Die Benutzer können die Ratschläge annehmen oder fortfahren, ohne Änderungen an der E-Mail vorzunehmen. Die Vorschläge des Produkts werden auf der Grundlage des Benutzerverhaltens aktualisiert.

Die automatische Datenverarbeitung in der Cloud umfasst den Betreff der Mail, Absender und Empfänger (jeweils Klartextname und Mailadresse), Art der Mail (neu, Antwort, Weiterleitung), Zeitpunkt des Versendens der Mail, Eingestellte Sprache des Outlook-Clients, alle Benutzer und Gruppen des Tenants, Anzahl der Empfänger in Verteilerlisten, Anzahl der versendeten Mails, ferner Performance-Statistiken des Outlook-Add-Ins.

Die automatische Datenverarbeitung im lokalen Outlook-Client umfasst den E-Mail Inhalt.

AI Recipient Validation verwendet weder generative KI noch Large Language Models (LLMs). Die Bewertung basiert auf einer regelbasierten Entscheidungslogik in Form eines Entscheidungsbaums. Rückmeldungen dazu, ob ein Empfänger im jeweiligen E-Mail-Kontext als valide oder unerwünscht bestätigt wurde, können zur Anpassung dieser Entscheidungslogik und damit zur Verbesserung zukünftiger Bewertungen verwendet werden. Dabei erfolgt weder ein Training noch ein Fine-Tuning eines LLM.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

8. AI Cyber Assistant: Conversational Agent

Der Conversational Agent ist über das Control Panel erreichbar und unterstützt Nutzer auf Partnerebene und Nutzer mit Berechtigung zur Nutzung des Agenten. Es werden Antworten zu Fragen des Vertriebs, der Technik und Nutzungs- und Leistungskennzahlen der Dienste bereitgestellt.

Der Conversational Agent verwendet ein vortrainiertes Large Language Model (LLM). Zur Beantwortung von Anfragen erhält das Modell Zugriff auf ausgewählte interne Vertriebs-, Marketing-, Technik- und Supportinformationen sowie, im Berechtigungskontext des Benutzers, auf relevante Kunden- und Nutzungsmetadaten aus dem Email Live Tracking.

Ein- und Ausgabedaten werden zur Laufzeit als Kontext verarbeitet und nicht zum Training des LLM verwendet.

Zu Zwecken der Qualitätssicherung werden die letzten 50 Benutzereingaben und LLM-Ausgaben gespeichert, längstens jedoch für 30 Tage.

Beachten Sie, dass die Antworten KI-erzeugt sind und unter Umständen nicht korrekt sein können.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Die Verarbeitung und Speicherung erfolgt in Deutschland. Für Nutzer in den USA erfolgt die Verarbeitung und Speicherung in den USA.

9. AI Cyber Assistant: Teams Protection

Teams Protection schützt Endbenutzer beim Nachrichtenaustausch in Microsoft Teams vor kompromittierenden Nachrichten, indem alle Nachrichten mit URLs gescannt werden. Wenn eine Bedrohung erkannt wird, erscheint eine Warnmeldung im Chatverlauf durch den AI Cyber Assistant Bot. Optional können Nachrichten mit potenziell bösartiger URL gelöscht werden. Teams Protection nutzt Datenbestand und Erkennungstechnologien aus Hornetsecuritys Secure Links (Teil von Advanced Threat Protection, Seite 18).

Administratoren erhalten im Control Panel eine Übersicht über Chats mit erkannten bösartigen URLs unter Angabe der beteiligten Gesprächspartner und der fraglichen URL. Konten, die schadhaften Inhalte verbreiten, können ausgesperrt werden.

Alle Teams-Nachrichten werden von unseren Servern in unseren eigenen Rechenzentren verarbeitet. Wir speichern erkannte bösartige URLs und die Teilnehmer der Kommunikation, um unsere Kunden zu warnen und Details zu diesen Bedrohungen anzuzeigen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

10. Control Panel, Anmeldung am

Wenn Sie bereits Kunde von Hornetsecurity sind, können Sie sich über unsere Website im Control Panel, von dem aus Sie Ihre Leistung nutzen und verwalten können, anmelden. Für die Anmeldung benötigen Sie jeweils Ihren Benutzernamen bzw. Ihre E-Mail-Adresse sowie Ihr Password. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

11. Hornet.email Webmail, Anmeldung an

Wenn Sie bereits Kunde von Hornetsecurity sind, können Sie sich über unsere Website im Control Panel, von dem aus Sie Ihre Leistung nutzen und verwalten können, anmelden. Als Kunde von Webmail können Sie sich über einen separaten Link in Ihrem Postfach anmelden. Für die Anmeldung benötigen Sie jeweils Ihren Benutzernamen bzw. Ihre E-Mail-Adresse sowie Ihr Password. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

12. Hosted Exchange

Der Auftraggeber kann zusätzlich zum Spam and Malware Protection Hosted Exchange Postfächer buchen, wenn kein eigener Mailserver genutzt werden soll. Hosted Exchange bietet Ihnen ohne zusätzlichen Aufwand den sicheren Betrieb eines professionell verwalteten Exchange Servers in Ihrer Maildomäne mit Active Sync, gemeinsamen Kontaktinformationen,

Online-Kalender, Gruppen-Collaboration und Zugriff von verschiedenen Clients und Hardware-Plattformen.

Die automatische Datenverarbeitung umfasst empfangene und gesendete E-Mails, Mailadresse des Nutzers, Gruppenmitgliedschaften, Erstellungsdatum des Postfachs, Berechtigungen von/auf andere interne Konten derselben Domäne und genutzte Mobilgeräte für Zugriff auf das Postfach. Ferner, sofern eingepflegt: Firma, Position, Abteilung, MA-Nummer, Vorgesetzter, Telefonnummern, Adresse. Die Daten werden spätestens 90 Tage nach Kündigung des Dienstes gelöscht.

E-Mails werden zur Verarbeitung und Speicherung an Server von Subunternehmen in der EU übermittelt (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Germany oder Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Germany).

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

13. KI, Einsatz von Künstlicher Intelligenz

a. Einleitung

Dieses Dokument erläutert unsere Praktiken in Bezug auf das Sammeln, Speichern und Verarbeiten von E-Mail-Metadaten und latenten Themen aus E-Mail-Inhalten für unsere maschinellen Lern- und KI-Projekte bei Hornetsecurity. Unser Ansatz stellt die Privatsphäre der Benutzer in den Vordergrund und steht im Einklang mit den bestehenden Datenschutzrichtlinien. Unser Hauptaugenmerk liegt zwar nach wie vor auf E-Mail-Metadaten, aber die Identifizierung von E-Mail-Themen liefert Erkenntnisse für die Verfeinerung von Modellen für maschinelles Lernen, insbesondere für die E-Mail-Klassifizierung, die für Services wie Targeted Fraud Forensics, Phishing Protection, AI Recipient Validation und Infomail-Filter-Produkte und -Features erforderlich ist.

b. Zweck der Verarbeitung

Kontinuierliche Verbesserung von Modellen zur Klassifizierung von E-Mails

Wir verfeinern und verbessern die Algorithmen des maschinellen Lernens durch die Nutzung von E-Mail-Daten, um die Genauigkeit und Relevanz ihrer Vorhersagen zu gewährleisten. Dies hilft uns, effektiv zwischen echter Kommunikation, Spam und bösartigen Inhalten zu unterscheiden.

E-Mail-Kategorisierung

Mithilfe von E-Mail-Metadaten und latenten Themen werden E-Mails in verschiedene Arten unterteilt, wie zum Beispiel „Werbung“ oder „Phishing“. Diese Vorgehensweise ist eng mit unserem Produkt Infomail-Filter verbunden, mit dem Benutzer unerwünschte E-Mails unter Quarantäne stellen können.

Teilen von sensiblen Informationen und Datenlecks

Für unsere Produkte Targeted Fraud Forensics und AI Recipient Validation ist es entscheidend, die Wahrscheinlichkeit der Weitergabe sensibler Informationen an Unbefugte vorher-

zusagen. Zu diesem Zweck analysieren wir E-Mail-Metadaten, soziale Graphen, z. B. Verbindungen zwischen E-Mail-Absendern und -Empfängern, sowie latente Themen, um potenzielle Datenlecks und Sicherheitsbedrohungen zu erkennen.

Verbesserung der Benutzerfreundlichkeit

Benutzeraktionen, wie das Melden unerwünschter E-Mails oder das Ändern von E-Mail-Inhalten auf der Grundlage von Vorschlägen, beeinflussen die Optimierung der Benutzerfreundlichkeit der Produkte von Hornetsecurity. Durch diese Optimierung werden unerwünschte E-Mails reduziert und es werden relevantere Warnungen und Handlungsempfehlungen angeboten.

Kontoschutz und Sicherheit

Die Auswertung von E-Mail-Daten und Trendanalysen zur Erkennung von Anomalien oder potenziellen Sicherheitsbedrohungen, wie z. B. aufkommende Phishing-Kampagnen oder kompromittierte E-Mail-Konten, hilft uns, unsere Benutzer und ihre Daten zu schützen.

c. Von uns gesammelte Daten

Grundlegende Identifikatoren:

- E-Mail-Adresse des Absenders
- E-Mail-Adresse(n) des Empfängers
- IP-Adressen, Hostnamen und ASN (Autonomous System Number) der Absender-Server

Zeitliche Daten:

- Zeitstempel von E-Mail-Zustellungen
- Zeitstempel für Rückmeldungen von Benutzern und Administratoren zu E-Mails, die als Spam, Infomail oder harmlos gemeldet wurden

Nachrichtenmerkmale und Authentifizierungsstatus:

- Größe der Nachricht
- Format der Nachricht (HTML, reiner Text und andere Details zum Inhaltstyp)
- Die Prüfsumme(n) des Bodys und des Headers der Nachricht
- Authentifizierungs- und Verifizierungsdetails (Einträge für DKIM, DMARC, SPF Records)

Interaktionsinformationen:

- Rückmeldung zur E-Mail (z. B. als Spam oder harmlos gemeldet)
- Antwortaktionen auf Nachrichten (z. B. beantwortet, weitergeleitet, erster Kontakt)
- Aktionen als Reaktion auf Warnungen und Benachrichtigungen (z. B. die Entscheidung, ob eine E-Mail gesendet werden soll, nach Aufforderung durch AI Recipient Validation)
- Metadaten wie die Anzahl der Nachrichten, Schlüsselwörter im Betreff und die Verteilung der zugehörigen Zeitstempel für bestimmte Empfänger / Verteilerlisten (AI Recipient Validation)

Metadaten von Anhängen:

- Anzahl der Anhänge

- Dateitypen (z.B. .pdf, .docx, .jpg)
- Dateigrößen
- Dateinamen mit anonymisierten personenbezogenen Daten
- Prüfsumme(n) der Datei(en)

Links und Domains:

- Links in einer E-Mail oder in E-Mail-Anhängen mit anonymisierten URL-Pfaden und Parametern
- Domains der extrahierten Links und ihre DNS-Informationen (z. B. A-Einträge des DNS)

Header-Daten:

- Informationen aus dem Header-Abschnitt der E-Mail, einschließlich:
- Von
- An
- Datum
- Betreff mit anonymisierten personenbezogenen Daten
- Message-ID
- User-Agent und X-Mailer-Daten
- Empfangene Zeilen
- Ergebnisse der Authentifizierung
- Inhaltsbezogene Nachrichten-Header (z. B. „Content-Type")

Ableitung des Themas aus dem Body der Nachricht:

Um unsere E-Mail-Klassifizierungsmodelle zu verbessern, extrahieren wir das allgemeine Thema des E-Mail-Inhalts. Dabei wird der Nachrichtentext verarbeitet, um eine übergeordnete Kategorie oder ein Thema zu erkennen, ohne konkrete oder sensible Details aus dem Nachrichtentext selbst zu speichern.

Beispiel: Eine E-Mail mit Einzelheiten zu einem bevorstehenden Warenverkauf könnte allgemein als "Werbeaktion" oder "Verkaufsveranstaltung" kategorisiert werden.

d. KI-Werkzeuge, Datenspeicherung und Aufbewahrung

Alle KI-Tools und -Modelle werden entweder intern selbst entwickelt oder über vertrauenswürdige Plattformen wie Azure bereitgestellt. Für den KI-Speicher nutzen wir sowohl unsere eigene Infrastruktur als auch von Microsoft Azure gehostete Large Language Models (LLMs), um fortschrittliche KI-Funktionen bereitzustellen. Unsere Prompt-Daten enthalten nur die minimal notwendigen personenbezogenen Daten zur Diensterbringung. Die Daten werden niemals ohne ausdrückliche Genehmigung gespeichert oder für das Modelltraining verwendet. Externe LLMs werden ohne unsere Daten vom Provider des LLM trainiert.

Die KI-Speicher- und Verarbeitungsinfrastruktur befindet sich entweder im Hornetsecurity-Rechenzentrum oder in der sicheren Cloud-Umgebung von Azure. Der Zugriff auf Daten und Modelle wird datenschutzrechtlich streng kontrolliert und überwacht. Dritte Parteien oder nicht autorisiertes Personal erhalten keinen Zugriff auf diese Daten. Die Modelle für maschinelles Lernen werden ausschließlich über unsere sichere Infrastruktur oder über gesicherte

Verbindungen zu Azure-Diensten bereitgestellt und genutzt. Jede Datentransaktion zwischen Kundensystemen und unserer AI/ML-API wird durch robuste End-to-End-Verschlüsselungsverfahren geschützt. Dies gewährleistet die Vertraulichkeit und Integrität der Daten während der Übertragung.

Protokolle zur Speicherung und Aufbewahrung

- Die Daten werden im Ruhezustand und während der Übertragung verschlüsselt. Die Verschlüsselungsverfahren entsprechen den Best Practices der Branche.
- Die Daten werden so lange aufbewahrt, wie es zur Erfüllung der angegebenen Verarbeitungsziele erforderlich ist. Einige Log-Dateien können in Übereinstimmung mit unseren Richtlinien zur Datenaufbewahrung bis zu 12 Monate lang aufbewahrt werden.
- Alle anderen Daten, die für den Betrieb oder die Erfüllung der Funktionen eines aktiven kostenpflichtigen Produkts oder Services gespeichert werden, werden so lange aufbewahrt, wie diese Daten benötigt werden.
- Beendete Services folgen anschließend einem Deaktivierungsverfahren.

Anonymisierung von persönlich identifizierbaren Informationen:

- Um die Privatsphäre der Benutzer zu gewährleisten und die Datenschutzstandards einzuhalten, werden personenbezogene Daten vor der Speicherung systematisch anonymisiert, sofern dies möglich ist.
- Die Anonymisierung von PII (Personal Identifiable Information) ist eine Maßnahme, die ergriffen wird, um potenzielle Verzerrungen in unseren maschinellen Lernmodellen zu beseitigen und sicherzustellen, dass die Modelle objektiv arbeiten.

14. Security Awareness Service

Beim Security Awareness Service werden Daten der Benutzer (Name, Abteilung, Mailadresse, zugewiesene Gruppe für die Auswertung) per CSV-Import, Abgleich mit MS365 oder per LDAP-Synchronisation erfasst. Die Daten dienen der Bereitstellung eines Awareness-Trainings (Videos, Fragebögen, Informationsblätter) und dem Versand simulierter Phishing-E-Mails an den Benutzer.

Die Ergebnisse der simulierten Angriffe (klickt ein Benutzer auf den simulierten Phishing-Link, gibt ein Benutzer Zugangsdaten auf einer simulierten Phishing-Webseite ein) werden statistisch ausgewertet und pro Gruppe und pro Benutzer ausgegeben. Die Ergebnisse werden pseudonymisiert gespeichert. Bei aktiviertem Privacy Mode entfällt die Möglichkeit einer personenbezogenen Auswertung. Aus den gesammelten Informationen wird ein Employee Security Index (ESI®) gebildet, der den Awareness-Fortschritt dokumentiert aber auch einen direkten Vergleich mit einer Gruppe sehr gut ausgebildeter Anwender erlaubt.

Zur realitätsnahen Simulation von Phishing Szenarien werden als Absenderadressen auch firmeneigene Mailadressen als gefälschte Absender verwendet. Ein Benutzer kann der Nutzung seiner Mailadresse zu solchen Zwecken widersprechen.

Zur realitätsnahen Simulation von Spear-Phishing-E-Mails auf OSINT-Basis (Open Source Intelligence) werden auch öffentlich verfügbare Firmendaten und Personenangaben ausge-

wertet, z. Bsp. Informationen von Firmenbewertungsportalen wie Kununu.com oder geschäftsbezogenen Social Media Quellen wie z. Bsp. Xing.com oder LinkedIn.com. Ebenso kann in höheren Trainings-Leveln auf frühere, real empfangene oder versendete Mails Bezug genommen werden, die mit der Phishing-Simulation gar nichts zu tun haben.

Informationen, die im Rahmen von simulierten Phishing-E-Mails durch Benutzer eingegeben werden, z. Bsp. Anmeldedaten auf von uns generierten und gefälschten Anmeldeseiten, werden weder verarbeitet noch gespeichert. Dokumentenanhänge, die im Rahmen von simulierten Phishing-E-Mails von Benutzern geöffnet werden, z. Bsp. Word-Dokumente oder Excel-Tabellen, enthalten keinen Schadcode.

Verarbeitung von Meldungen potenzieller Phishing-E-Mails in Outlook über die Schaltfläche des Hornetsecurity AddOns:

- Sofern es sich um eine simulierte Phishing-E-Mail im Rahmen des Security Awareness Service handelt, wird die erfolgreiche Meldung dem Nutzer bestätigt und statistisch erfasst.
- Sofern es keine simulierte Phishing-E-Mail ist und der Kunde auch den Service Spam und Malware Filter gebucht hat, wird die gemeldete E-Mail zur weiteren Analyse an unser Security Lab gesendet.
- Sofern es keine simulierte Phishing-E-Mail ist und der Kunde nicht den Service Spam und Malware Filter gebucht hat, wird die gemeldete E-Mail an ein vom Kunden zu wählendes Support-Postfach gesendet.

Die zur Konfiguration des Dienstes benötigten Kundendaten und alle statistischen Auswertungen werden spätestens 4 Wochen nach Vertragsende gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

15. Spam and Malware Protection

Bei Spam and Malware Protection werden eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf den IT-Systemen des Auftragnehmers gefiltert. Soweit der Auftraggeber es wünscht, werden auch ausgehende E-Mails gefiltert.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs und der -zustellung, IP-Adressen der an der Kommunikation beteiligten Server, SMTP-Errorcode und -text), Inhalt von E-Mails und die Klassifikation der Mail (Clean, Spam, Virus, Infomail). Die Nachrichten-Metadaten werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist.

Eine Weitergabe anderer Daten (Mailheader, Absender, Adressat, Betreff, Datum, Textinhalt) an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

a. Optional: Advanced Thread Protection (ATP)

ATP schützt den E-Mail-Verkehr des Auftraggebers vor gezielten und individuellen Angriffen, wie Spear-Phishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud. Zur Erkennung von Angriffen werden durch den Auftragnehmer als verdächtig eingestufte E-Mails des Auftraggebers durch erweiterte Filtertechniken untersucht.

Hierzu werden Metainformationen zum Mailinhalt sowie der Mailanhangstyp, -name und -inhalt automatisch verarbeitet. Die Metainformationen zum Mailinhalt werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail wird nach erfolgreicher Analyse aus dem ATP-System gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

b. Optional: Secure Links (als Bestandteil von ATP)

Zur Erhöhung der Sicherheit bei der Nutzung unserer E-Mail-Dienste setzen wir die Funktion „Secure Links" ein. Dabei werden in eingehenden E-Mails enthaltene Links technisch umgeschrieben und beim Aufruf zunächst über eine Sicherheitsinfrastruktur geprüft.

Im Rahmen dieser Prüfung werden die Zieladresse und die darüber erreichbaren Webinhalte automatisiert auf Anzeichen für Phishing, Schadsoftware oder andere sicherheitsrelevante Merkmale untersucht. Hierfür kommen regelbasierte Verfahren sowie Machine-Learning- und Deep-Learning-Verfahren zum Einsatz. Eine Verarbeitung von E-Mail-Inhalten durch Large Language Models oder generative KI findet nicht statt.

Die Sicherheitsanalyse beschränkt sich auf die aufgerufene URL und die darüber erreichbaren Webressourcen. Inhalte der E-Mail, Absender- und Empfängerinformationen sowie Anhänge werden nicht für das Training, Fine-Tuning oder die Weiterentwicklung der eingesetzten Erkennungsmodelle verwendet.

Soweit eine URL oder die aufgerufene Webseite selbst personenbezogene Daten enthält, können diese technisch im Rahmen der Sicherheitsprüfung verarbeitet werden. Eine Nutzung dieser Daten zu Trainingszwecken oder zur Optimierung der zugrunde liegenden Erkennungsmodelle erfolgt nicht.

c. Optional: Email Encryption

Der Auftragnehmer bestellt und verwaltet S/MIME-Zertifikate, verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien. Je nach Einstellung der Richtlinien werden ausgehende E-Mails im geschützten Websafe für den Empfänger bereitgestellt.

Die automatische Datenverarbeitung umfasst die E-Mail-Adresse des Absenders und Empfängers, den privaten und öffentlichen S/MIME bzw. PGP-Schlüssel, Inhalte von ausgehenden Emails an Dritte (Websafe), die Mailadresse in Public Keys von Dritten, den Status der Verschlüsselung und den Inhalt der Email. Die Daten Absender, Empfänger und Verschlüsselungsstatus werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist.

Zur Bestellung von S/MIME-Zertifikaten werden E-Mail-Adresse und Vor- und Nachname des Zertifikatsbestellers zur Verarbeitung an ein Subunternehmen in der EU übermittelt (InterNetX GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg, Germany).

Für eine Zwei-Faktor-Authentifizierung (2FA) des Websafe-Empfängers wird bei Einwilligung dessen Handy-Nummer zur Verarbeitung an einen Subunternehmer übermittelt (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA). Die Übermittlung erfolgt auf Basis von Standardvertragsklauseln. Dort wird die Handynummer nach Beendigung des Prozesses bei Twilio umgehend gelöscht. Der Auftragnehmer speichert die Handy-Nummer, solange das Postfach des Empfängers existiert.

Eine Weitergabe anderer als der zur S/MIME-Zertifikatsbestellung und Generierung eines 2FA-Schlüssels genannten Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

d. Optional: Archiving

Der Auftragnehmer archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen.

Die automatische Datenverarbeitung umfasst die Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs, IP-Adressen der an der Kommunikation beteiligten Server, den Inhalt von E-Mails und ggf. Name und Typ des Anhangs.

Die Daten Absender- und Empfängeradresse, Mailbetreff, Datum/Uhrzeit, Anhangsname und -typ werden zur Anzeige im Control Panel verwendet. Alle diese Daten inkl. der Nachricht selber werden nach kundenspezifischer Archivdauer zzgl. 1 Jahr gespeichert und danach gelöscht. Eine Löschhemmung auf Kundenwunsch kann die Speicherdauer erhöhen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

e. Optional: Continuity Service

Der Auftragnehmer stellt eingehende und ausgehende E-Mails des Auftraggebers für einen Zeitraum von 3 Monaten im Archiv bereit unter der Voraussetzung, dass diese E-Mails über die Server von Hornetsecurity geleitet werden.

Der Auftragnehmer stellt ferner je Benutzer ein E-Mail Postfach mit 10 GB Speicherplatz zur Verfügung. Auf E-Mails in diesem Postfach können autorisierte Benutzer über ein Webmail-Interface oder per IMAP und POP3 zugreifen.

Die automatische Datenverarbeitung umfasst Metadaten der Nachricht (die Mailadresse des Absenders und Empfängers, Datum/Uhrzeit des Maileingangs), Mailinhalte sowie Webmail-Metadaten (Anmeldename, IP-Adresse, Verbindungsdauer, Abrufvolumen, Protokoll). Nachrichten-Metadaten, Webmail-Metadaten und archivierte Nachrichten werden nach spätestens 14 Monaten gelöscht. Nachrichten im Webmail-Postfach werden spätestens gelöscht, wenn der Kunde den Dienst nicht mehr nutzt.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

f. Optional: E-Mail-Signature and Disclaimer

Für die Nutzung von Signature and Disclaimer wird der Einsatz eines Verzeichnisdienstes auf Seiten des Auftraggebers vorausgesetzt, der vom Auftragnehmer über das LDAP-Protokoll abgefragt werden kann. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein. Die Nachrichten müssen über die Relays des Auftragnehmers versendet werden.

Die automatische Datenverarbeitung umfasst die Mailadresse des Nutzers, zugeordneter Gruppenname im Verzeichnisdienst und weitere ggf. im Verzeichnisdienst verknüpfte Informationen wie Organisationszugehörigkeit, Position, Telefonnummer, Faxnummer und Mailfooter-Inhalte, die auf Seiten des Auftraggebers der Gruppe im Verzeichnis zugeordnet sind. Die personenbezogenen Daten, die dem Verzeichnis entnommen werden, werden nach Beendigung der Dienstnutzung gelöscht. Die verarbeitete Nachricht wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

g. Optional: E-Mail made in Germany

Der Auftragnehmer ermöglicht eine Anbindung der E-Mail-Infrastruktur des Auftraggebers an den E-Mail made in Germany (EmiG) – Verbund und realisiert hierfür die Mailserver-seitige Umsetzung, die für die Erfüllung der Anforderungen an eine durchgehende Transportverschlüsselung von E-Mails im EmiG-Verbund notwendig ist.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit Maileingang, IP-Adressen der an der Kommunikation beteiligten Server, Verschlüsselungsstatus) und Inhalt von E-Mails. Die Metadaten der Nachrichtenübermittlung werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

16. Test-Onboarding

Um die Leistung der Dienste zu testen, können Sie sich direkt über unsere Website anmelden. Hierfür benötigen wir verschiedene Informationen zu Ihnen persönlich, zu Domäne, Server und Nutzer, für welche die Leistung gewünscht ist, sowie zum gewünschten Service. Die Pflichtfelder sind entsprechend gekennzeichnet. Alle weiteren Informationen erfolgen freiwillig. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

Die Stammdaten des Auftraggebers werden zum Zweck der Kundenstammdatenpflege bei einem Unterauftragnehmer auf Systemen in einem Drittland verarbeitet (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). Die Übermittlung der Daten erfolgt auf Grundlage von Standardvertragsklauseln.

Rechtsgrundlage der Verarbeitung ist insoweit die Durchführung vorvertraglicher Maßnahmen bzw. die Erforderlichkeit für die Vertragserfüllung.

17. VM Backup

VM Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Backup- und Wiederherstellungslösung für virtualisierte Server in Hyper-V und VMware-Umgebungen sowie physische Microsoft Server.

VM Backup ermöglicht dem Kunden die Durchführung von Backups auf die vom Kunden festgelegten Orte in den vom Kunden festgelegten Zeitintervallen. Die Verschlüsselung der Backups wird durch vom Kunden konfigurierte AES-256-Verschlüsselungsschlüssel (Passwort) sichergestellt. Alle Offsite-Kopien sind AES-256-verschlüsselt. Für Onsite-Backups (primär) ist die Verschlüsselung optional und wird ebenfalls unterstützt.

Für Offsite-Kopien erfolgt optional eine Datenspeicherung auf durch den Kunden bei Drittanbietern angemietetem Cloud-Speicher (Microsoft Azure Blob Storage, Wasabi Cloud Object Storage, Amazon S3 oder BackBlaze Cloud Storage). Der Kunde agiert als Auftraggeber gegenüber diesen Drittanbietern.

Während des Betriebs wird die eingesetzte Softwarelizenz online mit der in den Stammdaten hinterlegten erworbenen Lizenz abgeglichen. Eine Übertragung an oder Verarbeitung der Nutzdaten der Dienste durch den Auftragnehmer erfolgt nicht.

18. Web Filter

Ausgehende http/https- und ftp-Aufrufe des Auftraggebers werden über Proxy-Server des Auftragnehmers geleitet. Datenverkehr wird auf potenziell schädliche Inhalte geprüft und ggf. ausgefiltert.

Die automatische Datenverarbeitung umfasst Datum und Uhrzeit des Aufrufs einer Webadresse, aufrufende IP-Adresse, aufgerufene URL, klassifizierte Kategorie des aufgerufenen

Objekts, authentifizierte Entität: entweder E-Mail-Adresse, u.U. pseudonymisiert, oder IP-Adresse oder Verzeichnisdienst-Name und -Objektpfad oder Web Filter-Connector-String (sAM AccountName, Domain-ID, Rechnername, Rechner-IP, aufrufendes Programm). Die genannten Daten (URL ohne Pfad) werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

19. Websafe, Datenschutzerklärung für Dritte

Damit wir Ihnen diesen Dienst bereitstellen können, ist es erforderlich, bestimmte Daten zu verarbeiten. Die Verarbeitung dieser Informationen und gespeicherten Daten ist für die Erfüllung der bestehenden Vertragsbeziehung mit unseren Kunden erforderlich. Dies bildet die Rechtsgrundlage der Verarbeitung. Bei der Nutzung des Websafe Dienstes unterliegen Sie keiner automatisierten Entscheidungsfindung im Sinne von Art. 22 DSGVO.

Die automatische Datenverarbeitung umfasst Metadaten der Nachricht (die E -Mail-Adresse des Absenders und Empfängers, Datum/Uhrzeit des E-Mail- Eingangs), E-Mail-Inhalt, Websafe-Metadaten (Anmeldename, Ihre IP- Adresse, Verbindungsdauer, Abrufvolumen, Protokoll) sowie ggf. die Nummer Ihres Mobilfunkgerätes. Ihre E-Mails werden für 3 Monate im Websafe aufbewahrt. Danach werden sie gelöscht. Ihr Websafe-Konto besteht grundsätzlich, solange Sie dort E-Mails empfangen. Falls Sie keine E-Mails mehr erhalten, wird Ihr Websafe-Konto 12 Monate nach Erhalt der letzten E-Mail automatisch gelöscht. Dabei werden alle Ihre persönlichen Daten und insbesondere Ihre Telefonnummer von unseren Servern entfernt.

Um Ihre Registrierung abzuschließen, müssen wir eine PIN an Ihr Mobilgerät senden. Alternativ können Sie den Absender Ihrer E-Mail kontaktieren, damit er die PIN auf andere Weise an Sie weiterleiten kann. Der Websafe-Dienstanbieter erhebt keine Gebühren für die Nutzung des Websafe-Dienstes und den SMS-Versand.

Der Unterauftragnehmer für den Versand der SMS an Ihr Mobilgerät ist die Firma Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA. Die Übermittlung der Mobilfunknummer erfolgt auf Basis von EU-Standardvertragsklauseln. Die Mobilfunknummer wird nach Nutzung bei Twilio sofort wieder gelöscht.

Die Datenverarbeitung der Nachrichten-Metadaten, Websafe-Metadaten und Nachrichten im Websafe-Postfach erfolgen auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert sind. Eine Weitergabe dieser Daten an Dritte erfolgt nicht. Neben der Hornetsecurity GmbH haben keine Dritten Zugriff auf diese Daten.

IV. Widerspruchs- und Beseitigungsmöglichkeit

Soweit die Datenverarbeitung auf Ihrer Einwilligung oder unserem berechtigten Interesse basiert, haben Sie jederzeit das Recht, der Verarbeitung zu widersprechen oder Ihre erteilte Einwilligung zu widerrufen. Ihr Widerspruch bzw. Widerruf hat lediglich Wirkung für die Zukunft. Sie können sich jederzeit zur Ausübung Ihres Widerspruchs- oder Widerrufsrechts an datenschutz@hornetsecurity.com wenden. Wenn Sie einer Verarbeitung aufgrund unseres berechtigten Interesses widersprechen, dürfen wir die Verarbeitung dennoch fortführen, wenn wir zwingende schutzwürdige Gründe für die Verarbeitung nachweisen können, die Ihre Interessen, Rechte und Freiheiten überwiegen.

V. Betroffenenrechte

Werden auf Ihre Person bezogenen Daten verarbeitet, sind Sie Betroffener im Sinne von Art. 4 Abs. 1 DSGVO. Als Betroffenem stehen Ihnen in Bezug auf Ihre personenbezogenen Daten die nachfolgenden Rechte zu. Zur Ausübung dieser Rechte können Sie sich unter den oben angegebenen Kontaktdaten an uns wenden.

a. Recht auf Auskunft nach Art. 15 DSGVO

Sie haben ein Recht auf Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten. Dies umfasst die in Art. 15 DSGVO dargestellten Pflichtinformationen.

b. Recht auf Berichtigung nach Art. 16 DSGVO

Sie haben das Recht, die unverzügliche Berichtigung falscher sowie die Vervollständigung unrichtiger personenbezogener Daten.

c. Recht auf Löschung nach Art. 17 DSGVO

Sie haben das Recht, die Löschung Ihrer personenbezogenen Daten zu verlangen, wenn einer der in Art. 17 DSGVO genannten Gründe eingreift, insbesondere, wenn keine Rechtsgrundlage mehr für die Verarbeitung vorliegt.

d. Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO

Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn einer der in Art. 18 DSGVO genannten Gründe eingreift, insbesondere auf Ihren Wunsch hin statt einer Löschung der Daten.

e. Recht auf Datenübertragbarkeit nach Art. 20 DSGVO

Sie haben das Recht, alle bei uns über Sie gespeicherten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format herauszuverlangen und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

f. Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, Art. 77 DSGVO

Sie haben gemäß Art. 77 DSGVO das Recht, eine Beschwerde bei der für Sie zuständigen Aufsichtsbehörde einzureichen.

VI. Empfänger von Daten

Die Verarbeitung Ihrer personenbezogenen Daten im Rahmen der *Dienste* erfolgt zum Teil auch durch Auftragsverarbeiter. Diese werden ausschließlich auf der Grundlage einer Vereinbarung zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO einbezogen.

VII. Datenübermittlung in Drittländer

Die personenbezogenen Daten, die wir von Ihnen im Rahmen der Leistungserbringung der *Dienste* erheben, werden nicht in Drittländer außerhalb des Europäischen Wirtschaftsraumes übermittelt.

Für den SMS-Versand einer Zwei-Faktor-Authentifizierung nutzen wir den Anbieter Twilio. mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Twilio nimmt am EU-U.S. DPF (Data Privacy Framework) teil und arbeitet nach Standardvertragsklauseln, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.

Für die Verwaltung Ihrer Vertragsdaten nutzen wir den Anbieter Salesforce mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Salesforce nimmt am EU-U.S. DPF (Data Privacy Framework) teil und arbeitet nach zertifizierten Standardvertragsklauseln, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.

Für die Verwaltung Ihrer elektronischen Unterschrift bei Verträgen nutzen wir den Anbieter Docusign mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Docusign arbeitet nach zertifizierten Standardvertragsklauseln, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.