LEISTUNGSBESCHREIBUNG der GBS Cloud-Dienste

Business User, im Folgenden **"Kunde"** und/oder **"Nutzer"** genannt; und

„GBS Europa GmbH", mit Sitz und eingetragener Adresse in: An der Zur Giesserei 19-27B, 76227 Karlsruhe, Deutschland, vertreten durch Andreas Philippi, in seiner Eigenschaft als Geschäftsführer, nachfolgend **„Anbieter"** und/oder **„GBS"** genannt.

1 PRÄAMBEL:

GBS stellt einen Security Cloud Service ("**Service**") zur Verfügung. Der Kunde erhält einen zentralen Service mit unterschiedlichen Komponenten auf Basis des gewählten Abonnements, der sich auf der Office 365 / Exchange Online Umgebung des Kunden integriert.

Diese Leistungsbeschreibung enthält detaillierte Informationen zu den verschiedenen Funktionen, die dem Kunden in Bezug auf die E-Mail Security zur Verfügung stehen, und das je nach dem vom Kunden gewählten Abonnement.

Für die Nutzung der Services gelten kundenseitig die folgenden technischen Voraussetzungen:

- Nutzung von Exchange Online oder O365;
- Internetzugang; und
- ein aktueller Internet-Browser.

GBS stellt dem Kunden eine detaillierte Übersicht über die technischen Voraussetzungen im Internet zur Verfügung. Die Bereitstellung und Übermittlung der technischen Voraussetzungen ist nicht Gegenstand dieser Leistungsbeschreibung.

2 Leistungsbeschreibung

2.1 Malware-Schutz für E-Mail

Dieser Service bietet erweiterte Malware-Erkennungs- und Schutzmechanismen, die es dem Kunden ermöglichen, seine eigenen Sicherheitsrichtlinien und Präferenzen auf den E-Mail-Verkehr anzuwenden und dabei vollständige Transparenz und Kontrolle zu haben.

Der Malware-Schutz von GBS für E-Mail ist eine Kombination aus proprietären Erkennungs-mechanismen und der Integration mit führenden Anti-Malware Engines von Drittanbietern. Der Kunde kann aus einer Liste von Anti-Malware Engines wählen, z. B. McAfee, Avira, Sophos und Kaspersky. Basierend auf der Wahl des Kunden wird einer oder eine Kombination aus mehreren der vorstehend genannten als Teil der Lösung verwendet.

Verdächtige E-Mails können entweder gekennzeichnet, blockiert oder in Quarantäne zur weiteren Prüfung und Bearbeitung gestellt werden.

Der Service erkennt und analysiert auch die wahre Dateierweiterung, erkennt das Dateiformat und bietet die Möglichkeit bestimmte Dateiformate zu blockieren.

2.2 SPAM Schutz für E-Mail

Der Service bietet einen verbesserten Anti-SPAM Schutz, der die GBS-eigene Inhaltserkennungs-Engine mit den branchenführenden SPAM-Bewertungsmechanismen von Sophos oder Kaspersky, je nach Wahl des Kunden, kombiniert, um maximalen Schutz, Sichtbarkeit und Flexibilität zu erreichen.

Die Inhaltserkennungs-Engine analysiert sowohl den Textkörper als auch den Inhalt der Anhänge und versucht, verdächtige Texte und Bedeutungen zu identifizieren, während die Engines der Dritthersteller hauptsächlich für RBL-Prüfungen und Reputationsvalidierung verwendet werden.

Es gibt zahlreiche Aktionen, die durchgeführt werden können. Sie hängen von den Richtlinien des Anbieters ab, so dass der Kunde zu jeder Zeit die Kontrolle über das Verhalten der Systeme hat. Die Standardeinstellungen sind: als Spam markieren, zu blockieren, in Quarantäne stellen, usw., es ist aber auch möglich deutlich kompliziertere Workflows und Abläufe zu konfigurieren.

3 Nachrichtenverschlüsselung für E-Mail

Dieser Service ermöglicht es dem Kunden die E-Mail-Kommunikation auf Nachrichtenebene zu verschlüsseln. Er erstellt eine PDF-Datei, die den E-Mail-Text enthält, sowie die eingebetteten Anhänge und schützt anschließend die PDF-Datei mit einem Passwort. Die flexiblen Konfigurationseinstellungen ermöglichen es dem Anbieter, verschiedene Richtlinien anzuwenden und geben dem Nutzer die entsprechende Flexibilität. Das Passwort kann voreingestellt sein, dynamisch vergeben werden oder vom Empfänger angefordert werden.

Diese Funktion kann in Verbindung mit der Inhaltserkennung auf Basis von Vertraulichkeit, Schlüsselwörtern usw. angewendet werden.

Dieser Service bietet eine einzigartige Nutzererfahrung, da weder der Absender noch der Empfänger seine E-Mail-Umgebung verlassen müssen, um ihn zu nutzen. Standardmäßig wird der Passkey / Passwort-Austausch für die Entschlüsselung direkt zwischen den beiden Nutzern entweder per E-Mail oder auf einem anderen Weg kommuniziert. Nutzer können sogar statische Passwörter festlegen – z. B. John legt ein Passwort <Passwort> für die Kommunikation mit Jean und ein anderes für die Kommunikation mit Reymond fest.

Es kann auch für interne Kommunikationen genutzt werden, wenn sensible Daten übertragen werden.

3.1 Server-zu-Server Verschlüsselung für E-Mail

Dieser Service richtet eine Server-zu-Server Verschlüsselung mit den Industriestandard-protokollen PGP oder S/MIME ein. Dies stellt sicher, dass beide E-Mail-Server immer verschlüsselte Kommunikation austauschen.

Dieser Service ist extrem nützlich, um sensible Daten mit bekannten dritten Parteien zu verschlüsseln, z.B. mit einer externen Rechtsberatungsfirma oder einer externen Finanzberatungsfirma. Auf diesem Wege ist sichergestellt, dass der Datenfluss zwischen den beiden Firmen immer verschlüsselt abläuft.

HINWEIS: Die Verwendung von S/MIME erfordert auch, dass eine Zertifikatsverwaltung vorhanden ist, die einen weiteren Service darstellt, welcher unten beschrieben wird.

3.2 Schlüssel/Zertifikatsverwaltung für E-Mail

Dieser Service erlaubt es Organisationen, alle Zertifikate/Schlüssel, die genutzt werden, zentral zu verwalten. Dies gilt bei Einsatz des S/MIME Verschlüsselungsmechanismus.

3.3 Verhinderung von Datenverlusten für E-Mail

Dieser Service arbeitet in Verbindung mit der GBS-Inhaltserkennungs-Engine und ermöglicht es dem Kunden, Datenrichtlinien auf den E-Mail-Flow anzuwenden, das 4-Augen Prinzip durchzusetzen und Anomalien im E-Mail Flow zu erkennen. Der Service kann entweder den Inhalt oder das Verhalten erkennen sowie einen Workflow auslösen, bei dem eine Genehmigung für eine Kommunikation erforderlich ist.

Für den Fall, dass sensible Daten erkannt werden, kann das System einen Workflow für das 4-Augen Prinzip auslösen und die Zustellung der E-Mail bis zur Freigabe aussetzen. Das System benachrichtigt auch die genehmigende Person, darüber dass eine Genehmigung ansteht.

Für den Fall, dass ein Nutzer anfängt, verdächtige E-Mail-Aktivitäten zu generieren, z. B. E-Mails zu nicht-standardmäßigen Zeiten an externe Parteien sendet, eine große Anzahl an kleinen E-Mails außerhalb des Unternehmens sendet usw., würde das System dies erkennen und einen Alarm über verdächtiges Verhalten auslösen, der vor gestohlenen Anmeldeinformationen oder einem böswilligen Insider schützen kann.

3.4 Anhangskonvertierung für E-Mail

Dieser Service ermöglicht es dem Kunden, Dateien mit aktivem Inhalt zu erkennen und sie in Dateien ohne aktiven Inhalt umzuwandeln, anstatt sie zu blockieren, während die ursprüngliche Datei weiterhin in Quarantäne verbleibt, falls sie benötigt wird. Dies ermöglicht dem Kunden, seine E-Mail-Kommunikation vor Anhängen mit aktivem Inhalt zu schützen, wenn diese von vertrauenswürdigen und in der Whitelist aufgeführten Domänen kommen.

3.5 Signatur-Management für E-Mails

Mit dem Signatur-Management können individualisierte Signaturen erstellt und regelbasiert als Disclaimer (sog. Trailer) an E-Mails angehängt werden.

E-Mails, die an externe Empfänger adressiert sind, können mit Grußworten, Firmeninformationen, Disclaimern, Verzichtserklärungen, rechtlichen Hinweisen etc. und bei Bedarf mit Bildern, Logos, vCards oder anderen Trailer-Dateianhängen versehen werden.

Durch die Flexibilität des Services, können individuelle Trailer für Abteilungen, Gruppen, Internet-Domains oder Einzelpersonen an beliebige Stellen in der E-Mail angehängt sowie zeitlich begrenzt werden. Unkomplizierte Konfiguration und zentrale Administration (auch über Abteilungen wie z.B. Marketing) ermöglichen eine optimale Nutzung und unterstützen einen einheitlichen Auftritt Ihres Unternehmens nach außen.

3.6 Abwesenheits-Management für E-Mails

Dieser Service ermöglicht ein zentrales Abwesenheits-Management, das zur Umleitung, Weiterleitung oder Generierung automatisierter Antworten genutzt werden kann. Dies ist sowohl für einmalige Abwesenheiten (z. B. für die Zeit eines Urlaubs, einer Krankheit oder einer Dienstreise) als auch für periodische Abwesenheiten an bestimmten Wochentagen (z. B. für Teilzeitkräfte) möglich. Auch eine rückwirkende Weiterleitung kann realisiert werden, z. B. für den Fall, dass ein Mitarbeiter vergessen hat, vor Urlaubsantritt eine Weiterleitung einzurichten. Bei entsprechender Konfiguration können Abwesenheitsbenachrichtigungen auch automatisch an den Absender und/oder Stellvertreter gesendet werden.

Der Service stellt so sicher, dass bei (geplanter oder unvorhergesehener) Abwesenheit keine wichtigen E-Mails unbearbeitet und/oder unbeantwortet bleiben.

Dies ist besonders wichtig, wenn es z. B. um zeitkritische Informationen, Rechnungen oder Angebotsanfragen geht.

GBS bietet den folgenden Service innerhalb der technischen und betrieblichen Möglichkeiten an.

3.7 Schutz vor Bedrohungen für SharePoint Online

Dieser Service bietet erweiterte Malware-Erkennungs- und Schutzmechanismen, mit denen der Kunde sicherstellen kann, dass keine bösartigen Dateien auf SharePoint Online gespeichert werden.

Der Service stellt eine Kombination aus proprietären Erkennungsmechanismen und Integration mit führenden Anti-Malware-Engines von Drittanbietern dar. Der Kunde kann aus einer Liste von Anti-Malware Engines wählen, z. B. McAfee, Avira, Sophos und Kaspersky. Basierend auf der Wahl des Kunden, wird einer oder eine Kombination aus mehreren der vorstehend genannten als Teil der Lösung verwendet.

Verdächtige Dateien werden sowohl während des Hochladens/Speicherns als auch auf der Grundlage eines vordefinierten Prüfplans identifiziert und zur weiteren Überprüfung und Verarbeitung in Quarantäne verschoben.

3.8 Schutz vor Bedrohungen für MS Teams

Dieser Service bietet erweiterte Malware-Erkennungs- und Schutzmechanismen, die sicherstellen, dass keine bösartigen Dateien auf MS Teams im Bereich “Dateien” gespeichert werden.

Der Service stellt eine Kombination aus proprietären Erkennungsmechanismen und Integration mit führenden Anti-Malware-Engines von Drittanbietern dar. Der Kunde kann aus einer Liste von Anti-Malware Engines wählen, z. B. McAfee, Avira, Sophos und Kaspersky. Basierend auf der Wahl des Kunden, wird einer oder eine Kombination aus mehreren der vorstehend genannten als Teil der Lösung verwendet.

Verdächtige Dateien werden sowohl während des Hochladens/Speicherns als auch auf der Grundlage eines vordefinierten Prüfplans identifiziert und zur weiteren Überprüfung und Verarbeitung in Quarantäne verschoben.

4 Services von GBS

4.1 Komponenten des Cloud Security Services

Der Service besteht aus verschiedenen Komponenten. Zu den wichtigsten gehören:

a) Core System

Die zentrale Komponente, die alle beschriebenen Services zur Verfügung stellt, wird in einer Umgebung installiert und eingerichtet, die auf Microsoft Azure basiert mit einer Architektur, die eine hohe Verfügbarkeit der Services und die nötige Performance zur Verfügung stellt.

Einige der zusätzlichen Funktionen, die nicht unter Artikel 1 “Leistungsbeschreibung” aufgelistet sind:

- Verbindung mit dem Azure Active Directory des Kunden;
- Verbindung mit dem Exchange Online/Office 365 des Kunden;

- Auditierung und Protokollierung;
- Verbindung mit Drittanbieter-Technologien.

b) WebClient

Der WebClient ermöglicht dem Kunden Zugriff auf seine Daten, Konfigurationseinstellungen, statistische Informationen und Auditing-Informationen. Der WebClient bietet den Nutzern auch, je nach zugewiesenen Rollen und Rechten, verschiedene Möglichkeiten.

Zu den wichtigsten Funktionen gehören:

- Konfiguration von Signaturen;
- Vorschau von Signaturen;
- Zentrales Abwesenheitsmanagement;
- Rollen und Rechte;
- Passwort-Manager.

c) Verwaltungskonsole

Einige der erweiterten Konfigurationen müssen über die MMC-Konsole durchgeführt werden.

Weitere Informationen finden Sie in der Produktdokumentation iQ.Suite.

4.2 Kundenspezifische Services

Der Kunde kann mit GBS kundenspezifische Leistungen vereinbaren, wie z. B. individuelle Systemanpassungen, Beratung zur Nutzung auf Basis von Best Practices, Design und Erstellung von Signaturen oder einen Proof of Concept. Der genaue Leistungsumfang wird in einem separaten Dokument festgehalten.

4.3 Zugang

Der Zugang des Kontoinhabers zur Verwaltung und Nutzung der Services von GBS erfolgt über das Internet. Jeder Zugang setzt voraus, dass sich der Account-Inhaber mit einer Zugangskennung, bestehend aus einer E-Mail-Adresse und einem Passwort, authentifiziert. Diese werden vom Kunden vergeben.

Weitere zusätzliche Details zur sicheren Erstauthentifizierung werden dem Kunden auf Informationsseiten im Internet mitgeteilt. Der Administrator kann Nutzer für die Nutzung der Module einrichten.

5 Support und Störungsannahme

a) Allgemeine SLA-Informationen finden Sie im Internet unter https://www.gbs.com

b) Online-Dokumentation

Bereitstellung von Online-Support in Form von FAQ;

Tipps, Anleitungen etc. in deutscher und englischer Sprache.

c) Störungsannahme und Hotline-Support

Die Annahme von Störungsmeldungen steht 24/7 als Online-Servicedesk zur Verfügung. Unter der Servicenummer beantwortet GBS auch produktbezogene und allgemeine Fragen zur Bedienung der GBS-Produkte.

Produktbezogene und allgemeine Fragen werden nur an Werktagen (montags bis freitags) von 8.00 bis 20.00 Uhr CET beantwortet.

Der Kundensupport gemäß Buchstabe b) steht nur dem Administrator oder seinem Stellvertreter zur Verfügung; die übrigen Nutzer haben keinen Anspruch auf Support.

Alle Informationen zu diesen Supportleistungen, einschließlich Servicezeiten und Kontaktdaten, finden Sie im Internet unter https://www.gbs.com.

6 Betrieb der Server- und Systemkomponenten

Alle für den Betrieb der Lösungen erforderlichen Server- und Systemkomponenten werden in einem technisch und organisatorisch sicheren, leistungsfähigen Rechnernetz betrieben, das gegen Angriffe und unberechtigte Zugriffe aus dem Internet geschützt ist.

Die Lösung ist mehrmandantenfähig. Die Umgebung und der Betrieb erfolgen innerhalb der Europäischen Union und damit unter Einhaltung der europäischen Datenschutz-Richtlinien. Je nach Wahl und Konfiguration der Dienste durch den Kunden, können einige Daten außerhalb der Europäischen Union verarbeitet werden.

Weitere Informationen hierzu finden Sie in unserer DPA und in den jeweiligen besonderen Bedingungen für die Datenverarbeitung der Unterauftragsverarbeiter. Das Computernetzwerk ist über den Internet-Backbone mit modernster Übertragungsgeschwindigkeit an das Internet angeschlossen.

Die Services für den Betrieb des Rechenzentrums stehen mit einer durchschnittlichen Verfügbarkeit von 99,9 % im Jahresmittel zur Verfügung.

Für den Betrieb und das Systemmanagement gelten die folgenden Leistungsmerkmale:

Betriebszeit 24/7;

Automatische Erkennung von Fehlern innerhalb des Rechnernetzes.

7 Betriebliche Bereitstellung

Die Zugangsdaten zur Freischaltung des Services werden dem Kunden oder dem vom Kunden benannten Administrator bei der erstmaligen Bereitstellung des Services durch GBS per E-Mail zugesandt.

8 Kompatibilität mit älterer Hardware und Betriebssoftware

GBS aktualisiert die Software kontinuierlich, um sie an neue oder aktualisierte Versionen der Betriebssysteme anzupassen.

Ältere Geräte- und Betriebssystemversionen werden so lange wie möglich unterstützt. Aus technischen Gründen kann jedoch weder sichergestellt werden, dass sie auf allen verfügbaren Hardwaretypen laufen, noch können veraltete Betriebssystemversionen unbegrenzt unterstützt werden. GBS behält sich das Recht vor, den Support für veraltete Betriebssystemversionen mit Vorankündigung einzustellen oder den Support für bestimmte Plattformen ganz einzustellen.

9 Laufzeit und Kündigung

Die Lösung wird dem Kunden mit einer Mindestlaufzeit von 12 (zwölf) Monaten zur Verfügung gestellt. Die Kündigungsfrist beträgt 30 (dreißig) Kalendertage zum Ende der Laufzeit. Wird der Service nicht fristgerecht gekündigt, verlängert er sich jeweils um 12 (zwölf) Monate.

Der Kunde kann die Lösung 30 (dreißig) Kalendertage im Voraus kostenlos testen. Die Testphase endet automatisch 30 (dreißig) Kalendertage nach Aktivierung, ohne dass ein Vertrag abgeschlossen wurde.