**Einführung Systemdesign nach VIVA Methode**

Version 1.2

Datum: 28.01.2022

David Nguyen

Klasse: 5bWI

Inhalt

[Aufgabenstellung 3](#_Toc94451560)

[VIVA 3](#_Toc94451561)

[Vertraulichkeit 3](#_Toc94451562)

[Integrität 3](#_Toc94451563)

[Verfügbarkeit 3](#_Toc94451564)

[Authentizität 3](#_Toc94451565)

[Bewertung von IT-Risiken 4](#_Toc94451566)

[Die Klassifizierung von IT-Systemen 5](#_Toc94451567)

[Vertraulichkeit 5](#_Toc94451568)

[Integrität 5](#_Toc94451569)

[Verfügbarkeit 5](#_Toc94451570)

[Authentität 6](#_Toc94451571)

# Aufgabenstellung

Erläutern sie die Parameter VIVA und deren Bedeutung

Erklären Sie ein betriebliches Schema zur Klassifikation von IT-Systemen

# VIVA

Das Confidentiality, Integrity, Availability, Authenticity Prinzip (deutsch: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) bezeichnet in der Computerwelt wesentliche Grundbedrohungen der Informationssicherheit. Zu diesen Bedrohungen zählen der Verlust der Verfügbarkeit, der Integrität und der Vertraulichkeit von Daten.

## Vertraulichkeit

Gerade für Firmen ist es von großer Bedeutung, dass Daten lediglich von autorisierten Benutzern eingesehen werden können. Hierbei ist zum einen die Sicherheit von gespeicherten Daten gemeint und zum anderen die Sicherheit der Informationen bei der Datenübertagung. Es ist unter allen Umständen zu vermeiden, dass vertrauliche Daten in unbefugte Hände gelangen. Auch wenn die Vertraulichkeit zumeist für Daten sichergestellt werden muss, kann es unter Umständen auch notwendig sein, Programme und Systemkonfigurationen von unbefugten Personen geheim zu halten.

Das Schutzziel Vertraulichkeit stellt sicher, dass personenbezogene Daten nur von Personen eingesehen, verändert oder gar gelöscht werden können, die dazu berechtigt sind. Sie müssen also dafür sorgen nur Befugten die Möglichkeit dafür zu geben. Andersherum bedeutet es aber auch, dass Unbefugte das nicht dürfen.  
Jedes Unternehmen muss die Vertraulichkeit von personenbezogenen Daten gewährleisten können. Egal ob so klein wie der Immobilienmakler, oder so groß wie ein Automobilhersteller.

## Integrität

Allgemein gesehen bedeutet der Begriff Integrität, dass jemand glaubwürdig ist. Weitere Bedeutungen sind Ehrlichkeit, Anständigkeit, Makellosigkeit, Rechtschaffenheit oder auch Unbestechlichkeit. Man spricht von glaubwürdigen und unverfälschten Daten. Integre Daten sind echte Daten, oder Daten, von denen die Echtheit nachvollziehbar ist.

Aus der Integrität ergibt sich im Datenschutz eine enge Verbundenheit mit der Vertraulichkeit – einem anderen Schutzziel im Datenschutz. Denn nur wenn Sie sicherstellen, dass Daten nicht unberechtigt verändert werden, verfügen Sie über echte unverfälschte Daten.

Unter der Integrität von Daten versteht man die Nachvollziehbarkeit von vorgenommenen Änderungen an diesen. Daten stehen immer einem gewissen Kreis von autorisierten Personen zur Verfügung. Bei den täglich anfallenden Geschäftsprozessen werden diese Daten natürlich verändert. Änderungen in den Dateien - seien dies Word-, Excel- oder andere Dokumente - müssen für jede zugriffsberechtigte Person nachvollziehbar sein. Dies kann zum Beispiel durch eine Versionsverwaltung sichergestellt werden, welche bei vielen Repositories bereits inbegriffen ist. Die Versionsverwaltung ist dafür verantwortlich sämtliche Änderungen an Dokumenten oder Dateien in einem Archiv mit Zeitstempel und Benutzerkennung zu speichern. So kann zu jeder Zeit nachvollzogen werden, welche Person zu welchem Zeitpunkt welche Veränderungen im Dokument vorgenommen hat. Durch das Versionsmanagement können somit auch alte Versionen der Dokumente und Dateien wiederhergestellt werden oder aber auch gelöschte Dateien wiederhergestellt werden.

Das bedeutet, Man kontrolliert alles, was mit der Übertragung von personenbezogenen Daten zu tun hat. Personenbezogene Daten dürfen während ihres Transports / ihrer Übertragung von Unbefugten nicht gelesen, kopiert, verändert oder gelöscht werden können. Diese Maßnahme nennt man Weitergabekontrolle.

Das erreichet man mit einer Verschlüsselung von Daten, verschlüsselter Verbindungen oder sicheren Transportbehältern wie abgeschlossene Aktenkoffer o.ä. Auch die sorgfältige Auswahl von Dienstleistern und deren vertragliche Verpflichtung kann darunterfallen.

Dabei ist die korrekte Funktion Ihrer Systeme maßgeblich. Ihre IT muss funktionieren.

Eine andere Methode ist die Protokollierung von Eingabe und Änderung. So kann man nachvollziehen, ob Daten von Unberechtigten verfälscht wurden.

## 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.

Stellt man sich vor, man speichert die Arbeitszeitdaten der Beschäftigten auf einem Server. (Egal ob Excel Tabelle, HR-Anwendung, oder Datenbank.) Das hat vermutlich unter anderem den Sinn, dass die Mitarbeiter am Ende des Monats für die Arbeitsleistung Geld bezahlen. Man will aber auch sicherstellen, dass nicht zu viel Urlaub genommen wird, müssen Krankheitstage erfassen, usw.

Damit man all das und mehr machen können, verarbeitet man diese personenbezogenen Daten. Wenn diese Daten nicht mehr da sind, kann man keine korrekte Abrechnung mehr erstellen. Die Mitarbeiter erhalten zu wenig Geld – vielleicht auch zu viel.

Alle Beteiligten haben also ein Interesse an der Verfügbarkeit der personenbezogenen Daten. Die betroffenen Personen, also die Beschäftigten am meisten, denn deren wirtschaftliche Existenz hängt von deren Einkommen ab.

Genau das ist Verfügbarkeit. Die Daten müssen vorhanden sein. Ihre Aufgabe ist das sicherzustellen.

Man können die Anforderungen an Verfügbarkeit umsetzen indem man die Daten sichert und vor Verlust schützen. Auch bekannt als Backup. Eigentlich ist das aber schon der zweite Schritt der Aufgabe „Verfügbarkeit umsetzen“.

Am besten erstellen man zuerst eine „Landkarte“ der Datenbestände in Ihrem Unternehmen. Man muss wissen wo welche Daten sind. Also auch auf welchen Geräten. Oft sind das Server, Clients oder mobile Geräte wie Smartphones und Tablets. Betrachtet man das aus dieser Perspektive, spielt es keine Rolle, ob Ihre Daten in Exceltabellen oder einem ERP-System gespeichert sind. Fest steht, dass man bei diesen Systemen eine regelmäßige Datensicherung durchführen müssen. Oft liest man in diesem Zusammenhang auch von kontinuierlicher Datensicherung oder Backups. Erst die nächste Aufgabe ist es die vorhandenen Daten zu sichern. Eigentlich geht es erst jetzt um Datensicherung und Backup.

## Authentizität

In der heutigen Zeit werden täglich zahlreiche Dateien elektronisch versendet. Bei besonders sensiblen Daten, wie bspw. Urkunden, muss alles Notwendige unternommen werden, um den Urheber der Daten korrekt authentifizieren zu können. Es dürfen also keine Zweifel am Urheber der Dateien entstehen, ansonsten könnten zum Beispiel in Firmen falsche Aufträge oder Anweisungen erteilt werden. Neben der Authentizität von Dateien und Dokumenten kann es in bestimmten Bereichen, wie dem elektronischen Zahlungsverkehr, auch notwendig sein, die Authentizität von Programmen und Hardware zu garantieren.

# Bewertung von IT-Risiken

Risiken sind ein betriebswirtschaftliches Konzept: Besteht eine hohe, mittlere oder geringe Wahrscheinlichkeit, dass das Unternehmen einen finanziellen Verlust erleidet, oder ist dies überhaupt nicht wahrscheinlich? Bei der Risikoermittlung spielen drei Faktoren eine Rolle: worin die Bedrohung besteht, wie anfällig das System ist und wie wichtig die Ressource ist, die Schaden nehmen oder nicht mehr verfügbar sein könnte.

Im Folgenden sind einige typische Szenarien aufgeführt, die zu finanziellen Verlusten führen können:

**Datenverlust:** Der Diebstahl von Betriebsgeheimnissen könnte dazu führen, dass Sie Kunden an die Konkurrenz verlieren. Der Diebstahl von Kundendaten kann einen Vertrauensverlust oder die Abwanderung von Kunden nach sich ziehen.

**System- oder Anwendungsausfälle:** Wenn ein System seine primäre Funktion nicht erfüllt, können Kunden möglicherweise keine Bestellungen aufgeben, Mitarbeiter ihre Aufgaben nicht erledigen oder nicht kommunizieren usw.

**Rechtliche Folgen:** Wenn jemand unerlaubt Daten aus Ihren Datenbanken ausliest, drohen Ihnen selbst dann, wenn diese Daten nicht besonders wertvoll sind, Bußgelder oder sonstige Rechtskosten.

Ziel des ganzen Prozesses der Klassifizierung und Bewertung von IT-Risiken ist, dass ein Überblick über die Problemfelder erhalten und gleichzeitig erkennen werden können, wie und wann diese behandeln sollten.

Grundsätzlich gelten folgende Regeln:

* Der technische Risikofaktor lässt sich mit Technik & Technologie behandeln.
* Der menschliche Risikofaktor lässt sich mit Schulung bzw. entsprechenden Verhaltensrichtlinien behandeln.
* Der rechtliche Risikofaktor lässt sich mit Organisation behandeln.
* Hohes Schadenspotenzial bedeutet dringende und rasche Behandlung.
* Hohe Eintrittswahrscheinlichkeit bedeutet dringende und schnelle Behandlung.

# Die Klassifizierung von IT-Systemen

## Vertraulichkeit

|  |  |  |  |
| --- | --- | --- | --- |
| **Öffentlich** | **Intern** | **Vertraulich** | **Streng vertraulich** |
| Daten sind für jedermann, auch außerhalb der Firma, zugänglich. | Daten sind für jedermann, auch außerhalb der Firma, zugänglich. | Vertraulich definierte Daten sind lediglich einer begrenzten Anzahl an Mitarbeitern zugänglich, z.B. Personaldaten, Kundenlisten, Kalkulationen. | Streng vertrauliche Daten sind punktuell und ausschließlich bestimmten definierten Personen zugänglich. Eine Weitergabe kann das Unternehmen nachhaltig schädigen. |

## Integrität

|  |
| --- |
| **Korrekter Inhalt** Diese Integritätsart liegt vor, wenn Sachverhalte der realen Welt korrekt abgebildet werden. Dies soll beispielsweise durch Integritätsbedingungen sichergestellt werden. |
| **Unmodifizierter Zustand** Diese Integritätsart liegt vor, wenn Nachrichten unverändert zugestellt werden und Programme und Prozesse wie beabsichtigt ablaufen. |
| **Erkennung von Modifikation**  Diese Integritätsart liegt vor, wenn unerwünschte Modifikationen, die nicht verhindert werden können, zumindest erkannt werden. |
| **Temporale Korrektheit**  Diese Integritätsart liegt vor, wenn Nachrichten ausgetauscht und relevante zeitliche Bedingungen, wie etwa Reihenfolgen oder maximale Verzögerungszeiten, eingehalten werden. |

## Verfügbarkeit

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

## Authentität

Hierbei wird einfach zwischen einer Nachvollziehbarkeit oder keiner Nachvollziehbarkeit unterschieden.