



# Anlage 1: Leistungsbeschreibung der NetPlans Systemhausgruppe

*STAND: JANUAR 2026*

## I. NetPlans Business Cloud

### 01 NetPlans Cloud Cockpit

Das NetPlans Cloud Cockpit dient als administrative Plattform für sämtliche virtuellen Maschinen, unabhängig vom Service-Modell (IaaS, PaaS, FaaS). NetPlans stellt dabei alle Infrastruktur-Komponenten gemäß Auftrag, wie z.B. Server, Rechenleistung, Netzkapazitäten, Speicher, Backup-Kapazitäten auf einer shared Hardware-Plattform zur Verfügung. NetPlans stellt das NetPlans Cockpit für die Administration der kundeneigenen virtuellen Infrastruktur innerhalb der NetPlans Business Cloud als Webservice zur Verfügung. Die NetPlans strebt dabei eine Verfügbarkeit von jeweils 99,5 Prozent im Monatsmittel an. Da es sich bei der Bereitstellung des NetPlans Cockpit um eine Zusatzleistung handelt, die dem Kunden kostenlos zur Verfügung gestellt wird, unterliegt die Einhaltung der Verfügbarkeit keiner Gutschrift-Regelung. Durch die Administration der virtuellen Infrastruktur sind Veränderungen von abrechnungsrelevanten Parametern (wie bspw. vCPU, RAM und Speicherplatz) durch den Kunden eigenständig möglich. Sowohl eine Erweiterung als auch eine Verringerung wird automatisch in der darauffolgenden Abrechnungsperiode berücksichtigt. Die Veränderungen werden über ein konsistentes Log-Protokoll auf Ebene der einzelnen Benutzer (NetPlans Cockpit User) durch die NetPlans als Nachweis erfasst und bei Bedarf ausgewertet. Für Veränderungen von abrechnungsrelevanten Parametern gelten, bis auf Widerruf der NetPlans, die zum Vertragsschluss vereinbarten Konditionen. Dem Kunden ist bekannt, dass für die Nutzung des NetPlans Cloud Cockpits fundierte Kenntnisse zur Administration von Serversystemen (Systemadministration) erforderlich sind. NetPlans ist nicht verpflichtet, die vom Kunden übermittelten und gespeicherten Informationen zu überwachen und/ oder nach Umständen zu forschen, die auf rechtswidrige Aktivitäten und/ oder Nutzungen hindeuten. Es obliegt ausschließlich dem Kunden, die auf seinem Rechenzentrum installierten Betriebssoftware, Anwendungen oder Entwicklungen zu aktualisieren und technisch zu kontrollieren und inhaltlich zu überwachen. Sofern sich ein Zugriff außerhalb eines vertrauten Netzwerks befindet, erfordert die Anmeldung eine 2-Faktor-Authentifizierung, die auf schriftliches Anfordern durch den Kunden als kostenlose Zusatzleistung bereitgestellt wird.

Nachfolgender Funktionsumfang ist für die Nutzung des NetPlans Cloud Cockpit vorgesehen:

- Grafische Übersicht zum Status und zu den genutzten Ressourcen pro virtuelle Maschinen.
- Log-Protokolle aller Aktionen pro VM und Username
- Logging aller Aktionen pro VM und Username
- Herunterfahren, Ausschalten, Starten, Neustart und Reset einer virtuellen Maschine.
- vCPU erweitern und reduzieren.
- Arbeitsspeicher (RAM) erweitern und reduzieren.
- Speicherplatz erweitert, hinzufügen und löschen.
- Speicherklasse ändern (HighPerf, Perf und Archiv).
- Snapshot der VM erstellen, löschen, wiederherstellen und verwalten.

Eine Veränderung von abrechnungsrelevanten Parametern ist innerhalb des Kunden-Account per Voreinstellung mit maximal 20% der bereits genutzten Ressourcen möglich, mindestens jedoch mit 2 vCPU, 8 GB RAM und 100 GB Speicherplatz. Dieser Wert bezieht sich jeweils auf den Vormonat und steigt dynamisch mit den vergebenen Ressourcen. Demnach lässt sich die Umgebung monatlich um bis zu 20% erhöhen. Sollte es notwendig sein, dass eine Veränderung von abrechnungsrelevanten Parametern diesen Wert übersteigt, kann eine gesonderte Anfrage bei NetPlans eingereicht werden oder eine individuelle Einstellung konfiguriert werden.

## **02 Infrastructure as a Service (IaaS)**

Das Infrastructure as a Service Modell bildet die Grundschrift für einen Cloud-Betrieb. NetPlans stellt dabei alle Infrastruktur-Komponenten gemäß Auftrag, wie z.B. Server, Rechenleistung, Netzkapazitäten, Speicher, Backup-Kapazitäten auf einer shared Hardware-Plattform zur Verfügung. Dabei endet die Betriebsverantwortung seitens NetPlans nach der Oberkante des Hypervisors (Virtualisierung). Administrationsrechte sind nur lokal möglich. Der Kunde ist für die innerhalb des Servers installierten Applikationen, deren Systempflege und Wartung selbst verantwortlich. Dieses Modell ermöglicht administrative Freiheiten u.a. auch über die Verwaltung Ihrer Microsoft-Systeme. Aufgrund administrativer Freiheiten können u.a. eigenständig weitere User angelegt und berechtigt werden. Werden eigenständig Erweiterungen vorgenommen, die eine Erhöhung oder Minderung der bestehenden Softwarelizenzen des Cloud-Vertrages bedeuten, müssen diese Änderungen unverzüglich an NetPlans übermittelt werden.

## **03 Managed Platform as a Service (PaaS)**

Der Cloud-Dienst „Managed Platform as a Service (PaaS)“ ermöglicht die Erweiterung von Infrastructure as a Service Umgebungen in der NetPlans Business Cloud für virtuelle Maschinen mit Microsoft Windows Server Betriebssystem. Dabei können zwei grundlegende Varianten Anwendung finden:

- Anbindung eines bestehenden Microsoft Active Directory,
- Aufbau eines eigenen Microsoft Active Directory.

Die Variante eines Shared Microsoft Active Directory ermöglicht dem Kunden ausschließlich lokale Administrationsrechte. Der Zugriff auf die Domain Controller sowie das Microsoft Active Directory sind eingeschränkt. Die virtuellen Microsoft Windows Maschinen werden innerhalb des Managed Platform as a Service (PaaS) mit dem Cloud-Dienst „Managed Windows Server Update Services (WSUS)“ versorgt und mit einem Monitoring-Service sowie einem Virenschutz-Agent versehen. Eine zusätzliche optionale Erweiterung stellt die IT-Orchestrierungssoftware „Atria“ dar, die über eine zentrale Management-Weboberfläche Windows-User und -Gruppen und definierte NetPlans Business Cloud Services verwaltet und eine neue Provisionierung ermöglicht. sind. Hierfür wird eine weitere virtuelle Maschine benötigt.

Der Kunde ist für die innerhalb des Servers installierten Applikationen, deren Systempflege und Wartung selbst verantwortlich. Nach Abstimmung können diese Arbeiten separat über einen Wartungsvertrag von NetPlans übernommen werden. Die initiale Bereitstellung wird nach tatsächlichem Zeitaufwand berechnet. Der Dienst wird ausschließlich von NetPlans betrieben. Aufwände für einen anfallenden Service-Request werden nach tatsächlichem Zeitaufwand berechnet.

#### **04 Full Managed as a Service (FMaaS)**

Der Cloud-Dienst Full Managed as a Service verfügt über ein mandantenfähiges Microsoft Active Directory sowie eine mandantenfähige Citrix Verwaltungsumgebung, die für die Bereitstellung der virtuellen Arbeitsplätze der Mitarbeiter, über eine kundenspezifische Citrix App und Desktop (Terminalserver) Umgebung, Anwendung findet. Die Lizenzierung des Dienstes erfolgt pro User (Mitarbeiter). Dem Kunden werden auf s.g. BusinessApp Servern virtuelle Windows Server bereitgestellt. Administrationsrechte sind nur lokal möglich. Der Kunde ist für die innerhalb des Servers installierten Applikationen, deren Systempflege und Wartung selbst verantwortlich. Nach Abstimmung können diese Arbeiten separat über einen Wartungsvertrag durch NetPlans übernommen werden. Es ist verbindlich an jedem Arbeitsplatz des Kunden zusätzlich ein Antivirenprogramm einzusetzen. Dieses Antivirenprogramm ist kein Bestandteil des Leistungsumfangs innerhalb des Full Managed as a Service. Sollte ein Arbeitsplatz nicht über ein gültiges Antivirenprogramm verfügen, ist dies vom Kunden NetPlans mitzuteilen. NetPlans wird sich dann, in Absprache mit dem Kunden, der Situation annehmen und Lösungsmöglichkeiten unterbreiten. Ein Zugriff auf die Verwaltungsinstrumente oder Datensicherung (RestorePoints bzw. Wiederherstellung von Daten und Dateien) ist ausschließlich über ein Service-Request und durch die Bearbeitung der NetPlans IT-Supportabteilung möglich. Aufwände für einen anfallenden Service-Request werden nach tatsächlichem Zeitaufwand berechnet.

#### **05 Full Managed as a Service DATEV (FMaaS)**

Im Rahmen des Full Managed as a Service (FMaaS) erhält der Kunde zusätzlich eine vollständig eingerichtete DATEV-Infrastruktur inklusive myUTN-Schnittstelle für den DATEV mIdentity. Die Verantwortung für die auf dem DATEV-Server installierten Anwendungen sowie deren Systempflege und Wartung liegt grundsätzlich beim Kunden. Alternativ können diese Aufgaben – nach individueller Abstimmung – im Rahmen eines optional buchbaren DATEV Maintenance Services durch NetPlans übernommen werden. NetPlans ist hierfür als zertifizierter DATEV-Systempartner qualifiziert. Die Infrastruktur wird abhängig von der Nutzeranzahl unterschiedlich bereitgestellt. Bei kleinen Umgebungen mit bis zu sieben Nutzern kommt eine All-in-One-Lösung zum Einsatz, basierend auf einem kundenspezifischen Citrix Apps und Desktop Server (Terminalserver) mit installierter DATEV-Software. Diese Lösung wird innerhalb eines mandantenfähigen Microsoft Active Directory bereitgestellt. Für größere Umgebungen ab acht Nutzern werden ein dedizierter Citrix Apps und Desktop Server sowie ein separater DATEV-Server eingerichtet – ebenfalls innerhalb des mandantenfähigen Active Directory. Die Anzahl der eingesetzten Terminalserver wird dabei flexibel

an die Nutzeranzahl angepasst. Ein späterer Wechsel von einer kleinen zu einer größeren Infrastruktur ist möglich, erfordert jedoch eine kostenpflichtige Trennung der All-in-One-Lösung in separate Serverinstanzen. Alle Infrastrukturen verfügen über einen hochverfügbaren DFS-FileServer-Speicher, der für Benutzerprofile und individuelle Kundendaten genutzt wird. Die Speicherkapazität kann kostenpflichtig in Einheiten von je einem Gigabyte erweitert werden. Wird ein definierter Schwellwert erreicht, erfolgt automatisch eine Erweiterung um zehn Gigabyte. Zum Schutz der Serverumgebung setzt NetPlans einen zentralen Antivirenschutz ein. Es wird empfohlen, auch auf den eingesetzten Endgeräten eine geeignete Antivirensoftware zu verwenden. Sollte an einzelnen oder allen Arbeitsplätzen kein gültiger Virenschutz vorhanden sein, ist dies NetPlans mitzuteilen. In Abstimmung mit dem Kunden werden dann geeignete Schutzmaßnahmen vorgeschlagen. Zugriffe auf Verwaltungsfunktionen sowie auf Datensicherungen (z. B. Wiederherstellungspunkte oder einzelne Dateien) erfolgen ausschließlich über einen Service-Request und werden durch den IT-Support von NetPlans bearbeitet. Der Aufwand für solche Anfragen wird nach dem tatsächlich entstandenen Zeitaufwand abgerechnet.

## 06 Hosted Exchange

Der Cloud-Dienst „Hosted Exchange“ wird über ein zentral bereitgestelltes Microsoft Exchange Cluster (DAG) realisiert. Die Lizenzierung erfolgt pro Postfach. Für jedes Postfach ist der verwaltete Service „Managed Mail Security“ bereits beinhaltet. Die Konfiguration und Ersteinrichtung erfolgt durch NetPlans. Dabei werden die MX-Resource-Record-Einstellungen (Mail Exchange Resource Record) der Kunden-Domain, auf die öffentlichen A-Resource-Record-Einträge von NetPlans konfiguriert. Der Kunde hat die Möglichkeit, über ein zentrales Web-Portal, die E-Mail-Einstellungen sowie Verteilergruppen und Kontakte selbst anzulegen und zu verwalten. Verbindungen werden ausschließlich durch HTTPS (Hypertext Transfer Protocol Secure) angeboten. Diese sind über einen zentralen WAF-Service (Web-Applikation-Firewall) abgesichert und stellen dabei Outlook-Web-Access (OWA), ActiveSync und Outlook Anywhere zur Verfügung. Wird als E-Mail-Client Microsoft Outlook verwendet, muss dieser immer, entsprechend den von Microsoft unterstützten Versionen, für die gängige Exchange-Version kompatibel sein. NetPlans behält es sich vor, unter Berücksichtigung von angekündigten Wartungsfenstern, die installierte Exchange-Version jederzeit durch ein Update anzuheben. Zentrale Updates der Server und deren benötigten Komponenten werden von NetPlans durchgeführt und sind im Preis mit inbegriffen. Individuelle Anpassungen oder Änderungen, die nicht im Self-Service-Portal gemacht werden können, müssen gemeinsam mit dem Supportcenter der NetPlans realisiert werden. Für das Versenden einer E-Mail von Services oder auch Druckern an einen SMTP-Relay-Server (s.g. Smarthost) empfehlen wir den externen Service namens Mailgun. Mailgun nimmt SMTP-Anfragen an und versendet im Anschluss an entsprechende Empfänger über eine verschlüsselte Verbindung. Darüber hinaus wird die Möglichkeit einer Authentifizierung gegeben. Dieser Service ist Bestandteil des Hosted Exchange und wird kostenfrei für Versand von Druck- und Scangeräten sowie dem Newsletter Versand zur Verfügung gestellt. Mailgun ist ein Cloudservice außerhalb der Business Cloud, der auf Server des Herstellers innerhalb der EU betrieben wird. Weitere Informationen finden Sie auf der Herstellerseite: <https://www.mailgun.com>

## **07 Managed E-Mail-Archivierung Service**

Der Cloud-Dienst „Managed E-Mail-Archivierung“ wird über eine mandantenfähige Archivierungs-Appliance vom Hersteller dataglobal mit dem Produkt dgmail realisiert und zentral von NetPlans verwaltet. Die Trennung der Mandanten erfolgt über sogenannte Departments. Pro Mandanten wird ein Department zur Verfügung gestellt welches sicherstellt, dass ausschließlich E-Mails des jeweiligen Mandanten enthalten sind. dataglobal bietet eine zertifizierte Lösung für rechtssicher E-Mail-Archivierung in Form einer Journal-Mailbox. Beim Journaling werden E-Mails in der Journal-Mailbox abgelegt, aus der sie anschließend unverändert archiviert werden. Alle E-Mails werden indiziert und sind durchsuchbar. Alternativ oder zusätzlich, kann durch ein entsprechendes Outlook Plug-In eine manuelle E-Mail-Archivierung (Mailbox-Archivierung) realisiert werden. Ein definiertes Regelwerk sorgt für eine automatische Archivierung nach ausgewählten Parametern, wie z.B. Alter einer E-Mail. Das Regelwerk wird durch NetPlans in Abstimmung mit dem Kunden konfiguriert. Der Zugriff auf archivierte E-Mails erfolgt über ein Plug-In des Herstellers und muss auf dem Client installiert sein. Ein Im- und Export von vorhandenen E-Mails im PST-Dateiformat ist gegen Aufwand möglich. Die Lizenzierung erfolgt pro Postfach.

## **08 Managed Exchange Archivierung Service**

Der Cloud-Dienst „Managed Exchange Online E-Mail-Archivierung“ wird über eine mandantenfähige Archivierungs-Appliance vom Hersteller dataglobal mit dem Produkt dgmail realisiert und zentral von NetPlans verwaltet. Die Trennung der Mandanten erfolgt über sogenannte Departments. Pro Mandanten wird ein Department zur Verfügung gestellt welches sicherstellt, dass ausschließlich E-Mails des jeweiligen Mandanten enthalten sind. Dataglobal bietet eine zertifizierte Lösung für rechtssicher E-Mail-Archivierung in Form einer Journal-Mailbox. Beim Journaling werden E-Mails in der Journal-Mailbox abgelegt, aus der sie anschließend unverändert archiviert werden. Alle E-Mails werden indiziert und können durchsucht werden. Ein Im- und Export von vorhandenen E-Mails im PST-Dateiformat ist gegen Aufwand möglich. Zentrale Updates der Server und deren benötigten Komponenten werden von NetPlans durchgeführt und sind im Preis inkludiert. Individuelle Anpassungen oder Änderungen, müssen gemeinsam mit dem Supportcenter der NetPlans realisiert werden.

## **09 BACKUP SERVICES**

### **09.01 Online Backup**

Das NetPlans Online Backup ist eine Speicherlösung auf Basis von Veeam Cloud Connect und stellt ein Backup Repository für die Auslagerung der Kundenbackups zur Verfügung. Auf diesen Backup-Speicher der NetPlans Business Cloud können Kopien der vorhandenen Backups ausgelagert werden. NetPlans repliziert ausschließlich Backups, die in der lokalen Infrastruktur erfolgreich erstellt worden sind, in die Cloud. Eine inhaltliche Prüfung oder Konsistenzkontrolle der Daten

erfolgt nicht. Für die Erstellung, Integrität und Funktionsfähigkeit der lokalen Backups ist der Kunde vor Ort in seiner lokalen Backup-Infrastruktur verantwortlich. Sollten fehlerhafte oder unvollständige Backups vorliegen, werden diese in gleicher Form in die Cloud übertragen. Die Replikation der Daten erfolgt verschlüsselt während des Transports; zusätzlich kann die Verschlüsselung der ruhenden Daten durch den Kunden aktiv festgelegt werden. Für den Upload in die NetPlans Business Cloud gilt eine standardmäßige Bandbreitenbegrenzung von 200 Mbit/s, die auf Anfrage erhöht werden kann. Da für das Backup Drittanbieter-Software verwendet wird, kann die Funktionsfähigkeit der Datensicherung nicht in jedem Fall garantiert werden. Im NetPlans Online Backup wird nur eine Kopie der Daten auf einem einzelnen Speichersystem vorgehalten. Eine redundante Speicherung oder zusätzliche Replikation innerhalb der Cloud erfolgt nicht. Die Abrechnung erfolgt nach tatsächlichem Verbrauch monatlich pro Terabyte und pro replizierte VM (virtuelle Maschine). Zusätzliche Kosten für die Datenübertragung (Traffic) fallen nicht an.

### **09.02 Cloud Backup**

Das NetPlans Cloud Backup ist eine Speicherlösung auf Basis der S3-API-Spezifikation (Simple Storage Service). Kunden können damit ihre Backups inklusive Metadaten in Buckets speichern und über ihre lokale Backup-Software darauf zugreifen. NetPlans repliziert ausschließlich Backups, die in der lokalen Infrastruktur erfolgreich erstellt worden sind, in die Cloud. Eine inhaltliche Prüfung oder Konsistenzkontrolle der Daten erfolgt nicht. Für die Erstellung, Integrität und Funktionsfähigkeit der lokalen Backups ist der Kunde vor Ort in seiner lokalen Backup-Infrastruktur verantwortlich. Sollten fehlerhafte oder unvollständige Backups vorliegen, werden diese in gleicher Form in die Cloud übertragen. Die Replikation der Daten erfolgt verschlüsselt während des Transports; zusätzlich kann die Verschlüsselung der ruhenden Daten durch den Kunden aktiv festgelegt werden. Für den Upload in die NetPlans Business Cloud gilt eine standardmäßige Bandbreitenbegrenzung von 200 Mbit/s, die auf Anfrage erhöht werden kann. Die Sicherung in die NetPlans Business Cloud wird durch sichtbare Kontrollmechanismen, in Form einer E-Mail-Benachrichtigung, überwacht. Da für das Backup Drittanbieter-Software verwendet wird, kann die Funktionsfähigkeit der Datensicherung nicht in jedem Fall garantiert werden. Im NetPlans Cloud Backup wird nur eine Kopie der Daten auf einem einzelnen Speichersystem vorgehalten. Eine redundante Speicherung oder zusätzliche Replikation innerhalb der Cloud erfolgt nicht. Die Abrechnung erfolgt monatlich pro Terabyte und nach tatsächlichem Verbrauch. Zusätzliche Kosten für die Datenübertragung (Traffic) fallen nicht an. Auf Wunsch kann kostenneutral ein Object Lock aktiviert werden. Diese Funktion schützt gespeicherte Backups vor versehentlichem oder vorsätzlichem Löschen oder Überschreiben. Der Kunde legt einen Aufbewahrungszeitraum fest, innerhalb dessen die Daten unveränderbar bleiben. Während dieser Zeit kann weder NetPlans noch der Kunde selbst die Backups löschen oder modifizieren. Diese Sperre ist bindend und kann nachträglich nicht aufgehoben oder verkürzt werden.

### **09.03. Managed Backup Office 365**

Der Cloud-Dienst „Managed Backup Office 365“ wird über eine zentrale Installation durch NetPlans administriert und dient der Datensicherung von Office 365 Daten. Als Sicherheitsquelle werden die

Cloud-Services „Exchange Online, SharePoint Online und OneDrive for Business“ unterstützt. Der Sicherungsintervall entspricht einer täglichen Sicherung, die auf Disk basierten Systemen der NetPlans Business Cloud gespeichert werden. Dabei findet das Datensicherungskonzept unter § 1.1 Vorbemerkung Anwendung. Der Service enthält ausschließlich die notwendigen Softwarelizenzen für die Datensicherung und die Infrastruktur. Die Lizenzierung erfolgt pro Office 365 User inkl. 50 GB Backup-Speicher. Softwarelizenzen für Office 365-Produkte werden in einer separaten Lizenzierung vorausgesetzt. NetPlans obliegt die Betriebsverantwortung der Infrastruktur inkl. Updates, Upgrades und Monitoring. Die initiale Bereitstellung wird nach tatsächlichem Zeitaufwand berechnet. Der Dienst wird ausschließlich von NetPlans betrieben. Ein Zugriff auf die Verwaltungsinstrumente oder Datensicherung (RestorePoints) ist ausschließlich über ein Service-Request und durch die Bearbeitung der NetPlans IT-Supportabteilung möglich. Aufwände für einen anfallenden Service-Request werden nach tatsächlichem Zeitaufwand berechnet.

## **10 NPbox Next**

Der Cloud-Dienst „NPbox Next“ wird über ein mandantenfähiges Setup der Enterprise Fileshare Lösung „FileCloud“ realisiert. Eine Integration eines Active Directory kann auf Wunsch über LDAP mit SSL-Verschlüsselung hergestellt werden, wenn eine private Netzwerkanbindung vorhanden ist. Bei FMaaS-Kunden erfolgt dies automatisch. Alle in FileCloud gespeicherten Dateien werden im AES-256 Verschlüsselungsverfahren verschlüsselt gespeichert. Zugriffs- und Aktivitätsprotokolle können für Sicherheits- und Compliance-Zwecke detailliert ausgewertet werden. Über das Versionsmanagement von FileCloud können (je nach kundenspezifischer Einstellung) vorgehaltenen Versionen wiederhergestellt werden. Eine andere Wiederherstellungsmöglichkeit ist nicht vorgesehen. Die Lizenzierung erfolgt pro User und anhand des benötigten Datenspeichers.

## **11 Managed Web Applikation Firewall Security Service**

Der Cloud-Dienst „Managed WAF Security Service“ wird über eine zentral bereitgestellte Web-Application-Firewall (WAF) realisiert. Die Lizenzierung des Dienstes erfolgt pro WebServer und wird zentral von NetPlans verwaltet. Die Konfiguration und Ersteinrichtung erfolgt durch NetPlans. Sämtliche Einstellungen und Anpassungen sind mit NetPlans abzustimmen. Je nach Art des WebService, können entsprechende Sicherheitschecks und Scans eingerichtet werden. Zentrale Updates der Appliance und die Überprüfung der Firewall werden von NetPlans durchgeführt und sind im Preis mit inbegriffen. Individuelle Anpassungen oder Änderungen pro WebServer sind kostenpflichtig und werden gemeinsam mit dem Supportcenter der NetPlans realisiert. Der zentrale Firewall-Service wird täglich gesichert, auf Konsistenz und Sicherheit geprüft. Die notwendigen Zertifikate im Bereich HTTPS muss der Kunden als Domaininhaber zur Verfügung stellen. Bevor der Produktivbetrieb des Service realisiert wird, ist seitens NetPlans eine Testphase anhand einer definierten Checkliste empfohlen. Die Checkliste kann gemeinsam mit NetPlans erarbeitet werden.

## 12 Managed Mail Security Service

Der Cloud-Dienst „Managed Mail Security“ sowie „Managed Mail Security für Office 365“ wird über eine mandantenfähige E-Mail-Firewall realisiert. Die Lizenzierung des Dienstes erfolgt pro Postfach. Die Konfiguration und Ersteinrichtung wird durch NetPlans übernommen. Hierbei werden die MX-Resource-Record-Einstellungen (Mail Exchange Resource Record) der Kundendomäne auf die öffentlichen A-Resource-Record-Einträge von NetPlans konfiguriert. Der Kunde hat über ein zentrales Web-Portal die Möglichkeit, die blockierten Nachrichten pro Mail-Domäne einzusehen, die Spam-Einstellungen zu definieren sowie eigenverantwortlich Black- und Whitelists zu pflegen. Zentrale Updates der Appliance sowie die laufende Überprüfung der E-Mail-Firewall werden durch NetPlans durchgeführt und sind im Preis inbegriffen. Die E-Mail-Firewall wird regelmäßig gesichert sowie auf Konsistenz und Sicherheit geprüft. Individuelle Anpassungen oder Änderungen an Mail-Domänen müssen gemeinsam mit dem Supportcenter der NetPlans realisiert werden und sind kostenpflichtig. Im Rahmen der Managed Mail Security lässt sich kostenneutral der Dienst für „Managed Sandboxing Security Service“ aktivieren. Der Cloud-Dienst „Managed Sandboxing Security Service“ wird zentral durch den Hersteller Barracuda Networks in einem Hochsicherheitsrechenzentrum in Frankfurt am Main bereitgestellt. Der Dienst bietet im Bereich AntiSpam weitergehende Funktionen wie beispielsweise Bulk E-Mail Protection, Typosquatting Protection oder Anti-Fraud- und Phishing-Schutz. Zusätzlich zum klassischen Antivirus-Scanning erfolgt ein ATD-Scanning (Advanced Threat Detection) von Dateianhängen in einer separaten, sicheren Cloud-Umgebung. Die Lizenzierung des Dienstes erfolgt pro Postfach und wird zentral durch NetPlans verwaltet. Die Konfiguration und Ersteinrichtung erfolgt über NetPlans. Zentrale Updates des Dienstes werden automatisiert durchgeführt und sind im Preis inbegriffen. Individuelle Anpassungen oder Änderungen müssen gemeinsam mit dem Supportcenter der NetPlans realisiert werden.

## 13 2-Faktor-Authentication Service

Der Cloud-Dienst „2-Faktor-Authentication Service“ wird über eine mandantenfähige Authentication Engin und einen NPS-Server bereitgestellt. Die Lizenzierung des Dienstes erfolgt pro User und registriertes Endgerät. Als Endgerät kann jedes gängige Smartphone kostenfrei durch die „MobilePass+“ App genutzt werden. Eine Möglichkeit ist die Installation auf einem Windows-Rechner. Wird ein Hardware-Token gewünscht muss dieser zusätzlich erworben und angebunden werden. Es können sämtliche Systeme mit dem Standard „RADIUS“ angebunden und zur Authentifizierung genutzt werden. Die Lösung stellt zwei unterschiedliche Möglichkeiten der Anbindung zur Verfügung.

### **13.01 Managed 2-Faktor-Authentication Service:**

Wird als Erweiterung eines bestehenden Cloud-Services (z.B. FMaaS) bereitgestellt. Im Falle eines Managed Services wird auch die 2-Faktor-Authentifizierung vollständig durch NetPlans verwaltet und der Kunde bekommt den Dienst in das CPSM-Self-Service-Portal integriert. Benutzer können sich mittels Web-Portal registrieren und die Anwendung nutzen. Ein administrativer Zugriff auf die zentralisierte 2-Faktor-Umgebung ist nicht möglich.

### **13.02 Dedicated 2-Faktor-Authentication Service:**

Wird als Erweiterung eines dedizierten Dienstes, der zwar in der NetPlans Business Cloud betrieben wird, aber als IaaS-Leistung mit administrativer Verantwortung dem Kunden obliegt, bereitgestellt. Wenn eine dedizierte Anbindung an eine eigenverwaltete Umgebung gebucht wird (IaaS), muss ein Software-Agent auf einem der Kundensysteme installiert und angebunden werden. Dieser Agent übernimmt dann die Kommunikation zum zentralen Backend. Hier ist ein administrativer Web-Zugriff zur Userverwaltung möglich.

Updates und Upgrades werden je nach Herstellerempfehlung und Erfahrung, im Ermessen der NetPlans, geplant und rechtzeitig angekündigt. Die Kompatibilität der Managed Services wird hier von NetPlans geleistet, die Agents die über IaaS-Leistungen bereitgestellt werden, müssen eigenverantwortlich durch den Kunden oder in Abstimmung durchgeführt werden.

## **14 Managed Client Service**

Der Cloud-Dienst „Managed Client Service“ wird über eine mandantenfähige Architektur zentral von NetPlans verwaltet und basiert auf Software des Hersteller baramundi. Die Lizenzierung des Dienstes erfolgt pro Device. Die Client Management Dienste erfordern die Installation eines Agenten auf dem zu verwaltenden Endgerät. Die Kommunikation erfolgt verschlüsselt über HTTPS (Port 443) über das Internet mit der NetPlans Business Cloud. Der Managed Client Service beinhaltet eine automatische Hardware- und Software Inventur, Installation und Aktualisierung der Software von folgenden Drittanbietern: HIER und von Windows Updates. Dabei wird regelmäßig die vordefinierte Software (Managed Software) auf Aktualisierungen geprüft. Bei Vorhandensein von aktualisierten Softwareversionen, werden diese auf den verwalteten Endgeräten installiert. Die Individualisierung der Installations-Jobs, sowie das Erstellen eigener Software-Pakete ist nicht im Preis inbegriffen, kann aber durch das Supportcenter der NetPlans realisiert werden. Ein administrativer Zugriff auf die zentralisierte Verwaltungsumgebung ist nicht möglich. Bei Bedarf können automatisierte Standard-Reports über die Inventarisierung der Client-Struktur dem Kunden zur Verfügung gestellt werden.

#### **14.01 AddOn: Client Vulnerability Scanner**

Der baramundi Vulnerability Scanner scannt wöchentlich die Clients im Unternehmen automatisiert auf bekannte und dokumentierte Schwachstellen wie Softwareschwachstellen, Fehlkonfigurationen und individuellen Schwachstellen, die von Angreifern ausgenutzt werden könnten. Der Schwachstellenscan nutzt dafür standardisierte Regelwerke, die von anerkannten Organisationen und Sicherheitsfirmen gepflegt werden. Die Auswertung des wöchentlichen Softwareschwachstellen-Scans (Report) wird dem Kunden per E-Mail zur Verfügung gestellt. Die Beseitigung von möglichen identifizierten Schwachstellen ist nicht im Service enthalten, kann aber durch das Supportcenter der NetPlans realisiert werden. Die Lizenzierung des Dienstes erfolgt pro Device und als optionales AddOn.

### **15 Managed AD-Sync Service**

Der Cloud-Dienst „Managed AD-Sync Service“ ist ein AddOn zu bestehenden Cloud-Services, für die ein Active Directory (AD) Userobjekt erforderlich ist. Die Lizenzierung erfolgt pro Windows-Domänenstruktur und ist damit unabhängig von der Anzahl an Benutzern oder Domaincontrollern. Der Service wird ausschließlich von Windows Active Directory Services unterstützt und dient zur Synchronisation von Benutzerobjekten und deren Kennwörtern. Damit ermöglicht der AD-Sync Service die Authentifizierung der User lokal und am Cloud-Service mit einheitlichen User-Credentials (Benutzer und Passwort). Die Synchronisation erfolgt unidirektional vom lokalen AD zum Service-AD in der NetPlans Business Cloud. Das lokale Active Directory (AD) ist dabei der Master und muss einem von Microsoft supporteten Betriebssystem unterliegen. Für den Betrieb wird ein Agent auf allen Domaincontrollern des Kunden installiert. Dieser verbindet sich via HTTPS mit dem zentralen Userportal (CPSM) in der NetPlans Business Cloud. Die Konfiguration und Ersteinrichtung erfolgt durch NetPlans. Individuelle Anpassungen oder Änderungen, müssen gemeinsam mit dem Supportcenter der NetPlans realisiert werden.

## II. NetPlans Managed Support Services

NetPlans erbringt für den Kunden, die im Angebot bzw. der Auftragsbestätigung aufgeführten Managed Support Services gemäß Leistungsbeschreibung.

Die IT-Supportabteilung bildet die Basis für die Erfüllung der kundenspezifischen Anforderungen unserer Managed Support Services. Mit qualifizierterem Fachpersonal erbringen wir für Kunden einen definierten Leistungsumfang unter Einhaltung der vereinbarten Reaktionszeiten. Neben einem Dispatcher- und Onboarding-Team ist die Abteilung in verschiedene Fachabteilungen unterteilt:

- Helpdesk-Team Application- & Desktop Virtualization
- Helpdesk-Team Managed Cloud Solutions
- Helpdesk-Team Virtualization & Infrastructure
- Helpdesk-Team Microsoft Technologies
- Helpdesk-Team DATEV Technologies
- Helpdesk-Team IT-Security

Die Bearbeitung von kundenspezifischen Incident-, Problem- und Change-Management Anfragen, erfolgt vorrangig über ein NetPlans Ticketsystem. Nach erfolgreicher Übermittlung der Kundenanfrage, erhalten die Kunden eine eindeutige Bearbeitungsnummer (Ticket-Nummer). Ein Zugriff auf das Ticketsystem durch den Kunden ist nicht möglich. Die Bearbeitung erfolgt innerhalb der Servicereichbarkeit (s.g. Service-Response-Level), die von Montag bis Freitag von 7.00 - 18.00 Uhr definiert ist. Grundsätzlich ist die Servicereichbarkeit an allen bundeseinheitlichen sowie den davon abweichenden gesetzlichen Feiertagen in denen die NetPlans Systemhausgruppe Standorte hat, ausgeschlossen, es sei denn, dass in der Auftragsbestätigung oder in einem individuell aufgesetzten Service-Level-Agreement eine andere Vereinbarung getroffen wurde oder ein Service-Response-Level 24x7 vorliegt. Stundensätze mit Kunden werden individuell vereinbart. Für Leistungen, die außerhalb der regulären Arbeitszeit (Mo – Fr von 7 Uhr bis 18 Uhr) erfolgen, gelten folgende Zuschläge auf den vereinbarten Stundensatz

- Werktags / Mo-Fr / 7-18 Uhr: (= regulärer Stundensatz)
- Abendzuschlag (18-22 Uhr): +25%
- Nacht- (22-7 Uhr), Samstagzuschlag: +50%
- Sonntagzuschlag: +100%
- gesetzliche Feiertage sowie am 31. Dezember ab 14 Uhr: +125%
- besondere Feiertage (24. Dezember ab 14 Uhr, 25. und 26. Dezember) und 1. Mai: +150%

## 01 Service-Response-Level

Die Managed Supportservices unterliegen den nachfolgenden Regelungen hinsichtlich Erreichbarkeit und Reaktionszeiten für kundenspezifische Incident-, Problem- und Change-Management Anfragen. Die Inanspruchnahme des Service-Response-Level für Managed Supportservices ist nicht Bestandteil des Standardleistungsumfangs und bedarf eines gesonderten, kostenpflichtigen Vertragsabschlusses durch den Kunden.

Die unterschiedlichen Prioritäten werden wie folgt definiert:

Priorität 1 „hoch“

- Wichtige Geschäftsprozesse können nicht durchgeführt werden.
- Eine große Anzahl von Mitarbeitern ist betroffen.

Priorität 2 „mittel“

- Wichtige Geschäftsprozesse sind beeinträchtigt bzw. können nur mit zusätzlichem Aufwand erfüllt werden.
- Es sind mehrere Mitarbeiter betroffen.

Priorität 3 „niedrig“

- Es sind keine wichtigen Geschäftsprozesse betroffen.
- Es sind nur einzelne Mitarbeiter bzw. eine minimale Anzahl von Mitarbeitern betroffen.
- Die Einschränkungen betreffen den Komfort.

Reaktionszeit gemäß Angebot bzw. Auftragsbestätigung:

Service-Response-Level Standard

- Priorität 1 Fälle: Reaktionszeit max. 8h
- Priorität 2 Fälle: Reaktionszeit max. 8h
- Priorität 3 Fälle: Reaktionszeit max. 8h

Service-Response-Level Advanced

- Priorität 1 Fälle: Reaktionszeit max. 4h
- Priorität 2 Fälle: Reaktionszeit max. 4h
- Priorität 3 Fälle: Reaktionszeit max. 8h

Service-Response-Level Premium

- Priorität 1 Fälle: Reaktionszeit max. 2h
- Priorität 2 Fälle: Reaktionszeit max. 4h
- Priorität 3 Fälle: Reaktionszeit max. 8h

Die resultierende Bearbeitung einer Incident-, Problem- und Change-Management Anfrage in Form einer Fernwartung oder eines vor Ort Termin liegt im Ermessen der NetPlans. Serviceeinsätze vor

Ort können in Einzelfällen (z.B. bei Störungen des Straßenverkehrs, bei schlechten Witterungsverhältnissen oder bei nicht an das Bundes- und Landesstraßennetz angeschlossenen Standorten) variieren.

### **01.01 Erweitertes Service-Response-Level**

Das NetPlans Service-Response-Level bietet für alle Kunden mit laufenden Verträgen zu unseren NetPlans Managed Support Services und unserer NetPlans Business Cloud eine erweiterte Erreichbarkeit für kundenspezifische Incident-, Problem- und Change-Management Anfragen, die ausschließlich den First-Level-Support betreffen, an Samstagen und Sonntagen von 7.00 - 17.00 Uhr (ausgenommen gesetzliche Feiertage in Baden-Württemberg).

### **01.02 Service-Response-Level 24x7**

Das NetPlans Service-Response-Level 24x7 bezeichnet eine Vereinbarung zwischen NetPlans und dem Kunden über erweiterte Erreichbarkeiten. Voraussetzung für den Service-Response-Level 24x7 bildet ein Service-Response-Level Advanced oder Premium. Außerhalb der Servicezeiten des Service-Response-Level Standard, Advanced oder Premium, steht dem Kunden eine Telefonbereitschaft an 365 Tagen im Jahr für Fälle mit ausschließlich Priorität 1 bei einer Reaktionszeit innerhalb von 2 Stunden zur Verfügung. Die Reaktionszeiten innerhalb der Servicezeiten des Service-Response-Level Standard, Advanced oder Premium finden unabhängig davon Anwendung. Bei Fällen mit Priorität 1 sind wichtige Geschäftsprozesse, die nicht durchgeführt werden können, sowie eine große Anzahl von Mitarbeitern betroffen. Es erfolgt kein Bereitschaftsdienst für planmäßige Systemupdates des Kunden.

Die Verwendung der 24x7-Supporthotline obliegt ausschließlich definierten Personenkreisen des Kunden. Die Annahme der telefonischen Störungsmeldungen erfolgt in erster Instanz durch Dritte (externe Firma), die die unmittelbare Kontaktaufnahme an die zuständige Person der NetPlans einleiten. NetPlans reagiert im Anschluss gemäß definierten Reaktionszeiten mit einem Rückruf. Ein Technikereinsatz erfolgt ausschließlich durch Fernwartung (Remote).

Der Kunde muss vor Vertragsbeginn die Systeme (u.a. virtuelle Maschinen) gemeinsam mit NetPlans benennen, die der zentralen 24x7 Rufbereitschaft unterstellt werden sollen. Die vorstehenden Verfügbarkeiten hinsichtlich Serviceerreichbarkeit und Reaktionszeit stehen unmittelbar in Abhängigkeit zu aktiven Serviceverträgen zwischen Kunde und dem Hersteller für Hardware und Software. D.h. Hardware und Software müssen mit entsprechenden Herstellersupport-Verträgen ausgestattet sein, welche die Verfügbarkeiten und Reaktionszeiten seitens der NetPlans gewährleisten können. Die notwendigen Voraussetzungen werden vor Vertragsbeginn seitens NetPlans geprüft und dokumentiert. Sollten die definierten Voraussetzungen seitens des Kunden nicht erfüllt sein, behält sich NetPlans vor, die Erfüllung des Vertrages bis zur Umsetzung der Voraussetzungen aufzuschieben oder den Vertragsschluss rückwirkend aufzulösen.

Der NetPlans Service-Response-Level (auch bei 24x7) beinhaltet keine inkludierten Dienstleistungsstunden und setzt ein Service-Response-Level Standard, Advanced oder Premium voraus. Anfallende Dienstleistung wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet.

## **02 Managed Monitoring**

Die NetPlans Managed Monitoring Services werden über ein mandantenfähiges Netzwerküberwachungs-Tool administriert und bereitgestellt. Der zentrale Überwachungsserver wird als Cloud-Dienst in der NetPlans Business Cloud betrieben. Ein sogenannter „Local Probe“ wird beim Kunden vor Ort installiert, der jeweils als Dienst auf einem beliebigen Windows-Rechner im Netzwerk initialisiert werden kann. Die Kommunikation zwischen dem zentralen Überwachungsserver und der „Local Probe“ ist verschlüsselt. Die Lizenzierung des Dienstes erfolgt pro Sensor. Derzeit werden etwa 10 Sensoren pro System (virtuell oder physikalisch) berechnet. Die tatsächlich benötigte Anzahl ergibt sich nach einer vorgelagerten IST-Analyse. Individuelle Anpassungen oder Änderungen müssen gemeinsam mit der IT-Supportabteilung der NetPlans realisiert werden. Anfallende Systemupdates und Überprüfungen des zentralen Überwachungsserver werden von NetPlans durchgeführt und sind im Preis inkludiert. Für sämtliche Cloud-Dienste gilt darüber hinaus das Service Level-Agreement der NetPlans Business Cloud, das Sie nachfolgend einsehen und herunterladen können: [www.netplans.de/sla](http://www.netplans.de/sla). Eine proaktive Reaktion per Telefon oder E-Mail erfolgt ausschließlich innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (ausgenommen gesetzliche Feiertage in Deutschland), definiert ist. Die NetPlans Managed Monitoring Services beinhalten keine inkludierten Dienstleistungsstunden. Bei Erkennung von systemkritischen Auffälligkeiten, übernimmt NetPlans das notwendige Eskalationsmanagement und tritt proaktiv mit dem Kunden in Kommunikation (Einleitung und Überwachung). Anfallende Dienstleistung wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet.

## **03 Managed Router Service**

Die NetPlans Managed Router Services basieren auf physikalischer Hardware, die zentral durch NetPlans mit Hilfe, der vom Hersteller LANCOM Systems GmbH bereitgestellten LANCOM Management Cloud, verwaltet und überwacht werden. Der Service wird über die LANCOM Management Cloud in einem in einen Hochsicherheitsrechenzentrum in Europa zur Verfügung gestellt und gewährleistet die zentrale Versorgung der Systeme mit Updates und Patches. NetPlans nimmt das System Vor-Ort in Betrieb und konfiguriert die Sicherheitsrichtlinien nach aktuellen Best-Practices (Erfolgsmethode). Es erfolgt mindestens ein Firmware-Update im Jahr. Sicherheitskritische Updates werden zusätzlich während einer nutzungsarmen Zeit (i.d.R. zwischen 22:00 und 06:00 Uhr) eingespielt. Bei der Router Hardware handelt es sich um ein Mietgerät mit einer Mindestvertragslaufzeit von 36 Monaten. Das Mietgerät wird dem Kunden zum Sachgerechten und pfleglichen Gebrauch überlassen. Mängel (unvollständiger Lieferumfang, Transportschäden, etc.) müssen vom Kunden unverzüglich der NetPlans gemeldet werden. Nach Ablauf der Vertragslaufzeit

ist der Kunde verpflichtet, dass Mietgerät betriebsbereit und mit allen Zubehörteilen, die zum Lieferumfang gehören, an die NetPlans zurückzugeben. Wird das Mietgerät nicht im zuvor gelieferten Zustand oder gar nicht zurückgegeben, so ist die NetPlans berechtigt, das Mietgerät in Rechnung zu stellen. Eine Weitergabe an Dritte ist nur mit ausdrücklicher Zustimmung der NetPlans zulässig. Sollten während der Vertragslaufzeit Hardwarefehler entstehen, so erhält der Kunde ein adäquates Ersatzgerät kostenneutral von NetPlans zur Verfügung gestellt. Der kostenneutrale Austausch bezieht sich ausschließlich auf die Hardware. Anfallende Dienstleistung für einen Austausch vor Ort wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet. Sollte die geplante Wartung und Instandhaltung der Systeme, eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (ausgenommen gesetzliche Feiertage in Deutschland) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt.

#### **04 Managed Firewall Service**

Die NetPlans Managed Firewall Services basieren auf physikalischer Firewall Hardware, die zentral durch NetPlans mit dem zentralen Control Center verwaltet und überwacht werden. Das Control Center gewährleistet die zentrale Versorgung der Systeme mit Updates und Patches und wird innerhalb der NetPlans Business Cloud bereitgestellt (für sämtliche Cloud-Dienste gilt darüber hinaus das Service Level-Agreement der NetPlans Business Cloud, das Sie nachfolgend einsehen und herunterladen können: [www.netplans.de/sla](http://www.netplans.de/sla)). NetPlans nimmt das System in Betrieb und konfiguriert die Sicherheitsrichtlinien nach aktuellen Best-Practises (Erfolgsmethode). Innerhalb der Vertragslaufzeit verweist NetPlans auf empfohlene und nötige Anpassungen hin und setzt diese nach Freigabe auch kostenpflichtig um. Bei der Firewall Hardware handelt es sich um ein Mietgerät mit einer Mindestvertragslaufzeit von 36 Monaten. Das Mietgerät wird dem Kunden zum Sachgerechten und pfleglichen Gebrauch überlassen. Mängel (unvollständiger Lieferumfang, Transportschäden, etc.) müssen vom Kunden unverzüglich der NetPlans gemeldet werden. Nach Ablauf der Vertragslaufzeit ist der Kunde verpflichtet, das Mietgerät betriebsbereit und mit allen Zubehörteilen, die zum Lieferumfang gehören, an die NetPlans zurückzugeben. Wird das Mietgerät nicht im zuvor gelieferten Zustand oder gar nicht zurückgegeben, so ist die NetPlans berechtigt, das Mietgerät in Rechnung zu stellen. Eine Weitergabe an Dritte ist nur mit ausdrücklicher Zustimmung der NetPlans zulässig. Sollten während der Vertragslaufzeit Hardwarefehler entstehen, so erhält der Kunde ein adäquates Ersatzgerät kostenneutral von NetPlans zur Verfügung gestellt. Der kostenneutrale Austausch bezieht sich ausschließlich auf die Hardware. Anfallende Dienstleistung für einen Austausch vor Ort wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet. Sollte die geplante Wartung und Instandhaltung der Systeme, eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (ausgenommen gesetzliche Feiertage in Deutschland) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt.

## 05 Remote Checkup-Services

Die NetPlans Remote Checkup-Services beinhalten pauschalisierte Leistungen für die Kontrolle und Überwachung von Kundensystemen gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung. Die dafür notwendigen Aufwendungen werden vor Vertragsschluss mit dem Kunden definiert und im Angebot bzw. der Auftragsbestätigung in den Leistungsumfang aufgenommen. Die Durchführung der Serviceleistung erfolgt durch einen qualifizierten System Engineer via Fernwartung über einen festen Prüfungsintervall, der definiert werden kann (wöchentlich, monatlich, vierteljährlich, halbjährlich oder jährlich). Falls nicht außerordentlich definiert, führt NetPlans die definierten Kontroll- und Überwachungsmaßnahmen mit festen Prüfungsintervall selbständig und eigenverantwortlich innerhalb der Servicezeiten, die von Montag bis Freitag von 7.00 - 18.00 Uhr (ausgenommen gesetzliche Feiertage in Deutschland) definiert ist, durch. Im Anschluss erfolgt ein Reporting per E-Mail über durchgeführte Arbeiten an den Kunden. Der Kunde muss vor Vertragsbeginn die Systeme (u.a. virtuelle Maschinen) gemeinsam mit NetPlans benennen, die den Remote Checkup-Services unterstellt werden sollen. Für die Erbringung der Remote Checkup-Services werden entsprechende Zugangsdaten für die Systeme benötigt (ggf. auch Administrationsrechte), die der Kunde NetPlans einräumen muss. Die notwendigen Voraussetzungen werden vor Vertragsbeginn seitens NetPlans geprüft und dokumentiert. Die NetPlans Remote Checkup-Services beinhalten keine Dienstleistung für die Wartung und Instandhaltung von Kundensystemen. Bei Erkennung von systemkritischen Auffälligkeiten, übernimmt NetPlans das notwendige Eskalationsmanagement und tritt proaktiv mit dem Kunden in Kommunikation (Einleitung und Überwachung). Anfallende Dienstleistung wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet.

## 06 Microsoft 365 - Security Check-Up

Der Microsoft 365 - Security Checkup beinhaltet pauschalisierte Leistungen für die Überprüfung von sicherheitsrelevanten Einstellungen der Microsoft/Office 365-Umgebung und fasst diese in einem Servicebericht gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung zusammen. Die Durchführung der Serviceleistung erfolgt durch einen qualifizierten System Engineer via Fernwartung über einen festen Prüfungsintervall. Falls nicht außerordentlich definiert, führt NetPlans die definierten Überprüfungsmaßnahmen mit festen Prüfungsintervall selbständig und aufgrund betriebsinterner Verfahren unter Ausschluss des Auftraggebers, innerhalb der Servicezeiten durch. Der Servicebericht enthält konkrete Maßnahmen als Handlungsempfehlung zur Reduzierung von identifizierten Risiken aus mehreren Teilbereichen (wie Microsoft/Office-365-Umgebung, Azure AD, Azure AD Connect, MFA, Teams etc.). Der Umfang der pauschalisierten Leistungen für die Überprüfung von sicherheitsrelevanten Einstellungen obliegt NetPlans. Eine Erweiterung des Leistungsumfang kann vor Vertragsbeginn seitens NetPlans geprüft und freigegeben werden. Für die Erbringung des Microsoft 365 - Security Checkup werden entsprechende Zugangsdaten benötigt (globaler Administrator), die der Kunde NetPlans einräumen muss. NetPlans kann trotz großer Sorgfalt bei der Zusammenstellung des Serviceberichts nicht die Vollständigkeit der identifizierten Risiken garantieren. Die enthaltenen Angaben können jederzeit ohne vorherige

Ankündigung (z.B. durch technische Anpassungen seitens des Herstellers) verändern werden. Der Microsoft 365 Security Checkup beinhaltet keine Dienstleistung für die Behebung der identifizierten Risiken der Microsoft/Office 365 Umgebung oder weitere Beratungsleistungen. Der Servicebericht stellt die notwendigen Maßnahmen als Handlungsempfehlung zusammen und NetPlans tritt proaktiv mit dem Kunden in Kommunikation). Die notwendige Dienstleistung für Behebung der identifizierten Risiken wird nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet. Einige Empfehlungen können auch eine kostenpflichtige Lizenz als Voraussetzung beinhalten.

## **07 Managed Maintenance-Services**

Die NetPlans Managed Maintenance-Services beinhalten pauschalisierte Leistungen für die Wartung und Instandhaltung von Kundensystemen gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung. Die Durchführung der Serviceleistung erfolgt durch einen qualifizierten System Engineer via Fernwartung oder als vor Ort Termin innerhalb der NetPlans IT-Supportabteilung bzw. der entsprechenden NetPlans Fachabteilung. Die Wahl (Fernwartung oder vor Ort) liegt im Ermessen der NetPlans. Bei Wahl eines Termins zur Umsetzung vor Ort, werden die Kosten für An- und Abfahrt separat berechnet. Dabei erfolgt die Berechnung nach tatsächlichem Zeitaufwand (= Fahrzeit) für die einfache Wegstrecke gemäß regulärem Stundensatz. Die Umsetzung erfolgt über einen festen Regeltermin, der gemäß Leistungsumfang im Angebot bzw. der Auftragsbestätigung, auf monatlich, vierteljährlich, halbjährlich oder jährlich festgelegt wird. Die Terminvereinbarung erfolgt proaktiv durch NetPlans und unter Abstimmung mit dem Kunden. Sollte die geplante Wartung und Instandhaltung der Systeme, eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (Feiertage ausgeschlossen) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt.

## **08 Managed Backup-Restore-Services**

Die NetPlans Managed Backup-Restore-Services beinhaltet eine pauschalisierte Leistung für die vierteljährliche Überprüfung der Datensicherung anhand einer manuellen Simulation der Wiederherstellbarkeit gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung durch einen qualifizierten System Engineer via Fernwartung. Die Definition von bis zu fünf kritischen virtuellen Maschinen, die innerhalb des vierteljährlichen Zyklus getestet werden sollen, erfolgt vor Vertragsbeginn gemeinsam mit dem Kunden. Eine Überprüfung der Datensicherung und dessen Wiederherstellbarkeit erfolgt anhand von sichtbaren Kontrollmechanismen. Durch den Einsatz von Dritthersteller-Software, sowie durch anwendungsspezifische Gegebenheiten, kann die Lauffähigkeit der Datensicherung seitens der NetPlans nicht garantiert werden. Der Kunde muss vor Vertragsbeginn die Systeme (u.a. virtuelle Maschinen) benennen, die eine applikationskonsistente Datensicherungen außerhalb der Microsoft VSS-Technologie (Volume Shadow Copy Service) benötigen und ein Funktionstest im Bereich Applikation-Aware-Backup (z.B.

Wiederherstellung einzelner E-Mails) voraussetzt. Sollte die geplante Überprüfung der Datensicherung eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (Feiertage ausgeschlossen) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt. Der Einsatz von VEEAM Backup & Replication Software oder Rubrik Backup-Software/Appliance für die Datensicherung, der Einsatz eines geeigneten Backup-to-Disk Systems, sowie freie Kapazitäten innerhalb der Virtualisierungsumgebung (Rechenleistung), werden für die Wiederherstellung der Backups und damit für die Erfüllung des NetPlans Managed Backup-Restore-Services vorausgesetzt. Die notwendigen Voraussetzungen werden vor Vertragsbeginn seitens NetPlans geprüft und dokumentiert. Sollten die definierten Voraussetzungen seitens des Kunden nicht erfüllt sein, behält sich NetPlans vor, die Erfüllung des Vertrages bis zur Umsetzung der Voraussetzungen aufzuschieben oder den Vertragsschluss rückwirkend aufzulösen.

## **09 Managed Windows Server Updates**

Der Cloud-Dienst „Managed Windows Server Update Service“ wird zentral durch NetPlans über eine mandantenfähige Architektur verwaltet und basiert auf der Update-Management-Plattform des Herstellers Baramundi. Die Lizenzierung des Services erfolgt paketweise in Einheiten zu jeweils 10 Servern.

Zur Nutzung des Dienstes ist die Installation eines Agenten auf den zu verwaltenden Servern erforderlich. Die Kommunikation mit der NetPlans Business Cloud erfolgt ausschließlich verschlüsselt über das Internet (HTTPS, Port 443). Für die einmalige Registrierung des Agenten muss zusätzlich der Port 8443, der ebenfalls verschlüsselt kommuniziert, geöffnet sein. Der Leistungsumfang des „Managed Windows Server Update Service“ umfasst die automatisierte Installation von Windows Updates sowie sicherheitsrelevanten Updates für SQL-Server, sofern diese über die Windows Update-Funktion bereitgestellt werden. Auf Wunsch können bestimmte Updates, insbesondere für SQL Server, vom Installationsprozess ausgeschlossen werden (Opt-Out). Der Service wird ausschließlich auf unterstützten Serverbetriebssystemen erbracht. Im Rahmen des Dienstes erfolgt eine regelmäßige Überprüfung auf verfügbare sicherheitsrelevante und empfohlene Windows Updates. Diese werden nach Ablauf einer definierten Wartezeit automatisiert installiert. Zusätzlich beinhaltet der Service die Durchführung einer Hardware- und Software-Inventarisierung der angebotenen Server. Folgende Leistungen sind ausdrücklich nicht Bestandteil des „Managed Windows Server Update Service“:

- Die Installation von Updates für Software von Drittanbietern (z. B. Java, Adobe, weitere SQL-Server-Editionen, Druckertreiber etc.)
- Manuelle Eingriffe nach der Update-Installation (z. B. individuelle Neustarts, Fehleranalysen)
- Benutzergesteuerte oder benutzerinitiierte Update-Prozesse
- Administrativer Zugriff des Kunden auf die zentrale Verwaltungsplattform

Die Steuerung und Durchführung der Updates erfolgt vollständig durch NetPlans gemäß der im Service hinterlegten und mit dem Kunden abgestimmten Zeitpläne und Konfigurationsrichtlinien.

### **08.01 AddOn: Server Vulnerability Scanner**

Der baramundi Vulnerability Scanner scannt die Server im Unternehmen wöchentlich automatisiert auf bekannte und dokumentierte Schwachstellen wie Softwareschwachstellen, Fehlkonfigurationen und individuellen Schwachstellen, die von Angreifern ausgenutzt werden könnten. Der Schwachstellenscan nutzt dafür standardisierte Regelwerke, die von anerkannten Organisationen und Sicherheitsfirmen gepflegt werden. Die Auswertung des wöchentlichen Softwareschwachstellen-Scans (Report) wird dem Kunden per E-Mail zur Verfügung gestellt. Die Beseitigung von möglichen identifizierten Schwachstellen ist nicht im Service enthalten, kann aber durch das Supportcenter der NetPlans realisiert werden. Die Lizenzierung des Dienstes erfolgt für je zehn Server (10er Pack) und als optionales AddOn.

## **10 Managed Microsoft SQL Service**

Der NetPlans Managed SQL Service umfasst die Wartung und Instandhaltung einer Microsoft SQL-Instanz gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung. Die Lizenzierung des Dienstes erfolgt je SQL-Instanz, eine Erweiterung ist pro Instanz kostenpflichtig möglich. Die Durchführung der Serviceleistung erfolgt durch einen qualifizierten System Engineer via Fernwartung oder als vor Ort Termin innerhalb der NetPlans IT-Supportabteilung bzw. der entsprechenden NetPlans Fachabteilung. Die Wahl (Fernwartung oder vor Ort) liegt im Ermessen der NetPlans. Bei Wahl eines Termins zur Umsetzung vor Ort, werden die Kosten für An- und Abfahrt separat berechnet. Dabei erfolgt die Berechnung nach tatsächlichem Zeitaufwand (= Fahrzeit) für die einfache Wegstrecke gemäß regulärem Stundensatz. Die Umsetzung erfolgt über einen festen Regeltermin, der gemäß Leistungsumfang im Angebot bzw. der Auftragsbestätigung, auf vierteljährlich festgelegt ist. Die Terminvereinbarung erfolgt proaktiv durch NetPlans und unter Abstimmung mit dem Kunden. Sollte die geplante Wartung und Instandhaltung der Systeme, eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (Feiertage ausgeschlossen) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt. Darüber hinaus erfolgt im Rahmen der o.g. Servicezeit ein softwaregestütztes Monitoring der SQL-Instanz für betriebskritische Parameter und eine Wiederherstellung der Datenbank aus dem Backup inklusive Funktionstest. Sofern es sich um eine ausfallsichere Installation (HA; Hochverfügbarkeitsinstallation) handelt, erfolgt auf Wunsch ein Hochverfügbarkeitstest (Simulation eines Ausfalls) Eine Überprüfung der Datensicherung und dessen Wiederherstellbarkeit erfolgt anhand von sichtbaren Kontrollmechanismen. Durch den Einsatz von Dritthersteller-Software, sowie durch anwendungsspezifische Gegebenheiten, kann die Lauffähigkeit der Datensicherung seitens der NetPlans nicht garantiert werden. Der Servicebericht dokumentiert die Wartung und Instandhaltung und stellt bei Bedarf notwendigen Maßnahmen als Handlungsempfehlung zusammen. NetPlans tritt in diesem Fall proaktiv mit dem Kunden in Kommunikation. Die mögliche Dienstleistung für

Behebung der identifizierten Risiken wird nach tatsächlichem Aufwand und Zeitznachweis gemäß regulärem Stundensatz berechnet. Der Einsatz von VEEAM Backup & Replication Software für die Datensicherung, der Einsatz eines geeigneten Backup-to-Disk Systems sowie freie Kapazitäten innerhalb der Virtualisierungsumgebung (Rechenleistung), werden für die Wiederherstellung der Datenbank aus dem Backup vorausgesetzt. Die Verfügbarkeit der kostenfreien Software „Microsoft SQL Management Studio“ ist für den gesamten Service eine Voraussetzung. Die notwendigen Voraussetzungen sowie der detaillierte Leistungsumfang, darunter auch Details zum Funktionstest im Zuge einer Wiederherstellung der Datenbank aus dem Backup werden, vor Vertragsbeginn seitens NetPlans geprüft und dokumentiert (darunter auch die vorhandene Lizenzierung der Microsoft SQL Edition). Sollten die definierten Voraussetzungen seitens des Kunden nicht erfüllt sein, behält sich NetPlans vor, die Erfüllung des Vertrages bis zur Umsetzung der Voraussetzungen aufzuschieben oder den Vertragsschluss rückwirkend aufzulösen.

## **11 Managed Fortinet Service**

Die NetPlans Managed Fortinet Services basieren auf bestehender Firewall Hardware, die zentral durch NetPlans mit dem zentralen FortiManager verwaltet und mit dem FortiAnalyzer überwacht werden. Der FortiManager bietet ein zentralisiertes Management der Firewall, Best-Practice Compliance und Möglichkeiten zur Workflow-Automatisierung, um einen besseren Schutz vor Sicherheitsverletzungen zu bieten. Die Verwaltung-Konsole wird in der NetPlans Business Cloud betrieben (für sämtliche Cloud-Dienste gilt darüber hinaus das Service Level-Agreement der NetPlans Business Cloud, das Sie nachfolgend einsehen und herunterladen können: [www.netplans.de/sla](http://www.netplans.de/sla)). Zusätzlich werden über den FortiAnalyzer System- und Eventlogs analysiert und in ein interpretierbares monatliches Reporting überführt. Pro Firewall Appliance ist das Logvolumen pro Tag und das bereitgestellte Volumen des Logspeichers begrenzt. Die beinhalteten Volumina entnehmen Sie bitte dem Angebot/der Auftragsbestätigung. Innerhalb der Vertragslaufzeit verweist NetPlans auf empfohlene und nötige Anpassungen hin und setzt diese nach Freigabe auch kostenpflichtig um. Sollte die geplante Wartung und Instandhaltung der Systeme, eine Downtime (= Zeit, in der ein System gewartet oder gestört wird und somit nicht verfügbar ist) benötigen, werden die Regeltermine nach Möglichkeit in nutzungsarmen Zeiten, jedoch innerhalb der Servicezeit, die von Montag bis Freitag von 7.00 - 18.00 Uhr (Feiertage ausgeschlossen) definiert ist und in vorheriger Absprache mit dem Kunden, durchgeführt.

## **12 Managed Client M365 Service**

Der Cloud-Dienst „Managed Client M365 Service“ wird über eine mandantenfähige Architektur für kundeneigene Microsoft Configuration Manager und Microsoft Intune Umgebungen zentral von NetPlans verwaltet. Diese Architektur greift unmittelbar auf die kundeneigene Microsoft Intune Umgebungen zu und ermöglicht die Vererbung von Richtlinien und Einstellungen, die zentral durch NetPlans verwaltet werden. Dabei finden NetPlans Best Practices hinsichtlich Compliance, Update Management, Konfigurationsprofile sowie optional Vorlagen für Conditional Access und EndPoint Security (auf Basis von Windows Defender) Anwendung, die einer kontinuierlichen Überwachung

gemäß definiertem Sicherheitsstandard (Compliance und Security) unterliegen. Bei Abweichungen und Auffälligkeiten, tritt NetPlans proaktiv mit entsprechenden Handlungsempfehlungen in Kontakt. Die resultierenden Aufwände zum Wiederherstellen des definierten Sicherheitsstandards sind nicht im Preis inbegriffen, können jedoch durch das Supportcenter der NetPlans separat realisiert werden. Die Lizenzierung des Dienstes erfolgt pro User und setzt die Lizenzierung dieses Users mit der Microsoft Business Premium oder Microsoft 365 E3 voraus. Der Managed Client M365 Service beinhaltet die automatische Hardware- und Software Inventur, Installation und Aktualisierung der Software von folgenden Drittanbietern: hier und von Windows Updates. Dabei wird regelmäßig die vordefinierte Software (Managed Software) auf Aktualisierungen geprüft. Bei Vorhandensein von aktualisierten Softwareversionen, werden diese auf den verwalteten Endgeräten installiert. Die Individualisierung der Installations-Jobs, sowie das Erstellen eigener Software-Pakete ist nicht im Preis inbegriffen, kann aber durch das Supportcenter der NetPlans realisiert werden. Ein administrativer Zugriff auf die zentralisierte Verwaltungsumgebung ist nicht möglich.

## **13 Managed Servicekontingent**

Das NetPlans Managed Servicekontingent definiert eine Anzahl an Servicestunden gemäß Leistungsbeschreibung im Angebot bzw. der Auftragsbestätigung, die innerhalb eines entsprechenden Monats dem Kunden auf Abruf zur Verfügung stehen. Die Durchführung der Serviceleistung erfolgt durch einen qualifizierten System Engineer innerhalb der NetPlans IT-Supportabteilung bzw. der entsprechenden NetPlans Fachabteilung via Fernwartung oder als vor Ort Termin. Für Termine zur Umsetzung vor Ort, werden die Kosten für An- und Abfahrt separat berechnet. Dabei erfolgt die Berechnung nach tatsächlichem Zeitaufwand (= Fahrzeit) für die einfache Wegstrecke gemäß regulärem Stundensatz. Die Fakturierung der im Angebot bzw. der Auftragsbestätigung definierten Servicestunden erfolgt vorschüssig pro Monat. Eine Reduzierung der Servicestunden im Servicekontingent ist innerhalb der Vertragslaufzeit nicht möglich. Eine Erhöhung des Servicekontingent ist jeweils zum Folgemonat möglich. Nicht benötigte Servicestunden verfallen nach Ablauf des Monats, es sei denn, dass in der Auftragsbestätigung eine andere Vereinbarung getroffen wurde. Bei vollständiger Überbuchung des Servicekontingent, werden anfallende Dienstleistungen nach tatsächlichem Aufwand und Zeitnachweis gemäß regulärem Stundensatz berechnet.

### **12.01 Servicekontingent Ticket**

Der Technikereinsatz erfolgt i.d.R. Remote (Fernwartung). Ein Servicekontingent Ticket dient als Kontingent für das NetPlans Ticketsystem zur Bewältigung von kundenspezifischen Incident-, Problem- und Change-Management Anfragen innerhalb des 1st, 2nd & 3rd Level Support. Weitere Anwendungsfälle sind nach Rücksprache möglich.

## 12.02 Servicekontingent für Regeltermine

Der Technikereinsatz erfolgt i.d.R. vor Ort. Es dient als Kontingent für Regeltermine, die nach Rücksprache mit dem Kunden in einem festen und planbaren Intervall, z.B. für die Bearbeitung einer ToDo-Liste, die Überbrückung geplanter personeller Engpässe (z.B. Urlaubs-/Krankheitszeiten) etc. Anwendung findet. Weitere Anwendungsfälle sind nach Rücksprache möglich.

## 14 NetPlans Hardwareverfügbarkeit

Der NetPlans Hardwareverfügbarkeits-Service basiert auf der Bereitstellung eines dedizierten Leihservers auf Mietbasis und ist ausschließlich für den Einsatz in Virtualisierungsumgebungen mit VMware vSphere oder Microsoft Hyper-V ausgelegt. Das Gerät wird als Leihserver dauerhaft bei NetPlans bereitgehalten und im Bedarfsfall innerhalb definierter Anwendungsszenarien an den Kunden ausgeliefert. Die Anforderung zur Auslieferung eines Leihservers erfolgt in enger Abstimmung zwischen dem Kunden und dem NetPlans IT-Support. Der Eingang eines Support-Tickets allein, stellt nicht den Beginn der Auslieferungsfrist von 4 Stunden dar. Maßgeblich ist die zuvor erfolgte Abstimmung mit dem Kunden und dem NetPlans IT-Support. Die Bereitstellung erfolgt ausschließlich im vertraglich vereinbarten Rahmen und ist auf Werktage (Montag bis Freitag) zwischen 8:00 und 17:00 Uhr beschränkt. Sobald eine qualifizierte Fehlermeldung beim NetPlans Service eingeht, wird ein Leihserver innerhalb von 4 Stunden ausgeliefert. Geht die Meldung vor 13:00 Uhr ein, erfolgt die Lieferung noch am selben Tag. Erfolgt die Meldung nach 13:00 Uhr, wird der Server am darauffolgenden Werktag bereitgestellt. Die genannten Reaktionszeiten sind Richtwerte. Abweichungen können in Ausnahmefällen bei starkem Verkehrsaufkommen, ungünstigen Witterungsbedingungen oder schwer erreichbaren Standorten begründet sein. An gesetzlichen Feiertagen im Bundesland Baden-Württemberg findet keine Auslieferung statt.

Die von NetPlans bereitgestellte Hardware erfüllt mindestens folgende technische Anforderungen: Sie ist mit zwei 8-Core-Prozessoren, 512 Gigabyte Arbeitsspeicher, sechs Gigabit-Netzwerkanschlüssen, zwei 10G SFP+ Netzwerkports, 15 Terabyte performanter Nettospeicherkapazität sowie redundanten High-Efficiency-Netzteilen ausgestattet. Die monatliche Pauschale umfasst ausschließlich die Vorhaltung und die logistische Auslieferung des Ersatzservers. Leistungen wie die Konfiguration des Ersatzsystems, die Wiederherstellung von Daten oder die Integration in die bestehende IT-Umgebung des Kunden sind nicht Bestandteil der monatlichen Pauschale. Sie werden im Bedarfsfall gesondert nach tatsächlichem Aufwand auf Basis des jeweils gültigen Stundensatzes abgerechnet. Für jeden Tag, an dem der Ersatzserver im Einsatz ist, fällt zusätzlich zur monatlichen Pauschale eine Nutzungsgebühr in Höhe von 70,00 Euro netto pro Kalendertag an. Der bereitgestellte Server kann in folgenden Szenarien zum Einsatz kommen:

1. Nutzung im Notfall als temporäre Failover-Lösung, etwa nach einem Ransomware-Angriff oder bei einem schwerwiegenden Hardwaredefekt

2. Geplante Durchführung von Wiederherstellungstests (Restore-Tests) vor Ort in der Kundenumgebung, optional in Kombination mit dem separat verfügbaren NetPlans Managed Restore Service

Bei der Durchführung von Restore-Tests vor Ort (Szenario 2) obliegt es dem Kunden, die technische Kompatibilität mit seiner bestehenden IT-Umgebung während der Vertragslaufzeit sicherzustellen. Dies schließt insbesondere die Verantwortung für aktuelle Softwarestände, Sicherheitsupdates und Firmwareversionen ein. Seitens NetPlans werden die Softwarestände, Sicherheitsupdates und Firmwareversionen auf dem neuesten Stand gehalten und basieren in der Regel auf dem aktuellsten Major-Release des Herstellers. Der Notbetrieb im Rahmen eines Failover-Szenarios erfolgt auf Grundlage der definierten technischen Mindestanforderungen des zur Verfügung gestellten Leihserver. Im tatsächlichen Einsatzfall wird das Mietgerät dem Kunden zum sachgerechten und pfleglichen Gebrauch überlassen. Mängel wie beispielsweise ein unvollständiger Lieferumfang oder Transportschäden sind NetPlans unverzüglich nach Erhalt zu melden. Nach Abschluss des Einsatzes ist der Kunde verpflichtet, das Gerät in betriebsbereitem Zustand und vollständig mit sämtlichem Zubehör an NetPlans zurückzugeben. Erfolgt die Rückgabe nicht oder nicht im ursprünglich gelieferten Zustand, ist NetPlans berechtigt, den Wiederbeschaffungswert oder die notwendigen Instandsetzungskosten in Rechnung zu stellen. Eine Weitergabe des Geräts an Dritte ist nur nach vorheriger schriftlicher Zustimmung durch NetPlans zulässig. Die maximale Leihdauer des Ersatzservers wird durch NetPlans festgelegt und richtet sich nach der jeweiligen Störungslage, dem Reparaturfortschritt sowie den verfügbaren Kapazitäten. NetPlans behält sich das Recht vor, den Leihserver jederzeit zurückzufordern oder die Leihdauer anzupassen, sofern dies technisch oder organisatorisch erforderlich ist.

## **15 NetPlans Managed Endpoint Service mit NinjaOne**

NetPlans stellt dem Kunden einen direkten und sicheren Fernzugriff auf Endgeräte (Windows, macOS, Linux) über verschlüsselte Verbindungen zur Verfügung. Eine zusätzliche VPN-Verbindung oder der Einsatz weiterer Drittsoftware ist nicht erforderlich. Der Dienst ermöglicht einen effizienten Support sowie Wartungsarbeiten an Windows-, macOS- und Linux-Endgeräten. NinjaOne ist ein Cloudservice außerhalb der Business Cloud, der auf der Infrastruktur externer Cloudanbieter betrieben wird. Die Serverstandorte für Kunden aus der Europäischen Union befinden sich innerhalb der EU. Weitere Informationen finden Sie auf der Herstellerseite <https://www.ninjaone.com>. Alle Sitzungen erfolgen über TLS-gesicherte Verbindungen. Ein unbeaufsichtigter Zugriff ist möglich, sofern dieser autorisiert ist. Der Zugriff ist rollenbasiert geregelt und ausschließlich für autorisierte Techniker gemäß der definierten Berechtigungen zulässig. Jede Fernzugriffssitzung wird mit Zeitstempel und Benutzer-ID dokumentiert. Der Dienst umfasst die zentrale Inventarisierung aller Geräte, auf denen ein NinjaOne Agent installiert ist. Hardware- und Softwareinformationen werden regelmäßig aktualisiert und stellen Transparenz

über Bestände und Konfigurationen her. Bei Bedarf können automatisierte Standard-Reports über die Inventarisierung der Client-Struktur zur Verfügung gestellt werden.

### **15.01 AddOn: NetPlans Managed Client Service mit NinjaOne**

Die Lizenzierung des Dienstes erfolgt pro Gerät. Der Managed Client Service umfasst die automatisierte Installation und Aktualisierung von Microsoft Windows Updates. Hierzu werden regelmäßig verfügbare Updates geprüft. Die Genehmigung der zu verteilenden Updates erfolgt vorab abhängig von Kritikalität und Kategorisierung.

Darüber hinaus beinhaltet der Managed Client Service die Installation und Aktualisierung von Software aus folgenden Drittanbieterquellen:

- <https://www.ninjaone.com/wp-content/uploads/2023/01/Windows-3rd-Party-Patching-List-NinjaOne-EN-120922.pdf>
- <https://github.com/microsoft/winget-pkgs/tree/master/manifests/>

Die vordefinierte Software wird regelmäßig auf Aktualisierungen geprüft. Sofern aktualisierte Versionen verfügbar sind, werden diese nach einem zuvor mit dem Kunden definierten Zeitplan auf den verwalteten Endgeräten installiert. Die Individualisierung von Installations-Jobs sowie das Erstellen eigener Software-Pakete ist nicht Bestandteil des Leistungsumfangs, kann jedoch durch das Supportcenter der NetPlans gegen Aufwand realisiert werden. Die Bereitstellung und Installation von Software erfolgt über die Funktionen der NinjaOne-Plattform. Softwarepakete werden nicht durch NetPlans erstellt oder gepflegt, sondern stammen aus den offiziellen Repositories des Herstellers NinjaOne sowie aus dem Microsoft Winget Repository. NetPlans übernimmt keine Gewährleistung für die Vollständigkeit, Aktualität oder Sicherheit der bereitgestellten Pakete. Die Verantwortung für die Lizenzierung sowie die rechtmäßige Nutzung der installierten Software liegt beim Kunden. Die Bereitstellung von Windows- und Software-Updates erfolgt vollständig automatisiert über die Plattform NinjaOne. Eine manuelle Kontrolle oder Verifizierung der erfolgreichen Installation ist nicht Bestandteil des Leistungsumfangs.

### **15.02 AddOn: NetPlans Managed Windows Server Updates mit NinjaOne**

Die Lizenzierung des Services erfolgt pro Server. Der Leistungsumfang des Managed Windows Server Updates Service umfasst die automatisierte Installation und Aktualisierung von Windows Updates. Im Rahmen des Dienstes erfolgt eine regelmäßige Überprüfung auf verfügbare sicherheitsrelevante sowie empfohlene Updates. Diese werden vorab abhängig von Kritikalität und Kategorisierung genehmigt und nach Ablauf einer definierten Wartezeit automatisiert installiert.

Nicht Bestandteil des Managed Windows Server Updates Service mit NinjaOne sind insbesondere:

- Updates für Software von Drittanbietern (z. B. Java, Adobe, SQL-Server-Editionen, Druckertreiber)
- manuelle Eingriffe nach der Update-Installation (z. B. individuelle Neustarts, Fehleranalysen)
- benutzergesteuerte oder benutzerinitiierte Update-Prozesse

Die Steuerung und Durchführung der Updates erfolgt vollständig durch NetPlans gemäß den im Service hinterlegten und mit dem Kunden abgestimmten Zeitplänen sowie Konfigurationsrichtlinien.

## **16 Scality ARTESCA MSP License**

Die Bereitstellung der Scality ARTESCA Software erfolgt durch NetPlans im Rahmen des Scality Cloud & Service Provider Program (SCSP), in dem NetPlans als autorisierter Managed Service Provider vertraglich mit dem Hersteller eingebunden ist. Die Lizenzierung erfolgt nicht durch Verkauf, sondern im Wege einer zeitlich befristeten und verbrauchsabhängigen Nutzungsüberlassung im Pay-as-you-Go-Modell. Die Abrechnung basiert auf der monatlich gemeldeten tatsächlich genutzten „usable storage capacity“. Die Lizenz bleibt Bestandteil des SCSP-Programms und wird durch NetPlans vermietet. Die Nutzung ist ausschließlich im vereinbarten Umfang und gemäß den jeweils gültigen Herstellerbedingungen zulässig. Nicht autorisierte Vervielfältigung, Modifikation oder Reverse Engineering sind ausgeschlossen. Die monatliche Verbrauchsmeldung gegenüber dem Hersteller erfolgt durch NetPlans entsprechend den vertraglichen Reportingpflichten. Supportleistungen des Herstellers werden im SCSP-Modell ausschließlich gegenüber NetPlans erbracht. Die Betreuung des Endkunden erfolgt durch NetPlans. Mit Beendigung des zugrunde liegenden Servicevertrages endet automatisch auch das Nutzungsrecht an der Software. NetPlans behält sich das Recht vor, diese Lizenz- und Nutzungsbestimmungen anzupassen, sofern sich die zugrunde liegenden Herstellerbedingungen, Programmrichtlinien oder vertraglichen Vorgaben ändern. In diesem Fall gelten die jeweils aktualisierten Bedingungen.

### III. DATEV PARTNERasp

NetPlans stellt, als qualifizierter und zertifizierter DATEV-System-Partner, dem Kunden, im Rahmen des DATEV PARTNERasp, flexible virtualisierte Services und Infrastruktur auf nicht für diese ausschließlich nutzbaren Server, Storage-Devices und Netzwerken im Rechenzentrum der DATEV zur Verfügung. Mit PARTNERasp lagern Sie Ihr IT-System und Ihre Daten in die zertifizierte DATEV-Cloud aus.

#### 01 Full Managed as a Service (FMaaS) DATEV PARTNERasp

Der Cloud-Dienst Full Managed as a Service DATEV PARTNERasp basiert auf einer mandantenfähigen Microsoft Active Directory-Umgebung sowie einer mandantenfähigen Citrix-Verwaltung. Diese dient der Bereitstellung virtueller Arbeitsplätze für die Mitarbeiter über eine kundenspezifische Citrix Apps und Desktop-Umgebung (Terminalserver). Die Abrechnung erfolgt benutzerbasiert, also pro Mitarbeiter. Für die Nutzung ist eine ergänzende Infrastruktur erforderlich, die sich nach der Anzahl der Nutzer richtet. Bei kleinen Umgebungen mit bis zu sieben Anwendern wird eine All-in-One-Lösung eingesetzt, bestehend aus einem einzelnen Citrix Apps und Desktop Server (auf Basis eines Terminalservers) inklusive der Installation der DATEV-Software. Diese Konfiguration wird innerhalb des mandantenfähigen Microsoft Active Directory bereitgestellt. Die maximale Auslegung dieser Lösung beträgt sieben Benutzer. Für größere Umgebungen ab acht Nutzern kommen ein dedizierter Citrix Apps und Desktop Server sowie ein zusätzlicher, kundenspezifischer DATEV-Server zum Einsatz. Beide Systeme werden ebenfalls innerhalb des mandantenfähigen Active Directory betrieben. Die Anzahl der benötigten Terminalserver richtet sich individuell nach der Benutzeranzahl und Auslastung, wobei üblicherweise mit sieben bis zehn Benutzern pro Server kalkuliert wird. Eine automatische Skalierung erfolgt nicht. Der Dienst erlaubt ausschließlich lokale Administrationsrechte auf dem Business App Server. Für alle innerhalb dieses Servers installierten Anwendungen, einschließlich deren Pflege und Wartung, ist der Kunde eigenverantwortlich. Auf Wunsch kann NetPlans – nach vorheriger Abstimmung – diese Aufgaben übernehmen, insbesondere die Wartung der DATEV-Software. Hierfür steht ein optional buchbarer DATEV Maintenance Service zur Verfügung, der ausdrücklich empfohlen wird. NetPlans ist in diesem Zusammenhang als zertifizierter DATEV-Systempartner tätig. Über PARTNERasp stehen zusätzlich auch Dienste aus dem DATEVnet zur Verfügung, wie beispielsweise die DATEV E-Mail-Verschlüsselung. Alle Infrastrukturen beinhalten einen hochverfügbaren DFS-FileServer-Speicher, der zur Ablage von Benutzerprofilen sowie individuellen Kundendaten genutzt wird. Der Speicher kann kostenpflichtig in Einheiten von jeweils einem Gigabyte erweitert werden. Bei Erreichen eines festgelegten Schwellwertes erfolgt eine automatische Erweiterung um zehn Gigabyte. Zum Schutz der Serverumgebung setzt NetPlans einen zentralen Antivirenschutz ein. Es wird empfohlen, auch auf den eingesetzten Endgeräten eine geeignete Antivirensoftware zu verwenden. Sollte auf einzelnen oder allen Arbeitsplätzen kein aktiver Virenschutz vorhanden sein, ist dies NetPlans mitzuteilen. In Abstimmung mit dem Kunden werden dann geeignete Schutzmaßnahmen besprochen und umgesetzt. Zugriffe auf Verwaltungsfunktionen sowie auf Datensicherungen – wie beispielsweise Wiederherstellungspunkte oder einzelne Dateien – sind ausschließlich über einen Service-Request möglich und werden durch den IT-Support von NetPlans durchgeführt. Die Abrechnung erfolgt auf Basis des tatsächlichen Zeitaufwands. Der Cloud-Dienst Full Managed as a

Service DATEV PARTNERasp erlaubt ausschließlich lokale Administrationsrechte. Der Kunde ist für die innerhalb des DATEV Servers installierten Applikationen, deren Systempflege und Wartung selbst verantwortlich. Nach Abstimmung können diese Arbeiten, einschließlich DATEV Softwarepflege, separat über einen DATEV Maintenance Service durch die NetPlans, als zertifizierter DATEV-Systempartner, übernommen werden. Dieser Softwarepflegevertrag stellt eine ausdrückliche Empfehlung dar. Im Rahmen von PARTNERnet ist verbindlich an jedem PARTNERnet-Arbeitsplatz des Kunden zusätzlich ein Antivirenprogramm einzusetzen. Dieses Antivirenprogramm ist kein Bestandteil des Leistungsumfangs innerhalb des Full Managed as a Service DATEV PARTNERasp. Sollte ein Arbeitsplatz nicht über ein gültiges Antivirenprogramm verfügen, ist dies vom Kunden NetPlans mitzuteilen. NetPlans wird sich dann, in Absprache mit dem Kunden, der Situation annehmen und Lösungsmöglichkeiten unterbreiten. Ein Zugriff auf die Verwaltungsinstrumente oder Datensicherung (RestorePoints bzw. Wiederherstellung von Daten und Dateien) ist ausschließlich über ein Service-Request und durch die Bearbeitung der NetPlans IT-Supportabteilung möglich. Aufwände für einen anfallenden Service-Request werden nach tatsächlichem Zeitaufwand berechnet.

## IV. NetPlans Services in Microsoft Azure

### 01 DATEV on Azure by NetPlans

Der Cloud-Dienst DATEV on Azure ist ein hochverfügbarer Service, der auf einer multisession-fähigen Microsoft Azure Virtual Desktop (AVD)-Umgebung betrieben wird. Für die Nutzung ist ein eigener Azure Tenant des Kunden erforderlich. Der Dienst lässt sich nahtlos in bestehende IT-Infrastrukturen integrieren. Die Datenverarbeitung und -speicherung erfolgt in Microsoft-Rechenzentren der Region North Europe (Irland), die geringe Latenzzeiten sowie eine hohe Ausfallsicherheit gewährleisten. Sicherheitsupdates und Patches werden automatisch und regelmäßig eingespielt, während die Aktualisierung der DATEV-Applikationen über den separat buchbaren DATEV Maintenance Service erfolgt. Der DATEV-Lizenzdongle wird in der NetPlans Business Cloud bereitgestellt und per Site-to-Site-VPN in die Azure-Umgebung des Kunden eingebunden. Zur Absicherung der Infrastruktur kommt auf den Azure-Servern Microsoft Defender for Server zum Einsatz. Der Benutzerzugriff wird durch die in Entra ID integrierte Multi-Faktor-Authentifizierung (MFA) geschützt; hierfür ist ein entsprechendes Microsoft-365-Paket mit Entra-ID-Plan erforderlich. Für den Zugriff auf die AVD-Umgebung ist pro Benutzer eine Windows Enterprise Lizenz notwendig, wie sie unter anderem in E3 VDA, Business Premium sowie Microsoft 365 E3 und E5 enthalten ist. Den Anwendern steht ein vollwertiger virtueller Arbeitsplatz inklusive Internetzugang zur Verfügung. Das Paket beinhaltet ein NAT Gateway für den Internetzugang sowie ein VPN Gateway mit einem inkludierten Datenvolumen von 500 GB für das NAT Gateway und 100 GB für das VPN Gateway. Bei deutlichen Überschreitungen der üblichen Verbrauchswerte behält sich NetPlans vor, entstehende Mehrkosten dem Kunden in Rechnung zu stellen. Die Datensicherung erfolgt geo-redundant mit täglichen Backups für 30 Tage, wöchentlichen Backups für 10 Wochen, monatlichen Backups für 6 Monate sowie zusätzlichen eintägigen Momentaufnahmen. Darüber hinaus umfasst der Dienst das NetPlans Managed Monitoring, das eine proaktive Reaktion unserer Experten auf mögliche Auffälligkeiten ermöglicht. Der Zugriff auf Verwaltungsfunktionen oder Datensicherungsprozesse (z. B. Restore Points oder die Wiederherstellung von Dateien und Daten) erfolgt ausschließlich über ein Service-Request und wird durch die NetPlans IT-Supportabteilung durchgeführt. Anfallende Aufwände werden nach tatsächlichem Zeitaufwand abgerechnet.

### 02 DATEV on Azure light by NetPlans

Der Cloud-Dienst DATEV on Azure light ist ein hochverfügbarer Service, der auf einer multisession-fähigen Microsoft Azure Virtual Desktop (AVD)-Umgebung bereitgestellt wird. Für die Nutzung ist ein eigener Azure Tenant des Kunden erforderlich. Der Dienst lässt sich nahtlos in bestehende IT-Infrastrukturen integrieren. Die Datenverarbeitung und -speicherung erfolgt in Microsoft-Rechenzentren der Region North Europe (Irland), die geringe Latenzzeiten sowie eine hohe Verfügbarkeit gewährleisten. Der Dienst wird regelmäßig und automatisch mit den neuesten Sicherheitsupdates und Patches versorgt. Die Aktualisierung der DATEV-Applikationen erfolgt über

den zusätzlich buchbaren DATEV Maintenance Service. Der DATEV-Lizenzdongle wird in der NetPlans Business Cloud bereitgestellt und über eine Site-to-Site-VPN-Verbindung in die Azure-Infrastruktur des Kunden eingebunden. Zur Absicherung der Umgebung wird auf den Azure-Diensten Microsoft Defender for Server eingesetzt. Der Benutzerzugriff wird über die in Entra ID integrierte Multi-Faktor-Authentifizierung (MFA) abgesichert; hierfür ist ein entsprechendes Microsoft-365-Paket mit Entra-ID-Plan erforderlich.

Für den Zugriff auf die AVD-Umgebung ist pro Benutzer eine Windows Enterprise Lizenz notwendig, wie sie unter anderem in E3 VDA, Business Premium sowie Microsoft 365 E3 und E5 enthalten ist. Ein vollwertiger virtueller Arbeitsplatz wird in dieser Variante nicht bereitgestellt; DATEV steht ausschließlich als RemoteApp zur Verfügung. Das Paket beinhaltet ein NAT Gateway für den Internetzugang sowie ein VPN Gateway. Als Standard ist ein inkludiertes Datenvolumen von jeweils 100 GB für das NAT Gateway und 100 GB für das VPN Gateway vorgesehen. Bei deutlichen Abweichungen von den üblichen Verbrauchswerten behält sich NetPlans vor, entstehende Mehrkosten dem Kunden in Rechnung zu stellen. Die Datensicherung erfolgt geo-redundant und umfasst tägliche Backups für 30 Tage, wöchentliche Backups für 10 Wochen sowie monatliche Backups für 6 Monate. Zusätzlich werden Momentaufnahmen für einen Tag vorgehalten. Der Dienst enthält außerdem das NetPlans Managed Monitoring, das eine proaktive Reaktion unserer Experten auf mögliche Auffälligkeiten ermöglicht. Der Zugriff auf Verwaltungsfunktionen oder Datensicherungsprozesse (z. B. Restore Points oder die Wiederherstellung von Dateien und Daten) erfolgt ausschließlich über ein Service-Request und wird durch die NetPlans IT-Supportabteilung durchgeführt. Anfallende Aufwände werden nach tatsächlichem Zeitaufwand abgerechnet.



360° Business-IT, auf die Sie sich verlassen können.



**DIN ISO**  
27001 | 27017 | 27018  
ZERTIFIZIERT

**BLEIBEN SIE AUF DEM LAUFENDEN!**  
Wichtige IT-Neuerungen, aktuelle  
Security-Themen und alles über NetPlans.

 [netplans.de](https://netplans.de)

