

Leistungsbeschreibung

ambiFOX GmbH

Fleehook 1
48683 Ahaus
Germany

+49 (0) 2561 8693 0

post@ambifox.com
www.ambifox.com



ambiFOX



Leistungsbeschreibung

Leistungsbeschreibung

1.1 Grundmodul	5
1.1.1 Grundmodul Lite	5
1.1.2 Benutzerpaket Standard	5
1.1.3 Benutzerpaket Standard Lite	6
1.1.4 Benutzerpaket Plus	6
1.1.5 Mandantenbenutzer	6
1.2 Projektierung	7
1.3 ambiCONNECT	8
1.3.1 Telefonanruf	8
1.3.2 Push-Benachrichtigung per App	8
1.4 ambiUSB	9
1.5 Benutzerkonto in der ASP-Umgebung	9
1.6 Fileserver	9
1.7 Appserver	10
1.7.1 Hardwarebereitstellung	10
1.7.2 Betriebssystem	10
1.7.3 Zusätzliche CPU	10
1.7.4 Zusätzlicher Arbeitsspeicher	10
1.8 Virtual Desktop	11
1.9 Monitoring der Systeme	11
2.0 Support und Service Levels	11
2.1 Administration und Konfiguration	12
2.1.1 Fileserver	12
2.1.2 Terminalserver	12
2.1.3 Mandantenserver	12
2.1.4 Appserver	12
2.1.5 ASP-Benutzer	12



Leistungsbeschreibung

2.2 Verfügbarkeit ambiFOX ASP	13
2.2.1 Berechnung der Verfügbarkeit.....	13
2.2.2 Verfügbarkeit bei einer Betriebsstätte des Kunden.....	13
2.2.3 Verfügbarkeit bei mehreren Betriebsstätten	13
2.2.4 Vereinbarte Verfügbarkeit	14
2.2.5 Abweichungen zur Verfügbarkeit.....	14
2.3 Servicezeiten des Anbieters.....	14
2.4 Branchensoftware.....	15
2.5 ambiNAS.....	15
2.5.1 Wartung	15
2.5.2 Kontrolle der Spiegelung.....	15
2.6 ambiBOX-Management.....	16
2.7 Datenkontingent.....	16
2.8 Zusätzliches Datenvolumen.....	16
2.9 Datensicherung.....	16
3.0 Monatliche Wartung der Systeme am festgelegten Wartungstermin	17
3.0.1 Wartung der Systeme	17
3.1 ambiVPN.....	17
3.2 ambiIPSEC.....	17
3.3 Öffentliche IP-Adresse.....	18
3.4 ambiMAIL ARCHIV	18
3.5 ambiCLOUD.....	19
3.6 Support und Implementierung	19
3.7 ambiCLOUD-Admin	19
3.8 ambiCLOUD-Benutzer	19
3.9 ambiBACKUP M365 Grundmodul	20
3.9.1 ambiBACKUP M365 Erweiterung	20



Leistungsbeschreibung

4.0 Mailgateway.....	20
4.1 Managed Reversproxy.....	21
4.2 Einrichtung der Remotedesktop-Verbindung	21
4.3 ambiSECURE M365 Produktlinie	21
4.3.1 Modul: Spam and Malware Protection (Basisleistung)	22
4.3.2 Modul: Signature and Disclaimer.....	23
4.3.3 Modul: Advanced Threat Protection (ATP)	24
4.3.4 Modul: Archiving.....	25
4.3.5. Modul: 365 Total Backup.....	27
4.3.6. Modul: Security Awareness Service (SAS)	30
4.3.7 Optionales Modul: E-Mail Encryption.....	32
4.3.8. Fair Use Limits (Einschränkungen zur angemessenen Nutzung)	34



Leistungsbeschreibung

1.1 Grundmodul

Das Grundmodul ist Voraussetzung für die Bereitstellung der Dienstleistung. Es enthält die wichtigsten Bestandteile der sogenannten „ASP-Umgebung“. Das ASP-Grundmodul enthält die folgenden Leistungen:

- 1 x Fileserver
- Virtual Desktop
- Datenkontingent: 300GB
- Datensicherung
- Monatliche Wartung der Systeme am festgelegten Wartungstermin
- Monitoring der Systeme
- Updates der Systeme
- Wartung der Systeme
- Administration & Konfiguration
- 1x ambiUSB
- Einspielen von zeitkritischen Updates zur Behebung von sog. „Zero-Day-Lücken“ außerhalb der Servicezeit

1.1.1 Grundmodul Lite

Das Grundmodul Lite ist Voraussetzung für die Bereitstellung der Dienstleistung. Es enthält die wichtigsten Bestandteile der sogenannten „ASP-Umgebung“. Das ASP-Grundmodul Lite enthält die folgenden Leistungen:

- 1 x Fileserver
- Virtual Desktop
- Datenkontingent: 300GB
- Datensicherung
- Monatliche Wartung der Systeme innerhalb der Geschäftszeiten
- Monitoring der Systeme innerhalb der Geschäftszeiten
- Updates der Systeme innerhalb der Geschäftszeiten
- Administration & Konfiguration
- 1x ambiUSB

1.1.2 Benutzerpaket Standard

Mit Hilfe des Benutzerpaket Standard ist es möglich sich an dem, im Rahmen des Grundmoduls zur Verfügung gestellten, Virtual Desktop anzumelden und die darauf installierten Programme zu nutzen. Der ASP-Benutzer enthält die folgenden Leistungen:

- Benutzerkonto in der ASP-Umgebung
- Microsoft-Lizenzen
- ambiCONNECT (1.3)
- Support
- Datenkontingent: 30GB
- 1 x Unterstützung Branchensoftware
- Administration & Konfiguration
- Einrichtung der Remotedesktop-Verbindung



Leistungsbeschreibung

Das Benutzerpaket Standard erfordert das ASP-Grundmodul.

1.1.3 Benutzerpaket Standard Lite

Mit Hilfe des Benutzerpaket Standard Lite ist es möglich sich an dem, im Rahmen des Grundmoduls zur Verfügung gestellten, Virtual Desktop anzumelden und die darauf installierten Programme zu nutzen. Der ASP-Benutzer enthält die folgenden Leistungen:

- Benutzerkonto in der ASP-Umgebung
- Microsoft-Lizenzen
- ambiCONNECT (1.13)
- Supportkontingent von 1h/Monat
- Datenkontingent: 30GB
- 1 x Unterstützung Branchensoftware
- Administration & Konfiguration
- Einrichtung der Remotedesktop-Verbindung

Das Benutzerpaket Standard Lite erfordert das Grundmodul Lite.

1.1.4 Benutzerpaket Plus

Mit Hilfe des Benutzerpaket Plus ist es möglich sich an dem, im Rahmen des Grundmoduls zur Verfügung gestellten, Virtual Desktop anzumelden und die darauf installierten Programme zu nutzen. Der ASP-Benutzer enthält die folgenden Leistungen:

- Benutzerkonto in der ASP-Umgebung
- Microsoft-Lizenzen
- ambiCONNECT
- Support
- Datenkontingent: 90GB
- 1 x Unterstützung Branchensoftware
- Administration & Konfiguration
- Einrichtung der Remotedesktop-Verbindung

Das Benutzerpaket Plus erfordert das Grundmodul.

1.1.5 Mandantenbenutzer

Mit Hilfe des Mandantenbenutzers ist es möglich sich an dem, im Rahmen des Mandantenservers zur Verfügung gestellten, Virtual Desktop anzumelden und die darauf installierten Programme zu nutzen. Der Mandantenbenutzer ist ein, unter Beachtung spezieller Vorgaben, erstellter Benutzer. Der Benutzer hat stark eingeschränkte Rechte, um nur die für den Mandanten relevanten Daten und Funktionen nutzen zu können. Der Mandantenbenutzer enthält die folgenden Leistungen:

- Benutzerkonto in der ASP-Umgebung
- Microsoft-Lizenzen
- ambiCONNECT



Leistungsbeschreibung

- Support
- Administration & Konfiguration
- Einrichtung der Remotedesktop-Verbindung

1.2 Projektierung

Nach Bestellung von ambiFOX ASP wird sich ein ambiFOX-Mitarbeiter mit dem Kunden in Verbindung setzen und einen Termin zur sogenannten Projektierung vereinbaren. Bei der Projektierung werden alle, für den Betrieb notwendigen, Daten erfasst. Dazu gehören z.B.:

- Anzahl und Namen der Mitarbeiter des Kunden
- Anzahl und Namen der genutzten Programme des Kunden
- Anzahl der Standorte des Kunden
- Internetverbindungen der jeweiligen Standorte des Kunden
- Informationen zur DNS-Verwaltung des Kunden
- Bestandsaufnahme der abzulösenden Systemumgebung des Kunden

Für das Erfassen der Daten ist die Mit- und Zuarbeit des Kunden zwingend erforderlich. Dem Anbieter muss ein technisch versierter Mitarbeiter als Ansprechpartner zur Verfügung gestellt werden. Nach Aufnahme der Daten wird unter Umständen ein aktualisiertes Angebot für die Bereitstellung von ambiFOX ASP durch den Anbieter erstellt.

Der Anbieter und der Kunde vereinbaren gemeinsam einen Zeitpunkt zu welchem die Umstellung der abzulösenden Systemumgebung auf das ambiFOX ASP vollzogen werden soll.

Der Anbieter importiert die Daten des Kunden in das vom Anbieter zur Verfügung gestellte Rechenzentrum. Zu den Daten zählen Dateien, Datenbanken und andere für den Betrieb der Systemumgebung, bzw. der Programme, benötigten digitalen Daten. Hierzu nutzt der Anbieter einen der folgenden technischen Umsetzungswege. Der Anbieter entscheidet auf Basis der technischen und organisatorischen Gegebenheiten, welcher Umsetzungsweg am besten geeignet ist.

- Synchronisierung über eine verschlüsselte Verbindung über das Internet: Auf dem abzulösenden System wird eine Clientsoftware installiert, welche regelmäßig eine Verbindung zum Rechenzentrum des Anbieters herstellt und die Daten des Kunden über eine verschlüsselte Verbindung in das Rechenzentrum des Anbieters kopiert. Die Synchronisation erfolgt mehrfach über einen längeren Zeitraum, um zu gewährleisten, dass alle benötigten Daten im Umstellungszeitraum übertragen werden können. Die letzte Synchronisation erfolgt in der Regel in der Nacht auf den Umstellungstag.
- Kopieren der Daten auf einen portablen Datenträger: Der Anbieter sendet dem Kunden einen portablen Datenträger zu. Der Datenträger ist verschlüsselt und wird vom Kunden im Netzwerk des Kunden installiert. Anschließend wird vom Anbieter auf dem abzulösenden System eine Clientsoftware installiert, welche regelmäßig eine Verbindung zum Datenträger des Anbieters herstellt und die Daten des Kunden auf den Datenträger des Anbieters kopiert. Die Synchronisation erfolgt mehrfach über einen längeren Zeitraum, um zu gewährleisten, dass alle benötigten Daten im Umstellungszeitraum übertragen werden können. Die letzte Synchronisation erfolgt in der Regel in der Nacht auf den Umstellungstag. Der Datenträger wird anschließend entweder am Umstellungstag vom Anbieter abgeholt oder über den Postweg, bzw. per Kurier, vom Kunden an den Anbieter gesendet.



Leistungsbeschreibung

Die Umstellung wird vom Anbieter aus den Räumlichkeiten des Anbieters durchgeführt. Der Kunde erhält vor dem Umstellungstag alle benötigten Geräte und Zugänge. Zu den vom Kunden durchzuführenden Umstellungsarbeiten gehört der Umbau des Netzwerks, um eine gesicherte Verbindung zum Rechenzentrum des Anbieters herzustellen, das Vorbereiten der lokalen Clients (Computer & Laptops) für die Verbindung zum ambiFOX ASP, sowie das Konfigurieren der Drucker und Scanner. Sollte die Anwesenheit eines Mitarbeiters des Anbieters benötigt werden, kann der Kunde diese Dienstleistung kostenpflichtig beim Anbieter buchen.

Der Anbieter stellt am Umstellungstag die ASP-Systeme zur Verfügung. Zur Bereitstellung gehört:

- Fileserver
- Virtual Desktop-Server
- Installation der Programme
- Erstellung der Benutzerkonten
- Import der Daten des Kunden

In der Regel stehen die ASP-Systeme dem Kunden am übernächsten Arbeitstag nach dem Umstellungstag zur Verfügung. Am Umstellungstag selbst ist kein Arbeiten möglich.

1.3 ambiCONNECT

ambiCONNECT stellt die Möglichkeit dar, die für den Kunden bereitgestellten Systeme aus einem externen, nicht per VPN an das Rechenzentrum angeschlossenen Standort, zu erreichen und sich daran über das Remotedesktop-Protokoll anzumelden. Die Anzahl der monatlichen Anmeldungen über das ambiCONNECT-Verfahren sind von Anbieterseite nicht begrenzt. Die Anmeldung wird per Multi-Faktor-Authentifizierung (MFA) abgesichert. Die MFA kann wie folgt durchgeführt werden:

1.3.1 Telefonanruf

- Bei der MFA durch den Telefonanruf, wird nach erfolgreicher Eingabe der Benutzer-Zugangsdaten in der dafür vorgesehenen Remotedesktop-Verbindung, ein Telefonanruf auf die Rufnummer des Nutzers ausgelöst. Die Anmeldung muss durch Annahme des Anrufs und anschließendem Betätigen einer spezifizierten Taste auf dem Tastenfeld des Telefons durch den Nutzer bestätigt werden.
- Voraussetzung für die Nutzung des Telefonanrufs ist, dass der Kunde dem Anbieter die Rufnummer des Nutzers, der authentifiziert werden soll, mitteilt. Die Rufnummer muss für den Zeitraum der Anmeldung per Anruf erreichbar sein.

1.3.2 Push-Benachrichtigung per App

- Bei der MFA durch eine Push-Benachrichtigung per App, wird nach erfolgreicher Eingabe der Benutzer-Zugangsdaten in der dafür vorgesehenen Remotedesktop-Verbindung, eine Push-Benachrichtigung an die zuvor eingerichtete App auf dem Gerät des Nutzers gesendet. Die Push-Benachrichtigung muss auf dem Gerät des Nutzers bestätigt werden, um den Anmeldevorgang erfolgreich abschließen zu können.
- Voraussetzung für die Nutzung der Push-Benachrichtigung ist ein, vom Technologiepartner des Anbieters, unterstütztes Endgerät. Auf dem Gerät muss die App des Technologiepartners installiert und konfiguriert sein.



Leistungsbeschreibung

ambiCONNECT erfordert das Benutzerpaket Standard oder Benutzerpaket Plus.

1.4 ambiUSB

Mit Hilfe von ambiUSB können USB-Geräte wie etwa Lizenzdongles oder Smartcards an das Kundensystem angeschlossen werden. Das USB-Gerät wird an einen USB-Port im Rechenzentrum des Anbieters angeschlossen. Auf dem Kundensystem wird eine Clientsoftware installiert, welche die Verbindung zum USB-Gerät herstellt. Das USB-Gerät kann dann auf dem Kundensystem genutzt werden. Pro erworbenem ambiUSB kann ein USB-Gerät angeschlossen werden. USB-Massenspeicher können mit ambiUSB nicht verbunden werden. Die verbundenen USB-Geräte befinden sich im verschlossenen Schrank des Anbieters. Die USB-Geräte werden vor dem Verbinden durch den Anbieter auf mögliche Mängel untersucht.

ambiUSB erfordert das Grundmodul.

1.5 Benutzerkonto in der ASP-Umgebung

Das Benutzerkonto in der ASP-Umgebung besteht aus den Zugangsdaten (Benutzername und Kennwort) und einem virtuellen Objekt in der Benutzerverwaltung des Anbieters. Das Benutzerkonto wird als *Microsoft Active Directory*-Benutzerobjekt geführt. An das Benutzerkonto können Zugriffsrechte gebunden werden, die den Zugriff auf Netzwerkordner, den Virtual Desktop sowie auf einzelne Programme auf dem Virtual Desktop ermöglichen. Die Vergabe dieser Rechte erfolgt individuell je Benutzerkonto.

Jedes Benutzerkonto verfügt über persönliche Ordner, die sich im Benutzerprofil des jeweiligen Benutzers befinden. Auf diese persönlichen Ordner können ausschließlich der jeweilige Benutzer und Administratoren zugreifen.

Im Benutzerkonto werden persönliche Attribute wie Rufnummern, Adresse, etwaige Titel oder Anrede gespeichert. Diese Daten werden im *Microsoft Active Directory*-Benutzerobjekt abgelegt. Der Zugriff auf diese Attribute ist auf den Benutzer und Administratoren beschränkt. Die Pflege und Änderung der persönlichen Attribute erfolgt durch die Mitarbeiter des Anbieters.

Die Erstellung, Änderung und Deaktivierung des Benutzerkontos erfolgt ausschließlich durch die Mitarbeiter des Anbieters. Die Daten des Benutzerkontos verbleiben auf den Systemen des Anbieters, bis ein expliziter Löschauftrag durch den Kunden erteilt wird. Erst nach Eingang eines solchen Löschauftrags werden die Daten gelöscht.

Der Support für das Benutzerkonto wird innerhalb der Servicezeiten des Anbieters erbracht.

1.6 Fileserver

Im Rahmen des ASP-Grundmoduls wird dem Kunden ein virtualisierter Fileserver bereitgestellt. Dieser Server verfügt in der Grundausstattung über zwei vCPU-Kerne und 6 GB RAM. Die Hardware kann bei Bedarf im Ermessen des Anbieters erweitert werden, ein Anspruch des Kunden auf eine bestimmte Hardwareausstattung besteht jedoch nicht. Als Betriebssystem kommt ein zum Bereitstellungszeitpunkt von Microsoft und vom Anbieter unterstütztes Windows Server-Betriebssystem zum Einsatz. Der Kunde hat keinen Anspruch auf ein bestimmtes Betriebssystem. Der Fileserver stellt die Dienste Dateiablage und -bereitstellung im Netzwerk, *Microsoft Active Directory* zur Benutzerverwaltung sowie einen FTP-Server für den Dateitransfer von Netzwerkgeräten zur Verfügung.



Leistungsbeschreibung

1.7 Appserver

Der virtuelle Applikationsserver, kurz Appserver, soll eine flexible und skalierbare Plattform für die Bereitstellung und Ausführung von größeren Anwendungen bieten, die signifikante Ressourcenanforderungen haben. Zusätzlich werden Appserver in das Backupsystem des Anbieters aufgenommen, um die Datenintegrität und Verfügbarkeit der auf dem Applikationsserver gehosteten Anwendungen sicherzustellen. Der Appserver kann entweder im Netzwerk des Kunden, im Rechenzentrum des Anbieters, oder in einem gesonderten Netz für die Erreichbarkeit aus dem Internet betrieben werden (sog. DMZ).

1.7.1 Hardwarebereitstellung

Der Appserver wird in der Grundausstattung mit einer Konfiguration von zwei CPU-Kernen und vier Gigabyte Arbeitsspeicher bereitgestellt. Zusätzliche Prozessoren und zusätzlicher Arbeitsspeicher können unter Berücksichtigung der verfügbaren Hardwareressourcen des Anbieters hinzugebucht werden.

1.7.2 Betriebssystem

Als Betriebssystem wird entweder ein zum Zeitpunkt der Bereitstellung von Microsoft unterstütztes Windows Server-Betriebssystem oder eine Linux-Distribution eingesetzt, je nach den Anforderungen des Kunden und den Systemvoraussetzungen der gehosteten Anwendungen. Die Auswahl des Betriebssystems erfolgt in Abstimmung mit dem Kunden, um sicherzustellen, dass die gewählte Plattform die Anforderungen der Anwendungen erfüllt und den Betrieb des virtuellen Applikationsservers unterstützt. Der Kunde hat keinen Anspruch auf den Einsatz eines bestimmten Betriebssystems.

Der Appserver erfordert das Grundmodul.

1.7.3 Zusätzliche CPU

Das Produkt „Zusätzliche CPU“ ermöglicht es dem Kunden, über die in der Standardkonfiguration des Appservers bereitgestellte Anzahl an CPU-Kernen hinaus, weitere CPU-Kerne hinzubuchen. Die Bereitstellung der zusätzlichen CPUs erfolgt virtuell und ist an die Nutzung eines Appservers gebunden, dessen Definition und Anforderungen in einer eigenen Leistungsbeschreibung geregelt sind. Die maximale Anzahl der hinzufügbaren CPUs ist durch die zum jeweiligen Zeitpunkt verfügbare Hardware des Anbieters begrenzt.

Zusätzliche CPU erfordert einen Appserver.

1.7.4 Zusätzlicher Arbeitsspeicher

Das Produkt „Zusätzlicher Arbeitsspeicher“ ermöglicht es dem Kunden, über die in der Standardkonfiguration des Appservers bereitgestellte Menge des Arbeitsspeichers hinaus, weiteren Arbeitsspeicher hinzubuchen. Die Bereitstellung des zusätzlichen Arbeitsspeichers erfolgt virtuell und ist an die Nutzung eines Appservers gebunden, dessen Definition und Anforderungen in einer eigenen Leistungsbeschreibung geregelt sind. Die maximale Menge des hinzufügbaren Arbeitsspeichers ist durch die zum jeweiligen Zeitpunkt verfügbare Hardware des Anbieters begrenzt.

Zusätzlicher Arbeitsspeicher erfordert einen Appserver.



Leistungsbeschreibung

1.8 Virtual Desktop

Der Virtual Desktop dient der Bereitstellung der Anwendungen des Kunden auf einer, von den Benutzern des Kunden, gemeinsam genutzten Plattform. Der Kunde kann auf den Virtual Desktop und die darauf installierten Anwendungen über das Remotedesktop-Protokoll von Microsoft zugreifen. Für den Zugriff ist zudem eine Verbindung zum Rechenzentrum des Anbieters, entweder mit Hilfe der **ambiBOX** oder per **ambiCONNECT** erforderlich. Zur Nutzung des Virtual Desktop ist zudem pro Mitarbeiter ein Benutzerpaket Standard oder Benutzerpaket Plus notwendig.

Die Virtual Desktop-Plattform wird in Form eines oder mehrerer virtualisierter Server bereitgestellt. In der Grundausstattung hat die Plattform die folgende Hardwarekonfiguration:

- **2 vCPU-KERNE**
- **6GB RAM**
- **75GB FESTPLATTENKAPAZITÄT, NUR FÜR DAS BETRIEBSSYSTEM**

Die Hardware sowie Anzahl der Virtual Desktop-Plattform(en) wird bei Bedarf im Ermessen des Anbieters erweitert. Ein Anspruch des Kunden auf eine bestimmte Hardwareausstattung besteht nicht. Als Betriebssystem wird ein, zum Zeitpunkt der Bereitstellung, von Microsoft und vom Anbieter unterstütztes Windows Server-Betriebssystem eingesetzt. Ein Anspruch des Kunden auf ein bestimmtes Betriebssystem besteht nicht.

1.9 Monitoring der Systeme

Monitoring ist die Überwachung der Server rund um die Uhr hinsichtlich der Lauffähigkeit der Dienste, Prüfung der Festplattenkapazität, Prüfung der Anti-Viren-Software, Prüfung des physischen Festplattenzustands, Überprüfung der Erreichbarkeit einer Webseite, Überprüfung der Server- und Umgebungstemperaturen, sofern die entsprechenden Hard- und Softwarekomponenten diese Informationen bereitstellen. Bei kritischen Ereignissen erfolgt eine Meldung per Mail an die Mitarbeiter des Anbieters, sowie per Warnhinweis über sogenannte Dashboards in den Räumlichkeiten des Anbieters. Die vom Monitoring erkannten Probleme werden innerhalb der Servicezeiten des Anbieters proaktiv behoben.

Monitoring erfordert das Grundmodul.

2.0 Support und Service Levels

Der Anbieter stellt eine Ansprechstelle für den Kunden (Helpdesk) zur Verfügung. Der Helpdesk ist per E-Mail unter **support@ambifox.com** und telefonisch unter **+49 (2561) 8693 700** erreichbar. Die Bearbeitung der Anfragen erfolgt innerhalb der Servicezeiten des Anbieters.

Außerhalb dieser Zeiten ist eine Notfall-Hotline aktiv. Bitte beachten Sie, dass die Notfall-Hotline nicht das gesamte Spektrum der Helpdesk-Leistungen abdeckt.

Fehler in den zentralen Komponenten des Anbieters werden vom Anbieter rund um die Uhr, von Montag bis Sonntag, überwacht und behoben. Eine proaktive Benachrichtigung der Kunden über mögliche Störungen erfolgt über das Statusportal:

[HTTPS://STATUS.AMBIFOX.COM](https://status.ambifox.com)



Leistungsbeschreibung

Die Verfügbarkeit des Dienstes „ASP Server Hosting“ stellt die Möglichkeit des Zugriffs auf, im Rahmen des ASP-Vertrages zur Verfügung gestellten Systeme, dar.

2.1 Administration und Konfiguration

Leistungen für Administration und Konfiguration sind alle Maßnahmen, die im Zusammenhang mit der laufenden Verwaltung installierter Systeme, Dienste und Applikationen sowie bestehender Benutzer erbracht werden. Administration und Konfiguration werden vom Anbieter für die folgenden Produkte erbracht:

2.1.1 Fileserver

Der Anbieter übernimmt die Administration und Konfiguration für den Betrieb sowie das Betriebssystem des Fileservers. Etwaige Zusatz-Software wie in etwa Branchensoftware, Office-Anwendungen oder andere, separat zum Betriebssystem installierte Software, ist nicht in der Administration und Konfiguration enthalten.

2.1.2 Terminalserver

Der Anbieter übernimmt die Administration und Konfiguration für den Betrieb sowie das Betriebssystem des Terminalservers. Etwaige Zusatz-Software wie in etwa Branchensoftware, Office-Anwendungen oder andere, separat zum Betriebssystem installierte Software, ist nicht in der Administration und Konfiguration enthalten.

2.1.3 Mandantenserver

Der Anbieter übernimmt die Administration und Konfiguration für den Betrieb sowie das Betriebssystem des Mandantenservers. Etwaige Zusatz-Software wie in etwa Branchensoftware, Office-Anwendungen oder andere, separat zum Betriebssystem installierte Software, ist nicht in der Administration und Konfiguration enthalten.

2.1.4 Appserver

Der Anbieter übernimmt die Administration und Konfiguration für den Betrieb sowie das Betriebssystem des Appservers. Etwaige Zusatz-Software wie in etwa Telefonsoftware, Datenbanksysteme oder andere, separat zum Betriebssystem installierte, Software ist nicht in der Administration und Konfiguration enthalten.

2.1.5 ASP-Benutzer

Der Anbieter übernimmt die Administration und Konfiguration des ASP-Benutzers. Dazu gehören unter anderem übliche Vorgänge wie:

- Kennwort zurücksetzen
- Benutzernamen anpassen



Leistungsbeschreibung

- Zugriffsrechte auf Netzwerkordner anpassen

2.2 Verfügbarkeit ambiFOX ASP

Die Verfügbarkeit der Dienstleistung ambiFOX ASP stellt die Möglichkeit des Zugriffs auf die Systeme des Anbieters innerhalb der Servicezeiten (Kapitel 2.3) dar. Die Lauffähigkeit der einzelnen Anwendungen ist hierfür nicht von Bedeutung.

Vorab mit dem Kunden abgesprochene oder vom Kunden verschuldete Unterbrechungen bleiben ebenfalls unberücksichtigt.

Somit wird die Funktionsfähigkeit der zur Verfügung gestellten Netzwerkelemente (vom Kunden bereitgestellte Leitungen bleiben unberücksichtigt) sowie der Serversysteme bei der Berechnung der Verfügbarkeit herangezogen.

Als Ausfallzeit wird die Zeit bezeichnet, in der die Systeme aufgrund einer Störung der vorgenannten Komponenten, nicht erreichbar sind.

2.2.1 Berechnung der Verfügbarkeit

Die Verfügbarkeit wird aus der tatsächlich zur Verfügung stehenden Betriebszeit der Systeme (Verfügungszeit) und der Summe der Ausfälle (Ausfallzeit) berechnet.

Die Verfügungszeit wird folgendermaßen berechnet:

Servicezeiten (Mo. bis Fr. 7:30 – 17:30 Uhr) 10 Std. 00 Min.

./.. Abzüglich mit dem Kunden vereinbarte Unterbrechungen (z.B. Datenrücksicherung, Software-Update usw.)

./.. Abzüglich vom Kunden verschuldete Ausfälle im Verantwortungsbereich des Kunden

./.. Abzüglich Ausfallzeiten

Verfügungszeit = 100 %

2.2.2 Verfügbarkeit bei einer Betriebsstätte des Kunden

$$\text{Verfügbarkeit} = \frac{\text{Verfügungszeit}}{\text{Verfügungszeit} + \text{Ausfallzeit}} \quad \%$$

2.2.3 Verfügbarkeit bei mehreren Betriebsstätten



Leistungsbeschreibung

$$\text{Verfügbarkeit} = \frac{\text{Summe der Verfügbarkeiten je Betriebsstätte} \times \text{multipliziert mit der Anzahl der Benutzer}}{\text{Summe aller angeschlossenen Benutzer}} \%$$

Bei mehreren Betriebsstätten, erfolgt die Berechnung der vereinbarten Verfügbarkeit als das arithmetische Mittel der Verfügbarkeiten der einzelnen Betriebsstätten, gewichtet nach Anzahl der Benutzer je Betriebsstätte.

2.2.4 Vereinbarte Verfügbarkeit

Aufgrund technischer Gegebenheiten der ambiFOX ASP-Dienstleistung können Störungen nicht vollständig ausgeschlossen werden. Der Anbieter ist jedoch bemüht alle Risiken so weit wie möglich zu minimieren und macht daher eine Verfügbarkeitszusage im Sinne der zuvor beschriebenen Definitionen von mindestens **99 %** über den Zeitraum eines Jahres. Der Berechnungszeitraum beginnt mit dem Monat, für den die erste Vergütung gezahlt wird.

2.2.5 Abweichungen zur Verfügbarkeit

Bei am Ende des Abrechnungszeitraumes festgestellten Abweichungen von der vereinbarten Verfügbarkeit, gelten folgende Minderungsbeträge, der im Abrechnungszeitraum gezahlten Vergütungen, als vereinbart:

Von	bis [...] der Verfügbarkeit	Minderung
99%	98%	5%
< 98,0%	97,0%	10%
< 97,0%	96,0%	15%
< 96,0%	95,0%	20%
< 95,0%		30%

Stehen die Systeme ohne Verschulden des Kunden über die gesamte Verfügungszeit (Kapitel 2.3.1) von zwei aufeinander folgenden Arbeitstagen nicht zur Verfügung, werden dem Kunden 30% der jeweiligen Monatsvergütung erstattet. Bei drei Arbeitstagen beträgt die Erstattung 60 % und ab dem vierten Arbeitstag 90%.

Minderungen und Rückerstattungen der monatlichen Vergütung werden vom Anbieter veranlasst und dürfen vom Kunden nicht selbständig verrechnet werden.

2.3 Servicezeiten des Anbieters

Die Servicezeiten umfassen die folgenden Zeiträume:

Störungsannahme per E-Mail: Montag bis Sonntag 00:00 Uhr - 24:00 Uhr
 Störungsannahme per Telefon: Montag bis Freitag 07:30 Uhr – 17:30 Uhr¹⁾²⁾
 Servicezeit: Montag bis Freitag 07:30 Uhr – 17:30 Uhr¹⁾²⁾



Leistungsbeschreibung

1. Ausgenommen 24.12., 31.12. und gesetzliche Feiertage am Standort des Anbieters
2. GZ (Gesetzliche Zeit) in Deutschland

Unter Störungsannahme versteht man den Zeitraum, in dem eine Störung beim Service-Desk gemeldet werden kann. Unter Servicezeiten versteht man den Zeitraum, in dem an den gemeldeten Störungen gearbeitet wird.

2.4 Branchensoftware

Als Branchensoftware bezeichnet der Anbieter spezialisierte Softwarelösungen, die für die Anforderungen und Bedürfnisse bestimmter Branchen entwickelt wurden. Beispiele hierfür sind DATEV, Addison, Simba und Agenda. Die Branchensoftware wird oft von Unternehmen oder Organisationen genutzt, um Geschäftsabläufe des Kunden zu optimieren, die Effizienz zu steigern und branchenspezifische Anforderungen zu erfüllen. Der Anbieter bietet durch die Unterstützung der Branchensoftware an die Administration, das heißt Benutzer- und Rechteverwaltung, sowie Helpdesk-Support zu übernehmen. Weitergehende Leistungen, wie z.B. aber nicht ausschließlich, Migration und Fusion von Daten oder Support über dem Helpdesk-Level hinaus, sind in der Unterstützung nicht enthalten und werden entweder kostenpflichtig erbracht oder an den Software-Hersteller weitergetragen.

2.5 ambiNAS

ambiNAS bietet die Möglichkeit, eine, in den Räumlichkeiten des Kunden befindliche, Spiegelung der Kundendaten zu erhalten. Der Kunde benötigt hierfür ein vom Anbieter und Technologie-Partner unterstütztes NAS-System, auf welchem die Kundendaten gespiegelt werden. Diese Spiegelung wird über die Internetleitung des Kunden durchgeführt und erfolgt nur in die Richtung vom Rechenzentrum zum NAS, nicht umgekehrt oder bidirektional. Während der Spiegelung kann es vorkommen, dass die Bandbreite des Internetanschlusses des Kunden höher ausgelastet ist als üblich. Die ambiNAS Lösung ist nur in einem aktuellen ASP-Vertrag möglich. Sobald das ASP-Vertragsverhältnis endet, endet auch der Support des Anbieters für ambiNAS. Die gekaufte Hardware und die bis zu dem Zeitpunkt gespiegelten Daten bleiben dem Kunden erhalten. Die Häufigkeit der Spiegelung ist flexibel.

2.5.1 Wartung

Das NAS-System wird vom Anbieter so eingestellt, dass aktuelle Updates, nach Möglichkeit, automatisch installiert werden.

2.5.2 Kontrolle der Spiegelung

Nach einem Durchlauf der Spiegelung, wird eine Status-E-Mail mit dem Ergebnis der Spiegelung vom NAS an den Anbieter geschickt. Der Kunde muss sicherstellen, dass das NAS eine aktive Internetverbindung hat und eingeschaltet ist, damit die Spiegelung durchgeführt und die Status-E-Mail verschickt werden kann.

ambiNAS erfordert das Grundmodul.



2.6 ambiBOX-Management

Für die Verbindung zum Rechenzentrum wird dem Kunden eine aktuelle Hardware (VPN-Router) des Technologiepartners des Anbieters im Rahmen des ambiBOX-Managements zur Verfügung gestellt. Die Betreuung umfasst die Unterstützung beim Aufbau und Betrieb der Hardware sowie Support im Fehlerfall, wobei die Unterstützung ausschließlich per Telefon und Remote-Anleitung erfolgt. Ein Vor-Ort-Service ist nicht enthalten und wird im Bedarfsfall nach Zeitaufwand berechnet. Im Falle eines Hardwaredefekts wird dem Kunden eine neue Hardware zugesendet; die defekte Hardware ist an den Anbieter zurückzugeben und umfasst nicht die am VPN-Router angeschlossenen Geräte wie etwa Switches, PCs, Notebooks oder ähnliches. Das ambiBOX-Management enthält zudem, evtl. durch den Technologiepartner notwendige Lizenzen zum Betrieb der Hardware des Technologiepartners. Zusätzliche Lizenzen, wie etwa Add-Ons, die für den Betrieb der Hardware nicht zwingend notwendig sind, sind nicht enthalten. Weiterhin beinhaltet das ambiBOX-Management die regelmäßige Wartung und das proaktive Einspielen von Updates der Router-Software.

Das ambiBOX-Management erfordert das ASP-Grundmodul.

2.7 Datenkontingent

Das Datenkontingent bezieht sich auf den Speicherplatz aller datenhaltenden Systeme wie z.B., aber nicht ausschließlich Fileserver, Appserver und Datenbankserver. Der Speicher des Virtual Desktops, sofern nur eine Systempartition (C:) vorhanden ist, ist hiervon ausgenommen. Speicher, der auf anderen Partitionen als der Systempartition (C:) liegt, wird für das Datenkontingent berechnet. Überschreitet der Kunde das vereinbarte Kontingent, wird durch den Anbieter automatisch zusätzlicher Speicher bereitgestellt. Der zusätzliche Speicher wird als Zusätzliches Datenvolumen bezeichnet und ist kostenpflichtig.

2.8 Zusätzliches Datenvolumen

Das zusätzliche Datenvolumen ist jeder benötigte Speicher, der über die Summe des Datenkontingents des Kunden hinaus geht. Das zusätzliche Datenvolumen wird pro angefangene Gigabyte in Rechnung gestellt.

Zusätzliches Datenvolumen erfordert das Grundmodul.

2.9 Datensicherung

Die Datensicherung erfolgt in der Regel täglich und wird über einen Zeitraum von 30 Tagen aufbewahrt. Die Sicherung selbst geschieht im Hintergrund und beeinträchtigt nicht die Verfügbarkeit der Systeme. Gesichert werden alle Datenführenden Systeme (z.B. Fileserver, Datenbankserver und Mailserver). Ausgenommen von diesem Verfahren sind Anwendungssysteme (z.B. Virtual Desktop- und Applikationsserver). Sollte es aus technischen Gründen (alte oder nicht für den Unternehmenseinsatz geeignete Software, die keine getrennte Datenhaltung unterstützt) notwendig sein, auf diesen Anwendungssystemen Daten abzulegen, kann die Sicherung dieser Daten in Einzelfällen nicht erfolgen. Die Datensicherung erfolgt einmal pro Woche als Vollsicherung, an den restlichen Tagen der Woche als inkrementelle Sicherung. Die Wiederherstellung der Daten erfolgt auf Anfrage des Kunden über die bekannten Support-Wege.

Datensicherung erfordert das Grundmodul oder ambiCLOUD.



3.0 Monatliche Wartung der Systeme am festgelegten Wartungstermin

Wartungsarbeiten werden jeden 3. Samstag im Monat an den Serversystemen sowie der Infrastruktur durchgeführt. In diesem Zeitraum ist die Nutzung der ambiFOX ASP-Systeme nicht möglich. Wird der Betrieb für den Kunden aufgrund von Wartungsarbeiten außerhalb der definierten Zeiten eingeschränkt, wird der Kunde fünf Arbeitstage vor Beginn der Wartungsarbeiten informiert. In Eilfällen kann sich diese Zeit jedoch verkürzen. An diesem Wartungstermin erfolgen Updates der Systeme und der installierten Software, sofern diese durch die Produkte „Branchensoftware“ oder „Zusätzliche Branchensoftware“ abgedeckt wurde.

Monatliche Wartung der Systeme am festgelegten Wartungstermin erfordert das Grundmodul oder ambiCLOUD.

3.0.1 Wartung der Systeme

Die Wartung der Systeme trägt dazu bei die Leistungs- und Lauffähigkeit dieser langfristig sicherzustellen. Die Wartung der Systeme beinhaltet unter anderem das Installieren von Softwarepatches, austauschen defekter Hardware im Rechenzentrum des Anbieters und die Prüfung der Systeme sowie daraus entstehende notwendige Reparaturen. Die Wartung der Systeme kann innerhalb der Servicezeiten des Anbieters oder am Wartungstermin des Anbieters durchgeführt werden.

Wartung erfordert das Grundmodul.

3.1 ambiVPN

ambiVPN ist ein VPN-Zugangsprodukt des Anbieters. Der Anbieter ermöglicht dem Kunden per VPN-Client auf einem Endgerät eine verschlüsselte Verbindung in das im Rechenzentrum des Anbieters bereitgestellte Kundennetzwerk. Darüber können die vom Kunden im Rechenzentrum gebuchten Dienste genutzt werden. Der VPN-Zugang ist nicht auf bestimmte Internetanschlüsse beschränkt; er kann grundsätzlich von jedem Internetzugang aus genutzt werden, kann aber scheitern, wenn am jeweiligen Standort/Netz (z. B. Gastnetz) erforderliche Ports/Protokolle gesperrt sind. Die erforderlichen Ports können beim Support des Anbieters erfragt werden. Ein ambiVPN-Zugang ist technisch auf die gleichzeitige Nutzung auf genau einem Endgerät begrenzt; ein Gerätewechsel ist jederzeit möglich. Der Anbieter liefert Zugang, Konfiguration, Installationsunterstützung und Troubleshooting und unterstützt Windows, macOS, Linux, iOS und Android, sofern die jeweilige Betriebssystemversion noch im Herstellersupport ist.

ambiVPN erfordert das Grundmodul.

3.2 ambiIPSEC

ambiIPSEC bietet die Möglichkeit eine gesicherte Verbindung zwischen dem lokalen Netzwerk des Kunden, welches durch den Kunden selbst verwaltet wird, und dem Netzwerk des Kunden im Rechenzentrum des Anbieters herzustellen. Die Verbindung erfolgt über das etablierte IPSec-Protokoll. Das vom Kunden eingesetzte Netzwerkgerät muss IPSec i.V.m. IKEv2 unterstützen. Der Kunde und der Anbieter einigen sich auf gemeinsame Verbindungseinstellungen und Sicherheitsmerkmale der IPSec-Verbindung.

Durch die IPSec-Verbindung kann ein Zugriff aus dem lokalen Netzwerk des Kunden in das Netzwerk des Kunden im Rechenzentrum des Anbieters, sowie umgekehrt, erfolgen. Der Kunde kann hierüber alle von ihm gebuchten Dienste im Rechenzentrum des Anbieters nutzen.



Leistungsbeschreibung

ambiPSEC erfordert das Grundmodul.

3.3 Öffentliche IP-Adresse

Der Anbieter stellt dem Kunden für die Vertragslaufzeit genau eine (1) aus dem Internet erreichbare IPv4-Adresse aus dem IPv4-Adressbereich des Anbieters zur Verfügung. Die IPv4-Adresse verbleibt im Besitz und Eigentum des Anbieters und wird dem Kunden zur monatlichen Nutzung überlassen. Die IPv4-Adresse dient dazu, Systeme des Kunden, die sich im Rechenzentrum des Anbieters befinden, aus dem Internet erreichbar zu machen; eine Nutzung für Systeme außerhalb des Rechenzentrums des Anbieters ist nicht Bestandteil der Leistung.

Die Veröffentlichung der Kundensysteme erfolgt in der Regel über Port-Forwarding (NAT) auf vom Kunden benannte Zielsysteme im Netzwerk des Kunden im Rechenzentrum des Anbieters. Der Anbieter richtet im Rahmen der Erstbereitstellung das notwendige NAT/Routing sowie die erforderlichen Firewall-Regeln ein. Standardmäßig sind eingehende Verbindungen über die bereitgestellte IPv4-Adresse gesperrt. Der Kunde kann über eine Supportanfrage die Freischaltung gewünschter Ports veranlassen; der Anbieter setzt die entsprechenden Firewall- und Port-Forwarding-Regeln nach Abstimmung mit dem Kunden um.

Je nach Anwendungsfall kann die bereitgestellte IPv4-Adresse auch geteilt genutzt werden (Shared Use). In diesem Fall erfolgt die Bereitstellung der Erreichbarkeit des Kundensystems ebenfalls über die vom Anbieter eingerichteten Port-Forwarding- und Firewall-Regeln.

Spätere Änderungen (z. B. Anpassungen von Weiterleitungen oder Firewall-Regeln) werden über den regulären Supportprozess des Anbieters beauftragt und umgesetzt.

Öffentliche IP-Adresse erfordert das Grundmodul.

3.4 ambiMAIL ARCHIV

ambiMAIL ARCHIV bietet eine Lösung, um E-Mails aus einzelnen Postfächern sicher und gesetzeskonform (DSGVO & IDW PS 880) zu archivieren. Der Anbieter stellt dem Kunden eine entsprechende Software des Technologiepartners, oder Zugriff auf eine Weboberfläche des Technologiepartners, auf den ASP-Kundensystemen zur Verfügung, um Zugriff auf die für den Benutzer berechtigten Archive zu gewähren. Voraussetzung für die Nutzung von ambiMAIL ARCHIV ist, dass die E-Mails des Kunden in einer, vom Anbieter administrierbaren, Exchange-Online-Umgebung oder in der Hosted-Exchange-Umgebung des Anbieters verwaltet werden. Zudem benötigt die Archivierungslösung des Technologiepartners Zugriff auf die zu archivierenden Postfächer. Dies wird in der Regel über Impersonation-/ Nachahmungs-Rechterealisiert.

Die archivierten E-Mails können dauerhaft (bis zur Kündigung des Produkts) oder für die Dauer eines zuvor definierten Zeitraums aufbewahrt werden. ambiMAIL ARCHIV archiviert nur E-Mails. Kalendereinträge, Aufgaben oder ähnliche Objekte in Postfächern werden nicht archiviert. Der Kunde kann wählen ob alle Postfächer des Kunden oder nur bestimmte Postfächer archiviert werden.

E-Mails, die archiviert wurden, können nachträglich nicht mehr aus dem Archiv entfernt werden. Die Archivierung kann Journal-basiert, das heißt alle Mails werden auf dem Transportweg von der Archivierungslösung gesammelt und im Archiv abgelegt, oder Abruf-basiert, das heißt die Postfächer werden zu fest definierten Zeiten nach neuen Elementen durchsucht, welche im Anschluss archiviert werden, durchgeführt werden. ambiMAIL ARCHIV wird pro Postfach berechnet. ambiMAIL ARCHIV wird so lange berechnet, wie das Archiv besteht.



3.5 ambiCLOUD

ambiCLOUD bietet dem Kunden eine über das Internet erreichbare Cloud-Speicher-Kundeninstanz. Diese Instanz ist über einen unterstützten Browser oder die vom Technologie-Partner zur Verfügung gestellte Desktop-App erreichbar und kann von dort aus mit einem gültigen ambiCLOUD Benutzer genutzt werden.

In der ambiCLOUD kann der Kunde, Mitarbeiter des Kunden oder Personen, denen der Zugriff zur ambiCLOUD vom Kunden zur Verfügung gestellt wurde, Dateien hochladen, bearbeiten und herunterladen.

ambiCLOUD enthält die folgenden Leistungen:

- Datensicherung
- Datenkontingent: 50GB
- ambiCLOUD-Benutzer
- ambiCLOUD-Admin
- Wartung und Updates

3.6 Support und Implementierung

Nachdem der Kunde ambiCLOUD beim Anbieter in Auftrag gegeben hat, wird die ambiCLOUD Infrastruktur vom Anbieter eingerichtet. Dazu gehört die Bereitstellung der vereinbarten Speichergöße und eines initialen ambiCLOUD Benutzerkontos. Die Ordner- und Dateistruktur wird nicht vom Anbieter verwaltet und obliegt der Verantwortung des Kunden. Die ambiCLOUD kann über einen DNS-Eintrag des Kunden erreicht werden. Der DNS-Eintrag muss hierfür vor der Implementierung bekannt sein und entsprechend angelegt worden sein. Sollte der Anbieter Zugriff auf die Domain-Verwaltung des Kunden haben, wird der Eintrag vom Anbieter vorgenommen. Sollte kein Zugriff durch den Anbieter möglich sein, liegt es in der Verantwortung des Kunden den DNS-Eintrag zu erstellen. Sollte es nicht möglich oder gewollt sein einen DNS-Eintrag in der Domain-Verwaltung des Kunden zu hinterlegen so erstellt der Anbieter einen DNS-Eintrag unter einer Domain des Anbieters und veröffentlicht die ambiCLOUD dort.

Sobald die ambiCLOUD Grundeinstellungen durchgeführt wurden, vereinbart der Anbieter einen Termin mit dem Kunden zur Einführung in das ambiCLOUD System. Nach der Initialen Einführung in das ambiCLOUD System, werden weitere Support-Anfragen zu ambiCLOUD während der Service-Zeiten bearbeitet und nach Aufwand berechnet.

3.7 ambiCLOUD-Admin

Der ambiCLOUD-Admin ist ein Benutzerkonto in der ambiCLOUD-Instanz des Kunden. Beim ambiCLOUD-Admin handelt es sich um einen ambiCLOUD-Benutzer mit erweiterten Rechten. Die Rechte umfassen unter anderem das Anlegen, Bearbeiten und Löschen von ambiCLOUD-Benutzern, sowie das Zuweisen zu Gruppenmitgliedschaften und Berechtigen auf Freigaben innerhalb der ambiCLOUD-Instanz. ambiCLOUD-Admin setzt ambiCLOUD voraus.

3.8 ambiCLOUD-Benutzer

Der ambiCLOUD-Benutzer ist ein Benutzerkonto in der ambiCLOUD-Instanz des Kunden. Der ambiCLOUD-Benutzer ermöglicht das Anmelden in der ambiCLOUD sowie das Hochladen, Bearbeiten, Herunterladen und Löschen von Dateien in der ambiCLOUD. Der Login möglich über das Webinterface der ambiCLOUD. Voraussetzung hierfür ist ein Mozilla Firefox, Google



Leistungsbeschreibung

Chrome, Microsoft Edge oder Safari Browser mit den aktuellsten Updates. Ein Login ist zudem über Desktop-Apps für Microsoft Windows sowie Apple macOS und mobile Apps für Android und iOS möglich.

3.9 ambiBACKUP M365 Grundmodul

ambiBACKUP M365 bietet eine Lösung zur Cloud-to-Cloud Sicherung von Microsoft-Office-365-Daten. In der Regel werden tägliche Online-Sicherungen auf dem Speicher des vom Anbieter gewählten Technologie-Partners erstellt und werden für einen Zeitraum von 180 Tagen aufbewahrt. ambiBACKUP M365 bietet Backup-Funktionen für die Microsoft-365-Suite, wie Exchange Online, OneDrive for Business, SharePoint Online und Microsoft Teams. Die Sicherung erfolgt über die Serversysteme des Technologie-Partners des Anbieters. Hierfür ist ein administrativer Zugang des Technologiepartners notwendig, welcher vom Anbieter eingerichtet wird. Der Anbieter kontrolliert täglich ob die Sicherungen erfolgreich durchgeführt wurden. Bei fehlerhaften Sicherungsversuchen wird eine proaktive Problemlösung innerhalb der Servicezeiten des Anbieters durchgeführt. Rücksicherungen erfolgen auf Anfrage durch den Kunden über den bekannten Supportweg, ausschließlich per Mail. Die Rücksicherung wird direkt in das gesicherte Objekt zurückgespielt. Der Kunde muss dem Anbieter Speicherort und Datum der gewünschten Sicherung mitteilen. ambiBACKUP M365 Grundmodul enthält 100GB zu sicherndes Datenvolumen. Die zu sichernde Datenmenge ist die Summe aller Elemente in den gesicherten Microsoft 365-Diensten, wie z.B., aber nicht ausschließlich: Mails, Kalendereinträge, Aufgaben in Exchange Online, Dokumente und Dateien in OneDrive for Business, Chatnachrichten und Dateien in Microsoft Teams. Überschreitet die zu sichernde Datenmenge das Datenvolumen von 100GB wird "ambiBACKUP M365 Erweiterung" benötigt.

3.9.1 ambiBACKUP M365 Erweiterung

Die ambiBACKUP M365 Erweiterung bietet die Möglichkeit, zusätzlich zum ambiBACKUP M365 Grundmodul, weitere 100GB zu sicherndes M365-Datenvolumen zu schützen. Für jede angefangene 100GB wird jeweils eine ambiBACKUP M365 Erweiterung berechnet. Die zu sichernde Datenmenge ist die Summe aller Elemente in den gesicherten Microsoft-365-Diensten, wie z.B., aber nicht ausschließlich: Mails, Kalendereinträge, Aufgaben in Exchange Online, Dokumente und Dateien in OneDrive for Business, Chatnachrichten und Dateien in Microsoft Teams.

4.0 Mailgateway

Das Mailgateway bietet einer Anwendung oder einem Dienst des Kunden, auf einem im Rahmen des ASP-Vertrages zur Verfügung gestellten Serversystem, den Versand von E-Mails über das SMTP-Protokoll. Bei unsachgemäßer Nutzung behält sich der Anbieter vor, die Leistung zu deaktivieren.

Der Anbieter stellt dem Kunden eine SMTP-Server-Adresse inklusive Port sowie Zugangsdaten zur Verfügung. Der SMTP-Server ist nur aus dem Rechenzentrum des Anbieters erreichbar und nutzbar. Eine Nutzung des Mailgateways außerhalb der Rechenzentrums-Umgebung des Anbieters ist nicht möglich. Die vom Kunden genutzte Software muss eine Unterstützung für das SMTP-Protokoll bieten. Damit die Zustellung der, über das Mailgateway versendeten, Mails gewährleistet werden kann muss der Kunde für jede Mail-Domäne, die im Zusammenhang mit dem Mailgateway genutzt werden soll, einen SPF-Eintrag, einen DKIM-Eintrag sowie unter Umständen ein DMARC-Eintrag in der DNS-Verwaltung des Kunden erstellen. Sofern die Voraussetzungen erfüllt sind, kann der Kunde das Mailgateway uneingeschränkt nutzen. Bei unsachgemäßer Nutzung wie z.B., aber nicht ausschließlich, dem Versand von Massenmails, dem Versand von Spam-Mails oder Mails mit schadhaftem Inhalt, dem Versand von Phishing-



Leistungsbeschreibung

Mails oder dem Versand mit nicht autorisierten Domänen, behält sich der Anbieter vor, den Zugang zum Mailgateway für den Kunden einzuschränken oder zu blockieren.

4.1 Managed Reversproxy

Mit Hilfe des Managed Reverseproxy ist es möglich mehrere, im Internet nicht veröffentlichte Webdienste, über eine öffentliche IP-Adresse und verschiedene Subdomänen, erreichbar zu machen. Es handelt sich um eine Verwaltungsoberfläche, in der der Kunde die Möglichkeit hat, das Routing seiner Subdomänen selbstständig zu verwalten. Die Verwaltungsoberfläche wird auf einem virtualisierten Server im DMZ-Netzwerk des Kunden installiert. Der Kunde erhält die Zugangsdaten für die Verwaltungsoberfläche. Die Verwaltungsoberfläche ist mit einem aktuellen und unterstützten Browser entweder über das Internet oder ausschließlich über das Netzwerk des Kunden erreichbar. Der Kunde kann Einträge für Subdomänen anlegen, löschen und bearbeiten. Der Managed Reverseproxy kann die HTTP- sowie HTTPS-Anfragen für die gewünschte Subdomäne an den, im internen DMZ-Netzwerk des Kunden erreichbaren, Webdienst weiterleiten. Der Kunde kann beliebig viele Subdomänen erstellen. Der Kunde ist für die korrekte Einrichtung der DNS-Einträge selbst verantwortlich. Hierzu wird dem Kunden ein DNS-Name bereitgestellt, unter welchem der Managed Reverseproxy aus dem Internet erreichbar ist. Der Kunde muss für jede Subdomäne oder Domäne, die über den Managed Reverseproxy erreichbar sein soll, einen CNAME-Eintrag in seiner DNS-Verwaltung erstellen, welcher auf den vom Anbieter genannten DNS-Namen weiterleitet.

4.2 Einrichtung der Remotedesktop-Verbindung

Im Rahmen dieser Leistung übernimmt ein Support-Mitarbeiter des Anbieters die vollständige Einrichtung einer Remotedesktop-Verbindung auf dem Endgerät des Benutzers. Voraussetzung für die Durchführung ist, dass auf dem betreffenden Computer ein aktuell von Microsoft unterstütztes Windows-Betriebssystem installiert ist, eine funktionierende Internetverbindung besteht und die lokale Komponente der Fernwartungslösung des Anbieters ausgeführt wird.

Dabei werden alle notwendigen Einstellungen vorgenommen, um eine Verbindung zum bereitgestellten Virtual Desktop des Anbieters herzustellen. Im Rahmen der Einrichtung wird eine Testverbindung zum Virtual Desktop durchgeführt, um die Funktionalität sicherzustellen. Der Support-Mitarbeiter überprüft, ob die Verbindung erfolgreich aufgebaut werden kann und ob die grundlegenden Funktionen (z.B. Anzeige, Tastatur- und Maussteuerung) ordnungsgemäß arbeiten.

4.3 ambiSECURE M365 Produktlinie

Produktstufen: Core · Advanced · Premium · Elite

Optionales Zusatzmodul: E-Mail Encryption

Die ambiSECURE M365 Produktreihe umfasst vier aufeinander aufbauende Leistungsstufen. Jede höhere Stufe enthält vollständig die Leistungen der jeweils darunterliegenden Stufe(n) und ergänzt diese um zusätzliche Module. Zusätzlich steht für alle Leistungsstufen das Modul E-Mail Encryption als kostenpflichtige Option zur Verfügung.

Produktstufe	Enthaltene Module (kumulativ)
ambiSECURE M365 Core	Spam and Malware Protection · Signature and Disclaimer



Leistungsbeschreibung

ambiSECURE M365 Advanced	Alle Leistungen aus Core zzgl. Archiving und Advanced Threat Protection
ambiSECURE M365 Premium	Alle Leistungen aus Advanced zzgl. 365 Total Backup
ambiSECURE M365 Elite	Alle Leistungen aus Premium zzgl. Security Awareness Service
Optional (alle Stufen)	E-Mail Encryption (kostenpflichtiges Zusatzmodul, ab Core zubuchbar)

Die nachfolgenden Kapitel beschreiben die einzelnen Module. Die Zugehörigkeit zu den Produktstufen ist jeweils im Kapitelkopf gekennzeichnet.

4.3.1 Modul: Spam and Malware Protection (Basisleistung)

Enthalten in: Core, Advanced, Premium, Elite

Die Spam and Malware Protection bildet die technische Grundlage der ambiSECURE M365 Produktreihe. Mehrere weitere Module (Signature and Disclaimer, Archiving, E-Mail Encryption) setzen deren Nutzung voraus.

Eingehende E-Mails des Auftraggebers werden auf schädlichen Inhalt (z. B. Viren), unerwünschte Werbung (z. B. Spam) und legitime Werbung (z. B. Newsletter) auf eigenen IT-Systemen gefiltert. E-Mails an den Auftraggeber werden dazu durch Umstellung der MX-Records für die zu filternden Domains des Auftraggebers auf die Server geleitet. Für die Umstellung des MX-Records besteht keine Verantwortung.

Die Spamerkennungsrate liegt bei mindestens 99,9 % im Monatsdurchschnitt, bezogen auf die Zahl aller E-Mails, die die Systeme für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme durch Umstellung der MX-Records der Domains des Auftraggebers.

Die Virenerkennungsrate liegt im Jahresdurchschnitt bei mindestens 99,99 %, bezogen auf die Zahl aller E-Mails, die die Systeme für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen.

Die Falsch-Positiv-Rate liegt unter 0,00015 im Monatsdurchschnitt, bezogen auf die Zahl aller Clean-E-Mails, die die Systeme für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Ausgenommen sind solche E-Mails, die durch falsch konfigurierte Server (nicht RFC-konform), über verifizierte Open Relays oder mangelhaft eingerichtete Mailclients versendet wurden.

Die Verfügbarkeit im Mailverkehr per SMTP beträgt 99,99 % im Jahresmittel. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme durch Umstellung des MX-Records. Geplante Wartungsarbeiten werden nicht berücksichtigt; diese werden, soweit möglich, am Wochenende nachts ausgeführt (MEZ).

Soweit der Auftraggeber es wünscht, werden auch ausgehende E-Mails gefiltert.

Empfangene E-Mails werden:

- geblockt (zurückgewiesen), soweit sie noch während der Aufnahme der Datenverbindung mit den Servern mit hoher Sicherheit als unerwünscht erkannt werden,
- wahlweise in Quarantäne gestellt oder mit einer Markierung im Betreff zugestellt, sofern sie nach vollständiger Annahme der E-Mail durch die Server als unerwünscht erkannt werden,
- zugestellt oder zur Abholung bereitgestellt, sofern sie als erwünschte E-Mail erkannt werden.
- Die Zustellzeiten liegen typisch im Durchschnitt bei unter 30 Sekunden, der maximale durchschnittliche Wert liegt bei 3 Minuten.



Leistungsbeschreibung

E-Mails in Quarantäne werden drei Monate zur Einsicht durch autorisierte Benutzer des Auftraggebers gespeichert. Auf Wunsch des Auftraggebers werden Benutzer über neue E-Mails in der Quarantäne informiert (in der Regel einmal täglich).

Auf E-Mails in der Quarantäne können autorisierte Benutzer aus dem Internet zugreifen. Autorisierte Benutzer können interaktiv die Zustellung von E-Mails in Quarantäne auf die Systeme des Auftraggebers veranlassen.

Autorisierte Nutzer können persönliche White- und Blacklists pflegen. Die Konfiguration kann über verschiedene Wege erfolgen, z. B. Control Panel, Quarantäne-Bericht oder das Outlook Add-In.

Soweit Eingriffe durch den Auftraggeber in die Filterstufen erfolgen (z. B. Einrichten von speziellen White- oder Blacklists), können Qualität und Erkennungsraten der Filterstufen nicht gewährleistet werden.

Autorisierte Nutzer des Auftraggebers (z. B. Support-Mitarbeiter und Administratoren) können über das Control Panel den kompletten Mailverlauf des Auftraggebers überblicken. Im Live-Monitor können zusätzlich auch alle geblockten (abgewiesenen) E-Mails der vergangenen 7 Tage nachverfolgt werden.

Optional werden ein- und ausgehende E-Mails entsprechend eingestellter Richtlinien gefiltert (Content- und Compliance-Filter). Je nach Einstellung werden E-Mails, die den Richtlinien nicht entsprechen:

- a. mit einer entsprechenden Fehlermeldung zurückgewiesen (eingehend),
- b. ohne Anhang zugestellt und mit Anhang in eine Quarantäne gestellt, aus der sie von Administratoren dem Empfänger zugestellt werden können (eingehend),
- c. mit einer entsprechenden Fehlermeldung zurückgewiesen (ausgehend).

Die Richtlinien zur Content- und Compliance-Filterung können von dazu autorisierten Benutzern des Auftraggebers im Control Panel eingestellt werden.

E-Mails werden über einen per TLS verschlüsselten Kanal übertragen, soweit die Gegenseite die Übertragung per TLS unterstützt. Weitere Verschlüsselungsverfahren können optional über das Modul E-Mail Encryption genutzt werden (siehe Kapitel 7).

Der Inhalt zugestellter E-Mails wird nur gespeichert, wenn ein Continuity Service oder das Archiving zusätzlich genutzt wird.

Neben den bereits bestehenden Methoden und Verfahren zur Erkennung von Viren können weitere AV-Engines von Antivirus-Spezialisten optional hinzugeschaltet werden.

Der Support autorisierter Benutzer wird sichergestellt, soweit es die eigenen Systeme betrifft. Der Support von Systemen des Auftraggebers ist nicht Bestandteil dieses Vertrags.

Auf Wunsch kann der Kunde Weiterleitungspostfächer definieren, über die der E-Mail-Verkehr an einen oder mehrere, bis zu 100, interne oder externe Postfächer weitergeleitet werden kann.

Die maximale Größe für die Weiterleitung von E-Mails über Weiterleitungspostfächer richtet sich nach der Anzahl der Weiterleitungsempfänger:

- a. Bei einem Weiterleitungsempfänger greifen die Standardeinstellungen des Kunden.
- b. Bei bis zu 9 Empfängern darf die Größe der E-Mail bis zu 50 MB betragen.
- c. Bei 10 bis 24 Empfängern darf die Größe der E-Mail bis zu 30 MB betragen.
- d. Bei 25 bis 49 Empfängern darf die Größe der E-Mail bis zu 15 MB betragen.
- e. Bei 50 bis 100 Empfängern darf die Größe der E-Mail bis zu 10 MB betragen.

4.3.2 Modul: Signature and Disclaimer

Enthalten in: Core, Advanced, Premium, Elite



Leistungsbeschreibung

Der Service Signature and Disclaimer ist eine Erweiterung des Spam and Malware Protection und setzt dessen Nutzung voraus. Zusätzlich muss der Versand von E-Mails über die Plattform aktiviert sein.

Die Nutzung von Signature and Disclaimer kann auf zwei unterschiedliche Arten erfolgen – über das LDAP-Protokoll oder über die statische Version ohne LDAP-Anbindung. Abhängig von der Nutzungsart gelten unterschiedliche Voraussetzungen und inbegriffene Serviceleistungen:

a. Für die Nutzung über das LDAP-Protokoll wird der Einsatz eines Verzeichnisdienstes vorausgesetzt. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein.

b. Für die Nutzung der statischen Version muss der Service über den Support aktiviert sein. In der statischen Version sind die Funktionen 4b, 4c, 4d und 5 nicht im Service inbegriffen.

Mit Signature and Disclaimer kann der Auftraggeber Signaturen und Disclaimer für Benutzergruppen erstellen. Diese werden beim Versand von E-Mails automatisch angehängt. Pro Benutzergruppe ist es möglich, eine Vorlage für eine Signatur und einen Disclaimer auszuwählen.

Der Zugriff durch autorisierte Benutzer erfolgt über ein Webinterface, in dem mit Hilfe eines WYSIWYG-Editors mit auswählbaren Attributen aus dem Verzeichnisdienst Vorlagen für Signaturen und Disclaimer erstellt werden können. Zusätzlich bietet der WYSIWYG-Editor folgende Funktionen:

a. Einfügen einer Signatur oder eines Disclaimers aus HTML-Quellcode,

b. Einbinden vordefinierter AD-Variablen,*

c. Einbinden zuvor erstellter Signaturen als Subsignaturen,*

d. Ausblenden von unbenutzten AD-Variablen in Signaturen und Disclaimern bei Benutzern mit der Funktion „If Not Empty“,*

e. Einbinden eigener Grafiken, Werbebanner oder Social-Media-Buttons über die Drag-&-Drop-Funktion oder über die direkte Einbettung einer URL.

Eine Vorschaufunktion ermöglicht eine mit Daten gefüllte Vorschau der Vorlage für Benutzer der ausgewählten Gruppe.*

Erstellte Vorlagen werden vom Kunden gespeichert und können für unterschiedliche Benutzergruppen ausgewählt werden. Für alle Benutzer, die keiner Gruppe zugewiesen sind, sowie Gruppen, denen keine eigene Vorlage zugewiesen wurde, gelten die Einstellungen der Standardgruppe.

Nach Einrichtung werden Signatur und Disclaimer beim Versand an ausgehende E-Mails angehängt, unabhängig vom eingesetzten Endgerätetyp. Dies gilt sowohl für extern als auch für intern verschickte E-Mails, sofern deren Routing über die Cloud eingerichtet ist.

* nicht in der statischen Version des Signature and Disclaimer enthalten

4.3.3 Modul: Advanced Threat Protection (ATP)

Enthalten in: Advanced, Premium, Elite

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

a. Sandboxing: Verdächtige E-Mail-Anhänge werden in mehreren separaten, geschützten Umgebungen geöffnet oder ausgeführt und ihr Verhalten auf mögliche Schadwirkung untersucht. Als verdächtig werden insbesondere Anhänge eingestuft, in denen ausführbarer Code gefunden wird.



Leistungsbeschreibung

- b. Secure Links: In E-Mails oder in E-Mail-Anhängen enthaltene URLs werden aktiviert und das resultierende Verhalten analysiert.
 - c. Secure Links: URLs in E-Mails werden durch andere URLs ersetzt, die die entsprechenden Inhalte bei Aktivierung über den Web-Filter abrufen. Ggf. werden heruntergeladene Daten per Sandboxing auf ihr Verhalten untersucht. Durch den Web-Filter als potentiell gefährlich erkannte Inhalte werden gesperrt. URLs ohne erkennbare Bedrohung nach einem Scan und URL-Einträge auf einer Whitelist werden nicht ersetzt.
 - d. Targeted Fraud Forensics: Heuristische Filter zur Erkennung gezielter Angriffe, mit Prüfung von Authentizität und Integrität von Metadaten und E-Mail-Inhalten, Erkennung und Blockierung gefälschter Absender-Identitäten, Erkennung gefälschter Inhalte, Erkennung von Angriffen auf besonders schützenswerte Daten, insbesondere Daten, die Zahlungsflüsse betreffen (z. B. Kreditkartendaten, Rechnungen, Zahlungsanweisungen), Erkennung gezielter Angriffe auf besonders exponierte Personen des Auftraggebers (z. B. Buchhaltung, CFO, CEO, Controlling).
 - e. Freezing: Zeitweiliges „Einfrieren“ verdächtiger E-Mails. Eingefrorene E-Mails werden nach einigen Minuten erneut mit aktualisierten Filtern verarbeitet.
 - f. Malicious Document Decryption: Verschlüsselte E-Mail-Anhänge in Form von Office-Dateien, Archiven und PDF-Dateien werden vor dem Eintreffen beim Empfänger entschlüsselt, sofern das Passwort aus der E-Mail rekonstruiert werden kann, und die Inhalte nach möglicher Schadsoftware untersucht.
 - g. Ex-Post-Alarmierung: Stellt sich im Nachhinein heraus, dass eine bereits zugestellte E-Mail doch als potentiell schädlich eingestuft werden muss, erhält das IT-Sicherheitsteam eines Unternehmens nach Bekanntwerden eine Alarmierung.
 - h. QR Code Analyzer: In E-Mails enthaltene QR-Codes sowie Bilder mit integrierten QR-Codes werden bedarfsorientiert und automatisch im Hintergrund beim E-Mail-Verarbeitungsprozess auf potenziell gefährliche Links überprüft.
- E-Mails können durch die zusätzliche aufwändige Filterung zeitlich verzögert zugestellt werden. Die Verzögerung beträgt im Einzelfall maximal 15 Minuten.
- Als potenziell schädlich identifizierte E-Mails werden in Quarantäne gestellt.
- Auf quarantänierte E-Mails kann der Auftraggeber über das Control Panel zugreifen.
- E-Mails mit geeigneten Anhängen in der Quarantäne können von Administratoren des Auftraggebers aus dem Control Panel heraus per Sandboxing geprüft werden. Detaillierte Ergebnisse der Prüfung werden über das Control Panel zur Verfügung gestellt.
- Sicherheitsverantwortliche des Auftraggebers werden bei erkannten Bedrohungen unmittelbar per E-Mail über die Bedrohung informiert (Real-Time Alerts).
- Für den ATP-Dienst wird eine Verfügbarkeit von 99,9 % garantiert, ausgenommen sind angekündigte Wartungszeiten.

4.3.4 Modul: Archiving

Enthalten in: Advanced, Premium, Elite

Archiving ist eine Erweiterung der Spam and Malware Protection und setzt dessen Nutzung voraus.

E-Mails des Auftraggebers werden revisionssicher auf eigenen IT-Systemen archiviert. Auf die archivierten E-Mails können autorisierte Benutzer aus dem Internet zugreifen. Archivierte E-Mails können nach bestimmten Kriterien und Inhalten durchsucht werden, um bestimmte E-Mails im Archiv ausfindig zu machen. Autorisierte Benutzer können interaktiv die erneute Zustellung archivierter E-Mails auf die Systeme des Auftraggebers veranlassen. Der Zugriff durch autorisierte Nutzer erfolgt über ein webbasiertes Frontend (Control Panel) oder die Progressive Web-App für iOS und Android.



Leistungsbeschreibung

Die Archivierungsdauer und Archivierungsausnahmen können auf Domain-, Gruppen- oder Nutzerebene festgelegt werden.

Es wird die Verfügbarkeit der archivierten E-Mails für den Auftraggeber garantiert, für die vorab durch den Auftraggeber konfigurierte Dauer in vollständigen Jahren ab Ende eines Kalenderjahres, in dem die jeweilige archivierte E-Mail versandt bzw. erhalten wurde.

Die Standardeinstellung für die Archivierung beträgt 10 Jahre. Der Auftraggeber kann per Control Panel oder API abweichende Einstellungen setzen, die ab dem Zeitpunkt der Einstellung für neu eingegangene E-Mails, jedoch nicht rückwirkend, gelten. Voraussetzung ist die Fortdauer des Vertrags und die Erfüllung der vertraglichen Pflichten durch den Auftraggeber. Für den Fall der Beendigung dieses Vertrags setzt die fortdauernde Verfügbarkeit den Abschluss eines Anschlussvertrags über die kostenpflichtige Aufrechterhaltung der Datenspeicherung voraus. Es wird vorbehalten, die archivierten Mails auch bei vorzeitiger Vertragsbeendigung für den vorab festgelegten Zeitraum zu archivieren. Eine explizit gewünschte Löschung vor Erreichen der Archivierungsdauer muss gesondert beantragt werden mittels Löschersuchen nach DSGVO.

Autorisierte Benutzer können E-Mails als „privat“ markieren. Auf als „privat“ markierte E-Mails ist anschließend kein Zugriff aus dem Archiv mehr möglich.

Es wird die Zugriffsmöglichkeit autorisierter Benutzer auf die archivierten E-Mails im Normalfall 24 Stunden am Tag an allen Tagen im Jahr garantiert. Ausgenommen sind Wartungszeiten.

Speziell autorisierte Nutzer können einen speziellen Zugang einrichten, der den Zugriff auf alle archivierten E-Mails eines bestimmten Zeitraums erlaubt (Prüfzugang, z. B. zum Zweck einer Betriebsprüfung). Einrichtung und Nutzung des Prüfzugangs werden geloggt.

Archiviert werden solche E-Mails, die

- a) durch den Auftraggeber über die Server an Dritte verschickt werden (ausgehende externe E-Mails),
- b) dem Auftraggeber durch Dritte über die Server zugeschickt werden (eingehende externe E-Mails),
- c) der Auftraggeber zur Archivierung über vereinbarte Schnittstellen zur Verfügung stellt (interne E-Mails, optional).

Die Archivierung genügt den derzeitigen gesetzlichen Auflagen in Deutschland bezüglich der elektronischen Archivierung von E-Mails. Es wird alles Mögliche veranlasst, um die Erfüllung dieser gesetzlichen Auflagen auch im Fall der Änderung dieser Auflagen sicherzustellen.

Der Support autorisierter Benutzer wird sichergestellt, soweit es die eigenen Systeme betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

Die Geheimhaltung der archivierten Daten und sonstiger im Rahmen dieses Vertrags bekannt gewordener geschäftlicher Geheimnisse des Auftraggebers gegenüber Dritten wird sichergestellt. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.

Im Preis ist die Bereitstellung von unlimitiertem Speicherplatz für alle lizenzierten Postfächer enthalten.

Optional wird der Nachimport bestehender Archivdaten angeboten. Die Archivdaten müssen in einem festgelegten Format angeliefert werden. Die technischen Voraussetzungen und Rahmenbedingungen können erfragt werden. Der Nachimport bestehender Archivdaten ist kostenpflichtig.

Auf Wunsch werden die bestehenden Archivdaten auf einen externen Datenträger exportiert. Der Export erfolgt im EML-Format auf einem verschlüsselten Datenträger, der anschließend an den Auftraggeber gesendet wird. Der Export von Archivdaten ist kostenpflichtig.

Mit dem Aeternum Export Manager ist es zudem möglich, archivierte E-Mails auf Postfachbasis im Selfservice zu exportieren und anschließend herunterzuladen. Für den Export stehen die Formate PST, EML und MBOX zur Verfügung. Der Export von Archivdaten mit dem Aeternum Export Manager ist kostenpflichtig.



4.3.5. Modul: 365 Total Backup

Enthalten in: Premium, Elite

365 Total Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Backup- und Recovery-Lösung für Microsoft 365-Postfächer und In-Place-Archivpostfächer, OneDrive, SharePoint-Dokumentenbibliotheken, Teams-Chats, Planner, OneNote, Entra ID-Benutzer und -Gruppen.

Um den 365 Total Backup-Service nutzen zu können, muss der Kunde über Microsoft Cloud-Lizenzen mit entweder Exchange-, Teams-, SharePoint- und/oder OneDrive-Funktionalität verfügen, die von Microsoft aktiviert wurden.

Alle Objekte innerhalb des gesamten Microsoft-Tenants, denen eine Microsoft 365-Lizenz zugewiesen ist, die entweder Exchange-, Teams-, SharePoint- oder OneDrive-Funktionalität gewährt, unterliegen unabhängig von ihrer aktiven Nutzung der 365 Total Backup-Lizenzierung. Die höchste Nutzungsmenge des Monats wird gemeldet und in Rechnung gestellt.

4.3.5.1 Backup-Funktionen

Mit 365 Total Backup können Backups der vom Kunden angegebenen Daten durchgeführt werden. Folgende Funktionen sind enthalten:

- a. Multi-Tenancy: Verwalten und überwachen aller Backups der Microsoft 365-Organisationen des Kunden über eine webbasierte Multi-Tenant-Konsole. Pro Organisation können unterschiedliche Einstellungen festgelegt werden.
- b. DSGVO-Compliance: Data Retention Policies (Richtlinien zur Datenaufbewahrung) erleichtern die Einhaltung der Datenschutz-Grundverordnung (DSGVO). Backup-Versionen können automatisch fortlaufend oder vollständig nach einer bestimmten Zeit für einen Benutzer/eine Gruppe gelöscht werden, der/die als aus einer Organisation entfernt erkannt wurde. Zusätzlich können Backups für einen ausgewählten Benutzer oder eine Gruppe manuell gelöscht werden.
- c. Datenverschlüsselung: Gesicherte Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand geschützt. Alle Datenübertragungen erfolgen über einen TLS-verschlüsselten Kanal, der den Schutz, der über das Internet oder ein Computernetzwerk gesendeten Daten gewährleistet. Ein TLS-verschlüsselter Kanal wird bei jeder Benutzer-Authentifizierungsinteraktion verwendet, einschließlich bei der Anmeldung, Änderungen von Einstellungen, der Verwaltung von Abonnements und dem Zugriff auf gesicherte Daten.
- d. Vier-Augen-Prinzip: Das Vier-Augen-Prinzip ermöglicht eine zusätzliche Sicherheitsebene, die dabei hilft, Risiken des Verlusts wertvoller Daten zu minimieren. Diese optionale Funktion ermöglicht es Organisationen, spezifische Administratoren als Genehmiger für sensible Vorgänge auszuwählen, wie z. B. Datenlöschung für Benutzer/Gruppen, Tenant-Löschung, Änderungen an Aufbewahrungseinstellungen sowie Änderungen an den Einstellungen für die Vier-Augen-Genehmigung. Wenn die Vier-Augen-Genehmigung aktiviert ist, muss jeder der oben genannten Vorgänge von einem zweiten Administrator genehmigt werden, der als einer der ausgewählten genehmigenden Administratoren aufgeführt ist.
- e. Dashboard: Mithilfe von Widgets können alle Sicherungs- und Wiederherstellungsaktivitäten, der Status der Backups sowie der Verlauf der letzten Wiederherstellungen überwacht werden. Wenn der autorisierte Administrator eine Organisation hinzufügt, kann er auswählen, welche Benutzer und Microsoft 365-Elemente er sichern möchte.

f. Backup-Pilot:



Leistungsbeschreibung

- a. Wenn aktiviert, erkennt 365 Total Backup automatisch neu erstellte Benutzer- und Gruppen-M365-Daten und SharePoint-Sites, die ohne manuelles Eingreifen automatisch gesichert werden können.
- b. Der Backup-Pilot kann so konfiguriert werden, dass er automatisch verschiedene Benutzer- und Gruppen-Workload-Typen wie Postfach, OneDrive, SharePoint, Teams, Planner und Entra ID Benutzer & Gruppen schützt.
- g. Backup-Frequenz: Microsoft 365-Backups werden bis zu viermal täglich automatisiert durchgeführt. Daten, die zwischen den Backup-Snapshots erstellt und gelöscht werden, werden nicht gesichert.
- h. Bulk-User-Management: Das De- und Aktivieren von Backups und das Löschen von Backup-Daten kann für mehrere Benutzer parallel durchgeführt werden. Gesicherte Daten bleiben erhalten, auch wenn ein Benutzer aus dem Microsoft 365-Tenant gelöscht wird.
- i. Backup-Mailbox: Backups für E-Mail-Benutzer enthalten E-Mails, Kalendereinträge und Kontaktadressen.
- j. Backup In-Place-Archivpostfächer: Möglichkeit, alle oder ausgewählte Benutzer- und freigegebene Postfächer mit In-Place-Archiven zu sichern.
- k. Backup OneDrive: Alle in OneDrive gespeicherten Dateien werden gesichert.
- l. Teams Chats Backup: Teams-Chats für Benutzer und Gruppen innerhalb der Organisation werden gesichert, einschließlich aller Dateien, die während der Konversationen geteilt werden.
- m. SharePoint-Backup: Dateien und Kommunikation in SharePoint-Dokumentenbibliotheken werden gesichert, einschließlich der Zugriffsberechtigungen.
- n. Microsoft Planner-Backup: Diese Funktion sichert die Pläne und Aufgaben, die zu Gruppen in der Microsoft 365-Organisation gehören, zusammen mit den Kommentaren und Anhängen in den Aufgaben.
- o. OneNote-Backup: OneNote-Notizbücher, die Benutzern und Gruppen gehören, werden gesichert und können direkt im OneNote-Dienst wiederhergestellt werden.
- p. Entra ID: Die Sicherung von Entra ID umfasst Eigenschaften und Beziehungen, die zu den Benutzern und Gruppen von Entra ID gehören. Gesicherte Eigenschaften und Beziehungen von Entra ID-Benutzern und -Gruppen können direkt in Entra ID wiederhergestellt (neu erstellt) oder in eine ZIP-Datei exportiert werden, die JSON-Dateien mit diesen Eigenschaften enthält.

Aufgrund von Microsoft-Einschränkungen können bestimmte Eigenschaften innerhalb der Entra ID-Benutzer- und Entra ID-Gruppen-Datensätze nicht gesichert oder wiederhergestellt werden.

4.3.5.2 Wiederherstellungs-Funktionen

365 Total Backup ermöglicht die Wiederherstellung von Backups. Dies umfasst die folgenden Funktionen:

- a. Microsoft 365 Versionierung und Wiederherstellung: Sicherungsdaten werden auf unbestimmte Zeit gespeichert, bis sie vom autorisierten Administrator gelöscht werden. Jede im Backup vorhandene Version der Datei, Konversation oder Mailbox kann jederzeit wiederhergestellt werden.
- b. Microsoft 365-Postfächer und In-Place-Archivpostfächer, OneDrive- und SharePoint-Dateien und -Dokumentbibliotheken, Planner, OneNote sowie Entra ID-Benutzer und -Gruppen können:
 - i. zum ursprünglichen Konto wiederhergestellt werden,
 - ii. auf ein anderes Konto innerhalb derselben oder einer anderen Organisation, die demselben Kunden gehört, übertragen werden,
 - iii. Entra ID-Benutzer und -Gruppen können nur in Entra ID der gleichen M365-Organisation neu erstellt werden,



Leistungsbeschreibung

- iv. als ZIP-Archiv heruntergeladen werden (im Falle von Entra ID-Benutzern und -Gruppen enthält das ZIP-Archiv JSON-Dateien mit Daten),
- v. im Falle von Postfächern als PST-Datei exportiert werden,
- vi. Microsoft 365 Teams-Chats können zu einem neuen Team wiederhergestellt oder als HTML-Dateien heruntergeladen werden.

c. Herunterladen und Wiederherstellen mit 365 Total Backup möglich:

- i. die Backup-Daten oder einen Teil davon („granulare Wiederherstellung“) aus einem bestimmten Zeitpunkt direkt in der ursprünglichen Backup-Quelle oder einer anderen Backup-Quelle innerhalb der Microsoft 365-Organisation wiederherstellen und/oder
- ii. die Backup-Daten (kennwortgeschützt) oder einen Teil davon, die zu einem bestimmten Zeitpunkt erstellt wurden, herunterladen. Falls gewünscht, wird ein Download-Link zu den neu gespeicherten Inhalten per E-Mail gesendet.

d. Schnelle und erweiterte Suchfunktion: Autorisierte Administratoren können nach Postfächern und In-Place-Archivpostfächern, Planner, OneNote, OneDrive, SharePoint sowie Entra ID-Benutzern und -Gruppen mithilfe mehrerer Filterkriterien suchen.

e. Granulare Wiederherstellung von Dateien oder E-Mail-Elementen: Das Durchsuchen der Inhalte der Backups ermöglicht autorisierten Administratoren die Auswahl spezifischer Dateien zur Wiederherstellung, einschließlich Postfächern und In-Place-Archivpostfächern, OneDrive, SharePoint-Dokumentbibliotheken, Planner-Plänen, OneNote-Notizbüchern.

f. Einfach zu bedienende Diagramme zeigen die monatliche Nutzung übersichtlich an.

g. Für erfolgreiche, fehlgeschlagene oder mit Warnungen versehene Backup-Status können E-Mail-Benachrichtigungen oder eine tägliche Zusammenfassungenbenachrichtigung konfiguriert werden.

h. Account Activity Audit: Alle Aktivitäten des Benutzerkontos in 365 Total Backup werden auditiert. Dies umfasst sowohl grundlegende und sicherheitsrelevante als auch datenschutzrelevante Informationen wie Browsing und Wiederherstellungsanfragen.

i. Microsoft 365-Daten wiederherstellen – Eine Self-Service-Funktion, die es Endbenutzern innerhalb der Microsoft-365-Organisation ermöglicht, ihre eigenen gesicherten Postfach-, OneDrive- und OneNote-Daten unabhängig und ohne Eingreifen eines Administrators wiederherzustellen. Der Zugriff erfolgt über das User Panel und ist für alle Kunden zugänglich, die über das Control Panel eingebunden sind.

4.3.5.3 Pflichten des Auftraggebers

Der Kunde ist verpflichtet:

- a. den Service gemäß der Acceptable Use Policy zu nutzen; die Fair-Use-Grenzen sind einzuhalten;
- b. die Backup-Daten in regelmäßigen Abständen auf Vollständigkeit, Korrektheit und Wiederherstellbarkeit zu prüfen.

4.3.5.4 Haftungsausschlüsse

a. Der Dienst kann möglicherweise nicht angeboten werden, wenn die Funktionen von Microsoft 365, die Struktur der zu sichernden Daten oder andere technische Spezifikationen von Microsoft oder einem anderen Dritten geändert werden. In diesem Fall besteht das Recht, das Abonnement zu kündigen; allerdings wird in diesem Fall der nicht genutzte Zeitraum des Abonnements anteilig erstattet.

b. Darüber hinaus kann eine Backup-Quelle nicht gesichert werden, wenn diese beschädigt ist, Fehler enthält oder anderweitig nicht lesbar ist oder wenn durch Microsoft oder eine andere Partei, auf die zur Erbringung der Services zurückgegriffen wird, daran gehindert wird.



4.3.6. Modul: Security Awareness Service (SAS)

Enthalten in: Elite

Der Security Awareness Service bietet ein kontinuierliches Security Training für Mitarbeiter (im Folgenden Benutzer). Dabei werden zur Trainingssteuerung verschiedene Mechanismen in Form der Awareness Engine und der Spear-Phishing-Engine eingesetzt. Auf diese Weise werden Mitarbeiter bedarfsgerecht trainiert, um Cyber-Angriffe sicher zu erkennen und effektiv abzuwehren – ohne dass sich Administratoren oder CISOs (im Folgenden Administrator) selbst in die zugrundeliegende Psychologie und Didaktik einarbeiten müssen.

Die Grundlage des Awareness Services bildet ein patentiertes Verfahren zur Messung des Sicherheitsverhaltens aller am Security Awareness Service teilnehmenden Gruppen und Benutzer. Auf Basis des gemessenen Sicherheitsverhaltens wird die wissenschaftliche Kennzahl Employee Security Index (ESI®) berechnet.

4.3.6.1 Funktionen

a. Administratoren können Benutzer im Control Panel über LDAP-Synchronisierung, über Microsoft 365-Synchronisierung oder über .csv-Upload erstellen, löschen und kontinuierlich synchronisieren.

b. Die Awareness Engine bildet den technologischen Kern für den Security Awareness Service im Auto-Pilot-Betriebsmodus. Sie wertet regelmäßig das Security-Verhalten der Benutzer aus und entscheidet auf dieser Grundlage, welche Benutzer zusätzliches Training oder Simulationen erhalten. Jeder Benutzer erhält je nach seinem Security-Level den erforderlichen Umfang an Training. Die Konfiguration umfasst eine Single-User-Booster-Option für Benutzer, die eine intensivere Schulung benötigen, und eine Productivity-Booster-Option für starke Benutzer, die sich mehr auf ihre tägliche Arbeit konzentrieren können. Zu den Schulungsaktivitäten gehören Spear-Phishing-Simulationen und E-Training-Inhalte.

Es ist möglich, die Trainingsmodule selbst zu orchestrieren und zu versenden, anstatt die Awareness Engine zu verwenden. Es können maximal 2 Trainingsmodule pro Monat versendet werden, um eine Überlastung der Benutzer zu vermeiden. In diesem Fall wird die Awareness Engine deaktiviert.

Die patentierte Spear-Phishing-Engine erlaubt das Versenden von Spear-Phishing-E-Mails in verschiedenen Schwierigkeits-Levels.

c. Spear-Phishing-Simulationen sind besonders effektiv, um das Sicherheitsverhalten von Benutzern zu verändern:

i. Erstens kann durch die Erzeugung eines Effekts der „Selbsterfahrung“ das Mindset überwunden werden: „Mich greift doch sowieso keiner an“.

ii. Zweitens bieten Phishing-Simulationen die Möglichkeit, kurze, relevante Lerninhalte in Form eines Nano-Learnings zu vermitteln: Auf der Erklärseite wird der Benutzer interaktiv aufgeklärt, wie er hätte erkennen können, dass diese E-Mail gefälscht war.

iii. Drittens ermöglicht eine Spear-Phishing-Simulation auf Basis der Spear-Phishing-Engine die Messung des aktuellen Employee Security Index (ESI®).

iv. Standardmäßig werden ca. zwei Spear-Phishing-E-Mails pro Monat je Benutzer versendet. Dabei erhält jeder Benutzer zu einem anderen Zeitpunkt eine andere E-Mail. Der Inhalt der E-Mail richtet sich nach Level (siehe v.) sowie vorhandenen Informationen zum Unternehmen bzw. zum Benutzer selbst. Die Intensität kann per Konfiguration im Control Panel erhöht (drei E-Mails pro Monat) bzw. gesenkt (eine E-Mail pro Monat) werden.

v. Die Level der Spear-Phishing-E-Mails basieren auf standardisierten Einteilungen: je höher das Level, desto höher der Zeitaufwand eines Angreifers. Die automatische Auswahl von Spear-



Leistungsbeschreibung

Phishing-E-Mails basiert auf verschiedenen Faktoren, wie z. B. Informationen über den einzelnen Benutzer, das Unternehmen, die Branche usw. Genau wie echte Angreifer wird ein vielfältiges Arsenal an Werkzeugen wie z. B. gefährliche Links, gefälschte Anmeldeseiten, Makros, Dateianhänge usw. verwendet. Spear-Phishing-E-Mails werden in verschiedenen Schwierigkeitsgraden versandt, bei denen unter anderem hochqualitatives Spear-Phishing mit der Simulation von gefälschtem, internen E-Mail-Verkehr realisiert wird:

Level 1: Massen-Phishing

Level 2: gezieltes Phishing sogenannter CEO-Frauds

Level 3: Spear-Phishing unter Einbeziehung von Informationen über das Unternehmen

Level 4: Spear-Phishing mit Bezug zur individuellen Job-Position des Empfängers sowie E-Mails von direkten Kollegen oder Vorgesetzten

Level 5: Spear-Phishing mit Domain-Spoofing

vi. Ein Benutzer muss zunächst ein Level „bestehen“, bevor er sich in das nächste Level steigern kann. Sollte er auf eine Spear-Phishing-E-Mail hereinfallen, wird er um ein Level zurückgestuft. So wird sichergestellt, dass Benutzer nicht überfordert, sondern jeweils auf ihrem individuellen Sicherheitsniveau abgeholt werden und dieses sukzessive gesteigert wird.

vii. Beim Credential-Phishing wird mittels fingierter Anmeldeseiten geprüft, wie viele Benutzer ihre Zugangsdaten auf einer gefälschten Webseite eingeben. Während der Phishing-Simulation werden dabei unter keinen Umständen Login-Daten an die Server übermittelt oder gespeichert.

viii. Beim Malware-Phishing wird mittels fingierter Dateianhänge geprüft, wie viele Benutzer einen Office-Anhang öffnen und ein Makro aktivieren. Die verwendeten Dateianhänge können beispielsweise .docm- und .xlsm-Dateien enthalten. Sie werden jedoch nach Bedarf auf ihre Relevanz geprüft und ggf. verändert. Beim Öffnen einer Datei oder Aktivieren eines Makros wird unter keinen Umständen Malware ausgeführt.

d. Erklärseite (Most Teachable Moment): Relevante Lerninhalte werden geliefert, wenn die Lernbereitschaft am größten ist – nämlich in dem Moment, wenn der Benutzer auf eine Phishing-Mail hereingefallen ist. Auf der interaktiven Erklärseite mit individuellen Trainingsinhalten zu der gerade simulierten E-Mail wird in einem Nano-Learning vermittelt, wie ein echter Angriff hätte erkannt und abgewehrt werden können. Dabei werden sowohl eindeutige Erkennungszeichen als auch psychologische Tricks der Angreifer aufgezeigt.

e. Der Phishing Reporter ist ein Outlook-Add-In für Desktop und mobile Endgeräte. Er vereinfacht den Meldeprozess für reale Angriffe und liefert gleichzeitig positive Rückmeldung für korrekt erkannte Phishing-Simulationen. Der interne IT-Support wird durch unterstützende Informationen und automatisierte Antwortprozesse entlastet. Im Control Panel kann eingesehen werden, wie viele der simulierten Phishing-E-Mails von Benutzern gemeldet wurden. Die geltenden technischen Voraussetzungen für die Nutzung des Outlook-Add-Ins entnehmen Sie dem Benutzerhandbuch.

f. Die E-Trainings vermitteln Benutzern unterhaltsam, anschaulich und verständlich Grundinhalte zu verschiedenen Themen der IT-Sicherheit. In den Trainings liegt der Fokus auf Inhalten, die auch von technischen Laien im Alltag direkt erkannt und umgesetzt werden können. Zu jedem Thema stehen verschiedene Lernmodule, zum Beispiel in Form eines interaktiven E-Trainings, Kurzvideos oder Dokuments, zur Verfügung.

i. Interaktive E-Trainings haben eine Dauer von bis zu 30 Minuten, abhängig von der Komplexität des Themas. Der Fortschritt des Benutzers wird gespeichert, sodass jedes Modul vom Benutzer in einem Stück oder in mehreren Sitzungen bearbeitet werden kann.

ii. In den Kurzvideos wird die Motivation der Lernenden angesprochen, und einzelne Lernziele werden wiederholt und vertieft.



Leistungsbeschreibung

- iii. Zusätzliche weiterführende Dokumente können unterstützende Informationen zu den E-Trainings enthalten, die die Benutzer für den Schnellzugriff abspeichern oder auch ausdrucken können.
- iv. Refresher-Module stehen zur Verfügung, um das Wissen der Benutzer aufzufrischen.
- v. Zusätzlich zu den klassischen E-Trainings bietet SAS auch Quizze zu bestimmten Themen an, um das Wissen zu testen. E-Training-Inhalte können diese Quizze enthalten, um den Benutzern eine unterhaltsame Möglichkeit zu bieten, ihren eigenen Wissensstand zu überprüfen und Konzepte aufzufrischen, die in Vergessenheit zu geraten drohen.
- g. Das User Panel fasst die persönlichen Lerninhalte der Benutzer zentral und bequem an einem Ort zusammen. Benutzer werden automatisch eingeloggt und müssen sich keine Zugangsdaten merken. Sie erhalten dort Zugriff auf ihre gebuchten und zugewiesenen E-Trainings und andere Lerninhalte. Das User Panel speichert alle Zwischenstände der Trainings und die Benutzer können auch bereits abgeschlossene Lerninhalte jederzeit anschauen. Benutzer können außerdem eine personalisierte Auswertung über die erhaltenen Phishing-Mails einsehen. Benutzer können über das User Panel ihr Widerspruchsrecht wahrnehmen und flexibel anpassen, sofern sie selbst nicht als Absender von Phishing-E-Mails fungieren möchten.
- h. Über das Control Panel erhalten Administratoren Zugang zu einem Dashboard, das ihnen jederzeit Einblick in den aktuellen Stand der Simulations- und Trainingsfortschritte und in das aktuelle Sicherheitsverhalten der Benutzer gibt. Zudem können hier die Konfigurationen für den Security Awareness Service angepasst werden.
- i. Nach mindestens einem Jahr erfolgreichem Security Awareness Service wird ein Unternehmenszertifikat ausgestellt, das als Nachweis für das durchgeführte Awareness Training und dessen Ergebnisse dient und bei Audits vorgelegt werden kann. Das Zertifikat wird auf Antrag des Kunden ausgestellt. Es wird jährlich erneuert und ist für ein Jahr gültig.
- j. SAS bietet optional einen Privacy Mode, der aktiviert werden kann, wenn ausschließlich anonymisierte Ergebnisse und Daten des Awareness Trainings reportet und dargestellt werden sollen, um keine Rückschlüsse auf Einzelergebnisse zu gestatten. Personenbezogenes Reporting kann nach lokalem Recht abstimmungsbedürftig oder mitbestimmungspflichtig sein. Wenden Sie sich an Ihren Rechtsbeistand oder Datenschutzbeauftragten. In diesem Fall wird die Verwendung des Privacy Mode empfohlen.
- k. Um den Mitarbeiterschutz zu gewährleisten, ist eine spätere Deaktivierung des Privacy Mode nicht möglich.

4.3.6.2 Pflichten des Kunden

Der Kunde ist verpflichtet, den Service in Übereinstimmung mit der Acceptable Use Policy zu nutzen und auf ihn zuzugreifen und sich an die Fair Use Policy (Richtlinie zur angemessenen Nutzung) zu halten.

4.3.7 Optionales Modul: E-Mail Encryption

Zubuchbar für alle Leistungsstufen (ab Core) – kostenpflichtige Option

Hinweis: Die E-Mail Encryption ist ein optionales Zusatzmodul, das ab ambiSECURE M365 Core gegen Mehrkosten hinzugebucht werden kann und somit für alle Leistungsstufen als optionales Paket verfügbar ist. Sie ist eine Erweiterung der Spam and Malware Protection und setzt deren Nutzung voraus.

Die E-Mail Encryption ist eine Erweiterung der Spam and Malware Protection und setzt die Nutzung des Spamfilterservice voraus.

Ausgehende E-Mails werden verschlüsselt und signiert, eingehende E-Mails des Auftraggebers werden auf eigenen IT-Systemen entsprechend den eingestellten Richtlinien entschlüsselt.



Leistungsbeschreibung

Ausgehende E-Mails werden per S/MIME signiert, sofern die dazu nötigen privaten Schlüssel im Zertifikatsspeicher vorliegen und im Control Panel im Bereich S/MIME Users die Signierung für den Benutzer aktiviert wurde.

Die Richtlinien zur Verschlüsselung ausgehender E-Mails können von dazu autorisierten Benutzern des Auftraggebers im Control Panel eingestellt werden.

Je nach Einstellung der Richtlinien werden ausgehende E-Mails:

- a. mit dem öffentlichen Schlüssel des Empfängers per S/MIME oder PGP verschlüsselt übertragen,
- b. nicht verschlüsselt, aber über einen per TLS verschlüsselten Kanal übertragen,
- c. im geschützten Websafe für den Empfänger bereitgestellt,
- d. unverschlüsselt übertragen.

Die Policies können durch autorisierte Benutzer z. B. im Control Panel gesetzt werden. Die Verschlüsselung einer Mail kann zusätzlich durch den Benutzer beim Versand über einen Betreff-Zusatz („Tag“) oder das Outlook Add-In sichergestellt werden.

Sofern die Richtlinie zwingend die verschlüsselte Übertragung vorsieht, aber der dazu nötige öffentliche Schlüssel des Empfängers nicht im Zertifikatsspeicher vorliegt und die ggf. eingestellte Übertragung per TLS vom empfangenden Server nicht unterstützt wird, werden ausgehende E-Mails an diesen Empfänger zurückgewiesen und nicht übertragen.

Eingehende, per S/MIME oder PGP verschlüsselte E-Mails werden automatisch entschlüsselt, sofern der dazu nötige private Schlüssel des Empfängers im Zertifikatsspeicher vorliegt.

Öffentliche Schlüssel werden automatisch aus Signaturen eingehender E-Mails extrahiert und im Zertifikatsspeicher hinterlegt.

S/MIME-Zertifikate für Benutzer des Auftraggebers können im Rahmen der S/MIME User Subscription per Control Panel bestellt werden. Alternativ können PGP-Keys für die Benutzer des Auftraggebers generiert oder vorhandene S/MIME-Zertifikate und PGP-Keys durch den Support im Zertifikatsspeicher abgelegt werden. Für die Nutzung von Zertifikaten und Keys wird eine jährliche Gebühr pro Zertifikat und Key des Benutzers gemäß der aktuellen Preisliste erhoben. Diese Subscription verlängert sich automatisch, sofern sie nicht 3 Monate vor Ablauf deaktiviert wird, und inkludiert die automatische Neubestellung von Zertifikaten und Keys bei Bedarf.

Die Geheimhaltung der im Zertifikatsspeicher gespeicherten privaten Schlüssel des Auftraggebers wird sichergestellt. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.

Über den Websafe können Kommunikationspartner verschlüsselte E-Mails sicher via HTTPS abrufen, sofern der Auftraggeber den Websafe in seinen Verschlüsselungsrichtlinien aktiviert hat. Hierfür erhält der Absender der Nachricht eine PIN, die er dem Empfänger zur initialen Authentifizierung und/oder zum Passwortreset zur Verfügung stellt. Im Rahmen des Websafe 2.0 besteht für den Login von Kommunikationspartnern am Websafe die Option, die PIN über einen weiteren Kanal auf mobile Endgeräte des Kommunikationspartners zu senden. Es wird vorbehalten, die Verwendung des SMS-Gateways bei Verdacht auf missbräuchliche Nutzung zu deaktivieren.

Der verschlüsselte Versand nach EDIFACT-Standard wird unterstützt. Die hierfür notwendigen S/MIME-Zertifikate mit RSASSA-PSS-Hashverfahren werden vom Auftraggeber für den Import bereitgestellt.

Der Support autorisierter Benutzer wird sichergestellt, soweit es die eigenen Systeme betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

Optional wird eine Anbindung der E-Mail-Infrastruktur des Kunden an den „E-Mail made in Germany“ (EmiG)-Verbund ermöglicht; hierfür wird die mailserverseitige Umsetzung realisiert, die



Leistungsbeschreibung

für die Erfüllung der Anforderungen an eine durchgehende Transportverschlüsselung von E-Mails im EmiG-Verbund notwendig ist.

- a. Es wird sichergestellt, dass eine als EmiG gekennzeichnete Nachricht nicht über andere, potenziell unsichere Kanäle zugestellt wird.
- b. Die durchgängig verschlüsselte Datenübertragung zwischen den Mail Transfer Agents (MTAs) wird sichergestellt mittels STARTTLS-Erweiterung gemäß RFC 3207.
- c. Die TLS1.2-Verbindung wird eingehend (TLS-Client) wie ausgehend (TLS-Server) realisiert.
- d. Es wird sichergestellt, dass EmiG-Kommunikation nur unter Verwendung Perfect-Forward-Secrecy(PFS)-fähiger Schlüsselaustauschverfahren basierend auf dem Diffie-Hellman-Verfahren aufgebaut wird.
- e. Bei Schlüsselneuverhandlungen für Mailkommunikation innerhalb des EmiG-Verbundes wird Secure Renegotiation gemäß RFC 5746 verwendet.
- f. Jeder Zertifikats-/Verschlüsselungsfehler beim STARTTLS-Aufbau wird genauso behandelt, als sei gar keine SMTP-Verbindung aufgebaut worden: Die Mail wird in eine Mail-Queue zurückgestellt, aus der weitere Zustellversuche unternommen werden. Bei dauerhaftem Fehlschlagen der Zustellung wird eine Bounce-Nachricht an den Sender geschickt.
- g. Anhand der innerhalb des EmiG-Verbunds annoncierten Zertifikatsfingerprints werden die Identität und EmiG-Verbund-Zugehörigkeit der Kommunikationspartner der Nutzer des Kunden überprüft.
- h. Der per MX-Lookup ermittelte Hostname eines Mailservers wird mit dem im Host-Zertifikat hinterlegten Namen abgeglichen.
- i. Es wird überprüft, ob der Fingerprint des vom Mailserver des Kommunikationspartners verwendeten Zertifikats dem über EmiG annoncierten Fingerprint entspricht.
- j. Schlägt diese Validierung fehl, wird die E-Mail-Kommunikation mit diesem Mailserver unterbrochen; die Mail wird nicht weitergeleitet.
- k. Die Zertifikatsprüfung wird gemäß PKIX einschließlich der Sperrprüfung der Server- und Sub-CA-Zertifikate durchgeführt.
- l. Die per HTTPS vom EmiG-Verbund bidirektional zur Verfügung zu stellenden JSON-MX-Infrastrukturlisten werden gemäß der EmiG-Vorgaben für den Kunden vollautomatisch generiert und gepflegt.
- m. Die notwendigen Informationen, die der Kunde dem EmiG-Verbund mitzuteilen hat, werden über die von EmiG vorgegebenen Verfahren (MX-Infrastruktur-Listen) annonciert.
- n. Die Authentifikation des sendenden Mailservers als Server eines EmiG-Teilnehmers wird mittels dynamischem Abgleich mit den bei EmiG registrierten IPs durchgeführt.
- o. Dem Kunden werden verschiedene Möglichkeiten der Darstellung angeboten, ob eine Nachricht gemäß den Vorgaben des EmiG-Verbunds versendet oder empfangen wurde:
 - i. Im Control Panel wird dem Nutzer dargestellt, ob eine Mailkommunikation gesichert über den EmiG-Verbund stattfand.
 - ii. Unter Verwendung eines Outlook-Add-ins kann der Nutzer den EmiG-Status seiner Nachrichten und Kommunikationspartner in Outlook einsehen.

4.3.8. Fair Use Limits (Einschränkungen zur angemessenen Nutzung)

- a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Software erforderlich sind und die in diesem Zusammenhang zur Verfügung gestellt werden, werden von allen Kunden gemeinsam genutzt. Daher besteht das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.



Leistungsbeschreibung

b. Es werden keine Richtwerte vorab festgelegt, die eine exzessive oder unangemessene Nutzung bestimmen, da nach eigenem Ermessen entschieden werden kann, die normalen Service-Levels aufrechtzuerhalten, indem für andere Nutzer reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zugewiesen oder Ressourcen anderweitig skaliert werden. Der Auftraggeber nimmt zur Kenntnis, dass ein Verzicht auf die aktive Durchsetzung dieser Richtlinie zur angemessenen Nutzung nicht als Verzicht auf das Recht zu deren Durchsetzung gilt und auch keine Zustimmung dazu darstellt, dass der Auftraggeber die Dienste weiterhin auf demselben Niveau nutzen darf, wie er es zu einem bestimmten Zeitpunkt tut.

c. Um die Dienste nutzen zu können, muss der Auftraggeber abrechenbare Einheiten erwerben. Die Anzahl der benötigten abrechenbaren Einheiten hängt von einer Reihe von Kriterien ab, wie z. B. der Größe des Unternehmens, der Anzahl der Nutzer und der Speichergröße der jeweiligen Datenquellen. Die Anzahl der benötigten abrechenbaren Einheiten kann anhand der auf der Webseite für Gebühren und Abrechnungen bereitgestellten Leitfäden oder mit Unterstützung des Vertriebsteams ermittelt werden.

d. Unabhängig von der Anzahl der erworbenen abrechenbaren Einheiten hat der Auftraggeber die Dienstleistungen zweckmäßig zu nutzen, und zwar in einer Weise, die es nicht erforderlich macht, unverhältnismäßig viele Ressourcen zuzuweisen. Zur Feststellung wird die Nutzung der Ressourcen und der Speicherbedarf des Auftraggebers mit dem eines durchschnittlichen Kunden verglichen. Der Durchschnittskunde wird ermittelt, indem die 5 % höchsten und die 5 % niedrigsten Kunden der jeweiligen Ressource unberücksichtigt bleiben und der Mittelwert über alle aktiven Kunden gebildet wird.

e. Spezifische Merkmale, die sich auf die Branche beziehen, in der der Auftraggeber tätig ist, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Sofern nach vernünftigem Ermessen und in gutem Glauben davon ausgegangen wird, dass die Nutzung der Lösung durch den Auftraggeber nicht sinnvoll ist oder gegen diese Richtlinie verstößt, wird nach eigenem Ermessen eine der folgenden Maßnahmen ergriffen:

i. Dem Auftraggeber wird die weitere Nutzung der Lösungen gestattet, jedoch vorbehaltlich der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die unter den gegebenen Umständen für angemessen gehalten werden.

ii. Der Auftraggeber wird darüber informiert, dass sein Konto innerhalb eines nach eigenem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die betroffenen Dienste ausgesetzt.

g. Wird von dem Recht Gebrauch gemacht, das Konto des Auftraggebers wie oben beschrieben zu kündigen:

i. Werden die im Rahmen des Dienstes gespeicherten Daten des Auftraggebers am Ende des in der diesbezüglichen Benachrichtigung festgelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.

ii. erhält der Auftraggeber eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage seines Abonnementzeitraums.