keSolutions GmbH

Ehemals KRK ComputerSysteme GmbH

Leistungsschein

IT Einfach Formel

keSolutions GmbH
Version vom 21.12.2022

Inhalt

IT Einfach Formel

Dieser Service ist der Einstieg in einen verwalteten Betrieb Ihrer Systeme bei gleichzeitiger Planbarkeit und Kostenkontrolle für Ihre IT-Systeme.

Festpreis für Fernwartung.
Festpreis für Vorort-Support.
Hardwarereparatur während der Garantielaufzeit.
Festgelegte Eskalationszeiten bei unternehmenskritischen Problemen.

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.

- Monitoring Ihrer Systeme.
- 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.

Neben alle diesen Leistungen 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.
- Überwachung der Benutzersynchronisation.
- Buchen der erforderlichen Lizenzen.
- Prüfen auf Überlizensierung.
- Information bei Servicestörungen.
- Überprüfung Secure Score.
- Überprüfung nicht genutzter Benutzer (Anmeldung älter als 30 Tage).
- Auffälligkeiten im Sicherheitssystem

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 wird automatisch durchgeführt.

Backup Microsoft 365

Die KRK Office Lösungen kombinieren die Lizenz von Microsoft mit einem täglichen Backup ihrer Daten für ein Jahr. Zusätzlich sind wir als KRK ihr direkter Ansprechpartner bei technischen Problemen oder einfachen Fragen zur Lizensierung.

KRK Cloud Backup

Zum Schutz Ihrer Daten, sowohl auf Servern als auch auf kritischen oder mobilen Arbeitsplätzen, bieten wir Ihnen eine einfache Möglichkeit, Ihre Daten von jedem beliebigen Ort über das Internet in unser deutsches Rechenzentrum zu sichern. Vermeiden Sie aufwendige Prozesse zum täglichen Medienwechsel und zusätzliche Arbeitsplatzsicherungen.
Die Übertragung und Ablage der Daten erfolgt dabei ausschließlich verschlüsselt. Nur Sie haben Zugriff auf Ihre, bei uns gespeicherten, Daten.

Durch Bandbreitenmanagement, Änderungsverfolgung und Duplizierung können auch große Datenmengen bis zu mehrmals täglich gesichert werden, während eine optionale lokale Kopie für schnelle Wiederherstellungen sorgt.

- Sicherung in unserem deutschen Rechenzentrum
- Lokaler Backup Manager
- Sichert nahezu alle Systeme
- Windows, Linux und MacOS X, MS- Exchange, SharePoint, SQL, Oracle und mehr
- VMware und Hyper-V
- Deduplizierung und Deltaermittlung vor Übertragung
- Nach Erstsicherung werden durchschnittlich nur noch 0,5% der ausgewählten Daten übermittelt
- Zusätzliche Sicherung auf lokales System möglich (z.B. NAS)
- Bare Metal Restore und Virtual Disaster Recovery
- Granulares Restore von Exchange Sicherungen
- Bandbreitenmanagement

- Komprimierung und Verschlüsselung mit AES 128-Bit bis Blowfish-448
- Archivierung von Sicherungen

Die Bereitstellung erfolgt auf Basis der in der Auftragsbestätigung genannten Leistungsdaten.

Die Aufbewahrungsfrist für die, bei uns gesicherten, Daten beträgt 30 Tage, zusätzlich wird eine Monatssicherung am letzten Tag des Monats archiviert und für 12 Monate aufbewahrt. Ein Datenexport zur Langzeitarchivierung kann jederzeit angefordert werden.

Sollte an Ihrem Standort keine Möglichkeit für die Nutzung eines Online Backup bestehen, realisieren wir eine Datensicherung vor Ort. Laufwerk und Medien werden unserer Empfehlung entsprechend von Ihnen beigestellt.

Firewall

Passend zu Ihrer Unternehmensgröße stellen wir Ihnen die passende Firewall zur Verfügung. Hardware und Lizenz sind genauso in der Monatlichen Pauschale enthalten wie auch kleinere Anpassungen am Regelwerk. Unsere Firewall entspricht aktuellen Technologien und schütz Sie vor potenziellen Gefahren aus dem Internet. Enthaltene Leistungen sind:

- Kostenloser VPN Zugang
- Zwei Virenscanner im Standard schützen Sie beim Surfen im Internet
- Der Inhaltsfilter kann beispielsweise den Jugendschutz sicherstellen oder die SocialMedia-Nutzung auf bestimmte Zeiten beschränken.
- Die Firewall schützt ihr Unternehmen intern und extern.

Mobile Device Management

Tablets und Smartphones etablieren sich immer mehr im Unternehmen. Unser Management System für diese Geräte umfasst folgende Funktionen:

- Zentrales Management über einen Unternehmensaccount
- Zentrale Bestellung, Abrechnung und Verwaltung von kostenpflichtigen Apps
- Konfiguration & Vorgabe von WLAN Eigenschaften und Sicherheitsstandards gezieltes Entfernen von Unternehmensdaten aus der Microsoft Cloud von Privatgeräten
- Remotelöschen und -sperren von verlorenen Geräten
- Blockieren von unbekannten / unsicheren Geräten

Unterstütze Betriebssysteme: Android, iOS, iPadOS, Microsoft Windows 10, Microsoft Windows 11

Microsoft 365

Die Services von Microsoft werden über einen sogenannten Tenant verwaltet. Gerne übernehmen wir auch diese Aufgabe für Sie, dazu gehören:

- Überwachung der Benutzersynchronisation
- Buchen der erforderlichen Lizenzen
- Prüfen auf Überlizensierung
- Information bei Servicestörungen
- Überprüfung Secure Score
- Überprüfung nicht genutzter Benutzer (Anmeldung älter als 30 Tage)
- Auffälligkeiten im Sicherheitssystem

KRK Cloud E-Mailarchiv

KRK stellt seinen Kunden ein System zur E-Mailarchivierung in seinem Rechenzentrum zur Verfügung. Bei steigenden Anforderungen können die bereitgestellten Sicherungsressourcen erweitert und modular ausgebaut werden. Folgende Optionen sind möglich:

- Einfache und schnelle Konfiguration
- Revisionssichere E-Mailarchivierung mit beliebiger Aufbewahrungszeit
- Kompatibel mit nahezu allen E-Mail-Infrastrukturen
    - Exchange Server 2003 - 2016
    - Microsoft Office 365
    - Google Apps
    - Alle IMAP- oder POP3-kompatiblen E-Mail-Server
    - MDaemon, IceWarp und Kerio Connect
    - PST, EML und andere Dateiformate
    - E-Mail-Clients wie Microsoft Outlook
- Archiviert ein- und ausgehende sowie interne E-Mails
- Schnelle Suche über E-Mails und Dateianhänge
- Ordnerstrukturen aus Outlook werden beibehalten
- Schutz vor Datenverlust
- Entlastung von E-Mail-Servern
- Reduzierung des Speicherbedarfs um bis zu 70%
- Deduplizierung und Komprimierung
- Vereinfachung von Backup und Restore
- Unabhängigkeit von PST-Dateien
- Abschaffung von Postfachbegrenzungen
- Delegation von Zugriffsrechten

Die Bereitstellung erfolgt auf Basis der in der Auftragsbestätigung genannten Leistungsdaten.

Verfahrensanweisung zur E-Mail-Archivierung

Das Archivierungsverfahren für E-Mails unterliegt nach den GoBD der Verpflichtung zu einer
Verfahrensdokumentation, welche auch als Teil der generellen Verfahrensdokumentation des
Archivierungs- bzw. Dokumentenmanagementsystems umgesetzt werden kann. Hierbei sollten jedoch die für die E-Mail-Archivierung spezifischen Aspekte, wie beispielsweise Regelungen zu SPAM, Konvertierungseinstellungen, Beschreibung der Maßnahmen zur Sicherung der Vollständigkeit, Nachvollziehbarkeit, Unveränderbarkeit und maschinellen Auswertbarkeit etc. berücksichtigt werden.

externer Datenschutzbeauftragter

Unternehmen ab 20 Mitarbeitern, die personenbezogene Daten verarbeiten oder besonders risikobehafteten Verarbeitungstätigkeiten nachgehen, müssen einen Datenschutzbeauftragten bestellen. Der Datenschutzbeauftragte stellt die Fortführung und Entwicklung der Datenschutzprozesse sicher und steht allen Mitarbeitern bei Fragen zum Datenschutz zur Seite.

Wir unterstützen Sie nach erfolgreicher Erstaufnahme und stehen Ihnen als externer Datenschutzbeauftragte mit unserem bewährten Dienstleistungspaket zur Seite. Dabei erbringen wir folgende Leistungen:

- Meldung als externen Datenschutzbeauftragten
- jährliche Revision des Datenschutzstatus
- Kontrolle und Fortführung des Maßnahmenplans
- Revisionsbericht
- Abstimmungen mit den Ansprechpartnern und Key Usern
- Beratung zu einfachen Fragen des Datenschutzes
- Jährliche Mitarbeitersensibilisierung vor Ort im Rahmen der Revision
- Zugriff auf unsere monatlichen Onlineschulungen zum Datenschutz
- Bereitstellung von standardisierten Organisationshilfen und Vorlagen
- Mandantenlizenz und Zugriff auf unsere digitale Datenschutzakte

Externer Informationssicherheitsbeauftragter

Wir unterstützen Sie bei der Entwicklung Ihrer Informationsicherheitsorganisation. In regelmäßigen Statusmeetings unterstützen wir sie bei der Entwicklung der Prozesse zur Informatonssicherheit und beraten zu notwendigen Maßnahmen bei neuen Projekten und Änderungen in Technik und Prozessen.

In einem Jährlichen Re-Audit bewerten wir die Entwicklung des Maßnahmeplans und dokumentieren damit die Fortschritte und anhaltende Umsetzung der Prozesse in der Informationssichereit.

Im Rahmen der Betreuung erbringen wir folgende Leistungen:

- Jährliches Audit der Maßnahmen zur Informationssicherheit,
- Quartalsweise Beratung zur Umsetzung von Maßnahmen und Sicherheitsfragen zu neuen Projekten,
- Zugriff auf unserer Umfangreiche Bibliothek an Richtlinien- und Konzeptvorlagen,
- monatlicher Newsletter zur Informationssicherheit als Awarenessmaßnahme für alle Mitarbeiter.
- Durch die kontinuierliche Umsetzung und Bewertung dokumentieren Sie gegenüber Partnern, Auftraggebern, Wirtschaftsprüfern, Banken und Versicherungen einen professionellen Umgang mit dem Thema IT- und Informationssicherheit. Die regelmäßig erstellen Auditberichte dienen dabei als Dokumentation.

Pentest / Schwachstellenanalyse

Eine gezielte und regelmäßige Schwachstellenanalyse sollte zu einem festen Bestandteil der Sicherheitsstrategie in Ihrem Unternehmen gehören.

Unser Penetrationstest bietet eine risikobasierte Prüfung von IT-Systemen im Hinblick auf vorhandene Sicherheitsschwachstellen, die sowohl von extern als auch von intern drohen können.

Während einer Simulation von externen Angriffen, innerhalb einer gegebenen Zeitspanne, identifizieren wir einmal in jedem Quartal Sicherheitslücken in ihren nach außen veröffentlichten Systemen und prüfen die Systeme innerhalb ihres Netzwerkes durch automatisierte Scans der exponierten Systeme und nicht-destruktive Prüfung auf Schwachstellen.

Die Ergebnisse bewerten wir im Rahmen der Beratungsgespräche zur Informationssicherheit.

Mitarbeitersensibilisierung – Awareness

Phishing Simulation
Über simulierte Phishing E-Mails testen wir den "Sensibilisierungsgrad" ihrer Mitarbeiter und sorgen gleichzeitig für eine Steigerung der Awareness.

Klicken Nutzerinnen oder Nutzer auf eine unserer simulierten Phishing-Mails oder geben sie Daten in einer gefälschten Login-Seite ein, gelangen sie zu einer Lernseite mit individuellen Hinweisen. Das Ganze geschieht vollkommen anonym und über das Jahr verteilt, sodass die Mitarbeiter kontinuierlich sensibilisiert werden.
Lernmodule
Interaktives und praxisnah gestaltetes E-Learning mit jährlich 6 kurzweiligen Modulen sowie diversen Awareness-Videos.
Jedes Modul beinhaltet konkrete Handlungsempfehlungen zum Sicheren Umgang mit IT Systemen und Informationen und endet mit einem abschließenden Quiz.

Beratung Digitale Prozesse

Bei der Beratung zu Digitalen Prozessen ist unser Ziel Sie im Tagesgeschäft zu unterstützen. Sowohl die Auswahl der passenden Lösung im Bereich Microsoft 365 und Azure sowie im Bereich der IT-Sicherheit stehen hier im Fokus. Die Beratung beginnt bereits bei der Anforderungsanalyse geht über die Auswahl der richtigen Lösung, die Implementierung in Ihrem System und die Schulung der Mitarbeiter gerne übernehmen wir auch später den Betrieb und die Pflege. Beste Erfahrungen haben wir mit unserer begleitenden Einführung gemacht. Dabei wird die Digitalisierung nicht als einmaliges Projekt gesehen, sondern als eigenständiger Prozess der sich mit maximal 1 -2 Tagen Aufwand sehr gut in Ihre Aufgabenplanung integrieren lässt.

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. Unsere Service Pläne IT Einfach umfassen 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.
Ein vom Businesssoftware-Hersteller bereitgestelltes, fehlerhaftes Update fällt nicht unter die Leistungen der IT Einfach Formel.

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 IT Einfach Formel 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. 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.
Nach Auftragserteilung richten wir die Entsprechenden Systeme und Services für ihr Unternehmen ein. Sollten einzelne Bausteine der Gesamtlösung nicht erst später auf Kundenwunsch eingerichtet werden, ist diese Einrichtung nicht über die Monatliche Pauschale abgedeckt und wird separat berechnet.
Virenbefunde die außerhalb der normalen Servicezeiten gemeldet werden können nicht mehr bearbeitet werden. Liegen Anforderungen an einer 24/7 Reaktion auf verdächtige Systemmeldungen vor, ist der Einsatz eines SOC (Security Operation Center) erforderlich.

KRK Managed Antivirus allgemein

Wir sorgen für eine zentrale Verteilung und regelmäßige Software-Updates. Die Lizenz sowie die Installation der neusten Version und der regelmäßigen Updates sind für Sie kostenlos enthalten. Bei Meldungen des Virenscanners entscheiden unsere IT-Sicherheitsexperten was zu tun ist und ergreifen automatisch die notwendigen Maßnahmen. Diese stehen zu der normalen Servicezeit zwischen 08:00 – 17:00 Uhr zur Verfügung. Sie müssen Sich nicht auf die Entscheidung der einzelnen Nutzer verlassen. Sie bekommen monatlich einen Report über Status und Gefahrenabwehr.
KRK Managed Antivirus Advanced
Gemeinsam mit führenden Herstellern 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.

Optionen

Aufwand für Arbeitsplatz-Tausch 1x alle 36 Monate
Als Zusätzliche Planungssicherheit für Sie, bieten wir Ihnen Optional die Möglichkeit den Austausch der Arbeitsplätze nach 36 Monaten kostenfrei durchzuführen. Die Hardware ist in dieser Pauschale nicht enthalten.
Lizenzen Windows Server inkl. RDP für alle User und Server
Optional ist es möglich, dass wir auch die Microsoft Server Zugriffslizenzen für Ihre IT Umgebung bereitstellen. Sie umgehen somit die Gefahr einer Unterlizensierung und ggf. einer Nachzahlung bei einem Microsoft Audit.
Firewall und Netzwerkmanagement für weitere Standorte
Die Betreuung und Anbindung weiterer Standorte ist ebenfalls zu einem Festpreis inkl. der benötigten Firewall möglich.
Client Backup, einzeln buchbar
Komplexe und Aufwendige Arbeitsplätze können vollständig und Cloudbasierend durch uns gesichert 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.

SLA

	IT Einfach Formel
Reaktionszeit Server	4 Werkstunden
Reaktionszeit Arbeitsplatz	12 Werkstunden
Eskalationszeit 1	Reaktion x 2
Eskalationszeit 2	Reaktion x 4
Bediente Servicezeit	08:00 – 17:00 Uhr
Notfallhotline	100,00 € zzgl. Arbeitszeit (06:00 – 22:00 Uhr an 7 Tagen in der Woche)
Servicelevel On premise	98 %
Servicelevel KRK Cloud Produkte	99 %

	Standard	Premium	Ultimate	Small Worker
Server VM / Tenant	1-5	6-15	11-20	1
Branchenanwendungen	1-2	1-6	1-10	1
User	5-25	10-50	20-50	ab 5
Office zur Nutzung auf Terminalserver / RDS	n.e.	x	x	n.e.
Reaktionszeiten Server/Arbeitsplatz Werkstunden	4/12	4/12	4/12	wie Hauptvertrag
Support Zeiten Mo. - Fr. 08:00 - 17:00 Uhr	5x9	5x9 + Bereitschaft	5x9 + Bereitschaft	wie Hauptvertrag
Infrastruktur- / Patch - Management				
Monitoring der Server, Endgeräte und Cloud-Dienste	X	X	X	X
Patchen der Server und Endgeräte	X	X	X	X
Betrieb Firewall, Netzwerk und WLAN	X	X	X	n.e.
Management Microsoft Cloud Tenant	X	X	X	n.e.
Updates Branchenanwendungen	bis 2	bis 6	bis 10	bis 1
IT Sicherheitsmanagement (inkl. Lizenzen)				
Firewall am Hauptstandort inkl. HW	X	X	X	n.e
Webfilter	X	X	X	n.e
Antispam	X	X	X	n.e
E-Mail Archivierung	X	X	X	X

VPN Server und Cllients	X	X	X	n.e.
Antivirus für Endgeräte und Server	Advanced	Advanced Plus	Advanced Plus	wie Hauptvertrag
Mobile Device Management	n.e.	X	X	X - Basis
Backup aller Server	bis 1 TB, kein SQL / Granular Restore	bis 2,5 TB inkl. SQL / Granular Restore	bis 2,5 TB inkl. SQL / Granular Restore	n.e.
Client Backup	bei Bedarf einzeln zubuchbar	bei Bedarf einzeln zubuchbar	bei Bedarf einzeln zubuchbar	bei Bedarf einzeln zubuchbar
IT Service				
User Helpdesk Flat	X	X	X	X
Vor Ort Support Flat	X	X	X	X
Störungsbearbeitung	X	X	X	X
Anwendungen				
Microsoft 365 Lizenz	Business Standard	Business Premium	Business Premium	F3
Unterstützung Hersteller Support für Fachanwendungen	bis 2	bis 6	bis 10	bis 1
TK Anlagen (sofern durch uns geliefert Pana/Starface/Teams)	X	X	X	X
Beratung				
Security Schwachstellenanalyse	n.e.	n.e.	X	25,00 € nur i.V. mit Ultimate
monatlicher Newsletter	n.e.	n.e.	X	
Security Mitarbeiter Sensibilisierung	n.e.	n.e.	X	
Digitale Prozesse	n.e.	n.e.	X	

Datenschutzbeauftragter	n.e.	n.e.	X	
Optionen				
Aufwand für Arbeitsplatz-Tausch 1x alle 36 Monate	10,00 €	10,00 €	10,00 €	10,00 €
Lizenzen Windows Server inkl. RDP für alle User und Server	11,50 € - 18,75 €	11,50 € - 18,75 €	11,50 € - 18,75 €	11,50 € - 18,75 €
Firewall und Netzwerkmanagement für weitere Standorte	99,00 €	149,00 €	199,00 €	99,00 €
Client Backup, einzeln buchbar	9,00 €	9,00 €	9,00 €	9,00 €
Was ist nicht enthalten	jegliche Hardware und Betriebssystemlizenzen (ausgenommen Firewall)			
	Lizenzen für Branchenanwendungen und Datenbankserver			
	Neueinrichtung von Servern und Clouddiensten			
	Rollout neuer Unternehmensanwendungen			
	Nutzungsgebühren für Server und Applikationshosting (ausgenommen Microsoft 365)			
	Wiederinbetriebnahme und Forensik nach Malwarebefall (sofern keine Pflicht aus Vertrag verletzt)			

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:

- Protokollierungs- 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:

- Protokollierungs- 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.