centron

IaaS so einfach und zugänglich wie möglich machen - für jeden.

centron hilft Unternehmen durch IaaS-, PaaS- und SaaS-Services und -Produkte, die gesamte IT-Infrastruktur auszulagern um sich auf das Wesentliche zu konzentrieren: ihr Geschäft. 1999 wurde centron als Webhosting-Anbieter von Wilhelm und Monika Seucan gegründet und begann 2014 mit dem Bau eines eigenen Rechenzentrums am Standort Hallstadt. 2023 betreut centron mit 50 Mitarbeitern erfolgreich ca. 2400 Kunden weltweit mit Managed Services, Cloud Services, Cloud Lösungen und mehr.

centron Trust Center

Die Sicherheit Ihrer Daten hat für uns höchste Priorität. Zusätzlich zu unseren **eigenen strengen Sicherheitsvorkehrungen** hält sich centron an die hier aufgeführten veröffentlichten **Standards**.

ISO 27001

Die Produkte und Dienstleistungen von centron sind nach der Norm **ISO27001 zertifiziert.** Um die Zertifizierung zu erhalten, musste centron **gegenüber** einem **externen Auditor nachweisen**, dass unsere Infrastrukturdienste die vorgegebenen **Sicherheitsstandards erfüllen.** Die ISO 27001-Zertifizierung zeigt das klare Bekenntnis der centron zum Informationssicherheitsmanagement und stellt sicher, dass adäquate Prozesse vorhanden sind, um das Risiko einer Datenverletzung zu verringern.

ISO 14001

In der heutigen Zeit, in der Umweltbelange höchste Priorität haben, ist es wichtiger denn je, sein **Engagement für Nachhaltigkeit zu demonstrieren**. Das nach **ISO 14001 zertifizierte centron-Rechenzentrum** in Hallstadt, Deutschland, **beweist unser Engagement**, unseren Teil dazu beizutragen.

ISO 9001

Diese Zertifizierung bietet einen Rahmen für die **Implementierung eines Qualitätsmanagementsystems**, das eine konsistente und hochwertige Dienstleistungserbringung gewährleistet. Mit der Zertifizierung zeigt centron sein Engagement für die **Erbringung qualitativ hochwertiger Dienstleistungen, die Einhaltung von Umweltvorschriften und die Umsetzung nachhaltiger Praktiken in** Kombination mit den Vorschriften der ISO 27001 und ISO 14001.

EU GDPR/DSGVO

Die **Einhaltung der DSVGO** ist eine **gemeinsame Verantwortung**. Die Produkte und Services der **centron GmbH bieten** eine breite Palette von **Kontrollen zur Einhaltung der DSGVO**. Wir haben bereits einen sehr hohen Standard an Datenschutzpraktiken für unser Cloud-Produkte und -Dienste , und sehen deshalb die DSVGO als eine Chance, die Praktiken zu verbessern und hat deshalb bei uns höchste Priorität.

Zugangskontrollen

Zugangskontrolle (physisch)

Zugangskontrollsystem

- **Türsicherung** im Bürogebäude
- Zusätzliche **biometrische Zugangssicherung** zum Rechenzentrum und elektronische Türsicherung für **zweistufige Zugangskontrolle**.
- Einrichtung von **Schutzzonen** und **Zugangsregelungen**
- **Besuchsregelungen**
- **360°-Videoüberwachung** des Gebäudeaußenbereichs mit **Sabotageerkennung** und **Aufzeichnung**
- **Videoüberwachung** des Innenraums des Rechenzentrums.
- **Einbruchmeldeanlage** mit **Sicherheitsdienst**

2 baulich getrennte Brand-abschnitte

Maßnahmen, die sicherstellen, dass für unterschiedliche Zwecke erhobene Daten getrennt verarbeitet werden können

- Alle Daten können **getrennt voneinander** verarbeitet werden
- Ausschließliche Verwendung von Software, die **Mandanten-fähigkeit** bietet
- **Trennung** der **Verarbeitungssysteme**
- Trennung der Systeme in **Produktions**- und **Testumgebung**
- Kunden haben **keinen gegenseitigen Zugriff** auf die Systeme

Zugangskontrolle (virtuell)

Maßnahmen zum Schutz der Datenverarbeitungssysteme vor der Nutzung durch Unbefugte

- Erteilung von **Berechtigungen**
- **Protokollierte Vergabe** von Berechtigungen
- Interne **Passwortrichtlinien** werden von MS-AD umgesetzt
- Die **lokalen Systeme** der Mitarbeiter **werden aktualisiert**, **sobald Updates verfügbar** sind
- **Automatische Sperrung**
- **Vorschaltung** einer **physikalischen Firewall** mit IDS und IPS
- Einsatz von **Virenscannern**
- **Physische Trennung** der Netzwerke
- **Überwachung** des **Netzwerkverkehrs**

Übermittlungskontrolle

Übermittlungskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können

- Eine **Übermittlung** von **personenbezogenen Daten** erfolgt **nur auf Anfrage von berechtigten Personen** oder **Institutionen**
- Wenn **personenbezogene Daten** an berechtigte Personen oder Institutionen übermittelt werden, werden sie **verschlüsselt**, nur auf ausdrücklichen Wunsch des Kunden unverschlüsselt übermittelt
- **Datenträger**, die personenbezogene Daten enthalten, **werden mehrfach mit verschiedenen Löschmethoden** bereinigt
- wenn der **Datenträger entsorgt** wird, dann wird der Datenträger **vernichtet** und ordnungsgemäß entsorgt.

- **Protokollierung** der **Systemaktivitäten** durch ein **Überwachungssystem**
- **Teilautomatisierte Auswertung** der Logfiles
- **Protokollierung** aller Arbeiten im ITIL-konformen Ticketsystem
- Neue Personendaten können nur von **autorisierten Personen** eingegeben werden
- Der **Zugriff** auf das Datenverarbeitungssystem wird **protokolliert** (siehe Punkt Zugriffskontrolle).

Zugriffskontrolle

Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, geändert oder entfernt wurden

Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten nur gemäß den Anweisungen des Auftraggebers verarbeitet werden können

- Aufträge von Kunden, die die Verarbeitung personenbezogener Daten verlangen, werden in einem **Ticketsystem** erfasst; für das Ticketsystem ist eine **Zugangskontrolle** eingerichtet
- Elektronische Bestellungen sind nur von **verifizierten Kontaktadressen** möglich
- Aufträge können auch per Post in schriftlicher Form nur über **verifizierte Adressen** versandt werden
- Personen, die Aufträge erteilen, müssen vom Vertragspartner **zur Auftragserteilung ermächtigt** worden sein

Kontrolle der Zuverlässigkeit

Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

- **RAID** (redundantes Schreiben von Daten auf Festplatten)
- **Rhythmus**: täglich oder je nach Kundenwunsch
- **Aufbewahrungsdauer**: redundant, 1-5 Wochen
- **Dateiformat**: binär, proprietär verschlüsselt
- **Speicherort** ist je nach Auftrag das dedizierte Speicher- oder Serversystem des Auftraggebers in eigenen oder fremden Rechenzentren oder das globale Speichersystem des Auftragnehmers
- **RAID** (Spiegelung der Festplatten),
- **redundante Netzteile**
- Regelmäßige **Überprüfung** der **Backups** auf Funktionalität
- Umsetzung des **Katastrophen**- und **Wiederherstellungskonzepts**, **Notfallkonzepts** und **Wiederherstellungsplans**
- **Rechenzentrum**: Unterbrechungsfreie Stromversorgung (**USV**), Notstromdieselanlage, redundante Klimatisierung, Brandfrüherkennungssystem, regelmäßige Brandbekämpfungsschulungen für Mitarbeiter

Zugangskontrolle (intern)

Maßnahmen, die sicherstellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die Daten zugreifen können, für die sie eine Zugangsberechtigung besitzen

- Das Passwort wird nur von **autorisiertem Personal** an **vom Auftraggeber benannte Personen** ausgegeben
- Die Kommunikation von Anweisungen erfolgt auf Seiten des Auftragnehmers über ein **ITIL-konformes Ticketsystem**
- Die Berechtigung zur Verarbeitung personenbezogener Daten wird über das **Active Directory** gesteuert und protokolliert
- **Protokollierung** der **Anmeldungen** an den Systemen
- **Vernichtung** von **Datenträgern** nach dem **Datenträgervernichtungskonzept**

centron Managed Backup

Was wird gesichert?

Gesichert werden **Datenträger** (**HDD, SSD, etc.**) des Betriebssystems, alle anderen **Datenträger** und **Partitionen** oder auch komplette **Exchange-Datenbanken**. Von anderen Datenbanken werden **täglich Dumps** erzeugt, die - je nach Größe - **bis zu sieben Tage** lokal auf dem System verbleiben.

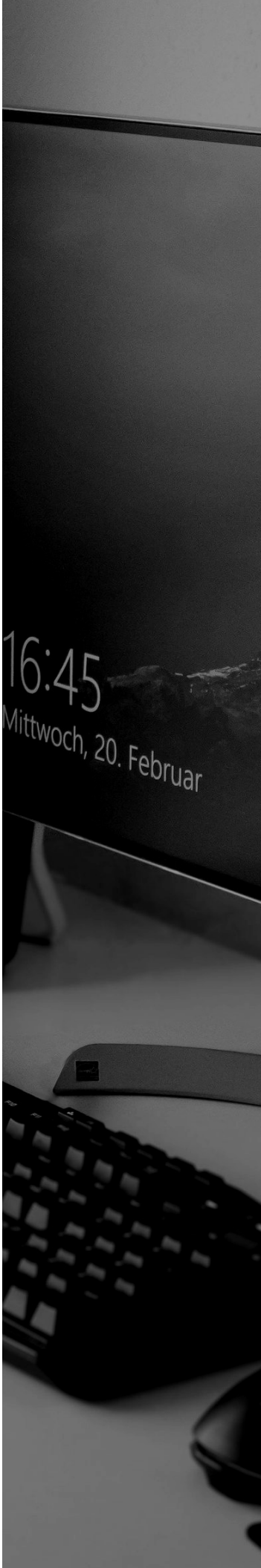
Auf diese Weise gewährleisten wir eine **noch schnellere Wiederherstellung**. Diese Dumps werden ebenfalls im **täglichen Backup** gehalten. **Temporäre Daten sind** davon **ausgenommen**, da diese im Betrieb vom System selbst erzeugt werden und für eine Wiederherstellung nicht relevant sind. Hiervon abweichende Vereinbarungen werden wir in einem gemeinsamen Gespräch festhalten.

Wohin geht mein Backup?

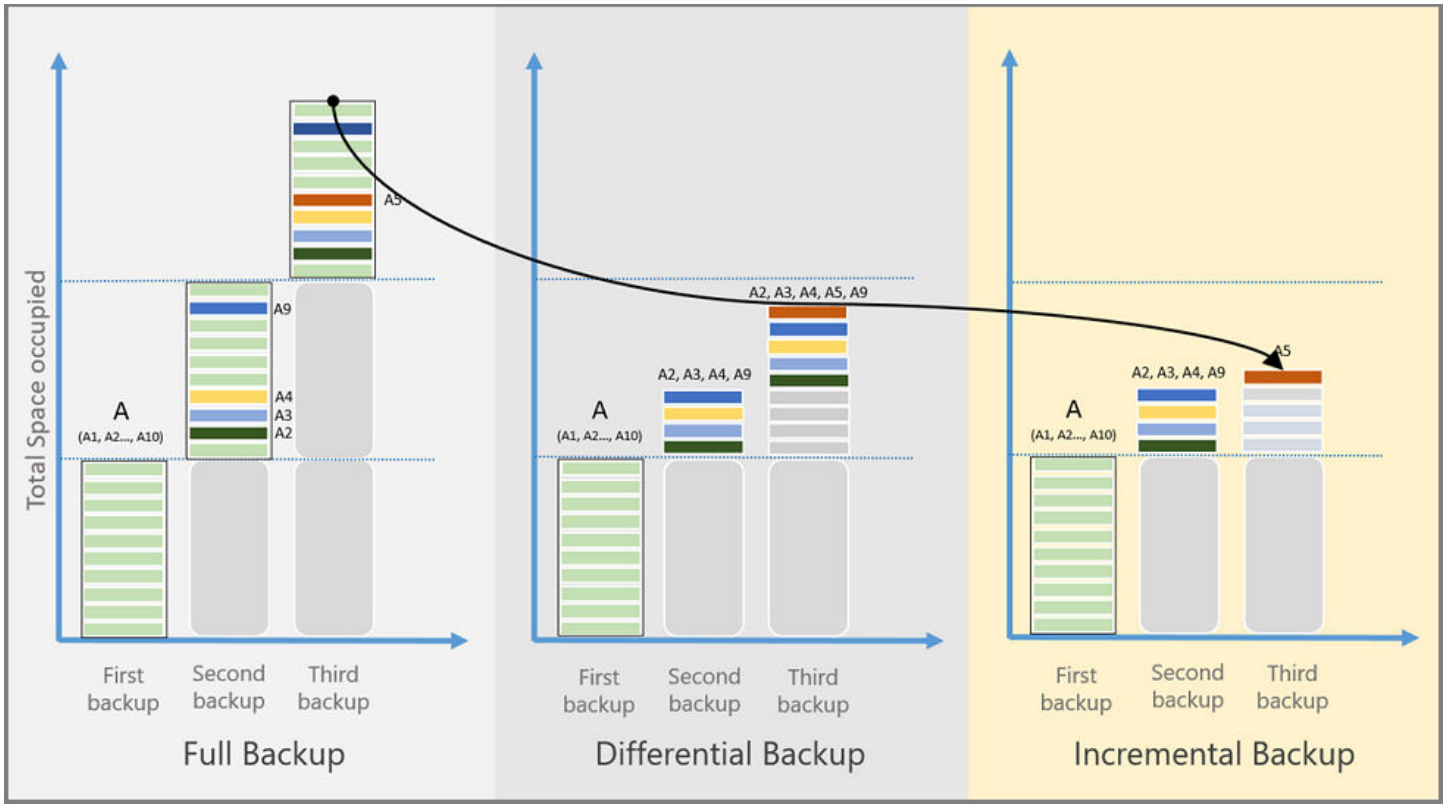
Um das Risiko physikalischer Einflüsse zu minimieren, werden die **Sicherungsdaten** bei centron **auf mindestens einen anderen Brandschutzstandort** des Rechenzentrums gespiegelt. Sollte Ihr System einen Hardwareschaden aufweisen, kann Ihre Datensicherung auf Ersatzhardware erstellt werden. Es besteht auch die Möglichkeit, Ihr Backup in ein zweites Rechenzentrum auszulagern (**redundante Speicherung**).

Wie wird gesichert?

Bei centron werden die Backups der Systeme nach dem **Generationenprinzip**, auch bekannt als **Großvater-Vater-Sohn-Prinzip**, gespeichert. Das bedeutet **eine monatliche Vollsicherung** Ihres Systems, auf der **wöchentliche** und **tägliche Sicherungen** aufbauen. Diese Sicherheitskette wird bis zum Erreichen ihres Verfallsdatums (EOL = End Of Life) aufbewahrt. Wenn ein Fehler in einer Datei erst später entdeckt wird, ist es möglich, eine andere als die letzte Version wiederherzustellen. Dabei handelt es sich jedoch nicht um eine Versionsverwaltung.



centron Managed Backup



alle 4 Wochen	wöchentlich	täglich
Vorhaltezeit: 4 Wochen	Vorhaltezeit: 2 Wochen lang ab dem letzten Vollbackup	Vorhaltezeit 1 Woche

centron Backup-as-a-Service

Dank unserer **neuen Backup-Landschaft** können wir Ihnen die Sicherung Ihrer Daten **zuverlässig**, **ressourcenschonend** und **kostengünstig** anbieten. Im Hinblick auf die Datensicherung haben Sie folgende Möglichkeiten:

- Absicherung in einem **anderen Brandabschnitt** (standardmäßig konfiguriert)
- **Exklusives Ziel** für Ihre Serverlandschaft
- **Georedundante Backups** an verschiedenen Standorten

Unsere Backup-Infrastruktur ist durch strenge Netzwerksicherheitsmaßnahmen von den produktiven Systemen der centron getrennt. Die produktive Infrastruktur wird selbst gesichert und in regelmäßigen Abständen durch Restore-Tests überprüft.

Contact

centron GmbH
Heganger 29
96103 Hallstadt, Deutschland
Phone: +49 951 968340
E-mail: info@centron.de
Website: https://www.centron.de

Copyright