CGM Clinical Deutschland GmbH

CGM CLINICAL DE Systeminformationen - Allgemeine Informationen - 2019-Q3

Synchronizing Healthcare

© CGM Clinical Deutschland GmbH 2019 | Seite 1/34 21.05.2019

CompuGroup Medical

INHALT

Hardware

Nachfolgend werden Beispielkonfigurationen anhand durchschnittlicher Erfahrungswerte für die Produkte dargestellt. Individuelle Faktoren, wie die Anzahl der Benutzer, gleichzeitige Zugriffe, zusätzliche Applikationen oder Datenbanken sind nicht berücksichtigt. Daher ist die Erstellung eines Feinkonzeptes zur Dimensionierung der Hardware notwendig. Auf diese Weise sind sowohl eine reibungslose Einführung und der laufende Betrieb gesichert.

Beispielkonfiguration für CGM REHA

Hardware/Virtuelle Hardware	Typ	RAM	HDD	Bemerkung
Arbeitsstation	Intel® Core™ i5/i7	>4 GB	100 GB	
Terminal/Citrix-Server	4 Core	16 GB	150 GB	max. 25 User
Anwendungsserver	8 Core	12 GB	200 GB	
G3-Anwendungsserver	8 Core	32 GB	200 GB	
Datenbankserver MSSQL	4 Core	48 GB	425 GB	SSD-Festplatten
G3-Webserver	4 Core	8 GB	150 GB	
Kommunikation/Druckserver	4 Core	8 GB	150 GB	

Beispielkonfiguration für CGM CLINICAL

Hardware/Virtuelle Hardware	Typ	RAM	HDD	Bemerkung
Arbeitsstation	Intel® Core™ i5/i7	>4 GB	100 GB	
Terminal/Citrix-Server	4 Core	16 GB	150 GB	max. 25 User
Anwendungsserver	8 Core	24 GB	150 GB	
G3-Anwendungsserver	8 Core	32 GB	200 GB	
Datenbankserver MSSQL	4 Core	48 GB	425 GB	SSD-Festplatten
Kommunikation/Druckserver	4 Core	8 GB	150 GB	

Beispielkonfiguration für CGM JESAJANET

Hardware/Virtuelle Hardware	Typ	RAM	HDD	Bemerkung
Anwendungsserver DMZ-Zone	4 Core	16 GB	200 GB	Inkl. IIS
Anwendungsserver PDTZ-Zone Inkl. MSSQL	8 Core	32 GB	500 GB	SSD-Festplatten
Anwendungsserver LAN-Zone Inkl. MSSQL	8 Core	32 GB	500 GB	SSD-Festplatten

Netzwerkprotokolle

Die Anbindung der Clients erfolgt in einem lokalen Netzwerk unter Verwendung des TCP/IP-Protokolls. Anbindungen über WAN-Strecken sind mittels TCP/IP ebenfalls möglich. Entscheidend für die Performanz und Stabilität sind die verwendeten Bandbreiten. Im lokalen Netzwerk muss eine Mindestbandbreite von 100 Mbit/s bis zu den Arbeitsplätzen vorhanden sein. Bei der Verwendung von Terminalserverkonzepten sind je nach Ausbaustufe sog. BackBones von min. 1 Gbit/s bzw. 10 Gbit/s empfehlenswert. Die notwendigen Bandbreiten bei Anbindung über WAN-Strecken hängen stark von dem verwendeten Client-Konzept, sowie von den anwendungsspezifischen Datenmengen ab. Daher muss dies im Einzelfall in enger Abstimmung mit der CGM Clinical geschehen. Bei Architekturen im Citrix XenApp-Umfeld gilt die Empfehlung von 128Kbit pro Arbeitsplatz / Anwender des jeweiligen Standortes, die im durchschnittlichen Regelbetrieb mit CGM Clinical Applikationen arbeiten. Empfehlenswert sind im Einzelfall Tools zum Bandbreitenmanagement, um vor allem Performanz-engpässe beim Abarbeiten von großen Druckaufträgen zu vermeiden.

Virtuelle Umgebungen

Die Architektur der CGM Clinical Software ermöglicht den Einsatz innovativer Serverkonzepte. Hierzu zählt beispielsweise die Server-Virtualisierung.

Beim Einsatz von virtuellen Umgebungen wie beispielsweise VMware, MS-HyperV oder Citrix XenServer weisen wir ausdrücklich auf die Freigabehinweise sowie technischen Informationen der Hersteller hin. (Hersteller z.B.: Hewlett-Packard, Fujitsu, Microsoft, Oracle, Citrix und VMware)

Eventuelle Einschränkungen der Hersteller bzw. besondere Verfahren im Supportfall bei virtuellen Umgebungen gelten uneingeschränkt auch für Systeme aus unserem Hause.

Drucken in Terminalserver-Umgebungen

Druckprobleme

Das größte Problem stellt die mangelnde Unterstützung der Hersteller für Terminalserver-Umgebungen dar. Druckertreiber werden für die gängigen Windows-Betriebssysteme entwickelt und beinhalten eine Vielzahl von Komfortfunktionen, die in einer Terminalserver-Umgebung nicht benötigt werden, aber einen Großteil der Probleme verursachen.

Für den Einsatz unter Terminalservern würde ein sogenannter Mini-Treiber vollkommen ausreichen. Diese Treiber werden aber nur von den wenigsten Herstellern zur Verfügung gestellt.

Aus diesem Grunde hat die CGM Clinical Deutschland GmbH eine **Printing Policy** definiert, welche Ihnen helfen soll, den richtigen Druckertreiber zu finden und zu verwenden.

Druckertreiberauswahl

Folgende Punkte sollten Sie in jedem Falle bei der Wahl eines Druckers bzw. Druckertreibers beachten:

- Verwenden Sie keine Tintenstrahldrucker.
  - diese Drucker sind HOST-BASED Drucker => diese Drucker verwenden den Prozessor des PCs bzw. Serversystems zur Abarbeitung des Auftrages. Dadurch werden die verfügbaren Systemressourcen eines Terminalservers stark dezimiert
  - die verwendeten Treiber verursachen die meisten Probleme aufgrund ihrer Menge an Funktionen

- Verwenden Sie immer den Treiber, der durch das **Betriebssystem** mitgeliefert wurde.

- Sollte kein passender Treiber für Ihren Drucker vorhanden sein, verwenden Sie einen kompatiblen Druckertreiber des Betriebssystems. Die meisten Laserdrucker sind mit dem HP Laserjet 4 oder 5 (PCL-Druckersprache) kompatibel. In Einzelfällen fragen Sie bitte beim Hersteller nach.

- Als letzte Instanz kann der Druckertreiber des Herstellers verwendet werden. Suchen Sie auf der Homepage des Herstellers zuerst immer nach einem Mini-Treiber (beinhaltet nur die notwendigsten Komponenten) oder Terminalserver-Treiber.

Prüfen Sie eine eventuelle Kompatibilität oder Freigabe immer vor Kauf eines neuen Druckers!

Beschränken Sie die Anzahl unterschiedlicher Druckerhersteller und Modelle auf ein Minimum!

Drucken in Terminalserver-Umgebungen

Freigaben

Hersteller	Link/Download
HP	Citrix Support Artikel CTX110571
Kyocera	bei Kyocera gibt es sogenannte Classic Mini Treiber. Ausschließlich diese Treiber verwenden, die KX Treiber beeinflussen Ihre Systemumgebung
Lexmark	Knowledge Base Lexmark
Ricoh/Aficio	bei Ricoh/Aficio gibt es auch sogenannte Mini-Treiber **Achtung:** den Mini-Treiber gibt es nicht für alle Druckertypen

Technische Hinweise zur Fernwartung bei CGM Clinical

Allgemeines

Zur Erbringung von Supportleistungen wie Fehlerbeseitigung, Unterstützung, Systemanpassung, Migration etc. ist es erforderlich, dass die CGM Clinical im Rahmen der Vertragsbeziehungen zeitweise Zugriff auf produktive Netze und Systeme von Kunden erhält, damit diese auf Protokollebene erreichbar und administrierbar sind. Diese Zugriffsmöglichkeiten dienen der schnellen, effektiven und unkomplizierten Unterstützung aus der Ferne.

Die in diesem Dokument beschriebenen Verfahren sind die unterstützten Standard Methoden zur Fernwartung, welche auch durch die ISO 27001 Sicherheitsnorm zertifiziert sind. Alle davon abweichenden Methoden werden durch die CGM Clinical nicht supportet und sind nicht in die ISO 27001 Zertifizierung mit integriert, d.h. die CGM Clinical kann hier keine Zusagen zu Vertraulichkeit, Verfügbarkeit und Integrität machen.

Der Standard - Fernwartung per VPN

Als Zugangsmethode wird bei der CGM Clinical die Verbindung zum Kundennetz über das Internet mittels eines verschlüsselten VPN Tunnels hergestellt. Dabei wird über zwei VPN Geräte mittels des Standards IPSec eine sichere Verbindung hergestellt

Hersteller	Link/Download
Technische Voraussetzungen	IPSec kompatible Hardware Internetanschluss mit fester IP Adresse für das VPN Gerät
IPSec Parameter	Mind. 3DES Verschlüsselung, DH Group 2, SHA-1 Verwendung von Pre-Shared Keys
Zugriff	Freier Zugriff auf gewünschte Zielsysteme für die IP Adresse 10.143.167.10
CGM Clinical Hardware	z.B.: Cisco Firewall ASA 5510

Zugangssoftware für VPN Fernwartung

Zum Zugriff auf die gewünschten Systeme nach Herstellung der Verbindung über VPN oder ISDN werden verschiedene Software Tools verwendet

Client-Server	Software-Version
	TeamViewer

Terminal-Server	Software-Version
Mindestens	Microsoft® Terminalserver-Remotedesktop-Client

Implementierung VPN & ISDN Fernwartung durch die CGM Clinical

Es können bestehende Internet Strukturen durch den Einsatz von Standards zur Implementierung der Fernwartung verwendet werden.

Zur vollständigen Unterstützung von Kunden, bietet die CGM Clinical auch die Möglichkeit, preisgünstig die komplette Struktur mittels bewährten Cisco Hardware Geräten zu besorgen, zu installieren und dafür den Support zu leisten.

Sicherheit

Der komplette Prozess der CGM Clinical wurde nach sicherheitsrelevanten Aspekten untersucht und angepasst. Relevante Aspekte der Sicherheit für Kunden sind:

Transparenter Zugriff

Die CGM Clinical empfiehlt die Möglichkeit der Abschaltung des Fernwartungszugriffes bei Nicht-Bedarf einzuführen. Dies kann z. Bsp. bei VPN Devices durch die Verwendung von Skripten geschehen. Dadurch werden Zugriffe auf Kundensysteme erst nach Rücksprache mit dem verantwortlichen Ansprechpartner freigeschaltet. Die Implementierung solcher Maßnahmen liegt im Ermessen des Kunden, wobei die CGM Clinical bei der Implementierung gegebenenfalls Unterstützung leisten kann.

Authentifizierung

Beim Zugriff auf die VPN Fernwartungsstruktur müssen sich interne Mitarbeiter erfolgreich authentifizieren, bevor der Zugriff auf Kundendaten möglich ist. Dadurch wird gewährleistet, dass nur CGM Clinical Mitarbeiter bei Kunden zugreifen können.

Protokollierung

Alle Verbindungen und Authentifizierungen werden protokolliert, wodurch eine spätere Überprüfung des Zugriffes möglich ist.

Sicherheit TeamViewer

Da beim Zugriff mit TeamViewer der Kunde erst selbstständig die Verbindung initiieren muss, ist eine Kontrolle des Zugriffes stets gegeben.

Betreiberverantwortung

Allgemeine Informationen

Eine stabile und gut gewartete IT-Infrastruktur ist eine wichtige Grundvoraussetzung zur Sicherstellung eines performanten und störungsfreien Betriebs von unternehmenskritischen Anwendungen der CGM Clinical Deutschland GmbH.

Nach erfolgreicher Installation und Konfiguration durch unsere Spezialisten geht die weitere Administration und Überwachung normalerweise an den Kunden über. Die daraus resultierenden notwendigen Maßnahmen lassen sich in verschiedene Kategorien und Aufgabenfelder zusammenfassen.

Jedes dieser Aufgabenfelder kann auch im Bedarfsfall an externe Spezialisten ausgelagert werden, gerne natürlich auch an unsere Spezialisten der IT Solutions und Services GmbH.

Das vorliegende Dokument fasst die wesentlichen Aufgaben aus Sicht der CGM Clinical-Anwendung zusammen und dient der Unterstützung zur Organisation und Strukturierung der entsprechenden Zuständigkeiten unserer Kunden. Die genannten Punkte stellen dabei lediglich Empfehlungen dar, kundenindividuell können daneben weitere Aufgaben notwendig sein, die hier nicht betrachtet werden können.

Systems Management

Zur Überwachung und Monitoring der IT-Infrastruktur ist ein ständiger Überblick über alle Ressourcen unbedingt erforderlich. Drohende oder bereits eingetretene Engpässe bei der Verfügbarkeit von Ressourcen müssen zeitnah erkannt und durch geeignete Maßnahmen behoben werden. Daneben müssen Fehlverhalten von Prozessen erkannt und behoben, sowie ausgefallene Prozesse bei Bedarf neu gestartet werden. Die Störungserkennung kann beispielsweise durch ständiges Überwachen von Log-Einträgen sichergestellt werden, zur Behebung stehen verschiedene Reaktionsmöglichkeiten zur Verfügung, beispielsweise von der automatisierten Benachrichtigung der IT-Mitarbeiter bis hin zu einer automatisierten Störungsbeseitigung (z.B. Virenscanner) zur Verfügung.

Zur Unterstützung dieser teilweise aufwändigen Tätigkeiten wird der Einsatz von System-Management-Werkzeugen empfohlen. Diese bieten neben vorkonfigurierten und automatisierbaren Überwachungsmodulen auch ausgefeilte Kommunikationsmodule zur zeitnahen Benachrichtigung der zuständigen Mitarbeiter an.

Reporting

Zur Beurteilung der Ressourcenauslastung sowie der Systemverfügbarkeit sind regelmäßige und standardisierte Reports und Statistiken unerlässlich. Diese sollten sowohl die Leistungsparameter der Systeme, wie Auslastung, Ressourcenverbrauch, Verfügbarkeit etc., als auch eine Statistik über alle festgestellten Problem- und Störungsmeldungen umfassen.

Dokumentation

Eine umfassende Dokumentation über sämtliche Eigenschaften der IT-Infrastruktur ist wesentliche Voraussetzung zur schnellen und gezielten Analyse, Lokalisierung und Behebung von Störungen. Die Dokumentation sollte möglichst graphisch aufbereitet und muss bei Änderungen unbedingt aktualisiert werden. Sie ist auch eine wichtige Unterstützung bei Entscheidungen für mögliche Erneuerungen bzw. Erweiterungen.

Betriebsführungshandbuch

Zur transparenten Dokumentation aller notwendigen Abläufe sowie organisatorischen Vorkehrungen und Zuständigkeiten wird das Führen eines Betriebshandbuches empfohlen. Neben den Festlegungen für die Betriebsführung, die zeitlichen Abstände der verschiedenen Maßnahmen etc. werden dort vor allem auch die Prozesse des „Change-Managements“ festgelegt.

Service-Verträge/Hotline

Zur Sicherstellung der unmittelbaren Unterstützung bei komplexen System-Störungen durch kompetente Spezialisten sowie der zeitnahen Analyse und Behebung von Hardwareproblemen wird der Abschluss sowie die fristgerechte Prüfung und ggf. Verlängerung von Serviceverträgen und Hotline-Vereinbarungen dringend empfohlen.

Produktiver Betrieb der Systeme

Betrieb Server-Systeme

- Überwachung aller Serversysteme
  - Zentrales Rechnersystem (z.B. CPU, I/O, HW-Komponenten, etc.)
  - Festplatten-Subsystem (z.B. Plattenauslastung, -Zugriffszeiten, Swap-Space)
  - Netzwerk-Parameter (z.B. IP-Adressierung, DHCP, DNS, WINS)
- Überwachung von Server-Funktionen
  - Standard-Dienste (z.B. Anmeldedienste, Serverdienste)
  - Printing (z. B. Printer-Queues)
  - Netzwerk-Dienste (z.B. DHCP, DNS, WINS)
- Analyse der Serverprotokolldateien auf Probleme oder Fehler
- Überwachung der Kapazität auf den Datenträgern
- Überprüfung und Überwachung der USV-Komponenten
- Einspielen von Servicepacks, Hotfixes oder Patches
- Reorganisation, Löschung und Archivierung von Datenträgerinhalten
- Aktualisierung der aktuellen Anti-Viren-Pattern-Files
- Einrichtung von Druckern (neue Drucker, Berechtigungen, Drucker-Queues)
- Einstellungen der spezifischen Druckeransteuerungen von den Client-Systemen aus
- Optimierung/Tuning-Parameter
  - Anpassung der Systemparameter für Auslagerungsspeicher, Datenträger, etc.
  - Analyse der Reports und Performancedaten zur Ermittlung von notwendigen Systemerweiterungen, Aufrüstungen und Auslagerung von Anwendungen

  - Defragmentierung von Datenträgern und Datenträger-Überprüfungen

Betrieb Backup-Mechanismen

- Überwachung der Backup-Hardware
- Auswertung von Sicherungsprotokollen und -logfiles
- Wechsel und Aufbewahrung der Datensicherungsmedien
- Konsistenzprüfungen nach Recovery
- Durchführen von Recovery-Tests

Betrieb Datenbank-Management-System

- Datenbank- und Instanz-Überwachung
  - Alert- und Trace-Files
  - Überwachung des Wachstums der DB-Ressourcen (z.B. Tablespaces, Tabellen, Archive-Filesystem)
- Performance- und Ressourcenüberwachung
  - I/O-Verhalten
  - Zugriffszeiten
  - Hit-Cache-Ratio
  - Connections
- Parameteranpassungen DB-Instanz
- Erweitern von Tablespaces
- Organisation und Pflege des Archiv-Filesystems
- Einspielen von Servicepacks, Hotfixes und Patches
- Reorganisation von DB-Objekten (z.B. Defragmentierung, Rebuild der Indizes)
- (Online-)Sicherung der Datenbanken
- Recovery-Tests

Betreuung Standard-Applikationen

- der Administration ADS/Domänenkonzept (z.B. Loginscripts, Policies, Berechtigungen)
- Administration Citrix- und Terminalserver-Umgebung (z.B. Loadbalancing, Published Applications, Profile)

Betrieb der Security- & Firewall-Struktur

- Überwachen und Sicherstellen von Security-Policies
- Administration Firewall (z. B. Cisco-PIX, KV-Connect, KV-SafeMail, CGM Connect)

Netzwerk-Betreuung

- Überwachung aller managebaren Komponenten im Netzwerk
- Verwalten der LAN-Verbindungen
- Verwalten der Router-Konfiguration
- Diagnose bei Störungen im Netzwerk
- Administration von VPN-Leitungen mit laufender Funktionsprüfung

Weitere produktspezifische Aufgaben

Betrieb Management CGM REHA-System

- Überwachung der CGM REHA-Dienste (z.B. CGM REHA Leistungsjob, CGM REHA DW-Dienste, CGM REHA Druck-Spooler, CGM LMZ Disposerver, CGM LMZ Service, CGM LMZ ServiceNext)
- Durchführen und Überwachen von Reorg-Maßnahmen (z.B. temp. Tabellen löschen, Zugriffe optimieren)
- Überwachung der Schnittstellen
- Überwachung der Kommunikationsserver (Com4Cure ehemals ProSoft)
- Überwachung der BediOnline-Konnektivität (XReha)
- Konfiguration von Usern und Berechtigungen
- Einspielen von neuen Releases, Servicepacks, Hotfixes und Patches der CGM REHA-Softwaremodule
- Installation und Konfiguration von CGM REHA-Clients

Einspielen von Servicepacks, Hotfixes und Patches von CGM REHA Partnersystemen nach Freigabe in CGM REHA (z.B. Com4Cure ehemals ProSoft, DRGScout, KodipSuite, DIACOS)

Empfehlungen zum Reboot von Windows Server Systemen

Die Notwendigkeit von regelmäßigen Server-Neustarts (reboot) ist weniger in unserer Software begründet als vielmehr in der Systemarchitektur von Windows. Im Gegensatz zu anderen Betriebssystemen wie z.B. Unix werden dort die Systemressourcen leider nicht vollständig gekapselt und können bei einem Fehler, sei es aufgrund eines Programmabsturzes oder auch aufgrund systembedingter Fehlfunktionen, vom Windows-Betriebssystem nicht immer vollständig freigegeben werden. Durch eine lange Laufzeit des Systems werden damit Systemressourcen immer knapper, was sich leider oft auch auf die Performance des gesamten Systems oder auch nur auf Teilbereiche auswirkt. Nach einem System-Neustart werden diese Ressourcen normalerweise wieder freigegeben, können von den Anwendungen wiederverwendet werden und tragen damit wieder zu einer besseren Performanz und teilweise auch Stabilität des Systems bei.

Auch wenn Microsoft die Notwendigkeit von regelmäßige System-Neustarts zumindest auf Marketing-Ebene teilweise verneint und auf die hohe Systemverfügbarkeit aufgrund neuer Architekturen verweist, zeigt doch die Erfahrung, nicht nur in unserem Hause, dass regelmäßige Reboots leider auch weiterhin notwendig sind. Der Aufwand für solche Reboots hält sich dank der Verfügbarkeit von automatisierbaren sog. Tasks in Grenzen.

Die Sicherstellung eines performanten und stabilen Systems gehört zu den Betreiberaufgaben und sollte daher vom Kunden durchgeführt und überwacht werden. Wir sprechen hier nur die Empfehlung aus, die Server im Interesse unserer Kunden regelmäßig neu zu starten. Eine Empfehlung, die im Übrigen auch von anderen namhaften Software-Herstellern wie Citrix etc. kommt und welche auch in verschiedenen Foren immer wieder auftaucht. Gerne sind wir natürlich bereit, im Rahmen von

Outsourcing-Verträgen die Administration sowie Überwachung ihres Systems teilweise oder auch komplett zu übernehmen. Sollten Sie hierzu Bedarf haben, so wenden Sie sich bitte an Ihren Ansprechpartner aus unserem Haus.

In der folgenden Tabelle sind unsere Empfehlungen aufgeführt:

Servertyp	Reboot empfohlen	Warum
Citrix / Terminalserver	JA (mind. 1x pro Woche)	Speicherfragmentierung
Domaincontroller	NEIN	
Fileserver	NEIN	
reiner Datenbankserver	NEIN	
Datenbankserver mit Applikation	JA (1x pro Monat)	alte Prozesse und Threads beenden
Applikationsserver	JA (1x pro Monat)	alte Prozesse und Threads beenden
Printserver	JA (mind. 1x pro Woche)	alte Druckaufträge löschen, Speicherfragmentierung
Exchange Server	JA (1x pro Monat)	Queues leeren, Speicherfragmentierung

Grundlagen Datensicherung

Die hier zusammengestellten Informationen sind auszugsweise dem IT-Grundsatzhandbuch des BSI entnommen.

Regelmäßige Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, IT-Benutzer

Um den eventuellen Verlust von Daten zu verhindern ist es notwendig regelmäßig Datensicherungen durchzuführen. Um den genauen Umfang der zu sichernden Daten und den zugehörigen zeitlichen Rahmen festzulegen wird ein Datensicherungskonzept erstellt. Das Datensicherungskonzept enthält auch den, oder die für die Sicherung verantwortlichen Mitarbeiter, der oder die sich auch um die Verwaltung der Speichermedien kümmert. Dieses wird weiterführend im Bänderverwaltungskonzept beschrieben. Die Durchführung der Datensicherung erfolgt in den meisten Fällen vollautomatisch.

Vor Erstellung des Datensicherungskonzeptes sind folgende Punkte festzulegen:

- Zeitintervall
  Beispiele: täglich, wöchentlich, monatlich,
- Zeitpunkt
  Beispiele: nachts, freitags abends,
- Anzahl der aufzubewahrenden Generationen,
  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate.
- Umfang der zu sichernden Daten
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.
  Beispiel: Selbsterstellte Dateien und individuelle Konfigurationsdateien.
- Speichermedien (abhängig von der Datenmenge)
  Beispiele: Bänder, Backup-To-Disk
- Vorherige Löschung der Datenträger vor Wiederverwendung
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollen zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. (Werden zwischen zwei Komplettsicherungen mehrere

inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.)

Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist in der Regel die Aufbewahrung der Originaldatenträger und deren Sicherungskopien ausreichend. Sie braucht dann von der regelmäßigen Datensicherung nicht erfasst zu werden.

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Datensicherungsplan

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Mit Hilfe des Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.

Ein Datensicherungsplan muss Auskunft geben können über:

- Speicherungsort der Daten im Normalbetrieb (Plattenspeicher-Belegungsplan),
- den Bestand der gesicherten Daten (Bestandsverzeichnis),
- die Zeitpunkte der Datensicherungen,
- Art und Umfang der Datensicherung (logische/physikalische, Teil-/Vollsicherung),
- das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
- den Ort der Aufbewahrung (Hinweis auf ggf. erforderliche Zutrittsmittel).

Ersatzbeschaffungsplan

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Um die im Falle eines Ausfalles notwendige Ersatzbeschaffung eines Teiles des IT-Systems durch den Verantwortlichen oder einen stellvertretenden Dritten zeitnah zu ermöglichen ist es notwendig einen Ersatzbeschaffungsplan zu erstellen.

Dieser muss die folgenden Angaben enthalten:

Übersicht über alle Teile des mit der Datensicherung verbundenen IT-Systems mit Angaben zu

- Produktbezeichnung
- Hersteller
- Seriennummer
- Kaufdatum
- Support-Hotline
- Support-Vertrag (sofern vorhanden)
- Lieferant
- Desaster Recovery für die Teilkomponente

Ersatzbeschaffungen müssen auch die technische Fortentwicklung der Teilkomponente berücksichtigen, da die Wiederherstellung des ursprünglichen Zustandes nicht ausschließlicher Zweck der Anschaffung ist. Aus diesem Grunde ist auch eine regelmäßige Überprüfung des Planes notwendig.

Für besondere kritische Systeme ist es eventuell notwendig ein entsprechend ausgestattetes Zweitgerät in einem separaten Raum oder Gebäude einsatzbereit vorzuhalten.

Dokumentation der Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich. So ist bei der Erstellung der Datensicherung für jedes IT-System zu dokumentieren:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.)

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes. Auch hier muss eine Beschreibung der erforderlichen Hard und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

Geeignete Aufbewahrung der Backup Datenträger

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Benutzer

Folgende Punkte sind in Hinblick auf die Aufbewahrung der Sicherungsdatenträger zu beachten:

- Die Sicherungsdatenträger sind nur autorisierten Personen zugänglich zu machen.
- Für den Katastrophenfall muss sichergestellt sein, dass Datenträger räumlich getrennt vom IT-System aufbewahrt werden müssen, wenn möglich in einen anderen Brandabschnitt.
- Der schnelle Zugriff auf die Datenträger muss gewährleistet sein.
- Die Aufbewahrungsvorschriften des Herstellers müssen eingehalten werden.

Datenträgerverwaltung

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Archivverwalter, IT-Verfahrensverantwortlicher

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben Auskunft über: Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der **Aufbewahrung** von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Der Versand oder Transport von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten

(z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, dass mit dem zugrunde liegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist. Weiterhin ist zu beachten, dass vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird.

Für die interne Weitergabe von Datenträgern können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muss die Löschung der gespeicherten Daten vorgenommen werden.

Überprüfung der Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung

Um die Wiederherstellung der Daten im Bedarfsfall sicherzustellen ist es notwendig, die gesicherten Daten zu verifizieren. Dies muss auf zwei Arten erfolgen.

Lesbarkeit der Daten

Unmittelbar nach dem Erstellen der Datensicherung ist der Inhalt des Datenträgers durch einen Lesevorgang zu Überprüfen. Dies kann in den meisten Fällen durch die eingesetzte Sicherungssoftware automatisch durchgeführt werden.

Wiederherstellbarkeit der Daten

Die Funktionsfähigkeit der Sicherungssoftware sowie die Qualität der Datenträger muss durch regelmäßige Wiederherstellung der Daten nachgewiesen werden

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss sporadisch, zumindest aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten ggf. auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

Datensicherung bei mobiler Nutzung des IT-Systems

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team, Leiter IT

Verantwortlich für Umsetzung: Administrator, IT-Benutzer

IT-Systeme im mobilen Einsatz (z. B. Laptops, Notebooks) sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

Datensicherung auf externen Datenträgern

Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk mitgeführt werden muss, und dass für den Benutzer zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhandenkommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhandenkommen.

Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können u. U. kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.

Datensicherung über temporäre Netzverbindungen

Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.

Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z. B. VPN, ISDN) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen.

Datensicherung Windows Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

- Die Sicherungssoftware ist in der Lage, wichtige Systemdateien, wie die Registry des lokalen Rechners, die COM+ Registrierungen sowie die Startdateien, zu sichern. Dies sollte in regelmäßigen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden. Dazu sind unter der Option *Systemstatus* die jeweiligen Auswahlboxen zu aktivieren.
- Auf Domänen-Controllern können zusätzlich auch die Active Directory Daten gesichert werden. Dies sollte bei jedem Backup durchgeführt werden. Die relevanten Optionen sind auf Domänen-Controllern ebenfalls unter der Option Systemstatus zu finden.
- Bei der Durchführung der Sicherung sollte unbedingt eine Protokolldatei angelegt werden. Nach Abschluss der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist es empfehlenswert, die Option *Details* zu aktivieren, da

damit auch festgestellt werden kann, ob alle zu sichernden Daten gesichert wurden und ob überhaupt die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollten.

- Bei der Wiederherstellung gesicherter Dateien kann deren Zugriffsschutz wiederhergestellt werden, sofern dies in den Eigenschaften des Wiederherstellungsauftrages spezifiziert wurde. Standardmäßig ist diese Option aktiviert. Dabei kann dies nur für Daten erfolgen, die von einem Windows NTFS-Dateisystem stammen.
- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann, im Gegensatz zur Windows Version des Programms, in einer Datei gespeichert werden, die später wieder geladen werden kann. Durch diesen Mechanismus ist es auch möglich, mehrere Sicherungsvarianten zu erzeugen, durch die unterschiedliche Daten erfasst werden.
- Sicherungen sollten in regelmäßigen Abständen durchgeführt werden. Damit kann die Sicherung auch automatisiert erfolgen.

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, so ist bei der Auswahl derartiger Sicherungssoftware darauf zu achten, dass sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS, sollten bei der Sicherung und Wiederherstellung unterstützt werden.
- Es muss möglich sein, auch Active Directory Daten sowie die Daten des SYSVOL-Ordners zu sichern.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.

Datensicherung einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherung der Daten eines Datenbanksystems kann in aller Regel nicht mit den Datensicherungsprogrammen auf Betriebssystemebene vollständig abgedeckt werden. Letztere bilden in den meisten Fällen lediglich das Bindeglied, um die zu sichernden Daten auf ein Sicherungsmedium zu schreiben. Zur Sicherung des DBMS und der Daten müssen dagegen für die meisten Datenbankprodukte zusätzlich die jeweiligen Dienstprogramme des DBMS eingesetzt werden.

Die einfachste Möglichkeit einer Datenbanksicherung, die zugleich die sicherste darstellt, ist eine Komplettsicherung der Datenbank in heruntergefahrenem Zustand. Dabei werden alle zur Datenbank gehörenden Dateien auf dem Sicherungsmedium gesichert. Meist ist dieses Vorgehen allerdings aus

Gründen der Verfügbarkeitsanforderungen an die Datenbank oder aufgrund des zu sichernden Datenvolumens nicht durchführbar.

Eine Alternative zur oben beschriebenen Komplettsicherung ist eine Online-Sicherung der Datenbank. Die Sicherung erfolgt dann während des laufenden Betriebs, d. h. die Datenbank muss nicht heruntergefahren werden. Online-Sicherungen sollten aus diesem Grund nur dann durchgeführt werden, wenn eine permanente Verfügbarkeit der Datenbank gefordert ist. Auf eine Offline-Komplettsicherung, die in vertretbar großen Zeitabständen durchgeführt werden kann, sollte trotzdem nicht verzichtet werden. Hierfür ist meistens der Einsatz einer Datensicherungssoftware notwendig.

Partielle Datenbanksicherungen stellen eine weitere Möglichkeit dar. Sie sollten immer dann verwendet werden, wenn das zu sichernde Datenvolumen zu groß ist, um eine vollständige Sicherung durchführen zu können. Dies kann daraus resultieren, dass die Kapazitäten der Sicherungsmedien nicht ausreichen oder dass der zur Verfügung stehende Zeitrahmen je Sicherung nicht genügt, um eine vollständige Sicherung durchführen zu können.

Falls möglich, sollten in jedem Fall alle Transaktionen zwischen zwei Offline-Komplettsicherungen archiviert werden. Oracle bietet dazu beispielsweise die Möglichkeit an, indem der so genannte ARCHIVE-Mode für die Datenbank aktiviert wird. Transaktionen werden bei Oracle in so genannten Log-Dateien protokolliert, von denen es mehrere gibt. Diese werden nacheinander beschrieben und sobald alle Log-Dateien voll sind, so wird wieder die erste Log-Datei überschrieben. Der ARCHIVE-Mode erstellt von diesen Log-Dateien eine Sicherungskopie, bevor sie wieder überschrieben werden. Auf diese Art und Weise können bei einer Zerstörung der Datenbank alle Transaktionen komplett rekonstruiert werden. Auch hierfür ist allerdings die Existenz einer Komplettsicherung der Datenbank die Voraussetzung. Die Dauer eines solchen Recovery wächst mit der Anzahl der zurückzuspielenden Archiv-Log-Dateien an.

Für die Datensicherung eines Datenbanksystems muss ein eigenes Datensicherungskonzept erstellt werden. Einflussfaktoren für ein solches Konzept sind:

Verfügbarkeitsanforderungen an die Datenbank

Wenn beispielsweise eine Datenbank werktags rund um die Uhr zur Verfügung stehen muss, so kann eine Komplettsicherung nur am Wochenende durchgeführt werden, da dies im Allgemeinen ein Herunterfahren der Datenbank erfordert.

Datenvolumen

Das gesamte zu sichernde Datenvolumen muss mit den zur Verfügung stehenden Sicherungskapazitäten verglichen werden. Dabei muss festgestellt werden, ob die Sicherungskapazitäten für das entsprechende Datenvolumen der Datenbank ausreichend dimensioniert sind. Falls dies nicht der Fall ist, muss ein Konzept zur Teilsicherung des Datenvolumens erstellt werden. Dies kann z. B. bedeuten, dass die Daten einzelner Anwendungen oder einzelner Bereiche der Datenbank immer im Wechsel gesichert werden bzw. nur die aktuellen Änderungen. Die Möglichkeiten einer Teilsicherung hängen von der verwendeten Datenbank-Software ab.

Maximal verkraftbarer Datenverlust

Hier muss festgelegt werden, ob bei einer Zerstörung der Datenbank der Datenverlust eines Tages verkraftbar ist, oder ob die Datenbank bis zur letzten Transaktion wiederherstellbar sein muss. Dies ist im Allgemeinen bei einer hohen Anforderung an die Verfügbarkeit bzw. Integrität der Daten der Fall.

Wiederanlaufzeit

Auch die maximal zulässige Zeitdauer des Wiederherstellens der Datenbank nach einem Absturz muss festgelegt werden, um den Verfügbarkeitsanforderungen zu genügen.

Datensicherungsmöglichkeiten der Datenbank-Software

Im Allgemeinen werden von einer Datenbank-Standardsoftware nicht alle denkbaren Datensicherungsmöglichkeiten unterstützt, wie z. B. eine partielle Datenbanksicherung. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann. Anhand dieser Informationen kann ein Konzept für die Datensicherung der Datenbank erstellt werden. In diesem Sicherungskonzept wird u. a. festgelegt (siehe hierzu auch Kapitel 3.4 Datensicherungskonzept)

- wer für die ordnungsgemäße Durchführung von Datensicherungen zuständig ist
- in welchen Zeitabständen eine Datenbanksicherung durchgeführt wird,
- in welcher Art und Weise die Datenbanksicherung zu erfolgen hat,
- zu welchem Zeitpunkt die Datenbanksicherung durchgeführt wird,
- die Spezifikation des zu sichernden Datenvolumens je Sicherung,
- wie die Erstellung von Datensicherungen zu dokumentieren ist, und
- wo die Datensicherungsmedien aufbewahrt werden.

Verpflichtung der Mitarbeiter zur Datensicherung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahmen ist, sollten die betroffenen Mitarbeiter auf die Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollten erfolgen.

Sicheres Löschen von Datenträgern

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert einen Missbrauch der gespeicherten Daten. Bevor Datenträger wiederverwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden, z. B. durch vollständiges Überschreiben oder Formatieren. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen. Auch der Empfänger des Datenträgers muss nach dem Empfang prüfen, ob der Schutzwert der Daten ein sofortiges Löschen des Datenträgers erfordert, nachdem die Daten auf ein anderes IT-System übertragen wurden.

Es gibt verschiedene Methoden um Informationen auf Datenträgern zu löschen, z. B. über Löschkommandos, durch Formatieren, durch Überschreiben oder durch Zerstörung des Datenträgers. Welche Methode gewählt werden sollte, hängt hierbei auch vom Schutzbedarf der zu löschenden Daten ab, der Schutz gegen die Restaurierung von Restdaten steigt in der genannten Reihenfolge.

Formatieren

Um Datenträger wieder in den "Urzustand" zu versetzen und damit auch vorhandene Informationen zu löschen, können diese formatiert werden. Wie zuverlässig dabei allerdings die alten Daten gelöscht werden, ist stark abhängig vom zu Grunde liegenden Betriebssystem. Ein Überschreiben der alten Daten ist auf jeden Fall zuverlässiger.

Überschreiben

Eine für den mittleren Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Es werden einige handelsübliche Produkte angeboten, die sogar die physikalische Löschung einzelner Dateien gewährleisten.

Zum Überschreiben sollten keine gleichförmigen Muster wie "0000" benutzt werden, sondern es sollten Muster wie "C1" (hexadezimal, entspricht der Bitfolge 11000001) benutzt werden. Dazu sollte bei einem zweiten Durchlauf ein dazu komplementäres Muster (also z. B. 3E, entspricht der Bitfolge 00111110) benutzt werden, damit möglichst jedes Bit einmal geändert wird.

Die Überschreibprozedur sollte daher mindestens zweimal, besser aber dreimal wiederholt werden, da hierdurch eine verbesserte Schutzwirkung erzielt wird.

Schreibgeschützte oder nicht mehrfach beschreibbare Datenträger wie DVD-Rs oder CD-Rs können selbstverständlich auch nicht gelöscht werden und sollten vernichtet werden.

Löschgeräte

Flexible magnetische Datenträger können mit einem Löschgerät gelöscht werden. Dabei werden die Datenträger einem externen magnetischen Gleich- oder Wechselfeld ausgesetzt (Durchflutungs-löschen). Geeignete Löschgeräte, die die Norm DIN 33858 erfüllen, sind in der BSI-Publikation 7500 aufgeführt.

Grundsätzlich sind die Datenträger nach dem Löschen wieder verwendbar. Es ist aber zu beachten, dass Datenträger mit einer magnetisch geschriebenen Servospur (z. B: Bandkassetten IBM 3590, Travan 4, MLR und ZIP-Disketten) nach einem Löschen unbrauchbar werden.

Vernichtung der Datenträger

Eine einfache Möglichkeit, Datenträger zu vernichten, besteht darin, dass Disketten und Magnetbänder zerschnitten und Festplatten mechanisch zerstört werden. Dies ist allerdings umständlich bei größeren Mengen an zu vernichtenden Datenträgern und auch nicht ausreichend bei höherem Schutzbedarf.

Geeignete Vernichtungsgeräte für Magnetbänder, Disketten und CD-ROMs, die der Norm DIN 32757 entsprechen, sind in der BSI-Publikation 7500 aufgeführt. Bei diesen Vernichtungsgeräten werden die Datenträger entweder zerkleinert oder eingeschmolzen. Vernichtungsgeräte für Festplatten sind nicht bekannt.

Minimaldatensicherungskonzept

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Für ein Unternehmen/eine Behörde ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Beispiel soll dies erläutern:

Minimaldatensicherungskonzept

Software
Sämtliche Software, erworben oder selbst erstellt, ist einmalig mittels einer Vollsicherung zu sichern.

Systemdaten
Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.

Anwendungsdaten
Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

Protokolldaten
Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

Datensicherungskonzept
Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. Sind die Anwendungsdaten oder die Kundenstammdaten verloren oder verfälscht, so können privatwirtschaftliche Betriebe in ihrer Existenz bedroht sein. Der Verlust oder die Verfälschung wichtiger Dateien kann in Behörden Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.

Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein:

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust) und
- vorsätzliche Datenzerstörung durch Computer-Viren usw.

Zur Realisierung der Datensicherung ist es notwendig das Datensicherungskonzept anhand der in den Punkten 1-12 beschriebenen Vorgaben zu Erstellen.

Inhaltsverzeichnis Datensicherungskonzept

1. Definitionen
- Anwendungsdaten, Systemdaten, Software, Protokolldaten

- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage

- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflussfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

4. Datensicherungsplan je IT-System

4.1 Festlegungen je Datenart

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

4.2 Festlegung der Vorgehensweise bei der Datenrestaurierung

4.3 Randbedingungen für das Datensicherungsarchiv

- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von Datensicherungen

- Vernichtung von unbrauchbaren Datenträgern

Empfehlungen zur Datensicherung

Die hier zusammengestellten Informationen stellen eine Empfehlung zur Datensicherung der CGM Clinical Deutschland GmbH dar. Die Durchführung und der Betrieb der Datensicherung, sowie das Restore und Recovery obliegt dem Kunden.

Domaincontroller

Sicherung

- z.B. Symantec Backup Exec mit Active Directory Agent verwenden
- tägliche Voll-Sicherung inkl. Systemstate (beinhaltet Active Directory) und Registry ab 20:00 Uhr
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, sowie einzelne Dateien und Objekte des Active Directory)

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

File, Print und Anwendungsserver

Sicherung

- z.B. Symantec Backup Exec Agent verwenden
- tägliche Sicherung der Benutzerspezifischen Daten inkl. Systemstate und Registry ab 20:00 Uhr
- wöchentliche Voll-Sicherung inkl. Systemstate und Registry oder nach Hardware-Änderung ab 20:00 Uhr
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, sowie einzelne Dateien)

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

Exchange Server

Sicherung

- z.B. Symantec Backup Exec Agent mit Granular Restore Technology verwenden
- tägliche Voll-Sicherung inkl. Systemstate ab 22:00 Uhr
- tägliche Sicherung der Exchange Datenbank ab 22:00 Uhr
- Sicherung der Exchange Logfiles im 3 Stunden Zyklus
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, der Exchange Datenbanken, einzelner Postfächer und öffentlicher Ordner, sowie einzelne Dateien)

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

Oracle Server

Sicherung

- z.B. Symantec Backup Exec Agent für Oracle-DB und Betriebssystem verwenden
- wöchentliche Voll-Sicherung inkl. Systemstate oder nach Hardware-Änderung ab 22:00 Uhr
- tägliche Sicherung der Oracle Datenbank ab 22:00 Uhr
- tägliche Sicherung der Logfiles 09:00 /12:00 / 18:00 Uhr oder nach Anforderung
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, der Oracle Datenbank, einzelner Datenbankfiles, sowie einzelne Dateien)

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

SQL Server

Sicherung

- z.B. Symantec Backup Exec Agent für SQL-DB und Betriebssystem verwenden
- wöchentliche Voll-Sicherung inkl. Systemstate oder nach Hardware-Änderung ab 22:00 Uhr
- tägliche Sicherung der SQL Datenbank ab 22:00 Uhr
- tägliche Sicherung der Logfiles um 09:00 /12:00 / 18:00 Uhr oder nach Anforderung
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, der SQL Datenbank, einzelner Datenbankfiles, sowie einzelne Dateien)

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

Terminalserver

Sicherung

- z.B. Symantec Backup Exec Agent verwenden
- tägliche Sicherung der Benutzerspezifischen Daten inkl. Systemstate und Registry ab 20:00 Uhr
- wöchentliche Voll-Sicherung inkl. Systemstate und Registry ab 20:00 Uhr
- Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

Restore

- Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal (Wiederherstellung des kompletten Systems, sowie einzelne Dateien Recovery
- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

Recovery

- Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

Sicherungsjobs

Die Sicherungsjobs für die filebasierte Sicherung werden in einem Sicherungsjob zusammengefasst. Das heißt, alle Betriebssysteme werden in einem Job gesichert.

Für die Sicherung der Datenbanken ist jeweils ein separater Sicherungsjob zu erstellen.

Die angegebenen Zeiten stellen Empfehlungen dar und können je nach Kundensituation angepasst werden

Werden bestimmte Server des Kunden im Outsourcing betreut wird die Sicherung dieser Server in separate Sicherungsjobs ausgegliedert. Es wird deshalb ein Sicherungsjob für die Outsourcing-Sever angelegt und ein weiterer für die Filesicherung der übrigen vom Kunden verwalteten Server.

Datenträgersätze

Filesicherung

- 2 Wochensätze á 4 Bänder (Mo-Do)
- 4 Freitagsbänder
- 12 Monatsbänder
- 2 Bänder pro Server für Offline-Sicherung

Datenbanken (Oracle, SQL)

Datenbanksicherung + Logfilesicherung

- 4 Wochensätze á 5 Bänder (Mo-Fr)
- 12 Monatsbänder

Datenträgernutzung

Die Datenträger sind nach Maßgabe des Herstellers zu verwenden. Ein Austausch ist nach einem Jahr notwendig

Bitte hierzu auch die Hinweise zur Verwaltung und Nutzung der Datenträger in den Grundlagen Datensicherung der CGM Clinical Deutschland GmbH beachten.

Server	Tägl. Voll	Wöchentlich Voll	Offline pro Quartal	Offline nach Hardware-Änderung	Datenbank	Logfiles 09:00 Uhr	Logfiles 12:00 Uhr	Logfiles 18:00 Uhr	Täglich Benutzerdaten
Domaincontroller	X		X	X	X				
File, Print und Anwendungsserver		X	X	X					X
Exchange	X		X	X	X				
Oracle		X	X	X	X	X	X	X	
SQL		X	X	X	X	X	X	X	
Terminalserver		X	X	X	X				X