KRK COMPUTERSYSTEME

IT-SERVICE | IT-SECURITY | IT-ACADEMY

Leistungsbeschreibung KRK Service Plan

Version 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 3
SLAs 3
Wartungspläne 4
Wartunsplan Basis 4
Wartunsplan Risikomanagement 4
Wartunsplan FullFlat 5
Geräte unter Wartung 5
Ausschlüsse 6
Zusätzliche Dienste 6
Malwareschutz 6
KRK Cloud Backup 7
Anlagen 9
Wartung Halbjahr 9
Wartung Monat / Quartal 11
Technische & organisatorische Maßnahmen für die KRK Support Dienste Fernwartung, Monitoring und Antivirus 13
Technische & organisatorische Maßnahmen für die KRK Online Backup Pläne 15

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 Stunden	4 Stunden	4 Stunden
Reaktionszeit Hoch	24 Stunden	12 Stunden	12 Stunden
Reaktionszeit niedrig	5 Tage	3 Tage	3 Tage
Eskalationszeit 1	Keine	Reaktion x 2	Reaktion x2
Eskalationszeit 2	Keine	Reaktion x6	Reaktion x4
Bediente Servicezeit	09:00 – 17:00	08:00 – 17:00	08:00 – 17:00
Notfallhotline	Kein Zugriff	100,00 € zzgl. Arbeitszeit (07:00 – 20:00 Uhr werktags/Samstag)	100,00 € zzgl. Arbeitszeit (06:00 – 22:00 Uhr an 7 Tagen in der Woche)
Servicelevel On Premise	Kein	98 %	98 %
Servicelevel KRK Cloud Produkte	98 %	99 %	99 %

Wartungspläne

Wartungsplan Basis

Dieser Wartungsplan 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 sowie einen wöchentlichen oder monatlichen detaillierten Bericht zu Ihrem Systemstatus.

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. Wartungsarbeiten führen wir monatlich oder quartalsweise nach Aufwand, gemäß unserem Wartungsprotokoll durch.

Außerdem erfolgt ein halbjährliches Beratungsgespräch zum Status Ihrer IT Systeme.

- 24x7 Monitoring Ihrer Systeme
- Automatische E-Mail Benachrichtigung an den Auftraggeber 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
- Inventarverzeichnis Ihrer Hard- und Software

Wartungsplan 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/Flash, 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 wir mit Ihnen abstimmen.

Des Weiteren sind folgende Leistungen enthalten:

- Monatliche Datenträgerbereinigung Ihrer Systeme
- Aktualisierung der Netzwerk- und USV-Systeme
- Restoretest 2x/Jahr bei gleichzeitiger Buchung Online-Backup/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.

Wartungsplan 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 Garantielaufzeit
- Erweitere Erreichbarkeit unserer Bereitschaftshotline
- Festgelegte Eskalationszeiten bei unternehmenskritischen Problemen
- Flatrate für vor Ort Support

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

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. Unser Wartungsplan 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 Fehler Behebung 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 Wartungsplan FullFlat gebucht wurde.

Durch einen Hersteller von Businesssoftware bereitgestellte, fehlerbehaftete Updates fallen nicht unter die Leistungen der Wartungspläne FullFlat und Risikomanagement, auch dann nicht, wenn diese eingeschlossen sind.

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 alle Fällen nicht durch die Leistungen der Wartungspläne 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 soweit 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 namhafter Hersteller zum Schutz gegen Malware und Datenverlust. Die Verantwortlichkeiten für die Überprüfung, Kontrolle und Aktualisierung richten sich nach dem gebuchten KRK Service Plan.

Malwareschutz

KRK Managed Antivirus Basic

Basierend auf der Avast Engine bieten wir einen Virenscanner mit folgenden Basisfunktionen für Ihre Arbeitsplätze und Server:

- Echtzeit Überwachung

- Zentrale Verwaltung
- Zeitgesteuerte Scans
- Definierbare Scantiefe
- Gerätebezogene Quarantäne

KRK Managed Antivirus Advanced

Basierend auf der Panda Engine 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
- Spam Schutz für Exchange
- Umfassendes Reporting

KRK Managed Antivirus Full Defense

Neben allen Features des Antivirus Advanced Paketes enthält unsere, auf Panda Adaptive Defense basierende, 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.

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
- Duplizierung 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 über Recovery - DB
- Bandbreitenmanagement
- Archivierung von Sicherungen

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.

Anlagen Wartung Halbjahr

Wartungsbericht (Halbjahr)

Patchmanagement (Windows/Office/Adobe/...keine Branchenlösung!)	
Installation durch:	
Patches auf allen Servern installiert	
Patches auf allen Workstations installiert	

Antivirus Check	
Produkt:	
Virenfunde überprüft	
Aktuelle Software im Einsatz	
Alte Einträge/Geräte bereinigt	
Software aktualisiert (mind. 1x jährlich)	

Firewall / UTM		
Produkt:		
Firewall aktiv		
Firewall Regeln geprüft		
Serververöffentlichung geprüft		
Log Dateien geprüft		
Firmware aktualisiert (mind. 1x jährlich)		
Zertifikate laufen ab am:		

Datensicherung	
Produkt:	
Sicherungsmedium:	
Sicherungsjobs to Disk fehlerfrei	
Sicherungsjobs to Tape/RDX fehlerfrei	
Sicherungsjobs to Online fehlerfrei	
Exchange / SQL Logfiles gekürzt	
Software aktualisiert (mind. 1x jährlich)	
Restoretest durchgeführt (Details in Bemerkung)	

Ereignisprotokolle Server	
Prüfung auf Disk Fehler	
Prüfung auf fehlgeschlagene Anmeldungen	

USV	
USV Batterie	
Batteriealter	
USV Selbsttest durchgeführt	

Netzwerk	
Fehlerprotokolle Switche	
Error Counter Ports	
Firmware aktualisiert (mind. 1x jährlich)	

Server	
Temp Dateien gelöscht	
Lüfter Sichtprüfung	
Festplatten Sichtprüfung	
Performance Daten ok	
Server in Garantie	

Active Directory	
Benutzerkonten bereinigt	
Computerkonten bereinigt	

Telefonanlage (nur wenn in Wartung)	
Sichtprüfung Fehler LED	
Prüfung Log	
Firmware aktualisiert (mind. 1x jährlich)	

Organisation

Dokumentation aktuell (Zugänge/IP Adressen/Systemübersicht)	
Wurde in den letzten 12 Monaten ein Lizenzcheck durchgeführt?	
Wurde in den letzten 24 Monaten ein Sicherheitscheck durchgeführt (BSC/Pentest)?	
Gibt es einen Datenschutzbeauftragten?	
Einverständniserklärung Fernwartung und Passwörter liegt vor	

Wartung Monat / Quartal

Wartungsbericht (monatlich)

Patchmanagement (Windows/Office/Adobe/...keine Branchenlösung!)	
Installation durch	
Patches auf allen Servern installiert	
Patches auf allen Workstations installiert	

Antivirus Check	
Produkt:	
Virenfunde überprüft	
Aktuelle Software im Einsatz	
Alte Einträge/Geräte bereinigt	

Firewall / UTM	
Produkt:	
Firewall aktiv	

Datensicherung	
Produkt	
Sicherungsmedium	
Sicherungsjobs to Disk fehlerfrei	
Sicherungsjobs to Tape/RDX fehlerfrei	
Sicherungsjobs to Online fehlerfrei	
Exchange / SQL Logfiles gekürzt	

Ereignisprotokolle Server	
Prüfung auf Disk Fehler	
Prüfung auf fehlgeschlagene Anmeldungen	

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