**Maßnahmen zur Sicherstellung der Verfügbarkeit**

Version 1.2

Datum: 28.01.2022

David Nguyen

Klasse: 5bWI

Inhalt

[Aufgabenstellung 3](#_Toc94449556)

[Verfügbarkeit 3](#_Toc94449557)

[Technischen Maßnahmen: 3](#_Toc94449558)

[Backup und Recovery 3](#_Toc94449559)

[Authentifizierungsmethoden 3](#_Toc94449560)

[Verschlüsselungsverfahren 3](#_Toc94449561)

[Softwareaktualisierungen 4](#_Toc94449562)

[Redundanzmechanismen (Failover) 4](#_Toc94449563)

[Organisatorische Maßnahmen: 4](#_Toc94449564)

[Physische Abtrennung von kritischer Hardware (Zonensicherheit) 4](#_Toc94449565)

[Schulung für Mitarbeiter 4](#_Toc94449566)

[Vier Augen Prinzip 5](#_Toc94449567)

[Personalplanung 5](#_Toc94449568)

[Regelmäßige Backup und Restore 5](#_Toc94449569)

[Klassifikation 5](#_Toc94449570)

# Aufgabenstellung

Erhebe und beschreibe technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit von IV-Systemen.

Beispielhaft:

technisch: Backup- und Restore

organisatorisch dazu: verantw. Funktionsträger für Backup/Restore, Backup-Konzept, Restore-Trainings, Awareness im Unternehmen bezüglich potenziellen Datenverlustes schaffen (Schulung)

# Verfügbarkeit

Die gespeicherten Daten müssen in einem größtmöglichen zeitlichen Rahmen verfügbar sein. So ist es unbedingt zu vermeiden, dass Daten verschwinden oder auf diese nicht zugegriffen werden kann, wenn sie gebraucht werden. Auch muss die Funktionsfähigkeit von Programmen jederzeit sichergestellt sein, um den betrieblichen Prozess nicht zu stören. Generell geht es darum, die gewünschten Funktionen eines Systems immer dann bereit zu stellen, wenn diese benötigt werden.

## Technischen Maßnahmen:

* Verschlüsselungsverfahren
* Softwareaktualisierungen
* Backupprozeduren
* Redundanzmechanismen (Failover)
* Authentifizierungsmethoden

### Backup und Restore

Backup und Restore sind Prozesse der Erstellung und Speicherung von Datenkopien, die Unternehmen vor Datenverlust schützen können. Dies wird manchmal auch als betriebliche Recovery bezeichnet. Der Zweck des Backups besteht darin, eine Kopie der Daten zu erstellen, die bei einem primären Datenausfall wiederhergestellt werden können. Primäre Datenausfälle können auf Hardware- oder Softwarefehler, Datenbeschädigungen oder menschliches Versagen, wie z. B. einen böswilligen Angriff (Viren oder Malware) oder das versehentliche Löschen von Daten, zurückzuführen sein. Mithilfe von Backup-Kopien können Daten von einem früheren Zeitpunkt aus wiederhergestellt werden, um das Unternehmen bei der Wiederherstellung nach einem ungeplanten Ereignis zu unterstützen. Backups sollten extern von der Firma gespeichert werden da Sie bei einem Ausfall nicht wieder aufrufbar wäre. Bei der Wiederherstellung von einem Backup werden Daten an ihrem ursprünglichen Speicherort oder an einem alternativen Speicherort wiederhergestellt, von wo aus sie anstelle der verlorenen oder beschädigten Daten verwendet werden können.

### Authentifizierungsmethoden

Authentifizierungen über Passwort, E-Mail, SMS, Token oder einen Key sichert, dass das System nur von berechtigten Personen geführt werden können und somit „keinen Schaden“ angerichtet werden können und somit, dass das System mit den vorhandenen Daten bleiben. Sonst können Menschen, die das Unternehmen schaden wollen, die Daten sperren/manipulieren und erpressen damit sie Daten wieder rausrücken.

### Verschlüsselungsverfahren

Mit einem Verschlüsselungsverfahren kann ein Klartext in einen Geheimtext umgewandelt werden (Verschlüsselung) und umgekehrt der Geheimtext wieder in den Klartext rückgewandelt werden (Entschlüsselung). Oft wird hierbei ein Schlüssel benutzt. Das heute aufgrund der digitalen Kommunikation am weitesten verbreiteten Verfahren ist das RSA-Verfahren.

Bei symmetrischen Verfahren werden Ver- und Entschlüsselung mit demselben Schlüssel durchgeführt. Das heißt, Sender und Empfänger müssen vorab diesen geheimen Schlüssel vereinbart haben und der Schlüssel muss natürlich geheim gehalten werden, um die Information zu schützen. Ein Sicherheitsproblem stellt hier die Übergabe des geheimen Schlüssels dar. Das erste bekannte dieser Art stellt die Caesar-Chiffre dar.

Bei asymmetrischen Methoden gibt es nicht einen Schlüssel zum Ver- und Entschlüsseln, sondern zwei; einen öffentlichen Schlüssel, der für jeden zugänglich ist, und einen privaten Schlüssel, der geheim gehalten werden muss. Die beiden Schlüssel hängen mathematisch zusammen. Der Text wird mit dem öffentlichen Schlüssel verschlüsselt und kann nur mit dem privaten Schlüssel entschlüsselt werden. Hier muss der Verschlüsselungsschlüssel nicht geheim gehalten werden, es muss aber sichergestellt werden, dass der öffentliche Schlüssel auch wirklich zu dem Empfänger gehört. Zudem sind asymmetrische Verfahren meist langsamer, weshalb in der Praxis meist Hybrid-Verfahren genutzt werden.

Damit Daten verschlüsselt versendet werden können und kein Dritte an die Daten rankommt, sonst könnte er diese manipulieren/abfangen und die Zielperson bekommt nicht die Informationen die er/sie braucht. Mit einem Schlüssel soll daher die Verfügbarkeit der Daten gesichert werden, da nur der/die den Key hat auf die Daten auch zugreifen kann. Wenn jemand die Leitung abhört und die Daten die ganze Zeit abfängt und nicht an die Zielperson schickt, dann ist die Verfügbarkeit der Daten bei der Zielperson nicht gegeben.

### Softwareaktualisierungen

Durch Softwareaktualisierung bleibt, dass System auf den neusten Stand. Falls man in einer alten Version einen Sicherheitslücke findet wie kürzlich z.B. Java, dass dieser behoben wird und nicht erhalten bleibt. Man sollte auch die Software aktualisieren, da es möglich ist das abhängige Programme sich ändern und der Zugriff auf das System und somit auch auf die Daten nicht mehr gewährt ist. Zum Beispiel will man auf die Daten einer Software zugreifen, aber diese ist nur in der neusten Version möglich, so muss man die Software aktualisieren.

### Redundanzmechanismen (Failover)

Ein Failover ist ein System zur Erhöhung der Ausfallsicherheit durch einen Wechsel zwischen zwei oder mehreren (redundanten) Netzwerkdiensten bei einem einseitigen Ausfall. Als Folge können die Dienste trotz des Ausfalls eines der Systeme hochverfügbar gehalten werden und auf Daten zugegriffen werden.

## Organisatorische Maßnahmen:

* Vier-Augen-Prinzip
* Physische Abtrennung von Hardware
* Personalplanung
* Schulungen für Mitarbeiter
* Backup and Release Management

### Physische Abtrennung von kritischer Hardware (Zonensicherheit)

Damit nicht unbefugte Personen einen Server-Raum betreten und die Hardware umkonfigurieren. Somit bleibt das System standhaft und die Daten sind verfügbar. Bekommt jeder den Zugang zur Hardware so kann jeder den Steckerziehen oder Festplatten stehlen und somit die Daten stehlen/manipulieren. Wenn die Hardware einen Schaden bekommt, kann es sein, dass der Zugriff auf die Daten nicht mehr gewährleistet ist oder sogar, dass die Daten verloren gegangen sind.

### Schulung für Mitarbeiter

Damit die Mitarbeiter wissen, wie sie mit dem System umgehen müssen, und es nicht zu dem ungewollten Absturz führt. So lernen sie mit Daten umzugehen und sichern die Verfügbarkeit der Daten. Es soll ihnen durch die Schulung beigebracht werden was und wie sie es machen sollen, und Fehler vermieden werden da sonst das ganze System daran leiten kann und die Daten nicht mehr abrufbar sind. Beispiel, das man keine Datei von unbekannt E-Mails öffnet, da dieser einen Virus beinhalten kann, der alle Dateien im Unternehmen sperrt bzw. verschlüsselt.

### Vier Augen Prinzip

Durch die Kontrolle einer weiteren Person abgesichert, meist durch einen gleichberechtigten oder übergeordneten Mitarbeiter, wird sichergestellt, dass der Fehler und Missbrauchsmöglichkeiten ausgeschlossen werden, damit das System in Zukunft normal weiterlaufen kann. Falls es nicht läuft kann man auch nicht auf Daten zugreifen.

### Personalplanung

Wie viel Personal setzt ich für welche Projekte an damit die Produktion am Laufen bleibt. Es ist wichtig zu wissen, wie und wo man die Personalressourcen aufteilt, damit nicht bei einem Projekt die ganze Mannschaft arbeitet und bei einem anderen Projekt keiner. So kann es sein, dass wenn keiner am Projekt arbeitet, dass die Daten nicht rechtzeitig bzw. überhaupt verfügbar sind. Beispiel, wenn keiner an Stelle X arbeitet, aber Stelle braucht die verarbeiteten Daten der Stelle X, so sind die Daten nicht verfügbar und die Mitarbeiter müssen warten.

### Regelmäßige Backup und Restore

Regelmäßig Backups machen, um den Fortschritt zu sichern falls, mal etwas schiefläuft und man auf die alten Daten zugreifen muss. Regelmäßig restore damit, man prüfen kann, dass das Backup funktioniert. So kann im Fall eines Fehlers schnell reagiert werden, damit im Notfall auch die Daten verfügbar bleiben.

### Klassifikation

Der Einteilung der Verfügbarkeitsklassen nach diesem System liegt die maximal zulässige Dauer der Ausfallzeit in vereinbarten Zeitintervallen – im Regelfall pro Monat oder Jahr – zu Grunde. Die Anzahl der Neunen in prozentualer Angabe der Verfügbarkeit, kennzeichnet hier die Verfügbarkeitsklasse. Nach diesem Verfahren spricht man bei 99 Prozent von einer Verfügbarkeitsklasse 2. Im Regelfall spricht man bei einer Verfügbarkeit von 99,9 Prozent (Klasse 3) oder höher von einem hochverfügbaren System.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

**Geringes Risiko**

Daten und Systeme werden als geringes Risiko eingestuft, wenn sie nicht als mäßiges oder hohes Risiko angesehen werden und:

Der Verlust der Verfügbarkeit der Daten oder des Systems hätte keine negativen Auswirkungen auf den Auftrag, die Sicherheit, unsere Finanzen oder auf den Ruf des Unternehmens.

**Mäßiges Risiko**

Daten und Systeme werden als mäßig riskant eingestuft, wenn sie nicht als hoch riskant gelten und:

Der Verlust der Verfügbarkeit der Daten oder des Systems könnte geringfügige negative Auswirkungen auf den Auftrag, die Sicherheit, der Finanzen oder auf den Ruf haben.

**Hohes Risiko**

Der Verlust der Verfügbarkeit der Daten oder des Systems könnte erhebliche negative Auswirkungen auf unseren Auftrag, unsere Sicherheit, unsere Finanzen oder unseren Ruf haben.