keSolutions GmbH

Ehemals KRK ComputerSysteme GmbH

Leistungsschein

Service Plan

keSolutions GmbH
Version vom 1.11.2023

Inhalt

Service Pläne

Service Plan Basis

Dieser Service Plan ist der Einstieg in einen verwalteten Betrieb Ihrer Systeme.
Sie erhalten Zugriff auf unsere Hotline und das angeschlossene Support-Team. Für die optimale Bearbeitung Ihrer Supportfälle stellen wir Ihnen unser Inventarisierungs- und Fernwartungssystem für die Vertragslaufzeit zur Verfügung. Ferner erhalten Sie einen Zugriff auf unser Ticketsystem.
Alle Meldungen, den Status Ihrer Systeme betreffend, gehen zuerst an einen Ansprechpartner in Ihrem Hause. Somit werden wir erst durch Ihre Beauftragung tätig und Sie erhalten die volle Kontrolle über unsere Arbeiten und Maßnahmen..

- 24/7 Monitoring Ihrer Systeme.
- Automatische E-Mail-Benachrichtigung an Ihren IT-Verantwortlichen im Fehlerfall.
- Webzugriff auf Ihren Systemstatus.
- „Gesundheitsstatus“ Ihrer Hardware
    - Prüfung Ihrer Datenträger und RAID Systeme
    - Netzwerk und TK-Systeme prüfen
    - Statusprüfung Backup und Virenscanner
    - Verfügbarkeitsprüfung von Systemen und Diensten
- Fernwartungsmodul.

Service Plan Risikomanagement

Neben allen Leistungen aus unserem Basis Sicherheitspaket übernehmen wir, im Rahmen der monatlichen Pauschale, die Aktualisierung und das Patchmanagement der für Ihre Infrastruktur relevanten IT-Systeme, soweit Sie zu den unten aufgeführten Systemen gehören:

- Betriebssystem-Updates für Microsoft Server und Clients.
- Updates für Microsoft Exchange und SQL-Server.
- Microsoft Office-Updates.
- Java Runtime, Adobe Reader, Firefox.
- Aktualisierung aller in diesem Paket enthaltenen Dienste.

Die Verteilung der Systemupdates erfolgt auf Basis der Herstellerempfehlungen und nach interner Prüfung bei uns im Hause an jedem Wochenende. Zur Sicherstellung der ordnungsgemäßen Installation werden wir, vor der Installation der Updates, einen Neustart der Systeme durchführen. Im Anschluss werden Updates installiert. Die Zeitpläne werden in Zusammenarbeit mit Ihnen abgestimmt.

.
Des Weiteren sind folgende Leistungen enthalten:

- Monatliche Datenträgerbereinigung Ihrer Systeme.
- Aktualisierung der Netzwerk- und USV-Systeme.
- Restoretest 2x/Jahr bei gleichzeitiger Buchung Online-Backup oder dem Einsatz von Veeam.
- Halbjährlich erfolgt eine Prüfung der Systeme bei Ihnen vor Ort.

Fehlermeldungen aus dem Monitoring-System werden durch uns qualifiziert. Die Behebung kleinerer Mängel bis 30 min Aufwand wird automatisch durchgeführt. Umfangreichere Arbeiten werden in Absprache mit Ihnen vorgenommen. Die Berechnung aller Fehlerbehebungen erfolgt nach tatsächlichem Aufwand.

Service Plan FullFlat

Neben allen Leistungen aus unserem Basis- und Risikomanagement-Paket ermöglicht Ihnen unsere FullFlat absolute Planbarkeit und Kostenkontrolle für Ihre IT-Systeme.
Zusätzlich stehen Ihnen im Rahmen der monatlichen Pauschale folgende Dienstleistungen zur Verfügung:

Flatrate für Fernwartung.
Hardwarereparatur während der Garantielaufzeit.
Erweiterte Erreichbarkeit unserer Bereitschaftshotline.
Festgelegte Eskalationszeiten bei unternehmenskritischen Problemen.
Flatrate für Vorort-Support.

Die Berücksichtigung von Businessanwendungen in der FullFlat (Warenwirtschaft, Buchhaltung etc.) nach vorheriger Absprache ist möglich.

Service Plan O365

Die Services von Microsoft werden über einen sogenannten Tenant verwaltet. Gerne übernehmen wir auch diese Aufgabe für Sie. Hierbei wird in folgenden Services unterschieden:

1. E-Mail (Exchange).
2. Dateiablage (OneDrive & SharePoint).
3. Kommunikation & Zusammenarbeit (Teams).

	Basis	Risikomanagement	FullFlat
Überwachung der Benutzersynchronisation	Ja	Ja	Ja
Buchen der erforderlichen Lizenzen	Ja	Ja	Ja
Prüfen auf Überlizensierung	Nein	Ja	Ja

Information bei Servicestörungen	Nein	Ja	Ja
Überprüfung Secure Score	Nein	Ja	Ja
Überprüfung nicht genutzter Benutzer (Anmeldung älter als 30 Tage)	Nein	Ja	Ja
Auffälligkeiten im Sicherheitssystem	Nein	Ja	Ja

Geräte unter Wartung

Alle Geräte, die uns vom Auftraggeber zur Wartung gemeldet und in unserem Monitoring System aufgenommen worden sind. Dies ist zugleich Berechnungsgrundlage für die monatliche Gebühr. Unser Service Plan FullFlat umfasst grundsätzlich alle, in einem gemeinsamen Netzwerk/Systemverbund enthaltenen, Geräte.

Ausschlüsse

Patch-Management ist ein wichtiges Element zur Aufrechterhaltung der Systemsicherheit und Systemverfügbarkeit. Der Auftraggeber akzeptiert die Gefahr eines möglichen fehlerhaften Systemverhaltens bzw. Auswirkungen auf andere Anwendungen und die ggf. erforderliche Fehlerbehebung bzw. Wiederherstellung des Systems, zum Zeitpunkt der letzten Datensicherung vor Installation des Patches, sowie einem eventuell damit verbundenen Verlust von Daten oder deren Änderungen im betroffenen Zeitraum. Die dadurch entstehenden Aufwände werden nach Aufwand abgerechnet sofern nicht der Service Plan FullFlat gebucht wurde.
Ein vom Businesssoftware-Hersteller bereitgestelltes, fehlerhaftes Update fällt nicht unter die Leistungen der Service Pläne, weder bei Fullflat noch Risikomanagement. Viren- und Malwareausbrüche (sofern sie sich auf mehr als 15% der Arbeitsplätze erstrecken) sowie mutwillige und grob fahrlässige Beschädigungen an Hard- und Software sind in allen Fällen nicht durch die Leistungen der Service Pläne abgedeckt. Dienste von Cloud-Providern wie z.B. Microsoft Office 365 und Azure oder Amazon Web Services werden im Rahmen der KRK Service Pläne integriert, kontrolliert und verwaltet so weit vereinbart. Die Verantwortlichkeiten für die Überprüfung, Kontrolle und Aktualisierung richten sich nach dem gebuchten KRK Service Plan. Es gelten ausschließlich die Service Level der jeweiligen Hersteller und Anbieter. KRK haftet nicht für Ausfälle und nicht Verfügbarkeit der Dienste sowie Verstöße der Anbieter

gegen ihre SLAs.

Zusätzliche Dienste

Zur vollständigen Absicherung Ihrer IT-Systeme und Netzwerk-Infrastruktur bieten wir folgende Zusatzdienste namenhafter Hersteller zum Schutz gegen Malware an. Die Verantwortlichkeiten für die Überprüfung, Kontrolle und Aktualisierung richten sich nach dem gebuchten KRK Service Plan.

Malwareschutz

KRK Managed Antivirus Generell
Wir sorgen für eine zentrale Verteilung und regelmäßige Software-Updates. Die Installation der neusten Version ist für Sie kostenlos. Bei Meldungen des Virenscanners entscheiden unsere IT-Sicherheitsexperten, Sie müssen Sich nicht auf die Entscheidung der einzelnen Nutzer verlassen. Sie bekommen monatlich einen Report über Status und Gefahrenabwehr.

KRK Managed Antivirus Advanced
Mit Hilfe des Herstellers Eset bieten wir einen Virenscanner mit erweitertem Funktionsumfang für Ihre Arbeitsplätze und Server.

- Echtzeit Überwachung
- Zentrale Verwaltung
- Zeitgesteuerte Scans
- Definierbare Scantiefe
- Gerätebezogene Quarantäne
- Profilbasierte Schutzrichtlinien
- Zentrale Gerätekontrolle (USB, DVD, ...)
- Kategorie basierter Webfilter
- Umfassendes Reporting

KRK Managed Antivirus Advanced Plus
Neben allen Features des Antivirus Advanced Paketes enthält unsere, ebenfalls von Eset unterstützte Lösung, einen Analyse-Service, der jede in einem Unternehmen laufende Anwendung exakt klassifizieren kann, sodass nur vertrauenswürdige Prozesse ausgeführt werden. Die Fähigkeiten resultieren aus einem Sicherheitsmodell, das auf drei Prinzipien basiert: (1) ständige Überwachung aller laufenden Anwendungen auf Firmencomputern und Servern, (2) automatische Klassifizierung durch eine cloudbasierte Datenbank und (3) die Analyse nicht automatisch klassifizierter Anwendungen durch den Hersteller. So kann das Verhalten jeder laufenden Anwendung eines Unternehmens kontrolliert werden.

Begriffsdefinition

Reaktionszeit	Nach Eingang einer MELDUNG wird KRK innerhalb der Reaktionszeit mit der Problemanalyse, der Problemlösung oder der Aufwandsanalyse beginnen. KRK wird im Rahmen seiner Möglichkeiten unter Beachtung der vertraglichen Pflichten tätig. Ein Anspruch auf die Beseitigung der Störung innerhalb einer bestimmten Zeit folgt daraus nicht.
Sofort	Bei Ausfall von Servern und TK-Anlagen sowie wesentlichen Teilen der Netzwerkinfrastruktur.
Hoch	Ausfall von Arbeitsplätzen und zentralen Druckern, ... sowie Ausfällen einzelner Anwendungen und Dienste.
Niedrig	Erweiterungen und Neueinrichtungen von Arbeitsplätzen, Updates von Anwendungen, Benutzeranlage und Berechtigungsänderungen.
Eskalation 1	Überschreitung der Reaktionszeit, nach der der Vorgang bei der Geschäftsführung der KRK eskaliert werden kann.
Eskalation 2	Zeit, nach der eine nicht erfolgte Wiederherstellung bei der Geschäftsführung der KRK eskaliert werden kann, gemessen als vielfaches der Reaktionszeit. Ein Anspruch auf Wiederherstellung kann hieraus nicht abgeleitet werden.
Servicelevel	Verfügbarkeit des Gesamtsystems im Jahresmittel
Geräte unter Wartung	Alle Geräte, die uns vom Auftraggeber zur Wartung gemeldet und in unserem Monitoring-System aufgenommen worden sind. Dies ist zugleich Berechnungsgrundlage für die monatliche Wartungsgebühr.
On premise	Systeme im Besitz des Auftraggebers, betrieben in dessen Räumlichkeiten.
KRK Cloud	Übergeordnete Bezeichnung für die KRK Cloud-Dienste.

SLAs

	Basis	Risikomanagement	FullFlat
Reaktionszeit Sofort	8 Werkstunden	4 Werkstunden	4 Werkstunden
Reaktionszeit Hoch	24 Werkstunden	12 Werkstunden	12 Werkstunden
Reaktionszeit niedrig	40 Werkstunden	24 Werkstunden	24 Werkstunden
Eskalationszeit 1	Keine	Reaktion x 2	Reaktion x 2
Eskalationszeit 2	Keine	Reaktion x 6	Reaktion x 4
Bediente Servicezeit	09:00 – 17:00 Uhr	08:00 – 17:00 Uhr	08:00 – 17:00 Uhr
Notfallhotline	Kein Zugriff	100,00 € zzgl. Arbeitszeit (07:00 – 20:00 Uhr werktags/samstags)	100,00 € zzgl. Arbeitszeit (06:00 – 22:00 Uhr an 7 Tagen in der Woche)
Servicelevel On premise	Keine	98 %	98 %
Servicelevel KRK Cloud Produkte	98 %	99 %	99 %

Technische & organisatorische Maßnahmen für die KRK Support Dienste Fernwartung und Monitoring

Unser Monitoring- und Fernwartungs-System wird im Rechenzentrum DU1 bei der Firma Equinix (Germany) GmbH in Düsseldorf gehostet. Das RZ ist nach ISO/IEC 27001:2005 zertifiziert.

Zutrittskontrolle

Die Zutrittskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

Der RZ-Anbieter sorgt für eine Zugangskontrolle nach ISO/IEC 27001:2005.

Zugangskontrolle

Die Zugangskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

- Individuelle Benutzeraccounts für den Zugriff auf das Monitoring und Fernwartungssystem.
- Separater Benutzer für den Zugriff durch KRK ComputerSysteme GmbH auf die Systeme des Auftraggebers (Zugriff nur über Monitoring und Fernwartungssystem).
- Kennwortkomplexität (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel).
- Automatische Sperrung (z.B. Kennwort Fehleingaben oder Pausenschaltung).

Zugriffskontrolle
Die Zugriffskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

- Rollen- und Rechtekonzept.
- Vergabe der Zugriffsrechte nach Prinzip der minimal erforderlichen Rechte.
- Protokollierung und Kenntnisnahme der Zugriffe und Veränderungen.

Weitergabekontrolle
Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung. Die Weitergabekontrolle wird durch Auftraggeber und Auftragnehmer wie folgt sichergestellt:

- SSL Verschlüsselte Kommunikation der Agenten
- SSL geschützte Zugriffe auf das Verwaltungsportal

Eingabekontrolle
Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind. Die Eingabekontrolle wird durch Auftraggeber und Auftragnehmer wie folgt sichergestellt:

- Protokollirungs- und Protokollauswertungssysteme.

Auftragskontrolle
Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:
Die Auftragskontrolle wird wie folgt sichergestellt:

- Eindeutige Vertragsgestaltung.
- Formalisierte und dokumentierte Auftragserteilung (per E-Mail/telefonisch nur über vorher definierte Ansprechpartner).
- Kontrolle der Vertragsausführung.

Verfügbarkeitskontrolle
Maßnahmen zur Datensicherung (physikalisch / logisch):
Die Verfügbarkeitskontrolle wird durch den Hersteller wie folgt sichergestellt:

- Redundante Server.
- Redundante Internetanbindung.
- Unterbrechungsfreie Stromversorgung (USV) 1+n redundant.
- Virenschutz / Firewall.
- Notfallplan.

Trennungskontrolle
Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken. Die Trennungskontrolle wird wie folgt sichergestellt:

Systembedingte, durchgängig logische Trennung aller betreuten Systeme nach Kunden in separatem Mandanten.

Technische & organisatorische Maßnahmen für die KRK Online Backup Pläne

Das Online Backup System wird in einem eigenen Bereich im Rechenzentrum der Hostway Deutschland GmbH am Standort Am Eisenwerk 29, 30519 Hannover in Niedersachsen, Deutschland betrieben. Das Rechenzentrum ist nach ISO 27001 zertifiziert.

1. Zutrittskontrolle

Die Zutrittskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

- Die Zutrittskontrolle erfolgt über einen Empfangsbereich am Eingang bzw. ein Zugangskontrollsystem an der Geländeumzäunung.
- Unterschiedliche Schließgruppen des Schließsystems für den Zutritt zu den Gebäudeteilen, den Bürobereichen sowie einem separaten Schließsystem zum Rechenzentrum.
- Eine 24/7 Videoüberwachung sowie Einbruchmeldeanlage sind vorhanden.

2. Zugangskontrolle

Die Zugangskontrolle wird durch Auftraggeber und Auftragnehmer wie folgt sichergestellt:

- Individuelle Benutzeraccounts für den Zugriff auf das Verwaltungsmodul.
- Individuelle Benutzeraccounts für den Zugriff die zu sichernden Kunden/Systeme.
- Kennwortkomplexität (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts).
- Automatische Sperrung (z.B. Kennwort Fehleingaben oder Pausenschaltung).

3. Zugriffskontrolle

Die Zugriffskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

- Rollen- und Rechtekonzept.
- Vergabe der Zugriffsrechte nach Prinzip der minimal erforderlichen Rechte.
- Protokollierung und Kenntnisnahme der Zugriffe und Veränderungen.

4. Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen

Überprüfung. Die Weitergabekontrolle wird durch Auftraggeber und Auftragnehmer wie folgt sichergestellt:

- Verschlüsselte Übertragung über VPN Verbindungen oder SSL geschützte Zugriffe.
- Verschlüsslung der Daten auf dem zu sichernden Client/Server.
- Passwortsatz für jedes System, ohne den eine Wiederherstellung nicht möglich ist.

5. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Die Eingabekontrolle wird durch Auftraggeber und Auftragnehmer wie folgt sichergestellt:

- Protokollirungs- und Protokollauswertungssysteme.

6. Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer.

Die Auftragskontrolle wird wie folgt sichergestellt:

- Eindeutige Vertragsgestaltung.
- Formalisierte und dokumentierte Auftragserteilung (per E-Mail).
- Kontrolle der Vertragsausführung.

7. Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):

Die Verfügbarkeitskontrolle wird wie folgt sichergestellt:

- Redundante Server.
- Redundante Internetanbindung.
- Spiegeln von Festplatten, RAID-Verfahren sowie Sicherung der Gesamtsysteme in einen anderen Brandabschnitt.
- Unterbrechungsfreie Stromversorgung (USV) 1+n redundant.
- Virenschutz / Firewall.
- Notfallplan.

8. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken. Die Trennungskontrolle wird wie folgt sichergestellt:

Systembedingte, durchgängig logische Trennung aller betreuten Systeme nach Kunden in separaten Mandanten sowie verschlüsselten Containern.