KRK COMPUTERSYSTEME

IT-SERVICE | IT-SECURITY | IT-ACADEMY

Leistungsbeschreibung KRK Cloud Services

vom 30.09.2019

KRK ComputerSysteme GmbH
Nienburger Str. 9a
27232 Sulingen

Tel.: +49 (0)4271 1000 0
Fax: +49 (0)4271 1000 8000
Mail: info@krk-computersysteme.de

Inhalt

Begriffsdefinition

Onlinezeit	Zeitraum, in dem die Server eingeschaltet und aktiv sind. Nur in diesen Zeiten ist ein Zugriff auf die bereitgestellten Dienste möglich.
Servicelevel	Verfügbarkeit des Gesamtsystems im Jahresmittel.
Betreute Betriebszeit	Zeitraum, in dem technisches Personal vor Ort ist.
Bereitschaft	Verfügbarkeitszeitraum der Rufbereitschaft RZ.

Allgemeine Maßnahmen zur Sicherung des laufenden Betriebs

Die zur Bereitstellung der Dienste erforderlichen Systeme werden 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.

Die Verpflichtungen aus dieser LB und die Datenschutzvereinbarungen werden auf das Rechenzentrum übertragen. Die Sicherheit der Kundendaten und die Verfügbarkeit der Dienstleistungen werden unter anderem durch die folgenden Maßnahmen sichergestellt:

Physische Sicherheit durch bauliche, betriebliche und technische Maßnahmen:

- 24 Stunden, 7 Tage pro Woche, 365 Tage im Jahr Personal vor Ort bzw. Bereitschaft
- Zugangskontrollsysteme
- Videoüberwachung vor und im Gebäudekomplex
- Brand- und Einbruchmeldeanlage mit Aufschaltung bei einem Sicherheitsdienst
- Klimatisierung (n+1)
- Redundante (n+1) unterbrechungsfreie und gefilterte Stromversorgung
- Notstromaggregate

Sicherheit und Verfügbarkeit der internen Netzwerkinfrastruktur:

- Segmentierung der Netzwerke und strikte Trennung der Datenströme
- Tägliches Backup der eigenen Systeme
- Einsatz von Firewalls an relevanten Netzwerkpunkten
- Netzwerküberwachung durch hauseigenes Monitoringsystem
- Ausschließliche Verwendung von Markenkomponenten

Verfügbarkeit der externen Netzwerkanbindung:

- Carrier-neutrale und redundante IP-Anbindung des Rechenzentrums

KRK setzt Maßnahmen gemäß §9 BDSG sowie der Anlage „technische und organisatorische Maßnahmen" ein, um die Vertraulichkeit, Verfügbarkeit und Integrität der gehosteten Systeme sicherzustellen. (Anlage 1).

Verfügbarkeit

Die folgenden SLAs (Service Level Agreements) beziehen sich auf die Verfügbarkeit des Rechenzentrums und der bereitgestellten Netzwerke, Host Server und bereitgestellten virtuellen Systeme. Die SLAs, für die individuellen Dienste des Auftraggebers, ergeben sich aus dem jeweiligen Wartungsvertrag gemäß LB KRK Service Plan.

Onlinezeit Netzwerk	betreute Betriebszeit	typischer Servicelevel	garantierter Servicelevel	Bereitschaft
0:00 bis 24:00 365 Tagen / Jahr	Mo - Fr. 8.00 -17:00 Uhr	99,9%	99 %	0:00 bis 24:00 365 Tagen / Jahr

Die Verfügbarkeit des Netzwerks bezieht sich auf die Verfügbarkeit der Internet-Anbindung des Rechenzentrums sowie die Verfügbarkeit der einzelnen Netzwerkkomponenten. Die Verfügbarkeit des Internets ist nicht Bestandteil dieser SLA.

Onlinezeit Server	betreute Betriebszeit	typischer Servicelevel	garantierter Servicelevel	Bereitschaft
0:00 bis 24:00 365 Tagen / Jahr	Mo - Fr. 8.00 -17:00 Uhr	99,9%	99 %	0:00 bis 24:00 365 Tagen / Jahr

Die Verfügbarkeit einer virtuellen Maschine gilt als gegeben, wenn die entsprechende Serverinfrastruktur aus dem Netz der KRK Computersysteme GmbH erreichbar ist bzw. das Betriebssystem läuft. Die Messung der Verfügbarkeit erfolgt auf Basis der Performance- und Statusüberwachung der Serversysteme. Einzelne, in der Umgebung des Auftraggebers bereitgestellte, Dienste fallen nicht unter diese SLA.

Datensicherung

Das System- und Datenbackup erfolgt über das zentrale Management System des Rechenzentrums. Die Datensicherung erfolgt einmal täglich zwischen 22:00 Uhr abends und 06:00 Uhr morgens, an 7 Tagen in der Woche. Es werden alle bereitgestellten Systeme als Abbild, d.h. Systemumgebung inklusive aller Daten und Konfigurationseinstellungen, gesichert. Der Auftraggeber akzeptiert diese Sicherungen als ausreichenden Ausgangspunkt für Systemwiederherstellungen nach einem Ausfall. Es werden jeweils die Sicherungen der letzten 14 Tage aufbewahrt. Individuelle Sicherungsintervalle und Rücksicherungen auf Anforderung des Kunden, sind nach gesonderter Vereinbarung möglich.

Die **virtuellen** Maschinen werden bei Ausfall oder Datenverlust spätestens innerhalb eines Arbeitstages mit dem Datenstand der letzten Datensicherung (siehe Datensicherung) wiederhergestellt. Im Fall eines Systemausfalls wird in der betreuten Betriebszeit innerhalb von 4 Stunden mit der Wiederherstellung begonnen.

Wartungsfenster

Für periodische, geplante oder ungeplante Wartungsarbeiten an den zentralen Systemen der KRK Computersysteme GmbH und dessen Zulieferern, die für den Erhalt und die Sicherheit des laufenden Betriebes bzw. der Durchführung von Updates oder Upgrades notwendig sind, wird ein Wartungsfenster vereinbart. In der Regel wird eine Systemwartung wöchentlich zwischen 18:00 Uhr und 22:00 Uhr oder nachts, an jedem Wochentag durchgeführt. In Ausnahmefällen kann eine Systemwartung, unter Berücksichtigung der geringsten Beeinträchtigung des laufenden Betriebs, auch in allen übrigen Zeiten durchgeführt werden. Die KRK Computersysteme GmbH informiert den Kunden über geplante Systemwartungen so früh wie möglich.

Die KRK Computersysteme GmbH kann Änderungen an der Software und/oder den Hardware Systemen außerhalb der Wartungsfenster durchführen, wenn diese nicht zur Beeinträchtigung der vereinbarten Verfügbarkeit führen bzw. ein Notfall dieses erforderlich macht.

Eine Wartung der einzelnen Systeme des Auftraggebers erfolgt im Rahmen dieser Arbeiten nicht. Hierzu ist ein entsprechender Wartungsplan gemäß der Leistungsbeschreibung KRK Service Plan abzuschließen.

KRK Cloud Produkte

KRK Cloud Server

KRK stellt seinen Kunden gehostete Serversysteme, auf Basis einer virtuellen Infrastruktur, zur Verfügung, die bei steigenden Anforderungen erweitert und modular ausgebaut werden können. Die Bereitstellung erfolgt auf Basis der, in der Auftragsbestätigung genannten, Leistungsdaten. Folgende Optionen sind möglich

- Ressourcenpool mit frei definierbarer Anzahl und Ausstattung hinsichtlich vCPU, vRAM und Festplattenspeicher
- Frei definierbare Anzahl virtueller Server im Ressourcenpool
- Betriebssystem Windows Server, Linux nach Wahl
- Applikationsserver mit Exchange, SQL, Remote Desktopservices, …
- Betrieb individueller Applikationen
- Eigenes VLAN und öffentliche IP mit Zugriff über VPN oder SSL
- 1x täglich Datensicherung auf Basis der VMs mit 14 Tagen Retention (Erweiterung über optionales KRK Cloud Backup)
- Eigene Firewall / VPN Gateway (optional Upgrade auf UTM Lösung für Spam und Malwareschutz)

Für diesen Dienst besteht die Möglichkeit der Ressourcenzuteilung und Abrechnung sowohl auf Basis der eingerichteten Benutzer als auch auf Basis der genutzten Ressourcen.

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 unser deutsches 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
- Komprimierung und Verschlüsselung mit AES 128-Bit bis Blowfish-448
- 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
- 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. Die Abrechnung erfolgt gemäß unserer Preisliste.

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- 2019
  - Microsoft Office 365
  - Google Apps
  - Alle IMAP- oder POP3-kompatiblen E-Mail-Server
  - MDaemon, IceWarp und Kerio Connect
- Archiviert ein- und ausgehende sowie interne E-Mails
- Schnelle Suche über E-Mails und Dateianhänge
- Ordnerstrukturen aus Outlook werden beibehalten
- Schutz vor Datenverlusten
- Entlastung von E-Mail-Servern
- Reduzierung des Speicherbedarfs um bis zu 70%
- Deduplizierung und Komprimierung
- Vereinfachung von Backup und Restore

  - PST, EML und andere Dateiformate
  - E-Mail-Clients wie Microsoft Outlook
- 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.

KRK Cloud Datenraum

KRK stellt seinen Kunden sichere Alternativen für den Dateiaustausch im Unternehmen zur Verfügung. Bei steigenden Anforderungen können die bereitgestellten Ressourcen erweitert und modular ausgebaut werden. Folgende Optionen sind möglich:

- Verschlüsselung der Datenübertragung nach neuesten Standards
- Speicherung ausschließlich in unserem Rechenzentrum
- SSL gesicherter Webzugriff von überall
- Berechtigungsmanagement auf Benutzerebene
- Active Directory Anbindung
- Logging von Zugriffen u. Änderungen
- Datei Checkout
- Automatischer Virenscan bei Upload
- Sync-Clients für Windows, Mac und Linux
- AddIn für Outlook und Office
- Kostengünstiger Gastzugriff über Webclient
- Mobile Clients für alle gängigen Geräte
- Versionierung und Papierkorb inklusive
- 2 Faktor Authentifizierung

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

Drittanbieter

Bei Bedarf und auf Wunsch integrieren wir Cloud Lösungen weiterer Anbieter wie z.B. Microsoft Office 365 und Azure oder Amazon Web Services in die durch uns bereitgestellten Umgebungen. Für diese Dienste 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. Die Verantwortlichkeiten für die Überprüfung, Kontrolle und Aktualisierung dieser Dienste richten sich nach dem gebuchten KRK Service Plan.

Anlage 1 technische & organisatorische Maßnahmen für KRK Cloud Server

Die Systeme werden 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 Managementsystem des Rechenzentrums durch den Auftraggeber.
- Individuelle Benutzeraccounts für den Zugriff auf das bereitgestellte System durch den KUNDEN.
- Kennwortkomplexität (u.a. Sonderzeichen, Mindestlänge u. regelmäßiger Wechsel des Kennworts).
- Automatische Sperrung (z.B. Kennwort Fehleingaben oder Pausenschaltung).

3. Zugriffskontrolle

Die Zugriffskontrolle wird durch den Auftragnehmer wie folgt sichergestellt:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte).
- 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.
- Protokollierung der ein- und ausgehenden Verbindungen über die Firewall.

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:

- Durchgängige logische Trennung aller bereitgestellten Systeme nach Kunden in separate virtuelle Netzwerke, direkt ab der Perimeter Firewall/VPN Router.

Anlage 2 technische & organisatorische Maßnahmen für die Produkte KRK Cloud Backup, Cloud Datenraum, Cloud E-Mailarchiv

Die Systeme werden 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 auf 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
- 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.

Ansprechpartner

Funktion	Ansprechpartner	Telefon	Email	Bemerkung
IT verantwortlicher beim Auftraggeber				
Vertreter beim Auftraggeber				
Notfallnummer Auftraggeber (24x7)				
Hotline	KRK Service Desk	04271 / 1000 399	Support@krk-computersysteme.de	08:00 – 17:00 Mo. – Fr.
Notfallhotline	KRK Störungshotline	04271 / 1000 888	--	0:00 – 24:00 Mo. – So.
Teamlead RZ KRK	Marco Gerdes	04271 / 1000 308	gerdes@krk-computersysteme.de	nur Eskalation
Geschäftsführung IT Service	Maik Bandolie	04271 / 1000 301	bandolie@krk-computersysteme.de	nur Eskalation
Geschäftsführung IT Sicherheit	Dennis Möllenbruck	04271 / 1000 501	moellenbruck@krk-computersysteme.de	nur Eskalation