Leistungsbeschreibung – managed Server (01/2024)

Vorbemerkung

Wenn im Folgenden zwischen Basis, Standard und Premium unterschieden wird, gilt eine Sache für ausschließlich das/die genannte(n) Pakete, andernfalls für alle drei Pakete.
Die Anzahl der abgerechneten Server ergibt sich aus der Anzahl der Systeme, welche über das Monitoring-System betreut werden, bzw. für die Anzahl der Switche, die unter den Vertragsbestandteilen aufgeführt sind.
Die Vertragslaufzeit richtet sich nach der aufgedruckten Vertragslaufzeit auf dem zugehörigen managed Services-Vertrag, beträgt mindestens jedoch 12 Monate. Der Vertrag verlängert sich um je zwölf Monate, sollte er nicht mit einer Frist von drei Monaten zum Ablaufdatum schriftlich gekündigt werden.

Voraussetzungen

Die zuverlässige, sichere und kostengünstige Betreuung innerhalb dieses Konzepts basiert auf bestimmten Voraussetzungen der IT-Struktur beim Auftraggeber. Dies umfasst:

- Der Auftraggeber ist für das tägliche Anfertigen von mindestens zwei Voll-Datensicherung sowie einer Archivierung verantwortlich, wobei eine in einem anderen Brandabschnitt aufbewahrt werden muss.
- Für die eingesetzte Hard- und Software ist erforderlich, dass sie über einen gültigen Herstellersupport (bspw. CarePack, Softwarepflegevertrag, Maintenance, Microsoft Lifecycle Support) verfügt.
- Eine Ist-Analyse mit den Komponenten Netzwerkstruktur inkl. IP-Adressliste, externe Provider-Anbindung, Firewall-Konzept, Softwarestände, Hardwareüberblick, Backup-Konzept, Ansprechpartner der involvierten Personen beim Auftraggeber und dessen Softwarelieferanten, Notfallplan ist vorhanden und entspricht der aktuellen Konfiguration.
- Auf Basis der Erkenntnisse der Ist-Analyse ist möglicherweise die Umsetzung eines Maßnahmenplans notwendig.

Für die Bereitstellung der Ziffer 11 ist die Buchung einer Managed Firewall Voraussetzung. Ansonsten verfällt der Anspruch.

1. Funktionsprüfung / Monitoring

Die Fernwartungssoftware ermöglicht die zeitnahe Problemlösung durch Techniker des Auftragnehmers aus der Ferne über eine nach dem üblichen Standard gesicherte Internetverbindung. Der Auftragnehmer versichert, diesen Zugang mit hoher Sorgfalt zu verwalten und versichert weiterhin, sämtliche in Kontakt mit den Systemen des Auftraggebers kommenden Mitarbeiter im Hinblick auf die Einhaltung der relevanten Datenschutzgesetze zu verpflichten.
Die benötigten Lizenzen zur Nutzung der Fernwartungssoftware für die Server sind enthalten. Weiterhin stellt der Auftragnehmer dem Auftraggeber eine über das IT-Management-System zugängliche Fernwartungs-Funktion für seine eigenen Zwecke zur Verfügung, sofern für die zu fernwartenden Geräte ein Managed Service Vertrag gebucht wurde.

Aus dem internen Netz des Auftraggebers erfolgt eine Prüfung der Verfügbarkeit der Windows-Dienste, Prüfung der Festplattenkapazitäten für alle Partitionen sowie der RAM und CPU-Auslastung. Prüfung des physischen Festplattenzustand (SMART) sowie des RAID-Systems, sofern die entsprechenden Hard- und Softwarekomponenten diese Informationen bereitstellen, Prüfung auf eine bestimmte Anzahl erfolgloser Anmeldeversuche, Überprüfung der Erreichbarkeit einer Internet-Website, Überprüfung der Servertemperatur, sofern die Serversysteme diese Daten per SNMP bereitstellen.
Prüfung der Lauffähigkeit der Windows-Dienste und Aktualität der Anti-Virus-Signaturen (bei Buchung der Pakete Standard oder Premium).
Im Fehlerfall erfolgt eine Alarmierung gemäß Ziffer 5. Die Überprüfung findet dabei im 60- (bei Basic), 30- (bei Standard) bzw. 15-Minuten-Takt (bei Premium) rund um die Uhr statt. Es gilt die Interventionszeit nach Ziffer 6.
Für die Funktionalität wird ein Agent auf den Servern installiert, der zwingend eine ausgehende SSL-Internetverbindung (Port 443) in ein bestimmtes Zielnetz nach außen nutzt.

2. Prüfung der Datensicherung

Tägliche Prüfung der definierten Backupjobs, welche auf Erfolg oder Misserfolg laut Softwarehersteller überprüft werden. Mögliche Status sind „Erfolgreich“ („Success“), „mit Warnung abgeschlossen“ („Warning“) oder „Fehlgeschlagen“ („Failed“).
Im Fehlerfall erfolgt eine Alarmierung gemäß Ziffer 5. Die Überprüfung findet dabei einmal täglich statt.
Der Auftraggeber ist damit einverstanden, dass aufgrund von Fehlermeldungen, die sich aus dem Monitoring der Server nach Ziffer 1 ergeben, bis zu einer Stunde pro Monat pro Server die notwendigen technischen Maßnahmen auf Basis der Vergütungsregelung in Ziffer 15 eingeleitet werden.

3. Inventarisierung

Tägliche automatische Aktualisierung der Auflistung der installierten Hard- und Softwarekomponenten der Server im vom Auftragnehmer für den Auftraggeber bereitgehaltenen Monitoring-System. Mit dem Monitoring-System unterstützt der Auftragnehmer die vertraglich vereinbarten Leistungen. Für die Funktionalität wird ein Agent auf dem Server installiert, der zwingend eine Internetverbindung über Port 443 nach außen benötigt. Auswertungen bzgl. der im Einsatz befindlichen Server können jederzeit abgerufen werden. Weiterhin ist ein Export der Daten als XML-Datei möglich.

4. Statusberichte

Der Auftragnehmer erstellt einen Bericht, in dem die wichtigsten Systemdaten erfasst sind. Der Auftraggeber erhält den Bericht automatisch per E-Mail. Im Basic-Paket erfolgt der Versand einmal monatlich und erhält Informationen zur Verfügbarkeit des Systems, sowie u.a Systemdaten wie Auslastung der Festplatten, Arbeitsspeichers und Dienstverfügbarkeit. Im Standard- bzw-. Premium-Paket erfolgt der Versand des Berichts wöchentlich und ist um die durchgeführten und anstehenden Sicherheits- und 3rd-Party-Updates erweitert.

5. Alarmierung

Die Alarmierung im Basic-Paket erfolgt an bis zu drei frei wählbare Empfänger des Auftraggebers. Eine Alarmierung des Auftragsnehmers erfolgt hierbei nicht. Sollte es aus Sicht des Auftraggebers notwendig sein, Fehlerlösungsmaßnahmen durch den Auftragnehmer einzuleiten, so wird der Auftraggeber den Auftragnehmer hierzu über folgende Kommunikationskanäle unter Ziffer 6 beauftragen (es gilt die Interventionszeit nach Ziffer 6).

Im Standard- und Premium-Paket erfolgt eine Alarmierung direkt an den Auftragnehmer. Es wird in diesem Fall die Interventionszeit nach Ziffer 6 angewendet sowie die Abrechnung nach Ziffer 15 vorgenommen.

6. Reaktions- / Interventionszeit bei unternehmenskritischen Problemen

Vom Auftragnehmer wird ein Problem als kritisch eingestuft, wenn dadurch Arbeitsausfall für mehrere Personen verursacht wird oder wichtige Kernprozesse laut Anlage 1 der Managed Server Servicebedingungen erheblich beeinträchtigt sind. Bei kritischen Problemen muss seitens des Auftragnehmers innerhalb des Next-Business-Day (Basic-Paket) bzw. acht Stunden (Standard-Paket) oder vier Stunden (Premium-Paket) während des Servicezeitraums Mo-Fr 8-17 Uhr mit der Problemlösung entweder beim Auftraggeber vor Ort, per telefonischer Hilfestellung oder per Fernwartung begonnen werden. Die Interventionszeit beginnt mit Mitteilung an den Auftragnehmer unter den folgenden Kommunikationskanälen:

- über das Ticket-Portal portal.kunze-ritter.de
- per E-Mail an support.it@kunze-ritter.de
- telefonisch über 0761 45554-77

Der Auftraggeber ist zur Mitwirkung bei der Problemanalyse und -lösung des Auftragnehmers verpflichtet. Bei unkritischen Problemen muss innerhalb von 48 Stunden während des Servicezeitraums Mo-Fr 8-17 Uhr mit der Problemlösung oder Terminierung der Problemlösung begonnen werden.
Der Auftraggeber benennt einen Systemverantwortlichen und einen Stellvertreter.

Leistungen ausschließlich im Standard- und Premium-Paket

7. Installation von Windows- bzw. 3rd-Party-Sicherheitsupdates

Bereitstellung und Installation aktueller Microsoft-Sicherheitsupdates sowie Sicherheitsupdates für die unter Anlage 2 aufgeführten 3rd-Party-Software.
Der Auftragnehmer führt auf den Servern wöchentliche Installationsroutinen gemäß „Anlage 3: Installationsmethoden für Microsoft- / 3rd-party-Sicherheitsupdates“ zur Implementierung von Sicherheitsupdates durch und lässt die Server nach erfolgter Installation neu starten. Der Auftraggeber ist mit diesem Prozess einverstanden und wird entsprechend notwendige Wartungsfenster für diese Maßnahme einrichten.
Der Auftraggeber ist damit einverstanden, dass die vom Hersteller veröffentlichten Sicherheitsupdates ohne vorherige Prüfung auf den Systemen installiert werden. Die Haftung für die Fehlerfreiheit der Sicherheitsupdates, die Sinnhaftigkeit der Risiko-Klassifizierung sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Hersteller. Die Sicherstellung der erfolgreichen Installation der Sicherheitsupdates erfolgt über eine tägliche Abfrageroutine. Ein monatlicher Bericht über den Erfolg der Sicherheitsupdates wird per E-Mail an den Auftraggeber versendet (siehe 4. Statusberichte).
Dem Auftraggeber ist bewusst, dass Softwareupdates Veränderungen an der installierten Software vornehmen, um die Sicherheit oder Stabilität zu verbessern. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand übernimmt der Auftragnehmer keine Haftung. Der Auftragnehmer wird die Problemlösung nach üblichen Standards herbeiführen.

8. Treiberupdates für physischen Server

Regelmäßige Prüfung und Installation (im Premium-Paket) der Treiber auf den physischen Servern.
Der Auftraggeber ist damit einverstanden, dass die vom Hersteller veröffentlichten Updates ohne vorherige Prüfung auf den Systemen installiert werden. Die Haftung für die Fehlerfreiheit der Updates, die Sinnhaftigkeit der Risiko-Klassifizierung sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Hersteller.
Dem Auftraggeber ist bewusst, dass Treiberupdates Veränderungen am physischen System vornehmen, um die Sicherheit oder Stabilität zu verbessern. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand übernimmt der Auftragnehmer keine Haftung. Der Auftragnehmer wird die Problemlösung nach üblichen Standards herbeiführen.

9. Bereinigung von temporären Dateien

Regelmäßige Bereinigung (Standard-Paket quartalsweise, Premium-Paket monatlich) der temporären Dateien auf den entsprechenden Systemen.

10. Antivirus-Software

Im Standardpaket wird für die Systeme der Sophos Antivirus Intercept X Advanced for Server, im Premiumpaket der Sophos Intercept X Advanced for Server with XDR, installiert und bereitgestellt. Der Aufwand für die Installation ist im Monatspreis enthalten.

11. Vernetzte Sicherheit zwischen Endpoint und Firewall

Im Standard- und Premiumpaket ist die vernetzte Sicherheit zwischen Endpoint und Firewall enthalten. Das bedeutet, dass der Endpoint der Firewall über seinen Gesundheitszustand in Form eines Ampelsystems Informationen mitteilt. Im weiteren Verlauf kann die Firewall die Datenübertragung zum Endpoint blockieren, um potenziellen Schaden abzuwenden.

Leistungen ausschließlich im Premium-Paket

12. Anfahrt IT-Support

Sind vor-Ort-Dienstleistungen zur angestrebten Störungsbeseitigung bzw. für Administrationstätigkeiten notwendig, so sind An- und Abfahrten zum Auftraggeber pauschal enthalten.
Dieser Service ist regional begrenzt verfügbar innerhalb des Verkaufsgebietes des Auftragnehmers (südliches Baden-Württemberg).

13. Beratungsgespräch über den IT-Status & IT-Strategie

Der Auftraggeber erhält bei Buchung des Premium-Pakets ein kostenfreies Beratungsgespräch über den IT-Status und die IT-Strategie im halbjährlichen Intervall. Bestandteil ist die gemeinsame Interpretation der durch das IT-Management-System generierten Berichte und die Ableitung etwaiger Maßnahmen. Des Weiteren werden aktuelle Trends der IT-Branche auf den sinnvollen Einsatz in seinem Unternehmen gemeinsam überprüft.

Sonstige Informationen

14. Einrichtungsgebühr pro Server

Die Server werden mit entsprechenden Agenten des IT-Management-Systems versehen und konfiguriert. Dieser Aufwand ist im Monatspreis des zugehörigen managed Service-Vertrages enthalten.
Kommt es zu einem Server-Austausch oder einer Server-Neuanschaffung, so wird die Einrichtung erneut notwendig und per Aufwand berechnet.

15. Stundensatz für weitere Leistungen

Der Stundensatz für die Erbringung von Dienstleistungen wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung und Dokumentation in der Zeit von Mo-Fr 8-17 Uhr gilt gemäß der aktuellen Preisliste. Abgerechnet wird im 15-Minuten-Takt.
Etwaige Fahrtkosten werden mit EUR 0,60 pro Entfernungskilometer berechnet. Fahrtzeiten werden zum Stundensatz abgerechnet.
Ein Fernzugriff auf die Systeme des Auftraggebers erspart diesem die Fahrtkosten, die Zeit wird wie zuvor genannt abgerechnet.
Der Auftraggeber ist damit einverstanden, dass aufgrund von Fehlermeldungen, die sich aus dem Monitoring der Server nach Ziffer 1 ergeben, bis zu einer Stunde pro Monat pro Server die notwendigen technischen Maßnahmen auf Basis der Vergütungsregelung in dieser Ziffer eingeleitet werden.
Außerhalb des Zeitraums werden 50 % Zuschlag (zwischen 18-20 Uhr), 100 % Zuschlag (zwischen 20-07 Uhr), 100 % Zuschlag für Samstagstätigkeiten bzw. 150 % Zuschlag an Sonntag- und Feiertagen berechnet.

16. Preisanpassungen

Kunze & Ritter kann jederzeit ohne eine begründete Erklärung eine Anpassung der Vergütung verlangen. Ab einer Preiserhöhung von mehr als 10 % wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

Erweiterungen

17. Quartals-Support-Flatrate

Wurde im managed Service-Vertrag die Option „Quartals-Support-Flatrate“ (möglich in Standard- und Premiumpaket) gebucht, so können Supportdienstleistungen, die die gebuchten Bestandteile des Servicevertrags betreffen (z.B. Client, Server, Firewall), zum vergünstigten Stundensatz über den managed Vertrag abgerechnet werden. Die Leistungen werden in der Zeit von Mo-Fr 8-17 Uhr erbracht. Es gilt die Interventionszeit nach Ziffer 6. Die Flatrate für Störungsbeseitigungen und Administrationstätigkeiten bezieht sich auf technische Dienstleistungen, die am Betriebssystem sowie an weiteren Anwendungen & Diensten laut Anlage 1 durchgeführt werden. Weitergehende Tätigkeiten an Softwareprogrammen oder angeschlossenen bzw. verbundenen Geräten wie NAS, SAN-Systeme sind nicht durch die Flatrate abgedeckt.

Die monatlich über die Quartals-Support-Flatrate gebuchten Stunden sind für das jeweilige Quartal gültig. Nach Ablauf eines jeden Quartals wird die tatsächliche monatlich benötige Dienstleistung der vergangenen drei Monate ermittelt. Sofern eine Abweichung von mind. 20% pro Monat besteht, wird die Höhe der Quartals-Flatrate-Stunden automatisch um diese Abweichung zur nächsten vollen Stunde erhöht oder verringert. Eine Nachberechnung oder Nachvergütung erfolgt nicht. Der Auftraggeber erhält jeweils eine Stundenübersicht zur besseren Nachvollziehbarkeit der getätigten Arbeiten. Projektdienstleistungen sind von der Quartals-Support-Flatrate ausgenommen.

18. Gültigkeit Servicebedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Servicebedingungen in der jeweils aktuellen Version. Abrufbar unter www.kunze-ritter.de/downloads Außerdem gelten nachrangig für die eingesetzten Softwareprodukte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller.

Anlage 1: Kernprozesse und Flatrate Anwendungen & Dienste

Im Kerngeschäft kann der Auftragnehmer über diesen managed Vertrag die nachfolgenden Anwendungen und Dienste betreuen.

Active Directory	DNS & DHCP	Lizenzdienste	Microsoft Druckdienste
Microsoft Filedienste	Microsoft Exchange Srv.	Microsoft Terminal Srv.	VMWare vSphere
Microsoft Hyper-V	Microsoft Office Suite	Adobe Reader	Mozilla Firefox
Google Chrome	Microsoft Teams	Reddoxx / Mailstore	Sophos Intercept X
AvePoint	timeCard10	Veeam Backup	Hornetsecurity

Abweichende Drittanbieter Anwendungen werden nur nach expliziter Absprache mitbetreut.

Anlage 2: Liste der unterstützen Software für Microsoft- und 3rd-Party-Updates

.Net Framework 3.5	.Net Framework 4.0	.Net Framework 4.5	.Net Framework 4.6
.Net Framework 4.7	.Net Framework 4.8	7-Zip	Adobe Air
Adobe Flash Player	Adobe Reader	Adobe Shockwave Player	Edge
Edge WebView 2	Filezilla	Google Chrome	GPL Ghostsript
Internet Explorer	Jabra Direct	KeePass	LibreOffice
Microsoft Office	Microsoft Windows	Mozilla Firefox	Mozilla Thunderbird
Notepad++	Office Viewer	Open Office	Opera
ownCloud	PDF Architect	PDF24 Creator	Quick Time
Silverlight	Virtual Box	Visual C++ Redistributable	VLC Player
VMware vSphere Client	Windows AIK	WinRAR / Win SCP	

Anlage 3: Installationsmethoden für Microsoft- / 3rd-party-Sicherheitsupdates

Als Wartungsfenster für die wöchentliche Installationsroutine der Microsoft- und 3rd-party-Updates wird folgender Zeitraum definiert:

Start	Ende
Mittwoch 20:00 Uhr	Donnerstag 06:00 Uhr