INDUSTRY 4.0 for VET

LERNMATERIAL

Inhalt

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Autor: bit schulungscenter

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. BASICS DIGITALISIERUNG UND ARBEITSWELT 4.0

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.1 Das Thema

Die erste Einführung

Unsere Unternehmens- und Arbeitswelt befindet sich im Wandel: In Fabriken übernehmen Roboter und Maschinen immer mehr Aufgaben, in Büros sind IT-Spezialisten gefragt, die neuartige Technologien bedienen und instand halten können, in Supermärkten ersetzen Kassenautomaten das Personal. Aber welche Auswirkungen hat die fortschreitende Digitalisierung auf unsere Gesellschaft und welche Vorteile und Herausforderungen sind damit verbunden? Müssen wir tatsächlich befürchten, dass wir in Zukunft komplett von Maschinen und Robotern ersetzt werden, oder bietet uns die neue Arbeitswelt 4.0 auch ganz neue Möglichkeiten und Chancen?

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Digitalisierung und Digitale Transformation sind aus unserer modernen Gesellschaft nicht mehr wegzudenken. Ob nun Studierende eine E-Learning-Plattform nutzen, Mitarbeitende in einem Automobilwerk mit Robotern zusammenarbeiten oder Übersetzer und Übersetzerinnen einen Text bearbeiten, der von einem maschinellen Übersetzungsprogramm erstellt wurde – die Arbeitswelt 4.0 ist bereits Realität. Es ist daher für alle Arbeitskräfte der Zukunft sehr wichtig, darüber in Grundzügen Bescheid zu wissen.

Lernziele und Kompetenzen im Überblick

Diese Lerneinheit vermittelt Ihnen die Basisbegriffe der Digitalisierung, Sie erfahren mehr über die Geschichte der industriellen Revolutionen und erhalten einen Einblick in die Herausforderungen und Chancen, die Digitalisierung und Digitale Transformation für Unternehmen und einzelne Personen bereithalten. Zudem lernen Sie, welche Fähigkeiten auf dem Arbeitsmarkt von Morgen gefragt sein werden und welche Tätigkeiten in Zukunft voraussichtlich in den Hintergrund treten. Dieses Grundwissen hilft Ihnen, die Arbeitswelt der Zukunft besser zu verstehen und die Chancen und Möglichkeiten der Digitalisierung bestmöglich für sich zu nutzen.

Lernziele
Erklären, was unter Digitalisierung verstanden wird.
Wissen, was eine industrielle Revolution ist und welche industriellen Revolutionen unterschieden werden.
Wissen, wie Unternehmen die Digitalisierung erfolgreich einsetzen können.
Wissen, was die Arbeitswelt 4.0 für die Arbeitnehmer und Arbeitnehmerinnen bedeutet.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Wissen, wie die Arbeitswelt von morgen aussehen könnte.

1.2 Was ist Digitalisierung?

Wie würden Sie Digitalisierung erklären? Verbinden Sie damit die digitale Verarbeitung und Wiedergabe eines Tons auf einer CD? Den Einsatz von Robotern an einem Fließband? Oder gar das scheinbar „intelligente“ Handeln von Figuren in einem Computerspiel? Vielleicht ist Ihnen bereits aufgefallen, dass zwar laufend über Digitalisierung gesprochen wird, der Begriff aber für viele Menschen unscharf und schwer zu fassen ist.

Streng genommen ist **Digitalisierung** nur die digitale Verarbeitung und Abbildung von Informationen, etwa in einem Video oder auf dem PC – analoge Informationen wie Bild oder Ton werden in digitale Einheiten gespeichert. Digitalisierung wird in unserem Sprachgebrauch aber oftmals mit Digitaler Transformation oder Automatisierung gleichgesetzt.

In unserer Welt passiert es ständig, dass analoge Signale in digitale Signale umgewandelt werden und umgekehrt. Aber wissen Sie eigentlich, was der **Unterschied** zwischen einem **analogen** und einem **digitalen Signal** ist?

Ein **analoges** Signal ist stufenlos und kann mehr als eine eindeutige Information transportieren. Dazu zählt etwa das Zwitschern eines Vogels, der Gesang eines Menschen, die Anzeige einer Uhr mit Ziffernblatt oder auch ein Foto in einem Album. Diese Signale haben gemeinsam, dass ihre Qualität mit der Zeit abnimmt (etwa vergilben Fotos) und sie räumlich nicht gut transportiert werden können.

Digitale Signale hingegen besitzen eine Information, die eindeutig erkannt wird. Sie können immer mit der gleichen Qualität wiedergegeben und räumlich problemlos transportiert werden. Dazu zählen etwa eine MP3-Datei, auf der Musik gespeichert ist, eine Uhr mit digitaler Anzeige oder eingescannte und digitalisierte Fotos, die auf dem PC abgespeichert werden. Die Qualität der Dateien nimmt mit der Zeit nicht ab, die Fotos können immer wieder in derselben Qualität ausgedruckt werden und die Musik kann immer mit derselben Qualität abgespielt werden.

Hier sehen Sie, wie eine Kasse mit analoger Anzeige ausgesehen hat:

Digitale Transformation bezeichnet das Einführen von digitalen Arbeitsweisen und Programmen **–** die Prozesse, die durch die Digitalisierung in Gang gesetzt werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unmittelbar verbunden mit der Digitalen Transformation ist auch die **Automatisierung** von einzelnen Arbeitsschritten oder gesamten Prozessen. Hierbei führen Maschinen, Anlagen oder Einrichtungen selbstständig Arbeitsschritte oder ganze Prozesse aus.

Eine wichtige Rolle spielt dabei die **künstliche Intelligenz**: Eine Maschine, ein Roboter etc. wird so gebaut, dass selbständig Arbeitsschritte ausgeführt und Probleme gelöst werden können. Bei Computerspielen wird zum Beispiel die Intelligenz des Menschen durch Algorithmen nachgeahmt, damit Spielfiguren „scheinbar" intelligent reagieren.

Definition

Digitalisierung

...steht ursprünglich nur für die **digitale Verarbeitung und Abbildung von Informationen.** In unserem Sprachgebrauch wird darunter aber auch oftmals **Digitale Transformation** und **Automatisierung** verstanden.

Definition

Digitale Transformation

...beschreibt die **durch die Digitalisierung ausgelösten Veränderungen in der Gesellschaft.** Dazu zählt auch die **Automatisierung von Arbeitsschritten und Prozessen.**

Digitalisierung (Erstellen einer CD oder eines Videos, Informationen am PC festhalten...) **-> führt zu**

Digitaler Transformation (Automatisierung, Einsatz von Computerprogrammen, Erstellen einer künstlichen Intelligenz, Einkaufen über Amazon...)

Beispiel

Herr Weber arbeitet seit 1990 als Kassier bei einer bekannten Supermarktkette. Seine Kassa zeigt die von ihm eingegebenen Zahlen digital an und rechnet den Endbetrag aus. Die **Digitalisierung** wurde damit bereits vollzogen.

Als die ersten Kassenautomaten erprobt werden, bei denen die Menschen selbstständig ihre Ware scannen und anschließend direkt am Automaten bezahlen, ist Herr Weber zunächst skeptisch. Was wird das für seine tägliche Arbeit bedeuten und wird er überhaupt noch gebraucht? Das Ersetzen dieser alten Kassen durch neue Kassenautomaten mit digitaler Anzeige und Scanvorrichtung ist als **Digitale Transformation** zu bezeichnen. Die Tatsache, dass diese Kassen nach der Eingabe der einzelnen Produkte selbstständig den fälligen Betrag anzeigen, kassieren und Restgeld geben, wird als **Automatisierung bezeichnet**.

Mittlerweile hat sich Herr Weber in seine neue Tätigkeit eingefunden: Er hilft nun den Kunden, die Probleme mit dem Automaten haben. Und diese sind vielfältig: Manche Produkte lassen sich nicht so leicht scannen, manchmal gibt es eine Fehlermeldung, weil die Ware nicht richtig abgelegt wurde, zudem muss beim Einkauf von Alkohol weiterhin von einem Menschen das Alter der Kunden überprüft werden und vieles mehr. Zu Spitzenzeiten sitzt Herr Weber weiterhin selbst an der Kasse, außerdem übernimmt er Aufgaben in der Geschäftsführung.

Herr Weber ist in der Arbeitswelt 4.0 angekommen, in der zum Glück immer noch auch menschliche Fähigkeiten gebraucht werden. Nichts desto trotz kann sich die Anzahl des im Geschäft beschäftigten Personals durch die Veränderungen allgemein reduzieren.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Aber wer ist nun eigentlich genau von der Digitalisierung bzw. der Digitalen Transformation betroffen und auf welche Weise?

Hier kann zwischen Unternehmen, Einzelpersonen, Wissenschaft & Forschung und Staat unterschieden werden, die zusammen als **Akteure der Digitalisierung** bezeichnet werden**:**

- **Unternehmen**
  Unternehmen setzen etwa Roboter am Fließband ein, um die Produktivität zu steigern, oder Kassenautomaten im Supermarkt, um die Personalkosten zu senken. Digitalisierung bedeutet daher zum Beispiel für eine **Supermarktkette** einerseits, dass Arbeitsabläufe effizienter gestaltet werden und dadurch Kosten gespart werden können, aber auch, dass sie immer auf dem letzten Stand bleiben muss, um mit der Konkurrenz mithalten zu können.

- **Einzelpersonen**
  Werden in einem Unternehmen Abläufe digitalisiert, sind davon meist Einzelpersonen betroffen. So erhält etwa der **Kassier im Supermarkt** eine neue Aufgabe oder wird entlassen, wenn Kassenautomaten eingesetzt werden. Betroffen sind aber auch die **Führungspersonen**, etwa der **CEO eines Mobilfunkunternehmens**, der sich eine neue Strategie ausdenken muss, um ein günstiges Smartphone zu entwickeln.

- **Wissenschaft und Forschung**
  Wissenschaft und Forschung beschäftigen sich im Detail mit Digitalisierungsprozessen, es werden neue Computerprogramme, Maschinen und Roboter entwickelt. Die Digitalisierung wird etwa an **Universitäten** auch aus ethischer Sicht betrachtet, indem die Auswirkungen der Digitalisierung auf unsere Gesellschaft und der beste Umgang damit untersucht werden.

- **Staat**
  Zu guter Letzt ist auch der Staat an der Digitalisierung beteiligt: So erlässt das **Bundesministerium für Digitalisierung und Wirtschaftsstandort** Gesetze und Verordnungen für die Umsetzung der Digitalisierung. Beispiele sind etwa die Verordnung zur digitalen Signatur, mit der Dokumente online unterzeichnet werden können, oder das Gesetz zum Schutz von personenbezogenen Daten wie Geburtsdatum, Autokennzeichen etc.

1.3 Die Industriellen Revolutionen im Überblick

Bestimmt haben Sie schon einmal etwas über die **Industriellen Revolutionen** gehört. Vielleicht denken Sie dabei an:

- die Erfindung der Dampflokomotive
- Henry Ford und die erste Massenherstellung von Autos
- die ersten PCs
- die Vernetzung von Robotern

Dies alles sind **wesentliche Neuerungen**, die in den verschiedenen Industriellen Revolutionen stattgefunden haben. Aber sehen wir uns zunächst einmal an, wodurch sich eine Industrielle Revolution auszeichnet:

Veränderung ist in einer Gesellschaft normal und natürlich, **Fortschritt** ebenso. Ab dem späten 18. Jahrhundert bezeichnet man Phasen, in denen es bahnbrechende Fortschritte in der Produktion gab,

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

wie etwa die Einführung von dampfgetriebenen Spinnrädern oder Fließbandarbeit, als **Industrielle Revolutionen**.

Ein Kennzeichen der Industriellen Revolutionen sind **Veränderungen der Lebensumstände** der Menschen. Denn neue Produktionstechniken wie etwa die Dampfmaschine oder der PC hatten tiefgreifende Auswirkungen auf die Wirtschaft und die Gesellschaft. Sowohl Arbeitgeber als auch Arbeitnehmer mussten sich an die **neuen Bedingungen** anpassen.

Definition
Industrielle Revolution ...beschreibt große Fortschritte in der Produktion, die dazu führen, dass sich wirtschaftliche und gesellschaftliche Verhältnisse verändern.

Man unterscheidet zwischen **vier Industriellen Revolutionen**, denen entsprechend **Industrie 1.0 bis 4.0** zugeordnet werden. Derzeit befinden wir uns in der Vierten Industriellen Revolution:

Die Erste Industrielle Revolution – Industrie 1.0

- **Mechanisierung**
- **ab 1784**

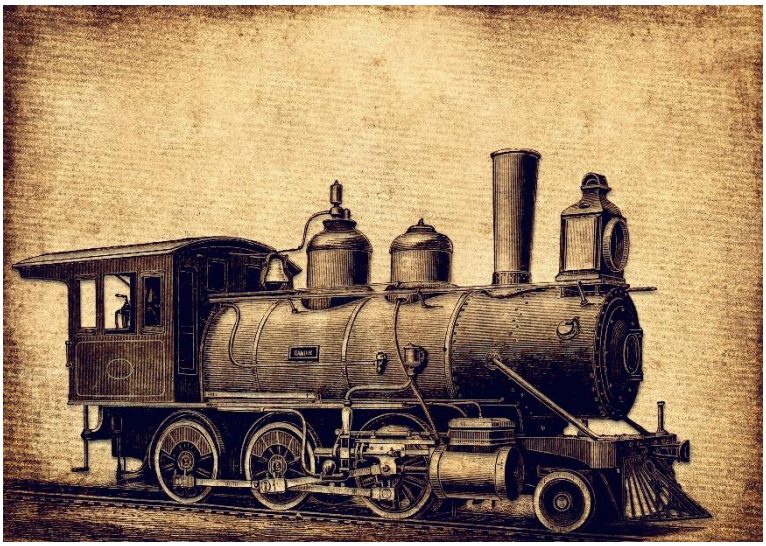
Die **Dampfmaschine** wurde in die Fabriken eingeführt, Webstühle oder Spinnräder wurden nun nicht mehr mit Muskelkraft, sondern mechanisch mit Dampfkraft angetrieben. Dadurch konnte in weniger Zeit und mit weniger Aufwand sehr viel mehr produziert werden, für die Menschen entstanden **neue Arbeitsplätze** in den Fabriken.

1802 wurde von dem Briten **Richard Trevithick** die erste **Dampflokomotive** gebaut. Diese war allerdings nicht funktionstüchtig, da die gusseisernen Schienen der Pferdebahn nicht widerstandsfähig genug waren. Nur wenige Jahre danach ging die erste Dampflok in Betrieb – auf geeigneten Schienen. Einige Jahre davor wurde bereits das erste **Dampfschiff** entwickelt.

Merken
Wichtigste Neuerungen der Ersten Industriellen Revolution sind **mechanische Produktionsanlagen**, die mit **Wasser- und Dampfkraft** betrieben wurden (z.B. Webstühle und Spinnräder), die **Dampflokomotive** und das **Dampfschiff**.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

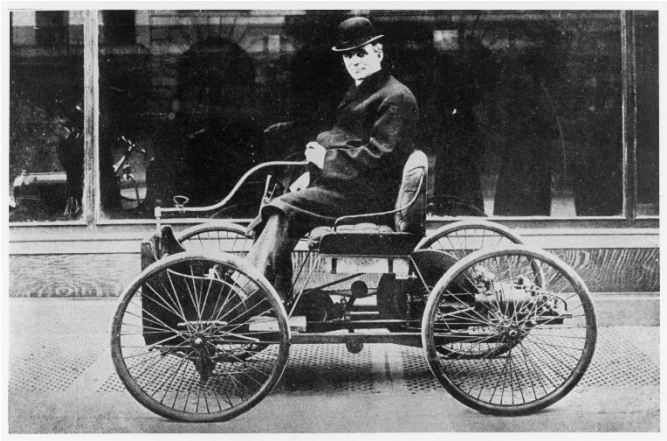


Die Zweite Industrielle Revolution – Industrie 2.0

- **Elektrifizierung**
- **ab 1870**

Die Elektrizität wurde entdeckt und als Antriebskraft eingeführt und in den Fabriken wurden die ersten **Fließbänder** eingeführt: Der Amerikaner **Henry Ford** übernahm die Idee des Fließbands von einem Schlachthof und führte sie 1913 für die Produktion seiner Automobile ein: Die Fahrzeugteile wurden am Fließband gefertigt, mehrere Arbeiter **teilten** sich die **Arbeitsschritte**.

Die Produktion wurde dadurch **schneller** und **günstiger** und immer mehr Menschen konnten sich ein Auto leisten. Da das Auto vom Luxusgut zum Massengut wurde und immer mehr Autos hergestellt wurden, gab es auch immer mehr **Arbeitsplätze** in den Fabriken.



Zudem wurde das **Telefon** erfunden, die Herstellung von **Kleidung** wurde zunehmend automatisiert und der Amerikaner Thomas Alva Edison erfand 1879 die **Glühbirne**.

Merken
Die wichtigsten Neuerungen der Zweiten Industriellen Revolution sind die **Massenproduktion** durch **Elektrizität**, die Arbeit am **Fließband**, das **Telefon** und die **Glühbirne**.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Die Dritte industrielle Revolution – Industrie 3.0

- **Produktionssteuerung**
- **ab 1969**

Die ersten programmierbaren **Steuerungen** wurden erfunden, was dazu führte, dass einzelne **Arbeitsschritte automatisiert** wurden und **ohne menschliche „Hilfe“** ausgeführt werden konnten. Ein gutes Beispiel hierfür sind **Roboter**, die selbstständig staubsaugen. In den Fabriken wurden dringend Programmierer benötigt, die diese Steuerungen bedienen konnten.

In Kalifornien wurde 1972 einer der **ersten Roboter** erfunden. Er konnte aber bereits seine Umgebung erfassen und ertasten und sich fortbewegen. Weil er noch recht wackelig auf den Beinen war, trug er den Namen **„Shakey“**.

Die **ersten Computer** waren riesengroße und unhandliche Rechenmaschinen, wurden aber schnell weiterentwickelt. 1982 wurde der **PC** (Personal Computer, dt. persönlicher Rechner) für Privathaushalte attraktiv, als der legendäre Commodore C64 auf den Markt kam.

Merken
Die wichtigsten Neuerungen der Dritten Industriellen Revolution sind die weitere **Automatisierung und Steuerung der Produktion** mithilfe von Elektronik und IT und der erste **Roboter**. Zudem hält der **PC** Einzug in die Privathaushalte.

Die Vierte Industrielle Revolution – Industrie 4.0

- **Vernetzung**
- **ab. ca. 2010**

Die industrielle Produktion wird immer mehr digitalisiert und es werden **moderne Informations- und Kommunikationstechnologien** eingesetzt. Diese werden miteinander **vernetzt**, um nicht nur einzelne Arbeitsschritte, sondern ganze **Prozesse** zu **automatisieren**.

In Automobilwerken werden bereits **Roboter** für die Montage eingesetzt, die auch in der Lage sind, selbstständig Probleme zu lösen. In den neuen digitalen Fabriken werden **Anlagen** miteinander **vernetzt**, Produktionssysteme, Bauteile und Menschen kommunizieren miteinander.

Co-funded by the Erasmus+ Programme of the European Union

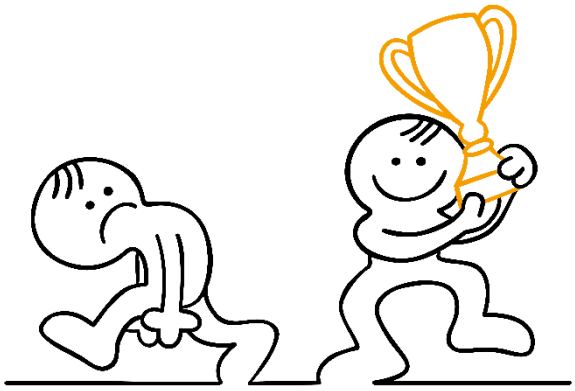
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Computer sind mittlerweile in der Lage, **aus Erfahrung** zu **lernen**, so gibt es heute beispielsweise selbstfahrende Autos, die vom Fahrer lernen und nach einigen Tagen **selbstständig Entscheidungen** wie Bremsen oder Beschleunigen treffen können. Außerdem können sie sich mit Handys und anderen Geräten **vernetzen**.

Merken
Die wichtigsten Neuerungen der Vierten Industriellen Revolution sind die zunehmende **Digitalisierung der Produktion**, die **Vernetzung intelligenter Systeme** und das **Zusammenspiel von Mensch und Maschine**. **Computer** können nun aus Erfahrung **lernen** (z.B. selbstfahrende Autos).

1.4 Digitalisierung in Unternehmen

Wir haben bereits gesehen, dass die Digitalisierung zahlreiche **Veränderungen** mit sich bringt. In diesem Kapitel konzentrieren wir uns speziell darauf, wie **Unternehmen** davon betroffen sind.
Im Folgenden erfahren Sie, welche **Chancen und Herausforderungen** die Digitalisierung für Unternehmen bereithält und worauf diese besonders achten müssen. Zudem erfahren Sie mehr über die **Gewinner** und **Verlierer der Digitalisierung**, denn in Bezug auf die Digitalisierung gilt:
Wer nicht mit der Zeit geht, der geht mit der Zeit!



Beginnen wir mit den **Vorteilen**, die der Einsatz von **digitalen Informations- und Kommunikationstechnologien** in Unternehmen mit sich bringt:
Sie alle haben wahrscheinlich schon einmal etwas Online gekauft und kennen die zahlreichen Vorteile, von denen Sie als Kunde profitieren – Sie sparen Zeit und Nerven und möglicherweise auch Geld, weil Sie online Angebote vergleichen können. Das führt dazu, dass die **Zufriedenheit der Kunden steigt**.
Da die neuen Technologien Arbeitsschritte effizienter gestalten oder automatisieren, kann die **Leistung** des Unternehmens **gesteigert werden**. Auch sind die Mitarbeitenden flexibler, Meetings können über Videokonferenzen stattfinden etc. Zudem können **Arbeitskräfte eingespart** werden, was die **Personalkosten** des Unternehmens **senkt**.
Die neuen Technologien ermöglichen außerdem **neue Geschäftsmodelle**, etwa Online-Shops oder die Zustellung von Essen, das online bestellt werden kann.

Merken
Zusammengefasst bietet die **Digitalisierung** Unternehmen die folgenden **Vorteile**: • Zufriedenere Kunden • Leistungssteigerung • Kostenersparnis • Neue Geschäftsmodelle

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Gewinner der Digitalisierung

Wenn es einem Unternehmen gelingt, diese Vorteile geschickt zu nutzen, zählt es zu den **Gewinnern der Digitalisierung**. Ein gutes Beispiel ist hier der Online-Versandhändler **Amazon**, der etablierte Versandunternehmen wie Quelle mit einem innovativen Online-Konzept mit Zwischenhändlern vom Markt verdrängte.

Bestimmt sind Ihnen noch viele andere **Gewinner der Digitalisierung** bekannt. Etwa der Vermittlungsdienst **Uber**, der online Möglichkeiten zur Beförderung von Personen anbietet, oder der Marktplatz **Airbnb**, der auf einer Online-Plattform kurz- oder längerfristig Unterkünfte vermittelt.

Ein weiterer bekannter Gewinner der Digitalisierung ist der Hard- und Softwareentwickler **Apple.**

Beispiel
1967 gründeten Steve Jobs und Steve Wozniak gemeinsam mit ihrem Freund Ronald Wayne in Kalifornien Apple Computers Inc. Das Trio arbeitet an den ersten **Personal Computers (PCs)**, erkannte allerdings bald, dass es innovative Ideen braucht, um sich gegen Konkurrenten wie IBM durchzusetzen. 1984 feiert das Unternehmen große Erfolge mit der Entwicklung des **Macintosh (Mac)**, der sich mit einer **Maus** steuern ließ und über eine **grafische Benutzeroberfläche** verfügte – beides Neuheiten auf dem Markt. 2007 wird schließlich mit großem Erfolg das **iPhone** eingeführt – ein **Telefon** mit neuartigem **Touchscreen**, das auch als „**Internet-Communicator**“ zu benutzen ist. Trotz anfänglicher technischer Probleme wie verstopften Mobilfunknetzen ließ sich Apple nicht von seiner Vision abbringen. Die Kunden waren bald überzeugt: Apple dominiert jahrelang den mobilen Markt für Smartphones und Tablets und zählt auch heute noch zu den wertvollsten Marken weltweit.

Das Beispiel von Apple zeigt, dass Unternehmen sowohl ein **Gespür für Trends** und **Erfindergeist** als auch den **Mut** benötigen, eine erfolgsversprechende Innovation einzuführen, auch wenn dabei das Risiko besteht, **zu scheitern**. Dies bringt uns zu den Herausforderungen, vor die die Digitalisierung Unternehmen stellt. Sehen wir uns im folgenden Teil die **Herausforderungen** an, denen sich Unternehmen stellen müssen, wenn sie zu den **Gewinnern der Digitalisierung** zählen wollen.

Herausforderungen der Digitalisierung für Unternehmen

Um mithalten zu können, muss ein Unternehmen eine **geeignete Strategie** entwerfen, die auch der Belegschaft mitgeteilt werden sollte. Denn gerade in Bezug auf die Digitalisierung benötigt das Personal Orientierung und Sicherheit.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Auch sollten **flexible Arbeitszeitmodelle** bzw. die Möglichkeit, **von zuhause aus** zu arbeiten, angeboten werden, weil die neuen Technologien dies einfach zulassen. Zudem sollte in **neue Informations- und Kommunikationsmittel** und **Weiterbildung** der Arbeitskräfte investiert werden, damit diese auch mit den neuen Technologien umgehen können.
Schließlich müssen **gesetzliche Vorgaben**, insbesondere in Bezug auf den Datenschutz, beachtet werden, denn die neuen Technologien werfen diesbezüglich zahlreiche Fragen auf. Größere Unternehmen haben daher bereits oftmals eigene Datenschutzbeauftragte.

Beispiel
Was bedeutet es nun für ein kleineres Bekleidungsgeschäft, dass man plötzlich auch alles online kaufen kann? Der Geschäftsführer entschließt sich möglicherweise dazu, einen Online-Shop einzurichten, um den Kunden dieselben Vorteile bieten zu können, wie ein großes Online-Versandunternehmen. Er hat damit bereits eine Strategie entworfen und investiert in eine Umstrukturierung: Es wird weniger Personal im Verkauf benötigt, dafür mehrere neue Personen, die den Online-Shop einrichten, betreiben und warten. Dabei müssen natürlich auch die geltenden Datenschutzrichtlinien beachtet werden. Einige Mitarbeiter und Mitarbeiterinnen werden umgeschult, andere neu aufgenommen.

Merken
Zusammengefasst sind die **Herausforderungen der Digitalisierung** für Unternehmen: • Entwerfen einer geeigneten Strategie • Anbieten von flexiblen Arbeitszeitmodellen und Home-Office • Investitionen in neue Informations- und Kommunikationsmittel und Weiterbildungen • Einhalten gesetzlicher Vorgaben

Verlierer der Digitalisierung
Unternehmen, die nicht rechtzeitig erkennen, dass es an der Zeit für einen Wandel ist, oder einfach nicht den Mut dazu haben, zählen zu den **Verlierern der Digitalisierung**.
Bestimmt ist Ihnen **Kodak**, der ehemalige Weltmarktführer für fotografische Ausrüstung, ein Begriff. Aus Angst, sein klassisches Filmgeschäft zu gefährden, entwickelte Kodak die Digitaltechnik nur langsam weiter. Zu langsam. Denn nach 2000 brach das traditionelle Geschäft mit Filmen regelrecht ein. Kodak schaffte den Anschluss an die Digitalfotografie nicht mehr und musste 2012 Insolvenz anmelden.
Auch **Quelle**, das ehemals größte Versandhaus Europas, scheiterte an der Digitalisierung, weil es zu spät in den Online-Handel einstieg. Ein weiteres Beispiel für einen Verlierer der Digitalisierung ist der finnische Mobilgerätehersteller und ehemaliger Weltmarktführer **Nokia**.

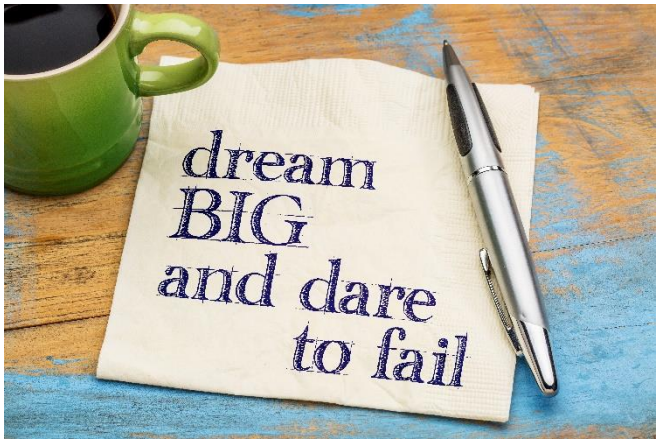
Beispiel
Bereits in den 90er-Jahren hatte Nokia noch vor Apple ein **Smartphone** entwickelt. Allerdings brachte Nokia das Gerät nicht auf den Markt. Der Grund dafür war die **Fehleinschätzung**, dass das Gerät **zu teuer in der Herstellung** sei und die Konsumenten nicht bereits sein würden, den Preis dafür zu bezahlen. Zudem wurde danach öffentlich bekannt, dass zu dieser Zeit im Nokia-Konzern ein sehr **schlechtes Arbeitsklima** herrschte, das vor allem von **Angst vor Fehlern** geprägt war. Die Belegschaft fürchtete sich zum Teil so sehr davor, die Jobs zu verlieren, dass sie die Ergebnisse von Studien fälschten, um den Geschäftsführer zufrieden zu stellen. Als Apple 2007 erfolgreich das **iPhone** auf dem Markt einführte, war es für Nokia zu spät – der Konzern schaffte den Anschluss nicht mehr. Nach Microsoft übernahm HMD Global das Unternehmen und hat heute mäßigen Erfolg.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Fassen wir also zusammen:
Wenn ein Unternehmen zu den Gewinnern der Digitalisierung zählen will, sind folgende Dinge besonders wichtig:

- Ein Unternehmensklima, das Innovationen fördert
- Langfristiges Denken
- Eine Kultur des Scheiterns



Denn wer sein erfolgversprechendes Produkt lieber monatelang diskutiert und prüft, anstatt es einfach auf dem Markt zu testen, und damit **bewusst ein Scheitern riskiert**, wird abgehängt. In einer Geschäftswelt, die einer immer **schnelleren Veränderung** unterworfen ist, sollte keine Zeit mit **unnötigen Zweifeln** verschwendet werden.

1.5 Die neue Arbeitswelt aus Sicht der Mitarbeiter und Mitarbeiterinnen

Neben den Unternehmen sind es vor allem die **Mitarbeitenden**, die von den Veränderungen betroffen sind, welche die Digitalisierung mit sich bringt. Viele Menschen sind verunsichert, andere haben sich bereits an die Veränderungen angepasst oder sogar davon profitiert. In der folgenden Einheit werden wir der Frage nachgehen, was das **„neue Arbeiten“** in einer **Arbeitswelt 4.0** eigentlich für die **Arbeitnehmer und Arbeitnehmerinnen** bedeutet.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Was verstehen Sie unter **Arbeitswelt 4.0** und **New Work**?

Wir haben bereits einiges über die Vierte Industrielle Revolution gehört und wissen auch, dass diese noch im Gange ist. Die Arbeitswelt 4.0 vereint nun alle **Arbeitsformen** und **Arbeitsbedingungen** der **Vierten Industriellen Revolution** bzw. der **Industrie 4.0.** Kennzeichnend für die Arbeitswelt 4.0 ist vor allem die **Digitalisierung**. Prozesse werden **digital unterstützt** und manchmal auch **vollständig automatisiert**, viele Menschen arbeiten **zeit- und ortsunabhängig** und die gesamte Wirtschaft ist **vernetzt**.

Oft verbringen Mitarbeitende in der **Arbeitswelt 4.0** einen Großteil Ihrer Arbeitszeit mit **digitalen Arbeiten** am **PC**. Mitarbeitende in der Produktion bedienen oftmals nur noch IT-Systeme, um die Maschinen zu steuern, welche die eigentliche Arbeit erledigen.

Natürlich gibt es auch immer noch Arbeiten, die **manuell** also mit den **Händen** ausgeführt werden. So wird sich wohl kaum jemand gerne von einem **Roboter** den Blinddarm entfernen lassen. Aber auch in den **OP-Sälen** halten bereits die **Roboter** Einzug. Allerdings bisher nur als **Assistenten**, da die Arbeit eines Chirurgen einfach **zu komplex** ist, um sie vollständig zu automatisieren.

Der Ausdruck **New Work** (dt. Neue Arbeit) wird verwendet, wenn darüber gesprochen wird, wie sich die **Digitalisierung** auf die **Arbeitswelt auswirkt.** Hier geht es vor allem darum, dass die Arbeitnehmer und Arbeitnehmerinnen die Freiheit haben, ihre Arbeit nach ihren eigenen Wünschen und Bedürfnissen zu gestalten. Hierzu zählen unter anderem die **zeitliche und örtliche Flexibilität**, die eine Arbeit vom eigenen PC aus mit sich bringt.

Definition
Arbeitswelt 4.0 ...beschreibt eine Arbeitswelt, die alle **Arbeitsformen** und **Arbeitsbedingungen** der **Vierten Industriellen Revolution** bzw. der **Industrie 4.0** vereint und die vor allem von der **Digitalisierung** geprägt ist.

Definition
New Work ...beschreibt, wie sich **Digitalisierung** auf die **Arbeitswelt auswirkt**. Dazu zählen insbesondere die **Freiheiten**, die **Arbeitnehmer und Arbeitnehmerinnen** bei der **Gestaltung** ihrer **Arbeitsbedingungen** in der neuen Arbeitswelt haben.

Vorteile der Arbeitswelt 4.0 für Arbeitnehmer und Arbeitnehmerinnen

Diese neuen Entwicklungen bringen für die Arbeitnehmer und Arbeitnehmerinnen zahlreiche **Vorteile**. Immer mehr Unternehmen bieten die Arbeit von zuhause, aus dem sogenannten **Home-Office**, an. Die Mitarbeitenden können so **Beruf und Familie besser vereinen** und etwa zuhause sein, wenn das Kind krank ist. Auch Reisen müssen nicht mehr unbedingt nur im Urlaub stattfinden, theoretisch ist ein Arbeiten auch von einem Strand in Thailand aus möglich – vorausgesetzt natürlich, die Internetverbindung funktioniert.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Durch neue Informations- und Kommunikationstechnologien wie etwa Skype ist die **Kommunikation** zwischen Mitarbeitern und Vorgesetzten auch über **Chats oder Videokonferenzen** möglich, Personal muss daher z.B. bei Besprechungen nicht immer persönlich anwesend sein, was oftmals mit einer Anreise verbunden ist. So kann Zeit und Geld gespart werden.

Auf der anderen Seite tragen die Mitarbeitenden die **Verantwortung** dafür, ihre Arbeitszeiten nach den Erfordernissen des Unternehmens zu **planen** und müssen dafür Sorge tragen, dass ihre Arbeit rechtzeitig erledigt wird. Diese größere **Eigenverantwortung** ist für viele Menschen eine Motivation, engagierter zu arbeiten, kann aber auch zur Belastung werden.

Zudem entstehen **neue Arbeitsmodelle**, etwa lagern immer mehr Unternehmen einzelne Arbeitsschritte an Freelancer aus, die diese zeitlich und örtlich unabhängig von ihrem eigenen PC aus erledigen. So beschäftigen Übersetzungsbüros oftmals freiberufliche Lektoren, die Texte von ihrem eigenen PC aus auf Fehler überprüfen.

Merken
Zusammengefasst bietet die Arbeitswelt 4.0 den Arbeitnehmern und Arbeitnehmerinnen folgende **Vorteile**: • Zeitliche und örtliche Flexibilität, bessere Vereinbarkeit von Beruf und Familie und einfachere Planung von Reisen, Freizeitaktivitäten etc. • Digitale Kommunikation mit Kollegen und Kolleginnen sowie mit Führungskräften • Größere Eigenverantwortung • Neue Arbeitsmodelle

Aber wo viel Licht ist, muss auch Schatten sein. Denn die Arbeitswelt 4.0 verlangt den Arbeitnehmern und Arbeitnehmerinnen einiges ab. Im Folgenden erfahren Sie, mit welchen **Herausforderungen** die Arbeitnehmer und Arbeitnehmerinnen in der Arbeitswelt 4.0 konfrontiert sind:

Herausforderungen der Arbeitswelt 4.0 für Arbeitnehmer und Arbeitnehmerinnen

Für zahlreiche Mitarbeitende bedeutet die Digitalisierung vor allem eines: **Unsicherheit.** Viele Menschen fürchten, dass sie durch einen **Roboter ersetzt** werden oder sich ihr Aufgabenbereich derartig verändert, dass sie sich völlig **neue Kompetenzen** aneignen müssen.

Allerdings ist hier, anders als bei Unternehmen, weniger Mut, sondern vor allem **Anpassungsfähigkeit** und **Flexibilität** gefragt. Aber Vorsicht: Bietet ein Unternehmen seinen Mitarbeitenden etwa die Arbeit aus dem Home-Office an, verlangt dafür aber, dass diese an abgesprochenen Tagen auch außerhalb

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

der regulären Arbeitszeiten zur Verfügung stehen, sollte es dafür klare Regelung geben, die mit dem Arbeitsrecht vereinbar sind.

Die **ständige Verfügbarkeit** ist die Schattenseite dieser besseren Vereinbarkeit der Berufstätigkeit mit Familie und Freizeit. Denn wer sich tagsüber Zeit für Kinder oder Freizeitaktivitäten nehmen darf, wird auch in Kauf nehmen müssen, abends noch vor dem PC zu sitzen, wenn andere längst ihren Feierabend genießen.

Dass man nicht mehr täglich die Kollegen und Kolleginnen im Büro triff, kann zudem zur **sozialen Vereinsamung** führen. Auch ist ein gutes **Zeitmanagement** ist ein Muss, damit der Traum vom flexiblen Arbeiten nicht zum Albtraum wird, der im Burn-out endet.

Denn der **Druck** auf die Arbeitnehmer und Arbeitnehmerinnen nimmt zu. Oftmals wird nicht mehr nur die ständige Verfügbarkeit erwartet, auch die **Aufgaben** der Mitarbeitenden werden **umfangreicher** und **komplexer**. Hinzu kommt noch, dass manche Mitarbeitenden auch in der ständigen Angst leben, bald vollständig von einem Computer ersetzt zu werden.

Wichtig sind in jedem Fall eine **zeitgemäße IT-Ausstattung**, **Weiterbildungen** und die Bereitschaft zu einem **lebenslangen Lernen**. Denn wenn ein Unternehmen neue Computerprogramme einsetzt, müssen die Mitarbeitenden auch damit arbeiten können.

Freelancer müssen mit der Zeit gehen, um mit den neuesten Programmen und Systemen ihrer Branche vertraut zu sein. Auch hier ist **Eigenverantwortung** gefragt, um in der Arbeitswelt 4.0 erfolgreich zu sein.

Merken
Zusammengefasst stellt die Arbeitswelt 4.0 die Arbeitnehmer und Arbeitnehmerinnen vor folgende **Herausforderungen**: • Flexibilität vs. ständige Verfügbarkeit • Steigender Druck auf Mitarbeitende • Soziale Vereinsamung • Zeitmanagement • Zeitgemäße IT-Ausstattung • Stetige Weiterbildungen und lebenslanges Lernen

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Doch wie sieht die **Realität in Europa** aus und welchen Einfluss hat der **Grad der Digitalisierung** eines Landes auf dessen Wettbewerbsfähigkeit?

Bereits 2016 zeigt eine Gegenüberstellung der Europäischen Kommission, dass die **Wettbewerbsfähigkeit** von Ländern (gemessen z.B. an dem Einkommen pro Kopf, der Produktivität oder dem Humankapital) direkt mit dem Grad der Digitalisierung zusammenhängt. Demensprechend erzielen Länder mit einem hohem Digitalisierungsgrad ein hohes Einkommen pro Kopf.

Ein Bericht der Kommission von 2019 zeigt außerdem, dass Investitionen und entschlossene Digitalisierungsmaßnahmen die Leistungsfähigkeit der Mitgliedstaaten fördern. Der **Digitalisierungsgrad** ist allerdings (gemessen am Entwicklungsniveau) in **Österreich** im Vergleich zu anderen EU-Ländern **unterdurchschnittlich**, an der Spitze stehen die skandinavischen Länder, die Beneluxstaaten und Irland. In einigen Einzelbereichen schneidet Österreich aber auch ganz gut ab:

So hat Österreich etwa in der **Digitalisierung öffentlicher Leistungen** und der **digitalen Kompetenzen und Fertigkeiten** die Nase vorn. Aufholbedarf besteht in den Bereichen **Konnektivität und Internetnutzung**, zudem ist die **Verfügbarkeit von schnellen Breitbandverbindungen** oftmals nicht zeitgemäß.

1.6 Die Arbeitswelt von morgen

Die Frage, die Arbeitnehmer und Arbeitnehmerinnen und auch die Auszubildende wohl am meisten beschäftigt ist: Wie wird mein **Arbeitsplatz** in der **Zukunft** aussehen? Denn wie bereits erwähnt sind viele Menschen durch die **Digitalisierung** und die damit einhergehenden **Veränderungen** verunsichert. Welche Tätigkeiten werden auch noch in der **Arbeitswelt von morgen** gefragt sein und welche **Rolle** werden **Computer** und **Roboter** dabei spielen?

Studien zeigen

Viel Lärm um eine Studie

Die beiden Forscher der Oxford Universität Carl Benedikt Frey und Michael A. Osborne veröffentlichten 2013 eine Studie zur **Zukunft der Arbeitswelt**, die vielen Menschen Angst machte: Die Studie gab an, dass **47 Prozent** aller **Jobs** in den USA Gefahr laufen, in den kommenden ca. 10-20 Jahren **automatisiert** zu werden (vgl. Frey and Osborne (2013): The Future of Employment: How Susceptible Are Jobs To Computerisation?, Oxford Martin School (OMS) working paper, University of Oxford, Oxford).

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Eine Studie der **Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD)** aus dem Jahr 2016 zeigte aber, dass diese Befürchtungen unbegründet sind und besagt, dass in den **21 untersuchten OECD-Ländern** nur durchschnittlich **9 Prozet aller Jobs automatisiert** werden können. Für Österreich liegt der Prozentsatz bei **12 Prozent** (Arntz, Gregory und Zierahn (2016): The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis, OECD Social, Employment and Migration Working Papers No. 189, Paris)

Um eine **Prognose für die Zukunft** erstellen zu können, ist es sinnvoll, sich zunächst die **Entwicklungen** in der **jüngsten Vergangenheit** anzusehen.

Zum besseren Verständnis teilen wir die Tätigkeiten in sechs verschiedene Kategorien ein:

- **analytische Tätigkeiten** (Tätigkeiten, für die abstraktes Denken erforderlich ist, etwa das Erstellen einer Prognose für die Marktforschung)
- **interaktive Tätigkeiten** (Tätigkeiten, in die andere Menschen einbezogen sind, etwa das Verkaufen von Schuhen)
- **kognitive Tätigkeiten** (Tätigkeiten, für die kognitive Prozesse wie Erinnern, Lernen, Vergleichen etc. erforderlich sind, etwa das Übersetzen eines Textes)
- **manuelle Tätigkeiten** (Tätigkeiten, die mit den Händen verrichtet werden, etwa das Anpflanzen von Gemüse)
- **Routinetätigkeiten** (Tätigkeiten, bei denen es sehr viele Wiederholungen gibt, etwa die Arbeit am Fließband)
- **Nicht-Routinetätigkeiten** (abwechslungsreiche Tätigkeiten, bei denen man sich immer wieder auf neue Gegebenheiten einstellen muss)

Können Sie sich vorstellen, welche Tätigkeiten in den vergangenen Jahren an Bedeutung gewonnen haben und welche unbedeutender geworden sind? In folgender Grafik sehen Sie, welche Entwicklung seit 1995 beobachtet werden kann:

Analytische kognitive Nicht-Routinetätigkeiten wie z.B.

- Forschen
- Ausarbeiten von Regeln
- Controlling
- Singen

Interaktive kognitive Nicht-Routinetätigkeiten

- Verhandeln
- Koordinieren
- Marketingtätigkeiten
- Training

Kognitive Routinetätigkeiten wie z.B.

- Kalkulieren
- Korrigieren von Texten
- Erstellen der Buchhaltung
- Mechatronik

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Manuelle Nicht- Routinetätigkeiten wie z.B.

- Häuser renovieren
- Therapie (manuell)
- Restaurieren von Kunst
- handwerkliche Tätigkeiten wie Tischlern

Manuelle Routinetätigkeiten wie z.B.

- Erzeugung
- Maschinen bedienen oder kontrollieren
- Ernten von Getreide, Obst oder Gemüse
- Anbauen von Nahrungsmitteln

Merken
Manuelle Tätigkeiten und **Routinetätigkeiten** (mit Ausnahme von **kognitiven Routinetätigkeiten**) haben seit 1995 an Bedeutung verloren und man kann davon ausgehen, dass dieser **Trend** auch in **Zukunft anhalten** bzw. sich noch weiter **verstärken** wird. Immer wichtiger werden jedoch **Analytische** und **Interaktive kognitive Nicht-Routine-Tätigkeiten.**

Jobs mit Zukunft
Die beste Maßnahme gegen Arbeitslosigkeit ist nach wie vor die **Bildung** – rund zwei Drittel aller durch die Digitalisierung gefährdeten Jobs sind Jobs von **Hilfsarbeitskräften, Handwerkern und Handwerkerinnen oder Dienstleistern und Dienstleisterinnen**. Je höher die abgeschlossene Bildung der Arbeitskräfte ist, desto geringer ist auch die Wahrscheinlichkeit, dass deren Tätigkeit vollständig automatisiert werden kann.

An Bedeutung gewinnen werden wahrscheinlich **soziale und kreative Berufe** wie Lehrer und Lehrerin, Grafiker und Grafikerin oder Pfleger und Pflegerin. Auch Tätigkeiten **im Management** wie Projektmanagement oder Controlling und **technische Berufe** bzw. Berufe, in denen ausgeprägte **feinmotorische Fähigkeiten** erforderlich sind, werden zunehmen gefragter. So werden Arbeitnehmer und Arbeitnehmerinnen in den folgenden Bereichen auch in Zukunft gefragt sein:

Soziale Berufe:
- Ärzte und Ärztinnen
- Lehrer und Lehrerinnen
- Pflegekräfte und -manager bzw. -managerinnen
- Sozialarbeiter und Sozialarbeiterinnen

Kreative Berufe:
- Grafiker und Grafikerinnen
- Texter und Texterinnen
- Social Media Manager und Managerinnen

Berufe im Management:
- Controlling
- Projektmanagement
- Kundenmanagement -und -betreuung

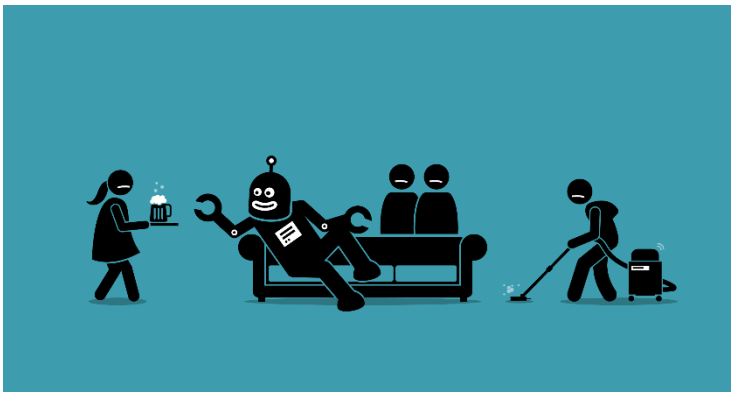
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

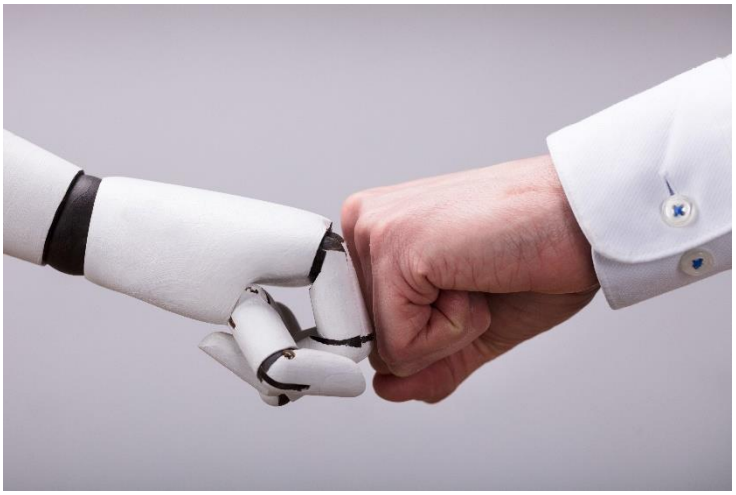
Technische Berufe:

- Mechatroniker und Mechatronikerinnen
- IT-Projektleiter und -Projektleiterinnen
- IT-Sicherheitsexperten und -expertinnen
- Lebensmitteltechniker und -technikerinnen

Zukunfts-Szenarien



oder



Wie stellen Sie sich konkret die **Arbeitswelt der Zukunft** vor? Sehen Sie die **Menschen** als **untertänige Diener** der **Maschinen** oder träumen Sie von einer Welt, in der die **Maschinen** den **Menschen** als **treue Assistenten** zur Seite stehen und ihnen zu **neuen Höhenflügen** verhelfen?

Tatsächlich existieren sowohl positive als auch negative Zukunftsprognosen, was das **Zusammenspiel von Mensch und Maschine** betrifft: Es könnte sein, dass immer mehr automatisiert wird, die **Maschinen** sich selbst steuern und für die **Menschen** nur noch „niedere“ ausführende Tätigkeiten (etwa im Lager) bleiben. Wünschenswerter ist allerdings, dass **IT-Assistenzsysteme hochqualifizierten Fachkräften** wie etwa Ärzten gute Dienste leisten, die Entscheidungen aber weiterhin der Mensch trifft.

Denn es sollte nicht vergessen werden, dass der Mensch über **Kreativität, Gefühle, Leidenschaft, Vorstellungskraft, Respekt, Meinung** und die Fähigkeiten verfügt, **unvorhergesehene Situationen zu bewältigen**, und dem Roboter daher in diesen Bereichen immer noch weit überlegen ist. Dass an der Digitalisierung dennoch kein Weg vorbeiführt, sollte in dieser Einheit bereits klargeworden sein. Wie

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

aber in der Praxis damit umgegangen wird, bleibt der Gesellschaft und damit jedem einzelnen von uns überlassen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.7 Zusammenfassung

Digitalisierung und **Digitale Transformation** – die digitale Verarbeitung und Abbildung von Informationen und die dadurch ausgelösten Veränderungen wie die **Automatisierung** von Arbeit und die Entwicklung von **künstlichen Intelligenzen** – sind heute allgegenwärtig und bringen sowohl Unsicherheit als auch Chancen und Möglichkeiten mit sich.

Dabei ist **Wandel und Veränderung** in einer Gesellschaft ganz natürlich. Eigentlich beeindruckend, dass wir es in den vergangenen ca. 250 Jahren von der **Ersten Industriellen Revolution** und der Erfindung der Dampfmaschine bis hin zur **Industrie 4.0** und vernetzten Fahrzeugen geschafft haben.

Digitalisierung ist heute ein wichtiger Faktor, um **wettbewerbsfähig** zu sein. Dies gilt sowohl für einzelnen Arbeitnehmer und Arbeitnehmerinnen als auch für Unternehmen und ganze Staaten. Während Unternehmen vor allem innovativ, schnell in der Umsetzung und mutig sein müssen, um mithalten zu können, geht es für Arbeitnehmer und Arbeitnehmerinnen eher darum, sich jene Fähigkeiten anzueignen, die in der Arbeitswelt 4.0 gefragt sind.

Für **Unternehmen** bedeutet eine erfolgreiche Umsetzung der Digitalisierung einerseits eine Steigerung der Leistung, Kostenersparnis, das Auftauchen von neuen Geschäftsmodellen aber auch zufriedenere Kunden. Sie müssen sich allerdings mehr Gedanken über Datenschutzvorschriften machen, eine geeignete Digitalisierungsstrategie entwerfen, in neue Informations- und Kommunikationsmittel investieren und den Arbeitnehmern und Arbeitnehmerinnen geeignete Weiterbildungen und flexible Arbeitsbedingungen bieten.

Arbeitnehmer und Arbeitnehmerinnen profitieren davon, zeitlich und örtlich flexibler zu sein, Beruf und Familie besser vereinbaren zu können und bei der Reiseplanung nicht mehr Rücksicht auf den Betriebsurlaub oder ähnliches nehmen zu müssen. Zudem erhalten sie im Zuge der Digitalisierung mehr Eigenverantwortung. Dies bringt allerdings auch einen steigenden Druck mit sich. Das Wissen, ständig verfügbar sein zu müssen und das zunehmende Verschwimmen von Arbeitszeit und Freizeit kann zu einem Absinken der Lebensqualität und im schlimmsten Fall zu einem Burn-out führen. Zudem sind Arbeitnehmer und Arbeitnehmerinnen gefordert, sich selbst um ein lebenslanges Lernen und eine zeitgemäße IT-Ausstattung zu bemühen.

In Bezug auf den **Arbeitsmarkt** ist es wichtig zu wissen, dass **manuelle Tätigkeiten** in Zukunft eher an Bedeutung verlieren werden, wohingegen **kognitive Tätigkeiten** immer bedeutender werden. Neben IT-Fachkräften wird auch in Zukunft ein großer Bedarf an Pflegekräften, medizinischem Fachpersonal, Lehrpersonal und Technikern und Technikerinnen bestehen. Es ist schwer vorauszusagen, wie die **Zukunft der Digitalisierung** aussehen wird. Fest steht allerdings, dass wir alle gefordert sind, sie

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.8 ÜBUNGEN

1. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Industrielle Revolution
_____ ist in einer Gesellschaft normal und natürlich, _____ ebenso. Ab dem späten 18. Jahrhundert bezeichnet man Phasen, in denen es bahnbrechende Fortschritte in der Produktion gab, wie etwa die Einführung von dampfgetriebenen Spinnrädern oder Fließbandarbeit, als _____. Ein Kennzeichen der Industriellen Revolutionen sind Veränderungen der _____ der Menschen. Denn neue Produktionstechniken wie etwa die Dampfmaschine oder der PC hatten tiefgreifende Auswirkungen auf die Wirtschaft und die Gesellschaft. Sowohl Arbeitgeber als auch Arbeitnehmer mussten sich an die _____ anpassen.

1 Lebensumstände, 2 Fortschritt, 3 neuen Bedingungen,4 Industrielle Revolution, 5 Veränderung

2. Digitalisierung bringt _____ Veränderungen für die beteiligten Unternehmen mit sich.
a. keine
b. einige
c. zahlreiche
d. manche

3. Einer der Vorteile, die die Digitalisierung den Unternehmen bietet, ist _____
a. zufriedene Kunden
b. Fixkosten
c. mehr Beschäftigung
d. weniger Videokonferenzen

4. Die Möglichkeit, von zu Hause aus zu arbeiten, sollte _____
a. weniger als üblich sein
b. allgemein angeboten werden
c. vermieden werden
d. nur für Verwaltungsangestellte möglich sein.

5. Ein weiterer Gewinner der Digitalisierung ist der Hard- und Software-Entwickler _____
a. Microsoft
b. Huawei
c. Apple
d. IBM

6. Beispiele für Verlierer der Digitalisierung sind _____
a. Motorola und Nokia
b. Kodak und Motorola
c. Nokia und Ericsson
d. Nokia und Kodak

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Arbeitswelt 4.0 und New Work
Wir haben bereits einiges über die Vierte Industrielle Revolution gehört und wissen auch, dass diese noch im Gange ist. Die Arbeitswelt 4.0 vereint nun alle Arbeitsformen und _____ der Vierten Industriellen Revolution bzw. der Industrie 4.0. Kennzeichnend für die Arbeitswelt 4.0 ist vor allem die _____. Prozesse werden digital unterstützt und manchmal auch vollständig automatisiert, viele Menschen arbeiten zeit- und ortsunabhängig und die gesamte Wirtschaft ist _____. Oft verbringen _____ in der Arbeitswelt 4.0 einen Großteil Ihrer Arbeitszeit mit digitalen Arbeiten am PC. Mitarbeitende in der Produktion bedienen oftmals nur noch IT-Systeme, um die Maschinen zu steuern, welche die eigentliche Arbeit erledigen. Natürlich gibt es auch immer noch Arbeiten, die manuell also mit den Händen ausgeführt werden. So wird sich wohl kaum jemand gerne von einem Roboter den Blinddarm entfernen lassen. Aber auch in den _____ halten bereits die Roboter Einzug. Allerdings bisher nur als Assistenten, da die Arbeit eines Chirurgen einfach zu komplex ist, um sie vollständig zu automatisieren. Der Ausdruck New Work (dt. Neue Arbeit) wird verwendet, wenn darüber gesprochen wird, wie sich die Digitalisierung auf die _____ auswirkt. Hier geht es vor allem darum, dass die Arbeitnehmer und Arbeitnehmerinnen die Freiheit haben, ihre Arbeit nach ihren eigenen Wünschen und Bedürfnissen zu gestalten. Hierzu zählen unter anderem die zeitliche und örtliche Flexibilität, die eine Arbeit vom eigenen PC aus mit sich bringt.

1 OP-Sälen, 2 Arbeitswelt, 3 vernetzt, 4 Arbeitsbedingungen, 5 Angestellte, 6 Digitalisierung

8. Richtig oder Falsch?

a. Um eine Prognose für die Zukunft abgeben zu können, ist es sinnvoll, zunächst die Entwicklungen in der jüngsten Vergangenheit zu betrachten.
   R □ F □
b. Es wird keine Nachfrage nach Managementjobs wie Projektmanagement geben.
   R □ F □
c. Die beste Maßnahme gegen Arbeitslosigkeit ist nach wie vor Bildung.
   R □ F □
d. Analytische und interaktive kognitive Nicht-Routine-Aktivitäten verlieren immer mehr an Bedeutung.
   R □ F □
e. Soziale und kreative Berufe wie Lehrer, Grafikdesigner oder Krankenschwester werden wahrscheinlich an Bedeutung verlieren.
   R □ F □

9. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Digitalisierung und Digitale _____ – die digitale Verarbeitung und Abbildung von Informationen und die dadurch ausgelösten Veränderungen wie die _____ von Arbeit und die Entwicklung von künstlichen Intelligenzen – sind heute allgegenwärtig und bringen sowohl Unsicherheit als auch Chancen und Möglichkeiten mit sich. Dabei ist Wandel und Veränderung in einer Gesellschaft ganz natürlich. Eigentlich beeindruckend, dass wir es in den vergangenen ca. 250 Jahren von der Ersten Industriellen Revolution und der Erfindung der Dampfmaschine bis hin zur _____ und vernetzten Fahrzeugen geschafft haben. Digitalisierung ist heute ein wichtiger Faktor, um _____ zu sein. Dies gilt sowohl für einzelnen Arbeitnehmer und Arbeitnehmerinnen als auch für Unternehmen und ganze Staaten. Während Unternehmen vor allem innovativ, schnell in der Umsetzung und _____ sein müssen, um mithalten zu können,

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

geht es für Arbeitnehmer und Arbeitnehmerinnen eher darum, sich jene Fähigkeiten anzueignen, die in der Arbeitswelt 4.0 gefragt sind.

1 mutig, 2 Transformation, 3 Industrie 4.0, 4 wettbewerbsfähig, 5 Automatisierung

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. CLOUD COMPUTING

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.1 Das Thema

Die erste Einführung

Sie kennen diese Situation bestimmt: Der Speicherplatz auf Ihrem Handy ist voll und der Download des aktuellen Software-Updates schlägt fehl. Doch das Problem ist rasch gelöst! Sie verschieben einfach den Ordner mit Ihren letzten Urlaubsfotos in die „Cloud".

Jetzt haben Sie wieder genug Speicherplatz auf Ihrem Handy und können das Update durchführen. Später am Abend können Sie Ihre Urlaubsfotos dann an Ihrem Computer bearbeiten und mittels eines Cloud Sharing Services wie etwa Dropbox oder Google Drive einfach mit Ihrer Familie und Ihren Freunden teilen. Und weil Sie schon dabei sind, speichern Sie auch gleich eine wichtige Word-Datei in der Cloud ab, die Sie morgen an Ihrem Arbeitsplatz benötigen.

Aber was bedeutet eigentlich „**etwas in der Cloud abspeichern**"? Was ist überhaupt eine „**Cloud**"? Welche Anwendungsbereiche gibt es und was steckt generell hinter dem Begriff „**Cloud Computing**"?

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Egal ob Sie ein etabliertes Unternehmen führen, ein Start-up mit einer innovativen Geschäftsidee gründen wollen oder das Internet nur als Privatperson nutzen. Der Begriff „Cloud Computing" ist in aller Munde und kaum mehr aus der modernen Informationstechnologie wegzudenken. Laut einer Umfrage der Europäischen Union nutzten 2018 bereits mehr als ein Viertel aller Unternehmen in der EU Cloud Computing Services. Und die Tendenz ist steigend!

Damit Sie sich selbst ein Bild über diesen zukunftsreichen IT-Trend machen können, werden Ihnen in dieser Lerneinheit die Grundideen des Cloud Computing nähergebracht. Sie erfahren, in welchen Bereichen die „Cloud" zum Einsatz kommt und wo Vorteile und Nachteile besagter Services liegen. So können Sie einschätzen, ob und in welcher Form Cloud Computing für Sie privat oder in der Berufswelt nützlich sein kann.

Lernziele und Kompetenzen im Überblick

Diese Lerneinheit gibt Ihnen einen Überblick über die Grundideen des Cloud Computing. Sie erfahren, was eine Cloud ist und wodurch Cloud Computing Services gekennzeichnet sind. Zusätzlich lernen Sie die wichtigsten Anwendungsbereiche des Cloud Computing kennen und erhalten Informationen zu den verschiedenen Typen von Clouds.
Außerdem erwerben Sie Wissen über die Vor- und Nachteile, die dieser IT-Trend mit sich bringt.

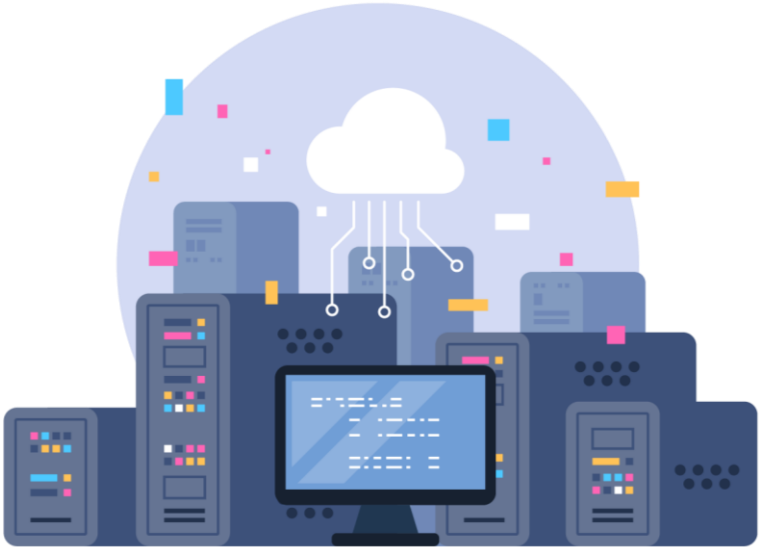
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Lernziele
Den Begriff Cloud Computing kennen und beschreiben.
Die fünf wichtigsten Merkmale von Cloud Computing aufzählen und definieren.
Die drei grundlegenden Anwendungsbereiche von Cloud Computing kennen und erklären.
Die vier Cloud Typen kennen und erklären.
Die Vorteile und Nachteile des Cloud Computing kennen und aufzählen.

2.2 Was bedeutet Cloud Computing?

Unter Cloud Computing versteht man ganz allgemein das **Anbieten und Nutzen von Informationstechnologie über ein Netzwerk** mehrerer verteilter Rechner. Im Normalfall handelt es sich bei diesem Netzwerk um das **Internet**.



Beim Cloud Computing werden Programme und auch Daten nicht mehr lokal auf dem eigenen Computer ausgeführt bzw. gespeichert, sondern sie liegen verteilt auf vielen verschiedenen externen Servern.

Auch auf **Rechenleistung** und auf **Plattformen** zur eigenständigen Softwareentwicklung kann auf diese Weise zugegriffen werden. Man nutzt dabei die geballten Ressourcen eines riesigen Netzwerks und ist nicht mehr auf die Leistung der eigenen Hardware angewiesen.

Das hat den großen Vorteil, dass Sie nicht mehr in eigene kostspielige IT-Infrastruktur investieren müssen. In der Regel bezahlen Sie beim Cloud Computing dann auch nur jenes Service, das Sie auch tatsächlich genutzt haben. **Sie „mieten" quasi IT-Dienstleistungen**.

Das Einzige, was Sie für den Zugriff auf die IT-Dienstleistungen via Cloud Computing unbedingt benötigen, sind ein **Browser** und eine **Internetverbindung**. Das Internet spielt also eine maßgebliche Rolle fürs Cloud Computing.

Tatsächlich spiegelt sich der zentrale Stellenwert des Internets für diese innovative Form der IT-Nutzung bereits im Namen selbst wider. Bestimmt fragen Sie sich schon die längste Zeit, warum es eigentlich „Cloud Computing" heißt, oder?

Co-funded by the Erasmus+ Programme of the European Union

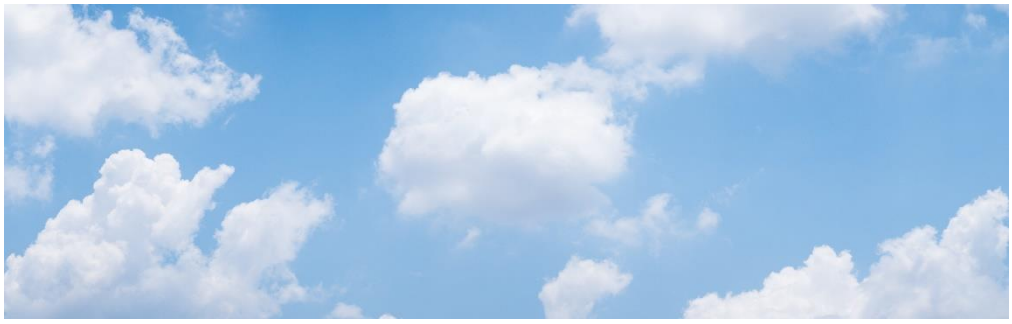
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Nun, die Beantwortung dieser Frage ist recht einfach: Der Begriff „Cloud“ (Englisch für *Wolke*) ist bloß eine **Metapher fürs Internet**. Man könnte Cloud Computing also im Prinzip auch einfach als **Internet-basiertes Computing** bezeichnen.

Exkurs

Warum ist die Wolke (engl. cloud) eine Metapher fürs Internet?

Mit dem bildhaften Vergleich mit einer *Wolke* (oder *cloud* auf Englisch) wird darauf angespielt, dass das Internet ein **abstrakter** und **formloser** digitaler Raum ist, der nur **schwer fassbar** ist – genauso wie eine Wolke.



Auch die Merkmale **Komplexität** und **Undurchsichtigkeit** kommen durch das Bild der Wolke in den Sinn.

In Wirklichkeit handelt es sich beim Internet bzw. der der Cloud natürlich um nichts Mystisches! Vielmehr steckt hinter dem Internet ein Netzwerk von **tatsächlich existierender Hardware**, also von vielen verschiedenen Computern. Diese bleiben allerdings bei der Nutzung des Internets für die Einzelpersonen unsichtbar.

Die Vagheit, die mit dem Begriff des Internets verbunden ist, trifft auch auf das Cloud Computing zu: Wenn Sie Cloud Computing nutzen, haben Sie keine Kenntnis darüber, auf welchem externen Server Ihre Daten gerade liegen oder von woher genau Sie die Rechenleistung beziehen. Dieses Wissen ist aber für Sie auch nicht notwendig. Der Zugriff auf die Ressourcen erfolgt ohne Ihr Zutun – gewissermaßen automatisch.

Das bedeutet, dass für Sie als Person, die Cloud Computing verwendet, die Metapher der Wolke durchaus zutrifft. Für ein besseres Verständnis sollten Sie allerdings in Hinterkopf bewahren, dass sich hinter dem Begriff der Cloud natürlich ein Netzwerk von tatsächlich existierenden Servern verbirgt.

Merken

Mit dem Begriff Cloud ist das Internet gemeint.

Wenn Sie z.B. etwas in der Cloud abspeichern, dann werden Ihre Daten in einem riesigen globalen Netzwerk von physikalisch realen Servern abgelegt. Dabei wissen Sie allerdings nicht, wo genau Ihre Daten gespeichert sind. Aus diesem Grund kommt die Metapher der komplexen und intransparenten Wolke bzw. Cloud zum Einsatz.

Jetzt wissen Sie also, was sich hinter dem – im wahrsten Sinne des Wortes – undurchsichtigen Begriff der Cloud verbirgt.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Auch haben Sie erfahren, dass es sich beim Cloud Computing im Grunde einfach um die **Internet-basierte Nutzung von IT-Ressourcen** handelt.

Wir können also folgende einfache Definition von Cloud Computing festhalten:

Definition
Cloud Computing **… bezeichnet die Bereitstellung und Nutzung von IT-Diensten über ein Netzwerk, in der Regel das Internet.** Beim Cloud Computing können Sie **überall** und **jederzeit** auf verschiedenste IT-Dienstleistungen zugreifen, ohne von der eigenen Hardware abhängig zu sein. Sie haben dabei Zugang zu Speicherkapazitäten, Rechenleistungen, Programmen oder sonstigen IT-Services eines riesigen Netzwerks an Servern. In der Regel bezahlen Sie allerdings nur für jenes Ausmaß an Service, dass Sie auch tatsächlich benötigen.

2.3 Merkmale von Cloud Computing

Nachdem Sie jetzt einen allgemeinen Überblick über das Thema Cloud Computing haben und wissen, was eine Cloud ist, wollen wir uns in einem nächsten Schritt die **wichtigsten Merkmale** dieses IT-Trends näher ansehen.

Die Bundesbehörde NIST (die Abkürzung steht für *National Institute of Standards and Technology*) der USA hat bereits 2011 einen Bericht zum Cloud Computing herausgegeben. Laut diesem Bericht gibt es **fünf wichtige Eigenschaften**, die Cloud Computing ausmachen.

Diese charakteristischen Merkmale von Cloud Computing sind wie folgt:

- **On-demand Self Service**
- **Broad Network Access**
- **Resource Pooling**
- **Rapid Elasticity**
- **Measured Services**

Bevor wir jedes dieser Merkmale genauer definieren, noch ein kurzes Beispiel:

Beispiel
Stellen Sie sich vor, Sie haben ein **kleines Unternehmen**, das aber **sehr große Datenmengen** verarbeiten und speichern muss. Eventuell haben Sie es mit hochauflösenden Bild- und Videodateien zu tun, die sehr viel Speicherplatz wegnehmen. **Ihre alte Festplatte ist schon ziemlich voll**. In ein paar Monaten erhalten Sie vielleicht einen sehr großen Auftrag, bei dem **noch viel mehr Daten** anfallen. Es kann aber auch sein, dass Sie den Auftrag doch nicht bekommen – Ihre Kundschaft möchte sich erst kurzfristig entscheiden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Was tun Sie?

Jetzt sind Sie sicher in der Zwickmühle! Sollen Sie sich eine neue sehr teure Festplatte leisten? Und wenn ja, wie groß soll sie sein? Und was ist, wenn es mit dem Auftrag doch nichts wird? Dann hätten Sie in neue kostspielige Hardware investiert, die Sie zurzeit gar nicht benötigen und die dann in Ihrem Materialraum verstaubt.

Vielleicht erkennen Sie schon, dass in diesem Fall **Cloud Computing** eine gute Lösung darstellt. Statt eine neue Festplatte zu kaufen, mieten Sie einfach Speicherkapazitäten über einen Cloud-Anbieter an.

Dabei können Sie **selbst entscheiden** und **anpassen**, wie viel Speicherplatz Sie nutzen wollen. Wenn Sie mehr brauchen, zahlen Sie mehr. Wenn Sie weniger brauchen, zahlen Sie weniger.

Es steht Ihnen die **komplette Kapazität der Cloud** auf Knopfdruck zur Verfügung und Sie sind dabei vollkommen **flexibel**.

An diesem Beispiel werden bereits einige der Hauptmerkmale des Cloud Computing ersichtlich. Gehen wir Sie gemeinsam durch.

Wie bereits oben erwähnt, ist eine wichtige Eigenschaft des Cloud Computing das so genannte **On-demand Self Service**. Damit ist einfach **Selbstbedienung** gemeint.

Beim Cloud Computing können Sie **selbständig** auf IT-Services aus der Cloud zugreifen – und zwar genau dann, wenn Sie diese brauchen. Sie müssen nicht mit jemanden telefonieren oder erst eine E-Mail schreiben, um z.B. mehr Speicherplatz zu bekommen. Der Zugriff erfolgt **automatisch**. Sie brauchen dafür nicht mit dem Cloud-Anbieter zu kommunizieren.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Definition
On-demand Self Service **… bedeutet, dass auf Cloud-Dienste automatisch, d.h. ohne Interaktionen mit den Cloud-Anbietern zugegriffen wird.** Sie bedienen sich also selbst. Sie nehmen sich einfach so viele Cloud-Ressourcen (z.B. Speicherplatz, Rechenleistung), wie Sie gerade benötigen und müssen dafür nicht erste beim Cloud-Anbieter anfragen.

Ein weiteres wichtiges Merkmal von Cloud Computing ist der **Broad Network Access**. Damit ist gemeint, dass Cloud Computing Services über ein **Netzwerk**, im Normalfall das Internet, angeboten werden.

So können Sie die Cloud-Dienste über verschiedenste Endgeräten (Stand-PC, Laptop, Smartphone etc.) nutzen und sind **lokal ungebunden**. Sie haben **immer und überall** Zugriff auf die Dienste und Daten. Die einzige Voraussetzung ist der Zugang zu einer Internetverbindung.

Definition
Broad Network Access **… bedeutet, dass der Zugriff auf Cloud-Dienste über ein Netzwerk erfolgt und Sie nicht an ein bestimmtes Endgerät gebunden sind.** Sie können somit überall und mit jedem internetfähigen Gerät (Laptop, Tablet, Smartphone usw.) auf die Cloud-Ressourcen zugreifen.

Ein ebenfalls sehr charakteristisches Merkmal von Cloud Computing ist das **Resource Pooling**. Das bedeutet, dass die IT-Ressourcen (z.B. Speicherplatz, Rechenleistung) quasi in einem großen geteilten „Becken“ (oder „Pool“) bereit liegen. Aus diesem **Becken an geteilten Ressourcen** können sich dann viele Personen bedienen.

Zu beachten ist, dass Anwender oder Anwenderinnen nicht wissen, von welchen spezifischen Servern gerade die IT-Ressourcen bezogen werden.

Sie können sich das auch so vorstellen: Angenommen Sie teilen sich mit Ihren Nachbarn einen Swimming Pool. Beim Befüllen liefert jeder Wasser aus seinem eigenen Gartenschlauch. Im Pool selbst,

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

weiß man aber dann natürlich nicht mehr, welcher Wassertropfen von welchem Gartenschlauch stammt.

Definition
Resource Pooling **… bedeutet, dass die IT-Ressourcen in einem gemeinsamen Sammelbecken zur Verfügung stehen und sich viele verschiedene Personen daran bedienen können.** Dabei fließen die IT-Ressourcen von verschiedenen Servern zusammen. Die Person, die Cloud Computing nutzt, weiß also nicht, von welchem Server genau die Ressourcen bezogen werden.

Ein weiteres sehr essentielles Merkmal des Cloud-Computing ist die **Rapid Elasticity**. IT-Ressourcen werden **schnell** und **elastisch**, d.h. flexibel und **an den Bedarf angepasst**, zur Verfügung gestellt.

Erinnern Sie sich an das Beispiel von vorhin? Da haben wir uns die Frage gestellt, ob Sie für Ihr Unternehmen eine neue Festplatte kaufen sollen und wenn ja, wie groß sie sein soll. Weil Sie nicht wussten, wie viel Speicherkapazität Sie tatsächlich brauchen, hätten Sie wahrscheinlich eine viel zu große Festplatte gekauft. Sie hätten also mehr Geld ausgegeben, als aktuell nötig gewesen wäre. Gleichzeitig hätten Sie sicher nach einiger Zeit wieder in eine neue Festplatte investieren müssen, sollte Ihr Unternehmen wachsen. Wenn Ihr Unternehmen hingegen stagniert oder schrumpft, würde die nagelneue Festplatte ungenützt herumliegen.

Mit Cloud Computing haben Sie diese Probleme nicht. Sie können rasch und flexibel IT-Ressourcen dazu mieten oder wieder kündigen. Einfach und genau in dem Ausmaß, in dem Sie die Ressourcen gerade benötigen.

Dieses Merkmal des Cloud Computing wird manchmal auch als **Skalierbarkeit** bezeichnet. Das bedeutet, dass die IT-Ressourcen mit Ihren Bedürfnissen oder Ihrem Unternehmen mitwachsen können. Sie können per Knopfdruck die Nutzung von Cloud-Dienste erweitern oder einschränken – je nach Bedarf.

Definition
Rapid Elasticity **… bedeutet, dass Sie beim Cloud-Computing die IT-Nutzung rasch und flexibel an Ihren tatsächlichen Bedarf anpassen können** Cloud-Dienste sind stufenlos erweiterbar. So können Sie zu Spitzenzeiten in Ihrem Unternehmen Dienste wie Speicherkapazitäten und Rechenleistungen dazukaufen. Wenn Sie die Dienste nicht mehr benötigen, schrauben Sie Ihre Nutzung einfach wieder zurück. So können Sie rasch und flexibel auf wirtschaftliche Entwicklungen reagieren.

Das letzte Merkmal von Cloud Computing, das Sie an dieser Stelle kennenlernen, wird als **Measured Services** bezeichnet. Das heißt, dass der Cloud-Anbieter die Nutzung der IT-Dienste durch die Einzelperson kontinuierlich misst und überwacht. So sorgt der Anbieter dafür, dass Sie immer so viele Ressourcen zu Verfügung haben, wie Sie benötigen. Gleichzeitig wird auch nur das abgerechnet, was Sie nutzen.

Definition
Measured Services **… bedeutet, dass die Nutzung der IT-Dienste vom Anbieter gemessen und kontrolliert wird.**

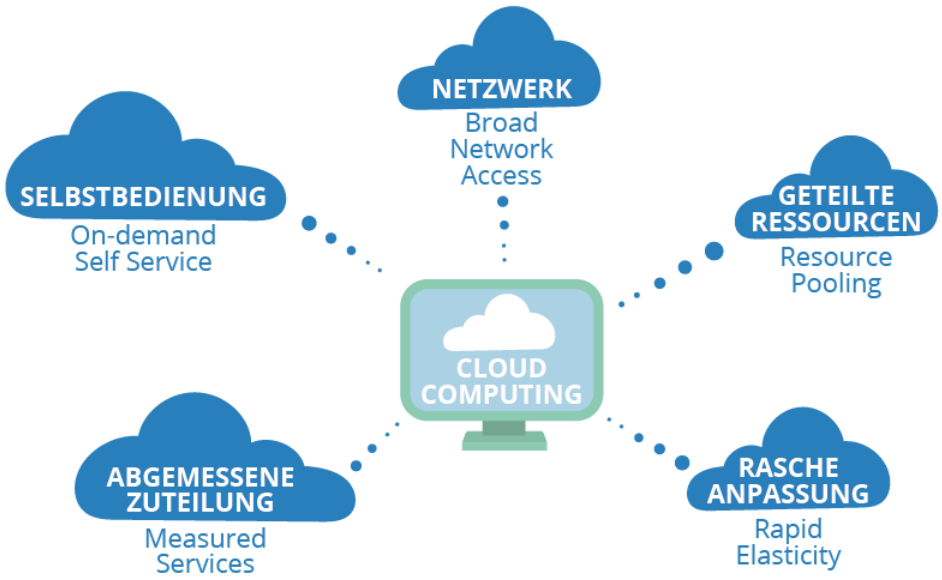
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Der Cloud-Anbieter kontrolliert und optimiert die Zuteilung der IT-Ressourcen. Man zahlt somit beim Cloud Computing üblicherweise keine fixe Gebühr, sondern je nach Verbrauch.

Damit hätten wir nun die fünf wichtigsten Merkmale des Cloud Computing erklärt. Fassen wir sie nochmal zusammen:

Merken
Cloud Computing ist charakterisiert durch: (1) **On-demand Self Service**, (2) **Broad Network Access**, (3) **Resource Pooling**, (4) **Rapid Elasticity** und (5) **Measured Services**.



2.4 Anwendungsbereiche von Cloud Computing

Sie haben nun bereits einiges über das Cloud Computing und seine Merkmale gelernt. Und bestimmt ahnen Sie es schon: Den Anwendungsbereichen dieses IT-Trends sind kaum Grenzen gesetzt!

Im Prinzip kann alles, was früher nur über die eigene IT-Infrastruktur gemacht wurde, heute über die Cloud ausgeführt werden. Dabei decken Cloud-Dienste alle Bereiche der modernen Informationstechnologie ab. Das bedeutet aber auch, dass die Anwendungen, die in der Cloud durchgeführt werden, nicht unbedingt neu sind. **Die Cloud-Nutzung selbst ist die Innovation**!

Wichtig
Cloud Computing als digitale Revolution Das Besondere am Cloud Computing ist nicht, was in der Cloud gemacht wird, sondern ***das*** es in der Cloud gemacht wird!

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Durch Cloud Computing wird **Informationstechnologie zu einer Dienstleistung** bzw. einem **Versorgungsgut** wie Wasser, Fernwärme oder Strom.

So wie heute nicht mehr jeder einen eigenen Brunnen, Kachelofen oder Stromgenerator besitzt, muss auch nicht mehr in die Anschaffung und Wartung eigener IT-Infrastruktur investiert werden. Rechenleistung, Speicherplatz und Anwendungen lassen sich via Cloud Computing unkompliziert über das Internet beziehen. Dabei wird dann auch nur das verrechnet, was wirklich verbraucht wird.

Dieses Abrechnungsmodell ähnelt sehr stark den Betriebskosten für Wasser oder Strom. Deswegen wird Cloud Computing auch manchmal als **Utility Computing** bezeichnet (vergleiche engl. *utility* = öffentlicher Versorgungsbetrieb; engl. *utility bill* = Gas-, Wasser-, Stromrechnung).

Und genau so wie bei Wasser und Strom nutzen Einzelpersonen heutzutage nicht mehr eigene Infrastruktur (Stellen Sie sich vor, jeder müsste sich seinen eigenen Brunnen graben!), sondern beziehen die Ressourcen von einem **externen Anbieter**.

Für die Wasserversorgung heißt das, dass Sie einfach nur den Wasserhahn aufdrehen und so viel oder wenig Wasser nutzen können, wie Sie brauchen.

Ähnlich ist es auch mit Cloud Computing. Anstatt dass Sie selbst in eine teure lokale IT-Infrastruktur investieren, nutzen Sie IT-Dienste über die Cloud. Sie drehen gewissermaßen den „Internethahn“ auf und verbrauchen und zahlen nur so viele Ressourcen, wie Sie tatsächlich gerade benötigen.

Zentral fürs Cloud Computing ist die Idee von **Informationstechnologie als Dienstleistung** (engl. *Service*). Das heißt, es kümmert sich nicht mehr jeder selbst um seine eigene IT-Infrastruktur, sondern mietet Ressourcen von einem Cloud-Anbieter.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Wie oben schon erwähnt, sind die Einsatzbereiche von Cloud Computing vielfältig. Trotzdem lassen sich **drei große Anwendungsbereiche** festhalten. Die Namensgebung der drei Bereiche folgt dabei dem Muster „X **a**s **a S**ervice“ (X**aaS**), also „X als eine Dienstleistung“.

Wir können unterscheiden:

- Infrastructure as a Service (Abkürzung: IaaS): Nutzung von Infrastruktur über die Cloud. Hier geht es vor allem um Speicherplatz, aber auch um Rechenleistung.

- Platform as a Service (Abkürzung: PaaS): Nutzung einer Entwicklungsumgebung und sonstiger Ressourcen zur Softwareprogrammierung über die Cloud. Dieses Service richtet sich an Personen, die selbst Anwendungen entwickeln wollen, d.h. hier werden Programmierer angesprochen.

- Software as a Service (Abkürzung: SaaS): Nutzung von diverser Software über die Cloud. Bei diesem Service wird auf fertige Programme zugegriffen. Sie werden nicht mehr am lokalen Rechner installiert, sondern über das Internet ausgeführt.

Infrastructure as a Service (IaaS) ist die **Basis** für alle anderen Dienste. Speicherplatz und rohe Rechenleistung werden über den Ressourcen-Pool der Cloud bezogen. Dabei wird aber dann die eigene Software ausgeführt. Dieses Service richtet sich vor allem an **IT-Abteilungen von Unternehmen** oder **Behörden**.

IaaS-Anbieter sind meist **große Firmen**, die ihre enormen IT-Ressourcen für andere Nutzergruppen bereitstellen.

Beispiele für IaaS-Anbieter sind:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud

Platform as a Service (PaaS) ist bereits eine Stufe höher. Hier wird nicht nur die grundlegenden Ressourcen (Speicher- und Rechenleistung) bereitgestellt, sondern auch eine Entwicklungsumgebung zur Erstellung von Software. Dieses Service richtet sich an Personen, die in der **Softwareentwicklung** tätig sind.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Beispiele für PaaS-Anbieter sind:

- Google App Engine
- Apache Stratos
- Salesforce App Cloud

Software as a Service (SaaS) ist schließlich die höchste Stufe der Cloud-Dienstleistungen. Dabei wird über die Cloud auf vollständige Programme zugegriffen. Diese werden nicht mehr „traditionell" am eigenen Computer installiert, sondern über das Internet verwendet. Mit dieser Form des Cloud-Services haben neben Unternehmen wahrscheinlich auch **Privatpersonen** am meisten zu tun.

Beispiele für SaaS-Dienste sind:

- Microsoft Office 365
- Dropbox
- ICloud
- Google Drive

Da SaaS mit dem Konsumenten bzw. der Konsumentin die größte Zielgruppe anspricht, spielt dieser Bereich wahrscheinlich auch für Sie im Alltag die größte Rolle. Deshalb wollen wir uns einen Aufgabenbereich der oben erwähnten SaaS-Dienste kurz näher ansehen:

Beispiel
Cloud-Storage-Anbieter: Speichern und Teilen von Daten in der Cloud Michael hat es geschafft! Er hat gerade seiner Masterarbeit fertiggeschrieben. Zufrieden lehnt er sich zurück und freut sich drauf, später mit seinen Freunden auf seinen Erfolg anzustoßen. Er will seinen Laptop schon runterfahren, da fällt sein Blick auf die Zeitung. Michael wird bleich im Gesicht. Denn er erinnert sich an den Bericht über Sabine Z., einer Studentin, die ihren Computer mit der einzigen Version ihrer Doktorarbeit im Zug vergessen hat. Alleine bei dem Gedanken wird Michael übel. Was ist, wenn sein Laptop ausgerechnet jetzt kaputt wird? Oder wenn jemand in seine Wohnung einbricht und den Laptop mitnimmt? Lieber nichts riskieren! Schnell speichern! Doch leider hat Michael seinen USB-Stick im Büro vergessen. „Mist", denkt sich Michael. „Okay, dann schicke ich mir meine Arbeit einfach selbst per E-Mail". Doch auch hier gibt es ein Problem, denn Michaels Masterarbeit ist als Emailanhang zu groß. Michael ist der Verzweiflung nahe. Je länger er darüber nachdenkt, desto sicherer ist er, dass sein Laptop genau heute Nacht den Geist aufgeben wird.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Glücklicherweise kommt in dem Moment Michaels Mitbewohner Alex nachhause. Er erkennt sofort das Problem und schlägt vor, dass Michael seine Arbeit in einem Cloud Speicher wie etwa **Dropbox, Google Drive** oder **Microsoft OneDrive** abspeichert. Damit sind der Abend und Michaels Nerven gerettet!

Aber was sind Cloud-Speicher-Dienste?

Bei Cloud-Speicher-Diensten können Dateien in der Cloud gespeichert und mit anderen Personen geteilt werden. Sie benötigen nur einen Account und erhalten dann einen Online-Speicherplatz. Bei manchen Anbietern ist ein gewisses Speicherausmaß sogar kostenlos.

Neben einfachem **Speichern** Ihrer Daten können Sie diese normalerweise auch freigeben und mit anderen Personen teilen. Das ist vor allem dann praktisch, wenn Sie gemeinsam mit anderen an einer Datei arbeiten möchten.

Auch zum **Datentransfer** eignet sich Cloud-Speicher-Dienste: egal, ob Sie Ihre Daten Freunde oder Kollegen zukommen lassen wollen oder einfach von einem Endgerät auf ein anderes übertragen möchten.

Cloud-Speicher-Dienste sind auch eine gute Möglichkeit, **Sicherungskopien** Ihrer Daten aufzubewahren. Genauso wie Michael müssen Sie sich bei Cloud-Speichern keine Sorgen machen, dass das Speichermedium kaputt geht oder im Zug vergessen wird.

Anmerkung: Bei Cloud-Speicher-Diensten steht die Nutzung von Speicherkapazitäten im Vordergrund. Sie greifen jedoch nicht direkt auf die rohen Speicher-Ressourcen der Cloud zu. Sie nutzen die Ressourcen über eine **fertige Software, d.h. ein Programm**. Deswegen ist ein Cloud-Speicher-Dienst also keine Infrastructure as a Service (Abkürzung: IaaS), sondern eine **Software as a Service (Abkürzung: SaaS)**!

2.5 Typen von Clouds

Sie wissen nun, dass den Anwendungsbereichen des Cloud Computing kaum Grenzen gesetzt sind. Jetzt bleibt nur noch zu klären, welche verschiedenen Typen von Clouds es gibt.

Die in den USA ansässige Behörde NIST (Abkürzung steht für *National Institute of Standards and Technology*) unterscheidet **vier unterschiedliche Grundtypen von Clouds**:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Bei dieser Kategorisierung geht es darum, wie das Cloud-Computing-Angebot bereitgestellt wird. Gehen wir die einzelnen Typen gemeinsam durch.

Public Cloud: Bei der Public Cloud, auch öffentliche Cloud genannt, stehen die Cloud-Ressourcen der breiten Öffentlichkeit zur Verfügung. **Sie ist gewissermaßen für alle da**. Dabei wissen die einzelnen Nutzer und Nutzerinnen der Public Cloud nicht, wer sonst alles auf die Cloud-Ressourcen zugreift. Die Cloud wird mit jedem geteilt, der sie nutzen möchte.

Bei dieser „klassischen Form" der Cloud wird die Cloud-Infrastruktur **von Cloud-Anbieter betrieben und gewartet. Das geschieht off-site**. Das heißt, die Infrastruktur befindet sich nicht bei den einzelnen Personen, die die Cloud verwenden, sondern sie ist auf externe Rechenzentren und Server verteilt. Die Anbieter von Public Clouds sind meist große Unternehmen.

Beispiele für Public Clouds haben wir oben bereits gesehen: Sowohl Amazon, Google als auch Microsoft betreiben Public Clouds.

Alle Cloud-Dienste, die der **breiten Öffentlichkeit zur Verfügung** stehen, fallen unter den Begriff Public Cloud Computing.

Exkurs

Amazon Web Services (AWS) als Pionier unter den Public Clouds und IaaS-Anbietern

Amazon Web Services (AWS), eine Tochterfirma des Versandriesens Amazon, war einer der Vorreiter, was das Cloud Computing angeht.

Bereits früh hatte sich Amazon entschlossen, seine riesigen Serverkapazitäten rentabel an andere Firmen weiterzuvermieten. Dass das eine sehr gute Idee war, zeigt sich an den Wirtschaftszahlen. Seit seiner offiziellen Gründung 2006 hat sich Amazon Web Services zu einer der umsatzstärksten Sparte des Unternehmens entwickelt.

Mit Stand 2019 ist AWS der auf der Welt führende Cloud-Anbieter bezüglich **Infrastructure as a Service (Abkürzung: IaaS)** und hat zahlreiche große Firmen als Kundschaft.

Haben Sie beispielsweise gewusst, dass 2019 u.a. der Streaming-Dienst Netflix, die Buchungsplattform Airbnb oder auch die US-amerikanische Raumfahrbehörde NASA Speicherkapazitäten bei Amazon Web Services genutzt hat?

Private Cloud: Eine private Cloud ist nun hingegen eine exklusive Cloud. **Die Cloud-Infrastruktur wird bloß von einem einzelnen Kunden genutzt.** Ein Netzwerk von Servern ist eigens für ein Unternehmen reserviert oder wurde sogar extra für dieses gebaut. Niemand sonst hat Zugriff auf diese Form der Cloud.

Private Clouds können sich entweder lokal auf dem Gelände des Unternehmens befinden oder von bestimmten Cloud-Anbietern gemietet werden. Sie können sich also **on-site oder off-site** befinden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Wenn eine Cloud nur für den **unternehmenseigenen Gebrauch** reserviert ist, handelt es sich also um eine private Cloud. Das heißt, dass Server-Netzwerk von Amazon war vor der Gründung von Amazon Web Services (AWS) eine private Cloud – nur Amazon selbst nutzte seine IT-Ressourcen.

Wichtig

Cloud Typ = Bereitstellungstyp

Bei den verschiedenen Typen von Clouds geht es nicht darum, wie die Cloud genutzt wird, sondern von wem. Das heißt, es geht um die **Bereitstellung des IT-Angebots** und darum, wie viele Unternehmen oder Personen zur Cloud Zugriff haben!

Daraus folgt, dass Ihr privat genutzter Cloud-Speicher wie etwa Dropbox keine private Cloud ist. Es handelt sich vielmehr um eine öffentliche Cloud.

Das liegt daran, dass hinter Dropbox keine exklusive Cloud steckt, die für Sie alleinig geschaffen wurde und die nur Sie nutzen. Ganz im Gegenteil: Die Cloud-Struktur hinter Dropbox steht jedem Unternehmen und jeder Person offen, der sie nutzen möchte.

Community Cloud: Die Community Cloud ist gewissermaßen eine private Cloud mit einem etwas erweiterten Kreis an Nutzern und Nutzerinnen. Bei diesem Modell teilt sich eine bestimmte **Gemeinschaft** (engl. *community*) die Cloud-Ressourcen.

Bei dieser Gemeinschaft handelt es sich typischerweise um Unternehmen, die im **gleichen Geschäftsfeld** tätig sind und ähnliche Interessen und Bedürfnisse haben.

Das Ziel bei der Community Cloud ist es im Vergleich zu mehreren einzelnen privaten Clouds Kosten einzusparen.

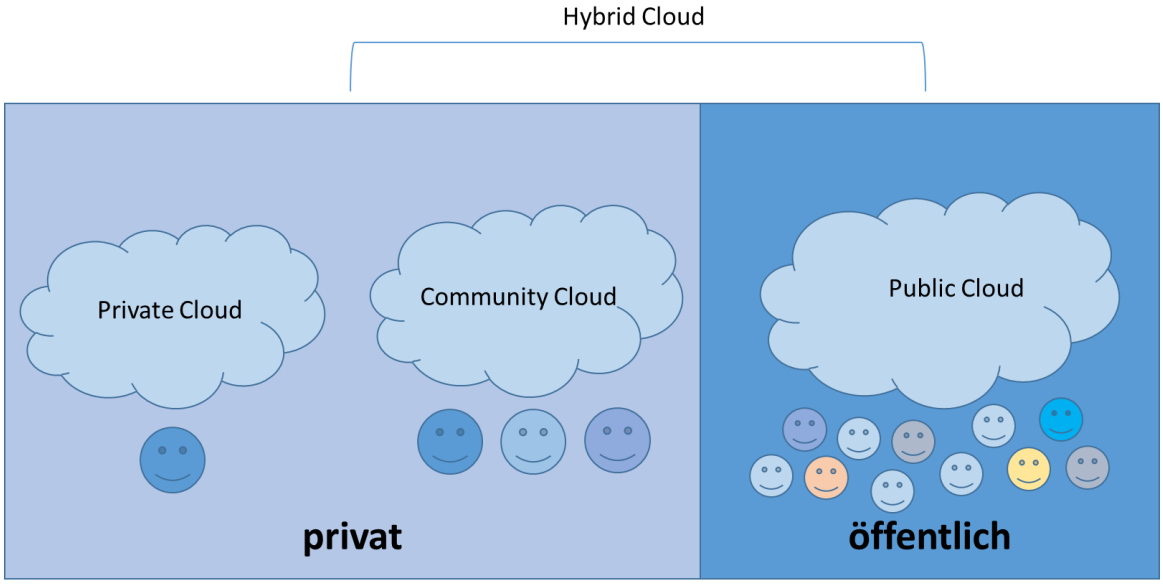
Hybrid Cloud: Schließlich gibt es noch das Modell der Hybrid Cloud. Sie ist eine **Mischform zwischen privater und öffentlicher Cloud**.

Bei der Hybrid Cloud entscheiden sich Unternehmen, **nur gewisse Bereiche ihrer IT-Bedürfnisse in öffentliche Clouds auszulagern**. Bestimmte Daten oder Prozesse möchte das Unternehmen aber lieber in privater Umgebung belassen – Sie nutzen dafür also eine private Cloud. Meistens stehen dabei Überlegungen zum Datenschutz im Vordergrund. So können Unternehmen beispielsweise sensible Daten bei sich in der privaten Cloud speichern und für andere Prozesse eine öffentliche Cloud nutzen.

Damit hätten wir die **vier Typen von Clouds** erklärt. Die folgende Grafik fasst sie nochmals zusammen. Sie sehen: Es geht hauptsächlich darum, wie viele Personen auf die Cloud-Struktur Zugriff haben.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



2.6 Vorteile und auch Nachteile des Cloud Computing

Kommen wir abschließend noch auf die **Vorteile sowie auch auf ein paar Nachteile** des Cloud Computing zu sprechen.

Beginnen wir mit den **Vorteilen**. Cloud Computing ist *der* Trend der modernen Informationstechnologie. Es scheint so, also müsste „alles in die Cloud“. Und es gibt tatsächliche viele gute Gründe, die fürs Cloud Computing sprechen.

Cloud Computing ist:

- kostengünstig: Investition in eigene IT-Ressourcen wird eingespart
- praktisch: Zugang zu IT-Ressourcen und Daten überall und jederzeit
- flexibel: Zuschalten oder Wegschalten von Ressourcen abhängig vom aktuellen Bedarf

Bei Cloud Computing müssen Sie nicht mehr in eigene teure Hardware investieren. Das betrifft Privatpersonen wie auch Unternehmen.

Wenn Sie ein Unternehmen führen, können Sie durch Cloud-Nutzung außerdem Ihr IT-Team **entlasten**. Es muss sich nicht mehr dauernd um die Wartung und Instandhaltung der Hardware und Software kümmern, sondern kann sich auf das Kerngeschäft konzentrieren. So **sparen Sie Geld** und machen Ihr Unternehmen **effizienter**. Außerdem nutzen und bezahlen Sie immer nur so viel, wie sie **gerade benötigen**.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Ein weiterer großer Pluspunkt des Cloud Computing liegt darin, dass Sie als Privatperson oder kleines Unternehmen bei den IT-Vorteilen der großen Unternehmen „mitnaschen“ können. Das betrifft sowohl die **Investitionskraft** in Hardware also auch **Innovationen** im Softwarebereich.

„Big Player“ wie Amazon, Microsoft und Google wollen immer am Puls der Zeit bleiben und die neueste IT verwenden. Und sie haben auch die finanziellen Mittel dafür! Alleine könnten Sie da niemals mithalten. Durch Cloud Computing haben Sie also die Möglichkeit stark **von großen Unternehmen zu profitieren**.

Manche Menschen vertreten sogar die Meinung, dass Cloud Computing zu mehr **Chancengleichheit** führt. Denn durch Cloud Computing hat im Prinzip jede Person, die über eine Internetverbindung und bestimmte finanzielle Mittel verfügt, Zugang zum aktuellsten Stand der Informationstechnologie. Und das unabhängig davon, wo auf der Welt sich diese Person befindet.

Ebenfalls zentral fürs Cloud Computing ist das Thema **Datensicherung**. Für viele von uns ist die **externe Datenspeicherung**, beispielsweise von wichtigen Dokumenten oder Urlaubsfotos, der erste Berührungspunkt mit Cloud Computing.

Nicht mehr vom „Gesundheitszustand“ und der „Lebensdauer“ der eigenen Festplatte abhängig zu sein, ist für viele Personen ein wichtiger Punkt, der fürs Cloud Computing spricht.

Mit dem Stichwort Sicherheit können wir aber auch gleich zu den Nachteilen des Cloud Computing übergehen. Zuvor allerdings ein kleiner Vergleich:

Beispiel
Datenspeicherung in der Cloud Sie können sich aus Aufbewahren Ihrer Daten in der Cloud wie das Aufbewahren Ihrer Wertgegenstände in einer Bank vorstellen. Im Normalfall sind Ihre Wertgegenstände im Banktresor viel sicherer aufgehoben als zuhause unterm Kopfpolster. Wenn allerdings die Bank überfallen wird, dann sind Ihre Wertgegenstände natürlich weg – und nicht nur Ihre, sondern die Wertgegenstände von sehr vielen anderen Personen auch.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Es liegt auf der Hand, dass die Bank alles daran setzt, nicht ausgeraubt zu werden. Nicht nur die finanziellen Aspekte, sondern auch der Imageverlust wären verheerend. Deshalb investiert die Bank großangelegt in ihr Sicherheitssystem und auch in den Brandschutz.

Genauso ist es mit Cloud-Anbietern. Sie sind stark daran interessiert, ihre Cyber-Security immer auf den neuesten Stand zu halten. Auch die Hardware, also die Server, werden aufwendig vor Diebstahl oder physikalischem Schaden geschützt.

Trotzdem gibt es natürlich keine hundertprozentige Sicherheit beim Cloud Computing. Und wenn der Cloud etwas passiert, dann sind nicht nur Ihre Daten weg, sondern auch die Daten von vielen anderen Personen auch.

Sie sehen also, Cloud Computing hat auch seine Risiken und Schattenseiten.

Einige **Nachteile**, die Sie unbedingt beachten sollten, sind:

- Abhängigkeit vom Anbieter: Wechsel des Anbieters kann schwierig werden
- Datenschutz und Sicherheit: problematisch, wenn mit sensiblen Daten gearbeitet wird
- Notwendigkeit einer stabilen Internetverbindung: ohne gut funktionierendes Internet nicht einsetzbar
- Klimaschutz: Energieverbrauch der riesigen Rechenzentren

Bevor Sie auf Cloud Computing zugreifen, ist es sicherlich ratsam, über die Nachteile und möglichen Fallen nachzudenken. Trotz der vielen Vorteile muss Cloud Computing nicht in jeder Situation die richtige Wahl sein!

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Nehmen wir beispielsweise an, dass Sie in einer Gegend wohnen, in der die **Internetversorgung** noch nicht so gut ausgebaut ist. In diesem Fall werden Sie wahrscheinlich lieber auf installierte Software zurückgreifen als auf Softwarenutzung in der Cloud. So vermeiden Sie, dass Sie Ihre Arbeit ständig unterbrechen müssen, weil die Internetverbindung instabil ist.

Ein weiterer negativer Aspekt des Cloud Computing ist natürlich, dass man sich vom Cloud-**Anbieter abhängig** macht. Wenn der Cloud-Anbieter pleite ist, dann haben auch Sie ein großes Problem. Deswegen setzten viele Unternehmen lieber auf große und etablierte Cloud-Anbieter. Aber auch hier kann es problematisch werden. Was ist, wenn Sie den Cloud-Anbieter wechseln wollen? Da können einige Kosten und Hürden auf Sie zukommen. Schon mal versucht, aus dem Vertrag Ihres Telefonanbieters auszusteigen? Ähnlich schwierig kann es beim Wechsel von Cloud-Anbietern sein.

Ebenfalls zu denken gibt die **Klimafrage**. Die riesigen Rechenzentren der Cloud fressen Unmengen an Strom und andere Ressourcen. Bei der Auswahl des Cloud-Anbieters könnte man also darauf achten, ob er versucht, **klimaschonend** zu arbeiten. Wird beispielsweise stark auf erneuerbare Energie gesetzt?

Ein sehr wichtiger Bereich ist abschließend der **Datenschutz**. Wie Sie bereits erfahren haben, wissen Einzelpersonen beim Cloud Computing nicht, woher genau die IT-Ressourcen bezogen werden. Das kann zu einem Problem werden, wenn Sie beispielsweise sensible Daten speichern möchten. Vielleicht werden die Daten nämlich auf einem US-amerikanischen Server gespeichert. Das könnte mit den Datenschutzrichtlinien Ihres Heimatlandes oder Unternehmenssitzes nicht kompatibel sein.

Auch sollten Sie sich darüber Gedanken machen, ob und wie sensible Daten **verschlüsselt** werden. Das betrifft sowohl die Speicherung in der Cloud selbst als auch die Übertragung der Daten über das Internet.

Halten wir also nochmal kurz einige Aspekte fest, die beim Thema Datenschutz und Cloud Computing zu beachten sind:

- Wo befindet sich die Cloud-Infrastruktur, d.h. die Server?
- Wo ist der Hauptsitz des Cloud-Anbieters? Gilt für ihn europäisches Recht oder beispielsweise US-amerikanisches Recht?
- Werden die Daten bei der Übertragung in und aus der Cloud verschlüsselt?
- Werden die Daten in verschlüsselter Form gespeichert?
- Von wem stammt der Verschlüsselungscode?

Wichtig

Verschlüsselung und Cloud Computing

Wer auf Nummer Sicher gehen will, sollte beim Cloud Computing auf **starke Verschlüsselungsmethoden** setzten.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Das betrifft sowohl die **Speicherung** als auch die **Übertragung** der Daten!

Im Idealfall verlassen Sie sich dabei nicht auf den Cloud-Anbieter, sondern führt die Verschlüsselung unabhängig von ihm durch. Wenn der Cloud-Anbieter nämlich gehackt wird, kann es sein, dass nicht nur Ihre verschlüsselten Daten, sondern auch der Code zum Entschlüsseln in falsche Hände gerät.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.7 Zusammenfassung

Mit Cloud Computing ist das Nutzen von Informationstechnologie über ein Netzwerk, im Normalfall das Internet, gemeint. Es handelt sich also um **Internet-basiertes Computing**.

Die Idee dahinter ist, dass nicht mehr jedes einzelne Unternehmen und jede Privatperson in ihre Hardware und Software investiert, sondern dass **IT-Ressourcen** innerhalb großer Netzwerke **geteilt** werden.

Cloud Computing ist aus der heutigen IT-Welt nicht mehr wegzudenken und ein **riesiger Wirtschaftsfaktor**. Es deckt alle Bereiche der **modernen Informationstechnologie** ab und die Möglichkeiten sind praktisch unendlich. Es gibt quasi nichts, was nicht „in der Cloud“ gemacht werden kann.

Trotz der Fülle an Angeboten und der Komplexität des Themas lassen sich die Grundlagen des Cloud Computing auf die einfache Formel: **5-3-4** herunterbrechen.

Es gibt **fünf Merkmale**, die für Cloud Computing charakteristisch sind:

- **On-demand Self Service:** Selbstbedienung
- **Broad Network Access:** Zugriff auf die Ressourcen über ein Netzwerk, jederzeit und überall
- **Resource Pooling:** geteilte Ressourcen
- **Rapid Elasticity:** schnelles Anpassen diverser Ressourcen an den tatsächlichen Bedarf
- **Measured Services:** gemessene und überwachte Nutzung

Es gibt **drei Anwendungsbereiche**:

- **Infrastructure as a Service (Abkürzung: IaaS)**: Nutzung von IT-Infrastruktur über eine Cloud
- **Platform as a Service (Abkürzung: PaaS)**: Nutzung von IT-Ressourcen zur Softwareprogrammierung über eine Cloud
- **Software as a Service (Abkürzung: SaaS)**: Nutzung einer Software über eine Cloud

Und es gibt **vier Cloud Typen**:

- **Public Cloud:** für die allgemeine Öffentlichkeit
- **Private Cloud:** für einzelne Unternehmen
- **Community Cloud:** für eine Gruppe von Unternehmen aus der gleichen Branche

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Hybrid Cloud:** Mischform aus Public Cloud und Private Cloud

Die wichtigsten **Vorteile** des Cloud Computing sind **Kosteneinsparung**, **Flexibilität** und **bequemer Zugang** zu IT-Ressourcen und Daten.

Nachteile sind die **Abhängigkeit** vom Cloud-Anbieter und die **Notwendigkeit einer stabilen Internetverbindung**. Viele Probleme und offene Fragen gibt es auch in den Bereichen **Datenschutz** und **IT-Sicherheit**. Außerdem sollte beim Cloud Computing das Thema **Klimaschutz** nicht vernachlässigt werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.8 ÜBUNGEN

1. Richtig oder Falsch?

a. Dem NIST-Bericht zufolge gibt es drei wichtige Merkmale, die Cloud Computing ausmachen
R □ F □

b. Mit Cloud Computing können Sie unabhängig auf IT-Dienste aus der Cloud zugreifen - genau dann, wenn Sie diese benötigen
R □ F □

c. Sie müssen nicht erst einen Telefonanruf tätigen oder eine E-Mail schreiben, um mehr Speicherplatz zu erhalten
R □ F □

d. Sie haben jederzeit, aber nicht überall Zugang zu den Diensten und Daten
R □ F □

e. Ressourcen-Pooling ist praktisch in einem großen gemeinsamen "Pool" verfügbar
R □ F □

2. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Durch Cloud Computing wird _____ zu einer Dienstleistung bzw. einem Versorgungsgut wie Wasser, Fernwärme oder Strom. So wie heute nicht mehr jeder einen eigenen Brunnen, Kachelofen oder Stromgenerator besitzt, muss auch nicht mehr in die _____ und Wartung eigener IT-_____ investiert werden. _____, Speicherplatz und Anwendungen lassen sich via Cloud Computing unkompliziert über das Internet beziehen. Dabei wird dann auch nur das verrechnet, was wirklich verbraucht wird. Dieses Abrechnungsmodell ähnelt sehr stark den Betriebskosten für Wasser oder Strom. Deswegen wird Cloud Computing auch manchmal als Utility Computing _____ (vergleiche engl. utility). Und genau so wie bei Wasser und Strom nutzen Einzelpersonen heutzutage nicht mehr eigene Infrastruktur (Stellen Sie sich vor, jeder müsste sich seinen eigenen Brunnen graben!), sondern beziehen die Ressourcen von einem externen Anbieter.

1 Anschaffung, 2 Rechenleistung, 3 Infrastruktur, 4 Informationstechnologie, 5 bezeichnet

3. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Public Cloud
Bei der Public Cloud, auch öffentliche Cloud genannt, _____ die Cloud-Ressourcen der breiten Öffentlichkeit _____ (1). Sie ist gewissermaßen für alle da. Dabei wissen die _____ (2) der Public Cloud nicht, wer sonst alles auf die Cloud-Ressourcen zugreift. Die Cloud wird mit _____ (3) geteilt, der sie nutzen möchte. Bei dieser „klassischen Form“ der Cloud wird _____ (4) von Cloud-Anbieter betrieben und gewartet. Das geschieht _____ (5). Das heißt, die Infrastruktur _____ (6) bei den einzelnen Personen, die die Cloud verwenden, sondern sie _____ auf externe Rechenzentren und Server _____ (7). Die Anbieter von Public Clouds sind meist _____ (8). Beispiele für Public Clouds haben wir oben _____ (9) gesehen. Alle _____ (10), die der breiten Öffentlichkeit zur Verfügung stehen, fallen unter den Begriff Public Cloud Computing.

1. a. stehen_nicht zur Verfügung	**b.** steht_zur Verfügung	**c.** stehen_zur Verfügung
2. a. einzelne Benutzer	**b.** gemeinsame Benutzer	**c.** einzelne Benutzer
3. a. jedem	**b.** einer Person	**c.** niemanden
4. a. das Cloud-Service	**b.** die Cloud-Infrastruktur	**c.** der Cloud-Anbieter
5. a. auf der Website	**b.** vor Ort	**c.** außerhalb des Standorts
6. a. ist nicht lokalisiert	**b.** befindet sich nicht	**c.** befindet sich
7.a. sind_verteilt	**b.** ist_verteilt	**c.** ist nicht_verteilt

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

8. a. kleine Unternehmen **b.** mittlere Unternehmen **c.** große Unternehmen
9. a. noch **b.** schon **c.** bereits
10. a. Cloud-Dienste **b.** Cloud-Infrastrukturen **c.** Cloud-Anbieter

4. Richtig oder Falsch

a. Wenn Sie ein Unternehmen betreiben, können Sie die Arbeitsbelastung Ihres IT-Teams nicht durch die Nutzung der Cloud reduzieren.
R □ F □
b. Cloud Computing bietet Ihnen die Möglichkeit, stark von großen Unternehmen zu profitieren
R □ F □
c. Einige Leute glauben sogar, dass Cloud Computing nicht zu mehr Chancengleichheit führt.
R □ F □
d. Externe Datenspeicherung ist der erste Berührungspunkt mit Cloud Computing
R □ F □
e. Bevor man auf Cloud Computing zugreift, ist es ratsam, über die Nachteile und mögliche Fallen nachzudenken
R □ F □

5. Eines der Merkmale, die für Cloud Computing charakteristisch sind, ist:

a. On-demand Self Service: Selbstbedienung
b. Broad Pooling: gemeinsame Ressourcen
c. Measured Elasticity: angemessene und schneller Ressourceneinsatz

6. Unter den drei Anwendungsbereichen gibt es:

a. Infrastructure as a Service (IaaS): Nutzung von Software über eine Cloud
b. Platform as a Service (PaaS): Nutzung von IT-Ressourcen zur Software-Programmierung über eine Cloud
c. Software as a Service (SaaS): Nutzung von IT-Infrastruktur über eine Cloud

7. Unter den 4 Cloud-Typen gibt es:

a. Public Cloud: für einzelne Unternehmen
b. Private Cloud: für die breite Öffentlichkeit
c. Hybrid Cloud: Hybrid aus Public Cloud und Private Cloud

8. Die wesentlichen Vorteile von Cloud Computing sind:

a. Ausgaben
b. Unbequemer Zugang zu Daten
c. Flexibilität

9. Nachteile von Cloud Computing sind:

a. Die Abhängigkeit vom Cloud-Provider
b. Kosteneinsparungen
c. Keine Notwendigkeit für eine stabile Internetverbindung

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. BIG DATA

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1 Das Thema

Die erste Einführung

Können Sie sich vorstellen, dass ein Mensch rund 181 Millionen Jahre brauchen würde, um alle Daten aus dem Internet herunterzuladen? Diese großen Datenmengen, die heute verfügbar sind, und ihre Verarbeitung bezeichnet man als **Big Data**.

Wie Sie in dieser Einheit sehen werden, sind wir damit nahezu täglich konfrontiert – oftmals auch ohne unser Wissen. Sie werden erfahren, welche **Vorteile** aber auch **Gefahren** Big Data bringt und warum ein **richtiger Umgang** mit diesen großen Datenmengen oftmals wichtiger ist als die Daten selbst.

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Nicht nur IT-Spezialisten, nahezu alle Menschen stoßen bei ganz **alltäglichen Situationen**, etwa bei einem Arztbesuch, beim Surfen in sozialen Medien wie Facebook und Instagram, bei einer Suchanfrage auf Google oder in einem vernetzten Fahrzeug auf die sogenannten großen Datenmengen.

Zu wissen, wie große Datenmengen genutzt werden und welche **Chancen** aber auch **Gefahren** damit verbunden sind, kann sowohl für Ihren **persönlichen Umgang** mit dem **Internet** als auch für Ihr **Berufsleben**, etwa in einem Unternehmen, das große Datenmengen analysiert, relevant sein.

Lernziele und Kompetenzen im Überblick

Diese Lerneinheit vermittelt Ihnen ein grundlegendes Verständnis von Big Data. Sie lernen das **3-V-Modell** kennen und erfahren, wie große Datenmengen erhoben und analysiert werden. Anschließend erfahren Sie, zu welchen **Zwecken** die **Erkenntnisse** genutzt werden, die aus den großen Datenmengen gewonnen werden und welche **Gefahren** der Umgang damit birgt. Sie erkennen, warum **Datenschutz** in den letzten Jahren an **Bedeutung** gewonnen hat und verstehen, dass der **Umgang** mit Big Data sowohl für Unternehmen als auch für Privatpersonen große Herausforderungen mit sich bringt.

Lernziele
Den Begriff Big Data verstehen und beschreiben
Wissen, wie Big Data eingesetzt werden kann
Verstehen und erklären, wie große Datenmengen erhoben und analysiert werden

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2 Was ist Big Data?

Haben Sie gewusst, dass rund 90 Prozent aller Daten, die heute auf der ganzen Welt verfügbar sind, in den vergangenen Jahren generiert wurden? Durch die zahlreichen neuen Informations- und Kommunikationstechnologien ist das **Datenvolumen** weltweit unglaublich gewachsen und bietet bisher unbekannte Möglichkeiten. **Big Data** steht für diese **Menge** von strukturierten und unstrukturierten **Daten**, die aufgrund ihrer Größe nicht mit herkömmlicher Soft- oder Hardware verarbeitet werden kann.

Diese angesprochenen Datenmengen entstehen unter anderem mit jedem unserer **Klicks im Internet**. Dabei kann es sich z.B. um einen Einkauf auf Amazon, um eine Suchanfrage an Google, um eine Aktivität in sozialen Netzwerken wie Instagram oder Facebook etc. handeln.

Aber große Datenmengen alleine machen noch kein Big Data. Erst die **Analyse** und **Verarbeitung** dieser Datenmengen, z. B. durch ein Unternehmen, zeichnet Big Data aus. 2001 entwarf der Analytiker **Doug Lane** mit seinem **3-V-Modell** eine Definition von Big Data, die bis heute anerkannt ist. Big Data verfügt nach Lane über die folgenden drei Eigenschaften:

- **Volume (dt. Volumen)**: Unternehmen sammeln große Datenvolumen aus verschiedenen Quellen. Dazu zählen etwa intelligente Geräte (IoT) wie Mobiltelefone, Videos, Soziale Medien etc. Früher wäre es nicht möglich gewesen, diese großen Datenvolumen zu speichern, heute gibt es zu diesem Zweck Speicherplattformen.

- **Velocity (dt. Geschwindigkeit)**: Aktuell werden Unternehmen von Datenströmen in nie da gewesener Geschwindigkeit überflutet, die rasch verarbeitet werden müssen.

- **Variety (dt. Vielfalt)**: Die erhobenen Daten sind vielfältig und haben verschiedenste Formate: So können sowohl numerische Daten, die in strukturierter Form vorliegen und in gewöhnlichen Datenbanken gespeichert sind, Teil von Big Data sein, wie auch unstrukturierte Textdokumente, Daten aus Finanztransaktionen oder E-Mails.

Definition
Big Data ...steht für eine **große Menge** an verfügbaren **Daten**, die zu einem bestimmten Zweck **analysiert** und **verarbeitet** werden. Nach Doug Lane zeichnet sich Big Data durch **Volumen**, **Geschwindigkeit** und **Vielfalt** aus.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Big Data vs. Small Data

**"Let's shrink Big Data into Small Data ...
and hope it magically becomes Great Data."**

Im Gegensatz zu Big Data bezeichnet Small Data (dt. kleine Daten) Daten in einem für Menschen zugänglichen Volumen und Format. Die folgenden Punkte zeigen, wie Big Data von Small Data abgegrenzt werden kann:

- **Ziele:** Small Data wird für ein festgelegtes Ziel genutzt, die Nutzung von Big Data entwickelt sich oftmals unerwartet.

- **Ort:** Small Data wird im Allgemeinen an einem Ort, meist in einer Datei auf dem PC, gespeichert, während Big Data meist auf zahlreiche Dateien auf verschiedenen Servern verteilt ist, die sich in unterschiedlichen Ländern befinden.

- **Datenstruktur:** Small Data ist geradlinig strukturiert, wohingegen Big Data unstrukturiert sein kann und viele Dateiformate aus unterschiedlichen Fachrichtungen aufweisen kann.

- **Datenvorbereitung:** An der Vorbereitung von Small Data ist meist nur ein Endnutzer beteiligt. Im Fall von Big Data ist es hingegen oftmals so, dass eine Personengruppe die Daten vorbereitet, diese Daten von einer weiteren Gruppe analysiert werden und schließlich eine dritte Gruppe die Daten nutzt. Jede dieser Gruppen kann andere Ziele verfolgen.

- **Langlebigkeit:** Small Data wird generell nach dem Abschluss eines Projekts eine bestimmte Zeit lang aufbewahrt. Im Fall von Big Data bleiben die Daten aber für unbegrenzte Dauer gespeichert.

- **Ursprung:** Small Data wird innerhalb von kurzer Zeit und in bestimmten Maßeinheiten gespeichert. Big Data hingegen entstammt verschiedenen Orten, Ländern, Unternehmen, Organisationen etc.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Reproduzierbarkeit:** Small Data kann generell vollständig reproduziert werden. Big Data stammt hingegen aus so vielen Quellen und liegt in derartig vielen Formen vor, dass eine Reproduktion unmöglich ist.

- **Qualität:** Die Bedeutungen der Daten eines Small Data Datensatzes sind eindeutig, diese Daten können sich daher selbst beschreiben. Big Data hingegen ist viel komplexer und kann auch nicht identifizierbare Informationen enthalten, die keine bestimmte Bedeutung haben. Dadurch kann die Datenqualität gemindert werden.

- **Analyse:** Für die Analyse von Small Data reicht meist ein einzelner Prozess aus, da die Daten aus nur einer Computerdatei analysiert werden. Im Fall von Big Data müssen die Daten hingegen aufwändig extrahiert, geprüft, reduziert etc werden.

Wie Sie an der Unterscheidung zwischen Big Data und Small Data sehen können, ist Big Data im wahrsten Sinne des Wortes oft schwer zu (er)fassen.

3.3 Verwendungsmöglichkeiten und Chancen von Big Data

Die **Analyse** von großen Datenmengen ermöglicht, **Erkenntnisse** zu gewinnen. Diese Ergebnisse können als Grundlage für Entscheidungen dienen, z.B. in Bezug auf die **strategische Ausrichtung** des **Unternehmens**. So wollen etwa Unternehmen mehr über die Vorlieben ihrer Kunden erfahren, um ihr Sortiment, ihre Werbung etc. daran anzupassen.

Auch **Deep Learning** (dt. tiefgehendes Lernen) nutzt Big Data: Es handelt sich um eine spezielle Methode der I**nformationsverarbeitung** und einen Teilbereich des **maschinellen Lernens**. Als Orientierung dient die Funktionsweise eines menschlichen Gehirns: Eine Maschine wird mit großen Datenmengen „gefüttert“, die analysiert und genutzt werden, um die Maschine zu trainieren. Die Maschine ist in der Lage, neue Informationen miteinander zu verknüpfen und kann auf dieser Basis Prognosen erstellen und eigene Entscheidungen treffen. Das Ergebnis ist allerdings immer nur so gut, wie die Daten, von denen die Maschine „gelernt“ hat.

Ein Beispiel hierfür ist etwa ein System zur maschinellen Übersetzung, das in einem Unternehmen durch eingegebene Daten (bereits existierende Übersetzungen) „lernt“, Fachbegriffe richtig zu übersetzen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Zudem nutzen **Behörden** und **Geheimdienste** große Datenmengen, um darin Abweichungen und Auffälligkeiten aufzuspüren, die möglicherweise auf kriminelle oder terroristische Aktivitäten hinweisen. In der **Wissenschaft** werden mithilfe von großen Datenmengen **komplexe Naturphänomene** wie der Klimawandel oder das Entstehen von Erdbeben und Epidemien untersucht.

Aber nicht immer wird **verantwortungsvoll** mit den großen Datenmengen umgegangen. Manche Unternehmen oder Institutionen halten sich nicht an Datenschutzvorschriften, was dazu führt, dass Informationen an die Öffentlichkeit gelangen. Das kann belanglos, in manchen Fällen aber auch gefährlich sein und zu **Betrug** und **Erpressung** führen.

Beispiel
2015 wurde das Seitensprungportal Ashley Madison, bei dem Menschen auf der Suche nach einem außerehelichen Abenteuer ein Profil anlegen können, Opfer eines Hackerangriffs. In Folge gelangten Informationen zu den auf dem Portal registrierten Personen in das allen zugängliche Internet. Informationen zu Seitensprüngen von Prominenten und persönliche Informationen wie Kreditkartennummern wurden öffentlich. Zudem wurden Betroffene per E-Mail aufgefordert, Lösegeld zu bezahlen, damit der Lebenspartner oder die Lebenspartnerin nicht von dem Profil auf dem Seitensprungportal erfährt.

Merke
Große Datenmengen können unter anderem zu folgenden **Zwecken** genutzt werden: • Strategische Ausrichtung von Unternehmen • Deep Learning • Bekämpfung von Kriminalität und Terrorismus • Wissenschaftliche Untersuchung von Naturphänomenen (z. B. Erdbeben und Klimawandel) • widerrechtliche Auswertungen, die Erpressung oder Betrug nach sich ziehen können Entscheidend sind in Bezug auf Big Data weniger die Daten selbst als vielmehr das, was damit geschieht.

Vor allem **Unternehmen** profitieren davon, Big Data zu analysieren und auszuwerten. Sowohl bewusst als auch unbewusst generieren und speichern sie heute Unmengen von Daten. Im Folgenden erfahren Sie, welche Möglichkeiten die richtige Analyse von großen Datenmengen Unternehmen im Detail bietet.

Entscheidungsfindung

Indem Unternehmen die im Betrieb anfallenden großen Datenmengen analysieren, können Muster erkannt und Informationen herausgefiltert werden. So können Unternehmen bessere Geschäftsentscheidungen treffen, die den Erfolg des Unternehmens erhöhen. Durch die Auswertung von Maschinendaten kann etwa berechnet werden, in welchen Abständen eine Maschine ausfällt. Das Unternehmen kann mit diesem Wissen die Maschine warten, bevor sie ausfällt. Auch in der Finanz- und Versicherungsbranche wird Big Data genutzt, um Risiken besser kalkulieren zu können.

Beispiel
Frau Schmidt ist 47 Jahre alt und möchte eine private Krankenversicherung abschließen. Bei einem Besuch ihres Versicherungsmaklers ist sie erstaunt über die hohen Kosten und fragt nach. Es stellt sich heraus, dass ihr Anbieter große Datenmengen analysiert, um die individuellen Versicherungskosten besser berechnen zu können. So findet das Unternehmen etwa heraus, welche besonderen Gesundheitsrisiken Frauen in diesem Alter tragen, die wie Frau Schmidt Raucherinnen sind, keine Kinder haben und nie Sport treiben.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Effizienzsteigerung

Wettbewerbsfähigkeit ist für Unternehmen sehr wichtig. Um mit der Konkurrenz mithalten zu können, müssen die Unternehmen Strategien entwerfen, wie sie Kosten sparen können, ohne dass dabei die Leistung beeinträchtigt wird. Große Datenmengen zu analysieren und miteinander zu verbinden hilft dabei.

Beispiel
Haben Sie schon einmal gehört, dass Fahrer des Paketdienstes UPS fast ausschließlich rechts abbiegen? Der Grund dafür ist, dass UPS mithilfe einer Big-Data-Analyse entdeckt hat, dass auf diese Weise in jedem Jahr rund zehn Millionen Dollar gespart werden können. Bestimmt fragen Sie sich wie das möglich ist: Die Zusammenführung von verschiedenen Datensätzen, etwa Unfallstatistiken, Daten zum Benzinverbrauch etc. hat ergeben, dass die UPS-Fahrzeuge viel seltener an Unfällen beteiligt sind, wenn sie nicht links abbiegen. So kann viel Geld gespart werden, auch wenn die Routen dadurch komplizierter werden.

Vorhersage in der Forschung und Entwicklung

Indem bestehende oder potenzielle Kunden oder Kundinnen ihre Vorliebe in Bezug auf bestimmte Produkte bekannt geben, kann die Forschung Trends erkennen und vorhersagen, passende Marketing-Strategien entwerfen und maßgeschneiderte Produkte entwickeln. Mit den geeigneten Analyseverfahren ist es z. B. auch möglich, die Bruchsicherheit eines Produkts noch während der Entwicklung vorherzusagen.

Beispiel
Ein Betreiber eines Online-Webshops installiert Cookies und Online-Tracking und verfolgt die Bewegungen seiner Besucher. Er kann feststellen, woher die Besucher kommen, welche Produkte sie anklicken, wie oft sie die Seite besuchen etc. Mithilfe dieser Daten kann der Betreiber die Inhalte der Seite und die angebotenen Produkte an die Präferenzen der Besucher anpassen und so seinen Umsatz erhöhen.

Personalisierter Kundenservice

Indem Unternehmen Entscheidungen von Kunden speichern, sind sie in der Lage, ihnen einen auf sie persönlich zugeschnittenen Kundenservice zu bieten.

Wenn etwa eine Nutzerin einen bestimmten Film oder eine bestimmte Serie auf Netflix ansieht, wird dies vom System gespeichert und die Nutzerin erhält beim nächsten Einloggen Empfehlungen, die sich an den bereits gesehenen Filmen oder Serien orientieren. Aber nicht immer stößt dieses personalisierte Angebot auf Gegenliebe:

Beispiel
Als Herr Maier feststellen muss, dass seine alten Bergschuhe nicht mehr zu gebrauchen sind, sucht er auf Google nach „Bergschuhe neu Herren“. Die vielen unterschiedlichen Angebote überfordern ihn, zudem stellt Herr Maier fest, dass viele Produkte nicht in sein Heimatland, Österreich, geliefert werden können. Herr Maier entschließt sich für eine persönliche Beratung in einem Fachgeschäft und kauft auch gleich ein Paar Bergschuhe. Dennoch wird ihm in den kommenden Tagen und Wochen im Internet vermehrt Werbung für Bergschuhe angezeigt, da seine Suchanfrage auf Google gespeichert und analysiert wurde. Herr Maier ist irritiert und fühlt sich beobachtet. Er beschließt, in Zukunft keine Suchanfragen auf Google mehr zu stellen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Fassen wir noch einmal zusammen:

Merke
Unternehmen haben zahlreiche Möglichkeiten, Big Data zu nutzen, um erfolgreicher zu sein. Dazu zählen: • **Entscheidungsfindung:** Die Analyse von Big Data ermöglicht Unternehmen, bessere Geschäftsentscheidungen zu treffen und Risiken besser einzuschätzen. • **Effizienzsteigerung:** Daten zu analysieren und miteinander zu verbinden (etwa Wetter- und Staudaten mit Benzinpreisen) hilft Unternehmen, Prozesse effizienter zu gestalten. • **Vorhersage im Bereich Forschung und Entwicklung** Mithilfe von Big Data können Vorhersagen im Hinblick auf Trends, Eigenschaften eines Produkts etc. getroffen werden. • **Personalisierter Kundenservice** Indem Unternehmen die von Kunden und Kundinnen getroffenen Entscheidungen speichern, können sie ihnen bei ihrem nächsten Besuch einen personalisierten Kundenservice anbieten.

3.4 Wie wird Big Data analysiert?

Sie haben nun erfahren, wie Big Data definiert wird und welche Möglichkeiten es gibt, die großen Datenmengen zu nutzen. In diesem Kapitel werden wir weiter in die Tiefe gehen, und uns mit der **Analyse** von Big Data beschäftigen. Dieser Fachbereich wird als **Big Data Analytics** bezeichnet.

Big Data Analytics – Theorie

Im ersten Schritt werden **große Mengen von Daten** aus unterschiedlichen Quellen **erfasst**, die verschiedene Formate haben. Dies geschieht oftmals mithilfe von Suchabfragen. Danach werden die Daten für die weitere Bearbeitung **vorbereitet**. Ein Problem ist oftmals, dass große Datenmengen

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

unstrukturiert und in ganz verschiedenen Formaten vorliegen und daher von einer herkömmlichen Datenbanksoftware nicht erfasst werden können.

Big Data Analytics setzt daher **komplizierte Prozesse** ein, um die Daten zu extrahieren und zu erfassen. Danach werden die Daten mit einer speziellen Big-Data-Software **analysiert**. Schließlich werden die Ergebnisse **aufbereitet** und **präsentiert**.

Wichtig dabei ist, dass die eingesetzte Software dazu fähig ist, viele Suchabfragen schnell umzusetzen und die verschiedenen Datensätze rasch zu importieren und zu bearbeiten. Um noch leistungsfähiger zu sein, nutzen viele Systeme bei der Datenverarbeitung nicht den **Festplattenspeicher** (wie herkömmliche Datenbankanwendungen), sondern den meist um einiges schnelleren **Arbeitsspeicher**. So kann die Zugriffsgeschwindigkeit erhöht werden und Analysen können nahezu in Echtzeit durchgeführt werden.

Merke
Die **Analyse** von Big Data lässt sich grob in drei verschiedene Bereiche gliedern: • Beschaffung der Daten aus vielen und unterschiedlichsten Quellen durch Einsatz von Suchabfragen • Auswertung und Optimierung der erfassten Daten • Datenanalyse und die Zusammenfassung sowie Präsentation von Ergebnissen Sehr wichtig dabei ist eine **leistungsfähige** und **geeignete Software**.

Big Data Analytics – Praxis

Interessant ist allerdings, dass Big Data Analytics in den meisten Unternehmen noch in den Kinderschuhen steckt und die sich daraus ergebenden **Möglichkeiten** bei weitem **nicht ausgeschöpft** werden. Durchschnittlich analysieren Unternehmen nur etwas mehr als ein **Drittel** der Daten, die beim digitalen Kontakt mit ihren Kunden (z. B. über Online-Shops oder Websites) entstehen.

Als Begründung werden oftmals die strengen **Datenschutzvorschriften** angeführt, die Big Data Analytics erschweren. Auf die Gesetze und Vorschriften, die den Datenschutz regeln, wird im folgenden Kapitel genauer eingegangen. In der Realität sind die Unternehmen aber meist in vielerlei Hinsicht noch nicht so weit, die großen Datenmengen effektiv für sich nutzen zu können. Folgende Bereiche spielen dabei eine wichtige Rolle:

Ratsam ist zunächst eine richtige Verteilung der Ergebnisse: die **Datenquellen** sollten aus verschiedenen Bereichen stammen, die Ergebnisse sollten in mehreren Bereichen des Unternehmens eingesetzt werden. Zudem ist eine geeignete **Strategie** erforderlich: Ein Unternehmen sollte wissen, zu welchem Zweck die großen Datenmengen analysiert werden. Sehr wichtig ist auch eine geeignete **Unternehmenskultur**, etwa sollten neue Technologien nicht grundsätzlich abgelehnt, sondern realistisch betrachtet werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Die meisten Unternehmen verfügen nicht über eine eigene Abteilung für Datenanalysen. Dennoch sollten einige Mitarbeitende das **erforderliche Fachwissen** mitbringen oder sich dieses in Schulungen aneignen. Gegebenenfalls müssen neue Mitarbeitende eingestellt werden. Zudem müssen innerhalb des Unternehmens Zuständigkeiten und Berechtigungen definiert werden.

Für die Analyse wird **leistungsfähige Technologie** in Form von geeigneten **Big-Data-Analyse-Tools** benötigt. Welche Tools geeignet sind hängt aber von der zuvor festgelegten Strategie bzw. dem definierten Zweck der Analyse ab. Zu guter Letzt ist auch eine geeignete Datenschutzstrategie erforderlich, um sicherzustellen, dass persönliche Daten von einzelnen Personen nicht an die Öffentlichkeit gelangen. Ein eigener Datenschutzexperte im Unternehmen stellt sicher, dass bei der Analyse der Daten die geltenden Gesetze und Vorschriften eingehalten werden.

Merke
Zusammenfassend sind folgende Punkte von Bedeutung, damit **Big Data Analytics** in einem Unternehmen **gelingt**: • Eine Big-Data-Strategie − Definition des Zwecks der Analyse • Eine geeignete Unternehmenskultur – Offenheit für neue Technologien • Personal mit dem erforderlichen Know-how – Schulungen oder Neueinstellungen • Eine leistungsfähige Technologie – Geeignete Big-Data-Analyse-Tools • Eine geeignete Datenschutzstrategie – Einhaltung der geltenden Gesetze und Vorschriften

3.5 Herausforderungen und Risiken von Big Data

In den vergangenen Kapiteln haben Sie gesehen, wie komplex es ist, Big Data zu analysieren und zu nutzen. Mindestens ebenso komplex sind die Herausforderungen und Risiken, die mit den großen Datenmengen verbunden sind. Die wohl größte **Herausforderung** für Unternehmen im Zusammenhang mit Big Data ist der **Datenschutz**:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Denn obwohl Unternehmen seit einigen Jahren verstärkt auf den Datenschutz achten, kommt es immer noch zu Problemen. So werden z.B. personenbezogene Daten von Internetnutzern ohne ihr Einverständnis verwendet werden und die Betroffenen können identifiziert, kontrolliert und im schlimmsten Fall erpresst werden.

Definition
Personenbezogene Daten ... bezeichnen **Daten**, die sich auf eine **Person** beziehen und Schlüsse über deren **Persönlichkeit** zulassen. Dazu zählen z.B. das Autokennzeichen von Werner Kogler, das Geburtsdatum Ihrer Nachbarin oder der Kontostand von Bill Gates.

Ein Beispiel für eine **Datenschutzverletzung** im Zusammenhang mit Big Data ist der Fall des Seitensprungportals Ashley Madison, der bereits in Kapitel 2 als Beispiel angeführt wurde. In diesem Fall gelangten die **personenbezogenen Daten** an die **Öffentlichkeit** und wurden benutzt, um die Eigentümer der Daten zu **erpressen**.

Datenschutzverordnungen und -gesetze helfen dabei, die Konsumenten vor Missbrauch zu schützen. **Grundlage** des **allgemeinen Datenschutzrechts** in der Europäischen Union und in Österreich ist die **Datenschutz-Grundverordnung**, die am 25. Mai 2018 in Kraft getreten ist.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Exkurs

Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung, kurz DSGVO, heißt vollständig „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“. Sie ist in Österreich unmittelbar anwendbar und wird durch das Datenschutzgesetz (DSG) und die Richtlinie für den Datenschutz ergänzt.

Diese Verordnung ermöglicht den EU-Bürgern, die Erhebung und Nutzung ihrer personenbezogenen Daten besser zu kontrollieren. Dies soll das Vertrauen der Konsumenten in die jeweiligen Unternehmen stärken. Bereits bestehende Rechte von EU-Bürgern und Bürgerinnen werden in der DSGVO gefestigt, zudem werden auch neue Rechte festgeschrieben. Die in der DSGVO festgeschriebenen Rechte umfassen:

- einen **vereinfachten Zugang zu personenbezogenen Daten** – dazu zählt, dass umfassende, klare und verständliche Informationen zur Verarbeitung der Daten bereitgestellt werden
- ein neues **Recht auf Datenübertragbarkeit** –personenbezogene Daten sollen vereinfacht übermittelt werden
- ein eindeutigeres **Recht auf** Löschung **(„Recht auf Vergessenwerden“)** –Daten werden gelöscht, wenn ein Bürger oder eine Bürgerin nicht damit einverstanden ist, dass seine oder ihre Daten verarbeitet werden und es keinen berechtigten Grund gibt, diese aufzubewahren
- ein Recht auf **Unterrichtung über gehackte personenbezogene Daten** –Unternehmen und Organisationen informieren die betroffenen Personen unverzüglich über ernsthafte Verletzungen des Schutzes personenbezogener Daten. Zudem muss die zuständige Datenschutzaufsichtsbehörde benachrichtigt werden

Für Unternehmen soll die DSGVO mehr Geschäftsmöglichkeiten schaffen und mit zahlreichen Maßnahmen Innovationen fördern. Unter anderem zählen dazu:

- die Schaffung von **einheitlichen EU-weiten Vorschriften**, was große Einsparungen ermöglicht
- die **Bestimmung eines Datenschutzbeauftragten** innerhalb von Behörden und Unternehmen, die sich mit umfangreichen Datensätzen beschäftigen
- die Benennung einer **zentralen Anlaufstelle** im eigenen Land, an die Unternehmen sich wenden müssen
- die Schaffung von **EU-Vorschriften für Unternehmen aus Drittländern**, an die sich Unternehmen aus Drittländern halten müssen, wenn sie Waren oder Dienstleistungen anbieten, oder beobachten, wie Personen sich verhalten
- die Schaffung von **innovationsfördernden Vorschriften**, die gewährleisten, dass die Datenschutzbestimmungen bereits in einer frühen Phase der Entwicklung von Dienstleistungen oder Produkten berücksichtigt werden
- die Anwendung von **datenschutzgerechten Techniken** wie **Pseudonymisierung** (Ersetzen von Stellen in einem Datensatz, die eine Identifikation der zugehörigen Person möglich machen) und **Verschlüsselung** (Daten werden so verschlüsselt, dass sie nur von befugten Personen gelesen werden können)
- Beseitigung von **Meldepflichten** für Unternehmen, um den freien Verkehr personenbezogener Daten innerhalb der Europäischen Union zu fördern
- Durchführung von **Folgenabschätzungen**, wenn die Verarbeitung der Daten die Rechte und Freiheiten von Personen mit hoher Wahrscheinlichkeit bedrohen könnte

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Die vollständige Datenschutz-Grundverordnung kann unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679 abgerufen werden.

Eine weitere Herausforderung ist, dass die bestehenden Mitarbeiter und Mitarbeiterinnen in Unternehmen nicht immer über das erforderliche **Fachwissen** verfügen und daher nicht offen für die Möglichkeiten sind, die die Analyse der großen Datenmengen für das Unternehmen bereithält.

So werden oftmals Zeit und Ressourcen vergeudet, weil den Beteiligten nicht klar ist, welches Ziel ein Big-Data-Projekt verfolgt oder welche Infrastruktur dafür erforderlich ist. **Kompetente Mitarbeiter und Mitarbeiterinnen** zu finden und zu halten ist für Unternehmen meist schwierig, da diese sehr gefragt sind.

Zudem ist die **Big-Data-Technologie** vielfältig und für Einsteiger **verwirrend**. Haben Sie schon einmal von Spark, Hadoop MapReduce, Cassandra oder Hbase gehört? Hierbei handelt es sich um Big-Data-Technologien mit verschiedenen Eigenschaften und Vorzügen.

Zudem entwickeln sich die Technologien auch noch in einem rasanten Tempo weiter, sodass Unternehmen mit der Einführung oftmals einfach nicht hinterherkommen. Für Unternehmen, die mit dem Gedanken spielen, eine Big-Data-Analyse einzusetzen, ist daher eine **fachkundige Beratung** sinnvoll.

Ein weiterer Punkt ist, dass Big-Data-Projekte sehr **kostspielig** sind. Dies gilt sowohl für Unternehmen, die sich für ein On-Premise-Modell entscheiden als auch für jene, die ein Cloud-Modell vorziehen. Der Unterschied ist, dass das Unternehmen die Big-Data-Software bei einem **On-Premise-Modell** im eigenen Rechenzentrum einsetzt und die Verantwortung für den Betrieb und die Wartung trägt. Bei einem **Cloud-Modell** hingegen wird die Software vom Unternehmen nur gemietet und die Daten verbleiben beim Anbieter.

Definition

On-Premise-Modell

...bezeichnet eine Lösung, bei der das Unternehmen Big-Data-Software **kauft** oder **mietet** und diese in seinem **eigenen Rechenzentrum** einsetzt. Um die Hardware muss das Unternehmen sich selbst kümmern, zudem übernimmt das Unternehmen die Verantwortung für die Nutzung der Software und die Daten werden beim Unternehmen gespeichert.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Definition

Cloud-Modell

...bezeichnet eine Lösung, bei der ein Unternehmen die Big-Data-Software als **Dienstleistung** bezieht, die Verantwortung für Wartungs- und Betrieb übernimmt der Anbieter. Das Unternehmen bezahlt einen Mietpreis, in dem die Hardware, der Betrieb und der Wartungsaufwand enthalten sind. Die Daten werden bei dieser Lösung beim Anbieter gespeichert.

Entscheidet sich ein Unternehmen für eine On-Premises-Lösung, muss es in neue Hardware investieren und neue Mitarbeitende einstellen, die das System bedienen und warten. Im Falle einer Cloud-Lösung müssen nur für die Bedienung und Wartung Mitarbeitende aufgenommen werden, zudem muss das Unternehmen die Kosten für die Cloud-Services tragen.

Schließlich ist die **Qualität** der Daten oft mangelhaft und Unternehmen stehen vor der Herausforderung, Daten aus verschiedenen Quellen mit verschiedener Qualität zu vereinheitlichen. Beispielsweise. analysiert ein Online-Händler Daten aus sozialen Medien, Webseite-Protokollen, Callcentern und Webseiten, die verschiedene Formate haben.

Aber selbst wenn alle angesprochenen Probleme gelöst sind, ist es für Unternehmen oftmals gar nicht so einfach, aus den großen Datenmengen nützliche **Erkenntnisse** zu gewinnen. Denn wenn z.B. Informationen miteinander **verknüpft** werden und daraus falsche Schlüsse gezogen werden, kann das gefährlich sein.

So kann etwa eine Person von einer Bank, die eine Big-Data-Analyse durchführt, als kreditunwürdig eingestuft werden, weil sie im selben Stadtviertel wohnt wie viele kreditunwürdige Personen und dasselbe Auto fährt wie zahlreiche als kreditunwürdig eingestufte Menschen. Auch das folgende Beispiel zeigt, warum die richtige Nutzung der großen Datenmengen so entscheidend ist:

Beispiel

Ein Online-Händler setzt auf Big-Data-Analytics, die sich auf historische Daten über das Verhalten der Kundinnen und Kunden stützt. So stellt sich heraus, dass Menschen, die schwarze Sneakers kaufen, oftmals auch ein Paar schwarze Sneaker-Socken dazu nehmen. Der Händler passt sein Sortiment für das Frühjahr dementsprechend an. Kurz vor Frühlingsbeginn postet aber ein bekannter Rapper auf Instagram ein Foto von sich mit schwarzen Sneakers und gelben Socken. Zahlreiche junge Leute sind daher auf der Suche nach gelben Socken zu ihren schwarzen Sneakers, die der Online-Händler aber leider schon bald nicht mehr vorrätig hat, weil er auf den Ansturm nicht vorbereitet war. Der Händler hat einfach die falsche Big-Data-Strategie angewandt und sich nur auf historische Ergebnisse verlassen und weitere wichtige Datenquellen wie soziale Medien, Shops von Mitbewerbern etc. außer Acht gelassen.

Merke

Zusammengefasst sind die wesentlichen **Herausforderungen**, denen Unternehmen bei der Nutzung von Big Data gegenüberstehen:

- Gewährleisten der **Datensicherheit** – Einhalten der Datenschutz-Grundverordnung (DSGVO)
- **Fachkompetenz** der Mitarbeiter und Mitarbeiterinnen – **fachkundiger Einsatz** der vielfältigen und sich rasch entwickelnden Big-Data-Technologie
- **Hohe Kosten** von Big-Data-Projekten (Hardware und Software bzw. Mietkosten, Mitarbeiter und Mitarbeiterinnen, Wartung etc.)
- **Mangelhafte Qualität** der Daten, Vereinheitlichung von Daten in verschiedenen Formaten und mit unterschiedlicher Qualität

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Richtige Interpretation** der Ergebnisse

Wie Sie gesehen haben, bietet Big Data enorme Möglichkeiten und Chancen, die von Unternehmen bisher nicht annähernd ausgeschöpft werden. Mit den großen Datenmengen sind aber auch Herausforderungen und Risiken verbunden, die nicht zu unterschätzen sind und viele Menschen verunsichern. Entscheidend dafür, dass Big Data erfolgreich genutzt wird, ohne dass dabei ein Schaden für andere Menschen entsteht, ist daher auch in Zukunft ein **verantwortungsvoller** und **sachkundiger** Umgang mit den großen Datenmengen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.6 Zusammenfassung

Unter **Big Data** versteht man große Datenmengen, die mit herkömmlicher Soft- oder Hardware nicht mehr verarbeitet werden können, und deren Verarbeitung und Analyse zu einem bestimmten **Zweck** geschieht. Im Gegensatz zu **Big Data** bezeichnet **Small Data** Daten, die aufgrund ihres Volumens und ihres Formats für den Menschen **zugänglich** sind.

Auf diese großen Datenmengen stoßen wir in ganz alltäglichen Situationen, etwa beim Surfen in sozialen Medien oder bei einer Suchanfrage auf Google. Zur besseren Definition von Big Data entwarf der Analytiker Doug Lane das **3-V-Modell**, das besagt, dass sich Big Data durch **Volumen**, **Geschwindigkeit** und **Vielfalt** auszeichnet.

Große Datenmengen können unter anderem zur besseren **strategischen Ausrichtung** von Unternehmen, für **Deep-Learning-Systeme**, zur **Bekämpfung von Kriminalität und Terrorismus**, zur **wissenschaftlichen Untersuchung von Naturphänomenen** (z. B. Erdbeben und Klimawandel), aber auch für **widerrechtliche Auswertungen** genutzt werden, die Erpressung oder Betrug nach sich ziehen können. Entscheidend sind daher weniger die großen Datenmengen selbst, sondern das, was damit geschieht.

Unternehmen können Big Data nutzen, um ihren **Geschäftserfolg zu steigern**. Unter anderem ermöglicht Big Data Analytics, bessere **Geschäftsentscheidungen** zu **treffen** und **Risiken** mit größerer Treffsicherheit **einzuschätzen**. Zudem kann die **Effizienz** von Unternehmensprozessen **gesteigert** werden, wenn Daten analysiert, ausgewertet und miteinander verbunden werden. Big Data hilft Unternehmen dabei, im Bereich Forschung und Entwicklung **Vorhersagen** bezüglich der Trends, Eigenschaften eines Produkts etc. treffen. Schließlich können die aus Big Data gewonnenen Erkenntnisse auch dazu genutzt werden, einen **personalisierten Kundenservice** anzubieten.

Damit die Analyse von Big Data erfolgreich ist, sind eine passende **Big-Data-Strategie**, eine geeignete **Unternehmenskultur**, **Personal** mit dem erforderlichen **Know-how**, eine **leistungsfähige Technologie** und nicht zuletzt eine **geeignete Datenschutzstrategie** erforderlich. Aber Big Data zu analysieren und zu verarbeiten bietet nicht nur Möglichkeiten und Chancen, sondern birgt auch Herausforderungen und Risiken.

Eine wesentliche Herausforderung für Unternehmen besteht darin, die **Datensicherheit** zu **gewährleisten** und die **Datenschutz-Grundverordnung** einzuhalten. Zudem ist es für Unternehmen oftmals schwierig, **geeignetes Fachpersonal** zu finden und zu halten, das mit der **komplexen Big-Data-Technologie** umgehen kann. Auch sind Big-Data-Projekte mit **hohen Kosten** verbunden und die **Datenqualität** ist oftmals **mangelhaft**. Zu guter Letzt müssen aus den Ergebnissen der Datenanalyse die richtigen **Schlüsse** gezogen und die richtigen **Entscheidungen** abgeleitet werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.7 ÜBUNGEN

1. **Etwa 90 Prozent aller heute weltweit verfügbaren Daten...**
   a. wurde in den letzten Jahren generiert.
   b. wurden im Laufe der Geschichte nach und nach generiert.
   c. wurden im letzten Jahrhundert produziert.
   d. Es handelt sich um sehr komplizierte Daten, weshalb sie unbekannt sind.

2. **Die Charakteristik(en) von Big Data sind:**
   a. Volumen
   b. Geschwindigkeit
   c. Menge
   d. Vielfalt

3. **Vervollständigen Sie den folgenden Text**

Die _____ von großen _____ ermöglicht, _____ zu gewinnen. Diese Ergebnisse können als Grundlage für _____ dienen.

4. **Was ist richtig?**
   a. Mit großen Datenmengen wird stets verantwortungsvoll umgegangen. Einige Unternehmen oder Institutionen halten die Datenschutzbestimmungen ein, was bedeutet, dass die Informationen der Öffentlichkeit zugänglich gemacht werden. Dies kann belanglos sein, aber in einigen Fällen kann es auch gefährlich sein und zu Betrug und Erpressung führen.
   b. Mit großen Datenmengen wird nicht immer unverantwortlich umgegangen. Einige Unternehmen oder Institutionen halten die Datenschutzbestimmungen nicht ein, was dazu führt, dass die Informationen der Öffentlichkeit zugänglich gemacht werden. Dies kann trivial sein, aber in einigen Fällen kann es auch vorteilhaft sein und Vertrauen schaffen.
   c. Mit großen Datenmengen wird nicht immer verantwortungsvoll umgegangen. Einige Unternehmen oder Institutionen halten sich nicht an die Datenschutzbestimmungen, was dazu führt, dass die Informationen der Öffentlichkeit zugänglich gemacht werden. Dies kann unbedeutend sein, aber in einigen Fällen kann es auch gefährlich sein und zu Betrug und Erpressung führen.

5. **Richtig oder Falsch?**

BIG DATA ist nützlich für:

   a. Schulung einer Maschine zur Verbesserung der maschinellen Übersetzung.
      T □ F □
   b. Aufdeckung von Diskrepanzen und Anomalien, die auf kriminelle oder terroristische Aktivitäten hinweisen könnten.
      T □ F □
   c. In der Wissenschaft werden große Datenmengen verwendet, um komplexe Naturphänomene wie den Klimawandel oder das Auftreten von Erdbeben und Epidemien zu untersuchen.
      T □ F □

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Im ersten Schritt werden große Mengen von _____ aus unterschiedlichen Quellen erfasst, die verschiedene Formate haben. Dies geschieht oftmals mithilfe von Suchabfragen. Danach werden die Daten für die weitere Bearbeitung vorbereitet. Ein Problem ist oftmals, dass große Datenmengen _____ und in ganz verschiedenen Formaten vorliegen und daher von einer herkömmlichen Datenbanksoftware nicht erfasst werden können.

Big Data Analytics setzt daher komplizierte _____ ein, um die Daten zu extrahieren und zu erfassen. Danach werden die Daten mit einer speziellen Big-Data-Software _____. Schließlich werden die Ergebnisse _____ und _____.

1 präsentiert, 2 Prozesse, 3 aufbereitet, 4 analysiert, 5 Daten, 6 unstrukturiert

7. Richtig oder Falsch?

Big Data in der Praxis:

a. Es ist interessant festzustellen, dass Big Data Analytics in den meisten Unternehmen noch in den Kinderschuhen steckt und die daraus ergebenden Möglichkeiten bei weitem noch nicht ausgeschöpft sind.
   T □ F □
b. Im Durchschnitt analysieren Unternehmen etwas mehr als ein Viertel der Daten, die durch den digitalen Kontakt mit ihren Kunden entstehen.
   T □ F □
c. Die meisten Unternehmen haben keine eigene Abteilung, die für die Datenanalyse zuständig ist.
   T □ F □

8. Was ist richtig:

a. Unternehmen haben dem Datenschutz in den letzten Jahren mehr Aufmerksamkeit geschenkt, es gibt aber immer noch Probleme. Beispielsweise werden die persönlichen Daten von Internetnutzern ohne deren Zustimmung verwendet und die Betroffenen können identifiziert, kontrolliert und im schlimmsten Fall erpresst werden.
b. Unternehmen haben dem Datenschutz in den letzten Jahren mehr Aufmerksamkeit geschenkt, und es gibt keine Probleme mehr. Beispielsweise werden die persönlichen Daten von Internetnutzern mit ihrer Zustimmung verwendet, und die Betroffenen können identifiziert, kontrolliert und im schlimmsten Fall mit Komplimenten beschenkt werden.
c. Unternehmen haben dem Datenschutz in den letzten Jahren weniger Aufmerksamkeit geschenkt, es gibt immer noch mehr Probleme. Beispielsweise werden die persönlichen Daten von Internetnutzern mit deren Zustimmung verwendet und die Betroffenen können identifiziert, kontrolliert und im schlimmsten Fall erpresst werden.

9. Vervollständigen Sie den Text mit den bereitgestellten Wörtern:

Big Data offers many _____ and _____ that companies have not even
Big Data bietet enorme _____ und _____, die von Unternehmen bisher nicht annähernd ausgeschöpft werden. Mit den großen Datenmengen sind aber auch _____ und _____ verbunden, die nicht zu unterschätzen sind und viele Menschen verunsichern. Entscheidend dafür, dass Big Data erfolgreich genutzt wird, ohne dass dabei ein Schaden für andere Menschen entsteht, ist daher auch in Zukunft ein _____ und _____ Umgang mit den großen Datenmengen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1 Herausforderungen, 2 verantwortungsvoller, 3 Möglichkeiten, 4 sachkundiger, 5 Chancen, 6 Risiken

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. SMART FACTORY

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.1 Das Thema

Die erste Einführung

„Sagt die eine Maschine zur anderen…“ – was klingt, wie ein kleiner Witz, ist der aktuelle große Traum der Fertigungsindustrie. Smart Factory ist DAS Stichwort in der aktuellen Industrierevolution – auch Industrie 4.0 genannt.

Denn smart ist King. Die digitale Revolution ermöglicht dem Menschen, in einer vernetzten Welt zu leben, in der Gebrauchsgegenstände zum Leben erwachen und ständig miteinander kommunizieren. Nicht nur Ihr Handy ist „smart“ – von Autos über den Sprachassistenten bis hin zum Kühlschrank findet ein ständiger Austausch an Daten und Informationen statt, der Ihr Leben angenehmer macht.

Nun stellen Sie sich das gewaltige Potential in der Produktion vor: Maschinen und Computer, die in ständigem Daten- und Informationsaustausch stehen, sich gegenseitig regulieren und aufeinander abstimmen – möglichst autonom und ohne menschlichen Handlungsbedarf Produkte herstellen und weiterverarbeiten. Nicht nur Fertigungsproduktivität und Effizienz könnten um ein Vielfaches gesteigert werden. Auch Unfälle, Produktionsüberschuss und Umweltbelastung könnten so reduziert werden.

Sie sehen also: Smart Factory ist die Zukunft. Aber sie ist auch schon Gegenwart: Viele Produzenten, zum Beispiel die Autoindustrie, setzen bereits Konzepte von Smart Factory erfolgreich um.

Natürlich ist Smart Factory nicht gerade simpel – aber auch nicht so kompliziert, wie Sie vielleicht glauben. In diesem Kapitel lernen Sie die Grundlagen und Anwendungsgebiete von Smart Factory.

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Smart Factory ist ein essenzieller Teil der Industrie 4.0. Die hier gelernten Grundlagen und Anwendungsgebiete helfen Ihnen, im Bereich der modernen Fertigungstechnik zukunftssicher mitreden und mitgestalten zu können.

Lernziele und Kompetenzen im Überblick

Diese Lerneinheit vermittelt Ihnen einen Überblick über die Grundlagen, Prozesse, Anwendungsgebiete und Problemstellungen der Smart Factory. Sie lernen die wichtigsten Begriffe zum Thema kennen, erfahren wie Smart Factory in der Industrie 4.0 verankert ist und welche

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bestandteile es gibt. Außerdem erhalten Sie einen Einblick in die Anwendungsgebiete sowie möglichen Probleme und lernen, warum diese für die Zukunft der Industrie so wichtig sind. Auch die Rolle des Menschen in einer automatisierten Umgebung soll erläutert werden.

Lernziele
Die Grundlagen, den Sinn und die entscheidenden Faktoren von Smart Factory verstehen können.
Die betrieblichen und technologischen Bestandteile von Smart Factory unterscheiden und verstehen können.
Die Anwendungsgebiete und aktuellen Problemstellungen verstehen können.

4.2 Was bedeutet Smart Factory?

Nicht nur Ihr Alltag und Berufsleben digitalisiert sich immer mehr, auch die Industrie durchläuft gerade einen weltweiten Prozess der Digitalisierung. Dieser Prozess trägt viele Namen: Industrial Internet, Internet der Dinge, Internet der Dienste – der wichtigste Begriff ist allerdings „Industrie 4.0“.

Definition
Industrie 4.0 … wird laut Duden als „Industrie, die auf weitgehend digitalisierten und untereinander vernetzten Prozessen beruht“ beschrieben. Damit ist der ständige Austausch von Informationen und Daten zwischen Mensch, Produktion, Logistik und Produkt gemeint.

Das Ziel ist es also, die Digitalisierung in der Fertigungsindustrie zu integrieren und damit optimierter produzieren zu können. Industrie 4.0 beinhaltet viele verschiedene Technologiefelder. Dazu gehören auch die Nutzung der sog. „Cloud“, Big Data Verwaltung sowie Datenschutz, der Mobilfunk und weitere.

Smart Factory (zu Deutsch: „Intelligente Fabrik“) ist nun ebenfalls einer der Bausteine von Industrie 4.0 – in der Fachpresse wird sie sogar als das Herzstück bezeichnet. Wenn Sie sich die Definition genauer ansehen, werden Sie merken warum:

Definition
Smart Factory … die REFA (der deutsche Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung) definiert den Begriff Smart Factory schlicht als „Produktionsumgebung, die sich selbst organisiert.“

Produktionsumgebungen sollen also autonom und möglichst ohne menschliches Zutun funktionieren. In einer solchen Produktionsumgebung eingeschlossen sind:

- **Fertigungsanlagen**
  Produktions- und Verarbeitungsmaschinen, die ein Produkt oder dessen Bestandteile herstellen und weiterverarbeiten (z. B. Fräs- oder Schweißanlagen aber auch Konstruktion und Verpackung).

- **Logistiksysteme**
  Die Bewegung und Lagerung von Produktionsgütern und Teilen (z. B. die Bereitstellung der richtigen Menge an Klebmaterial oder die Zwischenlagerung von fertigen Produkten).

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Produkt**
  Das Produkt selbst bzw. dessen Bauteile sind ebenfalls ein Teil der Produktionsumgebung (z. B. Autotüren oder Smartphone-Displays).

Die Grundlage für eine autonome Produktion ist die intelligente Vernetzung dieser drei Bestandteile. Das Produkt soll dabei in der Lage sein, mit der Fertigungsanlage und dem Logistiksystem zu kommunizieren und diesen eigenständig Informationen zur Herstellung mitzuteilen (z. B. welche Displaygröße der Rahmen erfordert, wie viele und welche Schrauben notwendig sind).

Das erfordert einerseits eine ganze Menge Daten, andererseits auch einen Weg, diese Daten überhaupt weiterzugeben. Die Lösung? Simpel: Chips und Sensoren!

Jedes Produkt (bzw. dessen Bauteile) in der Fabrik bekommt einen Chip mit und wird damit zum „Smart-Product." Der Chip enthält Informationen über Herstellung sowie logistische Anforderungen und teilt diese der Produktionsumgebung mit. Die Fertigungsanlagen und Logistiksysteme können diese Informationen richtig verarbeiten und sich wiederum untereinander für den notwendigen nächsten Arbeitsschritt abstimmen und diesen durchführen.

Die technologische Grundlage dafür wird übrigens „Cyber-Physical-Systems" genannt. Das bedeutet nichts anderes, als die Verbindung von mechanischen bzw. elektronischen Teilen mit software- bzw. informationstechnischen Komponenten – stark vereinfacht gesagt, passiert genau das, wenn man ein Produkt mit einem Chip versieht.

Ein jedes Produkt „weiß" also selbst, in welcher Produktionsstufe es gerade ist, wie und wo es weiterberarbeitet werden soll und was es dazu braucht. Es kommuniziert dieses Wissen mit der gesamten Produktionsumgebung, damit diese weiß, wie es damit umgehen muss.

Ein Beispiel zeigt den Prozess leicht verständlich:

Beispiel
Beispiel Autoindustrie Stellen Sie sich vor, Sie sind eine Autotür und haben das Glück, in einer Smart Factory hergestellt zu werden. Ihre Produktionsumgebung beinhaltet viele Bestandteile des fertigen Produktes – einem

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Auto. Hier werden Reifen gelagert, Fahrwerke hergestellt, die Bordelektronik zusammengebaut, einzelne Teile lackiert usw.

Dafür gibt es in der Fabrik die richtigen Fertigungsmaschinen und auch die richtigen logistischen Transportmittel (z. B. Förderband von Maschine A zu Maschine B).

Heute ist Ihr großer Tag, denn heute werden die Türen montiert. Das wissen Sie, weil das Produkt (Auto) über einen Chip der Produktionsumgebung mitgeteilt hat, dass alles andere im Auto bereits fertig eingebaut ist. Sie werden also über ein Logistiksystem aus der Zwischenlagerung geholt und erstmal grün lackiert – das Auto hat die Farbe im Vorhinein mitgeteilt. Aber auch Sie haben mithilfe Ihres Chips etwas zu sagen: „Ich bin eine Autotür vorne links. Ich brauche 8 Schrauben. Ich muss aber erst noch den Lack trocknen."

Die Produktionsumgebung weiß also, was sie zu tun hat, lagert Sie zur Trocknung, stellt 8 Schrauben zur Verfügung und montiert Sie vorne links.

Natürlich ist der eigentliche Produktionsprozess erst der Anfang. Denken Sie an das Beispiel vom Kühlschrank, der selbst die Milch bestellt, wenn er merkt, dass sie zur Neige geht. Oder das Autohaus, bei dem Ersatzteile oder gleich ganze Autos je nach momentanem Lagerbestand automatisch beim Autoproduzenten bestellt werden.

Sie sehen, die Möglichkeiten von Smart Factory sind nicht nur auf eine Fabrik selbst begrenzt. In Zukunft soll es möglich sein, dass in Echtzeit automatisch nach Angebot und Nachfrage produziert (auch „just-in-time Produktion" genannt), geliefert und verbraucht werden kann. Damit können Ressourcen viel genauer verbraucht und Engpässe vermieden werden.

Wichtig

Wirtschaftliche Faktoren

Die Entwicklung und Umsetzung solcher Technologien ist natürlich nicht gerade billig. Industrielle Unternehmen erhoffen sich auch wirtschaftliche Vorteile.

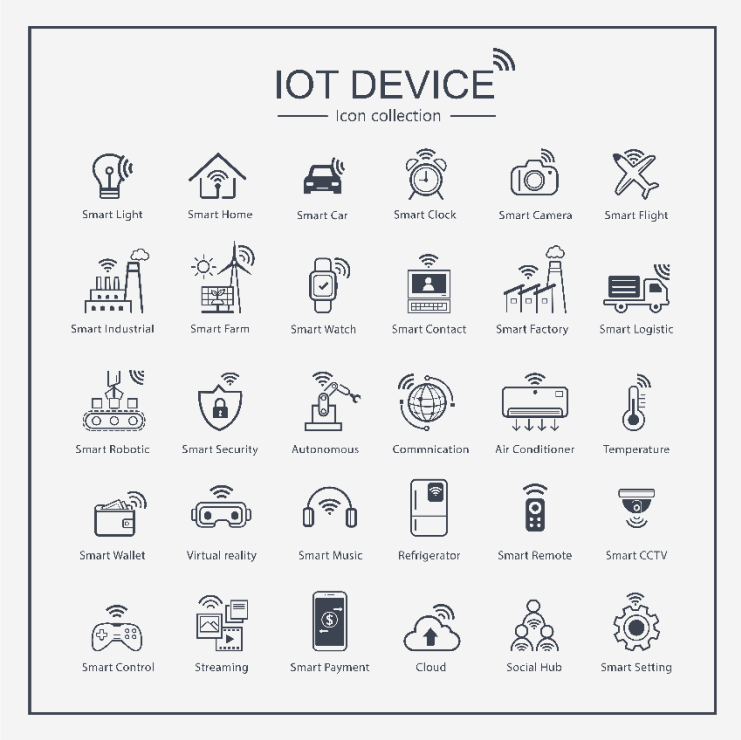
Smart Factory ermöglicht beispielsweise, dass Massenproduktion und Einzelproduktion in derselben Fabrik möglich sind. Damit kann in der Anschaffung von Maschinen gespart werden. Außerdem können Ressourcen und Industriegüter zeitnaher bestellt werden und teurer Überschuss oder Verschleiß vermindert werden.

Smart Factory ist also einer der wichtigsten Bestandteile der Digitalisierung und spielt eine große Rolle, nicht nur in der Industrie, sondern auch im vernetzten, „smarten" Alltag des Menschen.

Wieviel unterschiedliche Faktoren das sein können, zeigt folgende Grafik:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Smart Factory ist also nur ein Bereich in einem großem Pool an smarten Konzepten. Für die (Fertigungs-)Industrie ist er jedoch eben das Herzstück.

Merken
Smart Factory ist ein essenzieller Bestandteil der Digitalisierung in der Industrie. Dabei sollen… • Fertigungsanlagen, Logistiksysteme und Produkte miteinander selbstständig Informationen austauschen… • …damit sich die Produktionsumgebung möglichst selbst organisiert. Dazu benötigen die beteiligten Maschinen und Produkte… • eine Verbindung der mechanischen und elektronischen Komponenten mit einer Software bzw. Informationseinheit (Chip)… • …um an einem Netzwerk an Datenaustausch teilnehmen zu können. Damit wird erreicht, dass… • Produktion und Logistik in Echtzeit nach Bedarf gesteuert wird, • Ressourcen effizienter verwaltet werden, • und die Produktionskosten verringert werden.

4.3 Was braucht eine Smart Factory?

Eine Smart Factory ist also eine ziemlich moderne Sache. Damit das funktioniert braucht es ein paar betriebliche und technische Grundbedingungen. In diesem Abschnitt lernen Sie, was eine Smart Factory unbedingt benötigt. Sie werden sehen, das ist eine ganze Menge!

Wichtig
Der Datenaustausch Die Bedingungen beginnen schon beim Datenaustausch selbst. Eine Smart Factory tauscht eine große Menge an Informationen aus. Dieser Datenaustausch muss dabei nach folgenden Grundregeln ablaufen können:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Bidirektionaler Datentransfer**
  Der Informationsaustausch funktioniert in beide Richtungen (sowohl Informationen senden als auch empfangen).

- **Horizontaler und vertikaler Datentransfer**
  Der Informationsaustausch erfolgt sowohl vertikal über unterschiedliche Abteilungen (z. B: Kundenauftragsmanagement, Fabrikhalle, Produkt) als auch horizontal (Maschine A zu Maschine B in der Fabrikhalle).

Da das Ziel eine Erfassung der wichtigen Prozessdaten in der Produktion in Echtzeit ist, müssen betriebliche Steuerungssysteme im Datenaustausch integriert sein. Diese betrieblichen Steuerungssysteme sind Konzepte, die bei der Führung, Kontrolle und Steuerung von Unternehmen im Produktionssektor helfen. Folgende sind dabei unbedingt miteinzubeziehen:

- **Enterprise-Resource-Planning**
  Hier werden Ressourcen wie Material und Betriebsmittel, aber auch Personal, Kapital und generell Informationstechnik geplant, gesteuert und verwaltet.

- **Manufacturing-Execution**
  Damit ist die Steuerung und Kontrolle der Echtzeit-Produktion gemeint (im Deutschen auch als Produktionsleitsystem bezeichnet).

- **Product-Lifecycle-Management**
  Ein Konzept, bei dem es um den Lebenszyklus (von Entwurf über Konstruktion und Produktion bis zum Verkauf, Nutzung und Entsorgung) geht und der Verwaltung der dabei generierten Informationen.

- **Supply-Chain-Management**
  Die Verwaltung und Verbesserung der Lieferkette, also das Zuliefern und Empfangen von Produktions- und Dienstleistungsgütern.

Selbstverständlich braucht es auch technologische Bausteine und Vorrausetzungen, damit eine Smart Factory in Echtzeit funktionieren kann. Einige der wichtigsten sind bereits entwickelt und im Einsatz. Das sind ganz allgemeine Bauteile wie Sensoren („Messfühler“ die ihre Umgebung auf physikalische oder chemische Eigenschaften erfassen können) und Aktoren (Bauteile die elektrisch angesteuert mechanische Bewegungen ausführen). Wichtig sind hier moderne automatisierbare Produktionstechniken wie Robotik und der 3D-Druck aber auch verschiedene betriebliche Anwendungen der IT, z. B. für die Produktionssteuerung und das Controlling. Auch die Vernetzung über Breitband-Internet und die Ansteuerung über Cloud-Systeme (externe Server, die Rechenleistung zur Verfügung stellen) sind bereits technisch möglich.
Andere Systeme und Bausteine stecken allerdings noch in den Kinderschuhen, wie beispielsweise Augmented-Reality – hier wird die wahrgenommene Realität mit den Informationen eines Computers „erweitert“ (Bsp.: Google Glass). Folgende Tabelle gibt einen kleinen Überblick über die benötigten technologischen Bausteine:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	SENSORIK	INNOVATIVE PRODUKTE	ICT
TECHNOLOGIE	Aktoren Sensoren Cyber-physikalische Systeme Logistiksysteme	Digital aufgerüstete Fertigungsstraßen Cyber-physikalische Systeme MES M2M-Lösungen HMI Human Machine Interface (sichere Endgeräte) Additive Fertigung (3D-Druck) Robotik	IP v6 Cyber-Physikalische Systeme IKT-Infrastruktur Breitband Netzkommunikation ERP PLM SCM Datenbanken, In-Memory Cloud Computing Big Data Analytics Augmented Reality Cyber Security
PROZESSLEISTUNG	Echtzeitfähigkeit Verfolgbarkeit Zuverlässigkeit Vollständigkeit	Vollständige Vernetzung Selbstkonfiguration	Wireless & Mobile Vernetzung Echtzeitfähigkeit Datenschutz

Exkurs

Industrie und Fabriken im Wandel

Wenn man Smart Factory als einen Teil von Industrie 4.0 definiert ist es logisch, dass es da auch eine Industrie 1.0., 2.0 und 3.0 gegeben haben muss.

Während die erste und zweite Stufe der Industrialisierung die Einführung von mechanischen Produktionsanlagen und der Massenproduktion zur Folge hatte, ging es in der Industrie 3.0 bereits um Automatisierung, den Einsatz von IT und Elektronik – allerdings ohne dass diese Komponenten miteinander in Echtzeit kommunizieren und Einfluss aufeinander ausüben.

Wie eben erwähnt, sind einige notwendige Technologien bereits im Einsatz, als Weiterentwicklungen dieser industriellen Vorstufen, andere müssen jedoch erst komplett neu entwickelt werden. Dabei gibt es auch Einflüsse aus nichtindustriellen Bereichen. Das „Internet der Dinge“ spielt hier eine große Rolle und ist im privaten Sektor bereits breiter bekannt als die Vernetzung der Haushaltsgeräte (Beispiel: Handy erkennt, dass Sie nach Hause kommen und schaltet automatisch die Lichter in der Wohnung ein, gleichzeitig kocht die Kaffeemaschine einen Espresso und der Fernseher schaltet die Nachrichten ein).

Die Industrie 4.0 muss die Internet-der-Dinge-Technologien auf eine industrielle Ebene befördern und in einen wirtschaftlich profitablen Rahmen setzen. Nur so kann eine wirklich neue und vierte „Industrierevolution“ gelingen.

Natürlich sind viele diese Technologien auf den ersten Blick allein dem Namen nach in Sinn und Funktion etwas intransparent. Deshalb sollen die wichtigsten in der Folge etwas genauer erläutert werden:

Cyber-physikalische Systeme (CPS)

Das wichtigste zuerst: CPS sind der technische Grundbaustein einer jeden Smart Factory. Auch als Embedded Systems (zu Deutsch: eingebettete Systeme) bezeichnet, ist damit jegliche elektronische und informationstechnische Ausrüstung von Objekten in der Produktionsumgebung gemeint. Das können sein:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Sensoren**, für das direkte Umfeld des Objekts
- **Aktoren**, die Objekte aktiv bewegen (zum Beispiel Hebel)
- **Identifikatoren**, um Objekte eindeutig identifizieren und zuordnen zu können (z. B. Barcode)
- **Mikrocontroller** (oben erwähnte Chips), die Daten analysieren, den Status feststellen und die nächsten Arbeitsschritte bestimmen
- **Kommunikationssysteme**, die über Kabel oder Funk Zugang ins Netzwerk ermöglichen

Damit wird ein Objekt erst „smart" – also intelligent. Beispiele für so ein smartes Objekt in der Produktionsumgebung sind Werkzeuge oder auch intelligente Behälter. Ein so ein Behälter ist über seinen Barcode identifizierbar und liefert aufgrund von Sensoren und Mikrocontrollern Auskunft über Position und Inhalt.

IPv6 – viele, viele Internetadressen

Eine weitere Basis für die Smart Factory Entwicklung stellt ein neues Internetprotokoll dar. Ein solches kann erst einen ausreichend großen sogenannten „Adressraum" gewährleisten. Je mehr intelligente Objekte miteinander verbunden sind, desto mehr Internet-Adressen muss es auch geben, damit diese unmissverständlich angesprochen werden können.

Breitbandnetzwerke

Smart Factories erzeugen, senden, empfangen und verarbeiten eine Unmenge an Daten. Das muss schnell passieren – sonst kann nicht in Echtzeit gearbeitet werden. Dafür werden Breitbandnetzwerke benötigt, um genügend hohe Datenübertragungsraten zu gewährleisten, Verzögerungszeiten gering zu halten und eine Ausfallsicherheit zu bieten.

Wichtig
WLAN und Mobilfunk Innerbetrieblich ist damit natürlich simpel gesagt einfach ein starkes WLAN notwendig – außerbetrieblich muss aber auch an die Mobilfunknetze gedacht werden (Beispiel: LKW, der über den Mobilfunk automatisch die empfangende Fabrik von einem Stau und damit verspäteten Ressourcen informiert).

Machine-to-Machine Kommunikation (M2M) – intelligente Maschinen

Weitere technologische Bausteine sind interagierende Maschinen, die sich automatisiert mit anderen Maschinen und den Produkten austauschen können. Dabei werden Materialdaten, Auftragsinformationen, der aktuelle Status und Instandhaltungsmaßnahmen kommuniziert. Außerdem sammeln sie Daten über ihren Systemzustand – im Prinzip, „wie es ihnen so geht". Laufende Prozesse können so in Echtzeit analysiert und (nach-)geregelt werden.

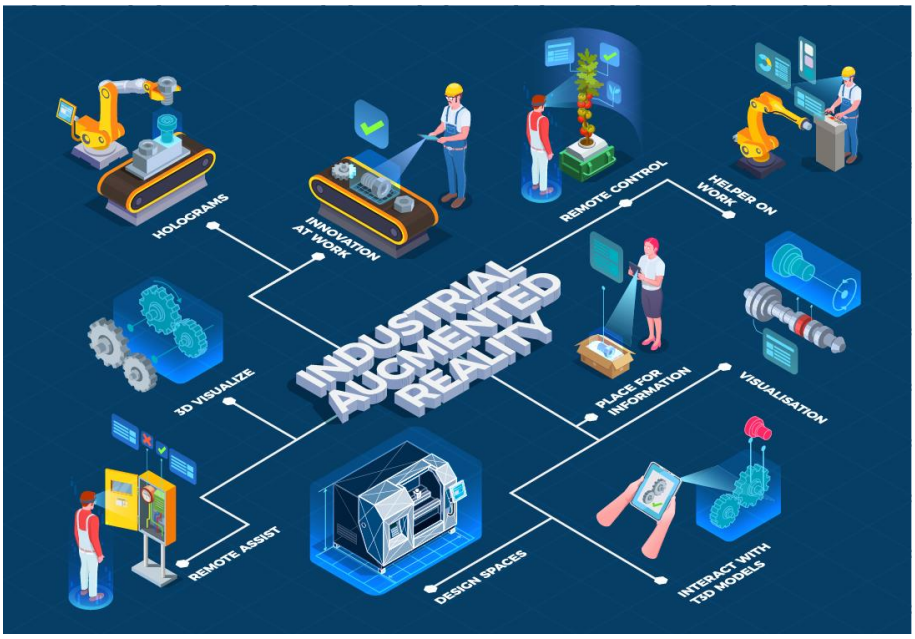
Human-Machine-Interfaces (HMI)

Die Interaktion von Mensch, Maschine und Produkt (merke: in echten Smart Factories müssen alle drei intelligent sein) ist besonders spannend. Während hochmobile Geräte wie Tablets und Smartphones zwar bereits eine unmittelbare Einbindung des Menschen in das Netzwerk und die Kommunikation einer Smart Factory bietet, ist hier noch viel Forschungsspielraum.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Eine hochmoderne, alternative Methode ist bereits der vereinzelte Einsatz von Augmented-Reality Brillen, die virtuell ergänzend die Beschäftigten in der Produktionsumgebung mit Informationen versorgen.



Produktionsleitsysteme – Manufacturing-Execution-Systems (MES)

Diese wurden oben in den betrieblichen Steuerungssystemen bereits erwähnt und dienen zur Verwaltung von Ressourcen (Betriebsmittel, Personal und Lieferteile) und zur umfassenden Erfassung von Produktionsdaten (Betriebs-, Maschinen- und Personaldaten).

Solche Produktionsleitsysteme existieren zwar bereits schon sehr lange, allerdings sind sie noch nicht vollständig vernetzt. Erst wenn sie in Echtzeit mit Fertigungsanlagen, den Logistiksystemen und den Produkten Informationen austauschen können, wird das volle Potential einer Smart Factory freigesetzt.

Big Data Analytics

Wenn in Echtzeit alles und jeder Daten generiert, verarbeitet und sendet, dann ergeben sich natürlich enorme Datenmengen – diese wollen und müssen von entsprechender IT-Infrastruktur und IT-Ausrüstung ordentlich behandelt werden. Die weitere Analyse setzt ebenfalls eine hohe Rechenkapazität voraus.

Big-Data-Management und Big-Data-Analytics werden mit Standardlösungen am Markt zwar schon angeboten bzw. als integrierte Cloud-Lösung durchgeführt – die Anforderungen steigen jedoch immer weiter.

Cloud-Computing und Speicherplatz

Cloud-Computing meint das externe Nutzen von Rechenleistung und Speicherplatz, die über ein Inter- oder Intranet zur Verfügung gestellt werden. Bei den hohen Ansprüchen zur Datenleistung ist die Integration einer „Cloud“ in einer Produktionsumgebung keine schlechte Idee. So können alle Anwendungen und Daten zentral verwaltet und koordiniert werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bisher verwendete, innerbetriebliche Serverlösungen können den Ansprüchen von Big Data Verarbeitung und den Voraussetzungen einer Smart Factory für Analyse, Planung, Regelung und Optimierung in Echtzeit nicht mehr gerecht werden.

Wichtig

Und der Mensch?

In diesem Kapitel haben Sie gelernt, dass die Produktion weitgehend ohne den Menschen auskommen soll, jetzt allerdings wieder, dass der Mensch über Augmented-Reality doch integriert wird – ja was denn jetzt?

Nun, auch wenn sich die Smart Factory grundlegend selbst organisieren und den Fertigungsprozess automatisieren soll, ist der Mensch trotzdem noch ein Teil – nur eben nicht mehr in der Rolle der Produktion, sondern der weiteren Optimierung und Kontrolle der produzierenden Systeme. Dabei stimmt er beispielsweise Schnittstellen zu anderen Systemen oder Produktionsumgebungen ab. Hier ist auch Augmented-Reality als Konzept wichtig – sie ermöglicht ein virtuelles Eingreifen, ganz ohne physischen Kontakt.

Eine Smart Factory braucht außerdem noch generalisierte Standards und Normen. Eine gemeinsame semantische Basis (d. h. kompatible Programmiersprachen und eine universelle Produktionssprache) ist unbedingt notwendig. Eine Standardisierung von Smart Factory Betrieben kann verhindern, dass Systeme, die eigentlich miteinander kommunizieren sollten, sich am Ende aufgrund technologischer Unterschiede doch nicht verstehen.

Beispiel

Rechtliche Herausforderungen in der Smart Factory

Die raschen technologischen Entwicklungen werfen auch rechtliche Fragen auf, die zum Teil noch nicht vollständig gelöst sind. Ein Beispiel verdeutlicht die Problematik:

Ein Lieferant bekommt von einem Unternehmen eine Bestellung. Das Unternehmen verarbeitet Knetmasse zu lustigen Tieren und verkauft diese dann an Spielwarenläden. Dabei nutzt das Unternehmen eine Smart Factory, ist also sowohl mit dem Lieferanten (rohe Knetmasse) als auch mit den Abnehmern (Spielwarenladen) automatisiert vernetzt. Eine Bestellung wurde nun jedoch aufgrund einer vom System fehlerhaft verarbeiteten Kundennachfrage geschickt und ist viel höher, als das Unternehmen verarbeiten oder lagern kann. Das Unternehmen will natürlich den Überschuss nicht bezahlen, die Spielwarenhändler brauchen sowieso keine so riesige Menge an Knetmassetierchen und der Lieferant ist sauer, weil er umsonst Knetmasse hergestellt hat.

Wer ist nun schuld? Wer muss zahlen, wenn der Fehler ein System verursacht hat, das alle drei Parteien miteinbezieht? Hier ist das Recht noch nicht klar genug ausgelegt.

Außerdem stellt sich noch die Frage des Datenschutzes, der Compliance und der Verschwiegenheit innerhalb von Partnerschaften. Wenn alle Daten ausgetauscht werden, ist auch gleichzeitig alles offengelegt. Welche der zur Verfügung gestellten Daten dürfen beispielsweise vom Lieferanten genutzt werden? Zu welchem Zweck? Auch hier müssen noch Konzepte entwickelt werden.

Merken

Smart Factory bedarf einiger betrieblicher und technischer Voraussetzungen, um die angestrebte Vernetzung und den Datenaustausch in Echtzeit zu ermöglichen.

Die wichtigsten technologischen Bausteine sind:

- Cyber-Physical-Systems

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- Big Data und Cloud-Computing
- Breitband und ausreichender Adressraum
- Human-Machine-Interfaces
- Integration von betrieblichen Produktionsleitsystemen

Der Mensch ist nicht mehr Teil der Produktion, sondern **kontrolliert und optimiert die Produktionsprozesse.**

Smart Factories müssen auch in einem rechtlichen Rahmen betrachtet werden – Standards und Normen können dabei helfen.

4.4 Welche Anwendungs- und Problemfelder gibt es aktuell bei Smart Factories?

Smart Factories sind also der wichtigste Teil der digitalisierten Industrie 4.0 und somit die Zukunft der Fertigungs- und Produktionsindustrie. Doch wie weit sind Fabriken und Industrie in der Praxis? Welche Anwendungsgebiete gibt es und welche Probleme gilt es noch zu lösen?

Wichtig

Innovation vs. Standardlösung

Wie bereits erläutert, würden Standards und Normen auf (Software-)technischer Ebene der Entwicklung von Smart Factories durchaus zugutekommen. Hier gibt es allerdings ein großes Problem.

Um als Unternehmen erfolgreich zu sein, muss man der Konkurrenz voraus sein – wer hier auf Standardlösungen wartet, der ist dann unter Umständen im Wettbewerb klar im Nachteil.

Deshalb wird mit Hochdruck individuell an unterschiedlichen, eigenen Lösungen geforscht und gearbeitet. Das wiederum widerspricht natürlich einer universellen Gesamtlösung.

Vor allem Autohersteller wie BMW und Audi sind bereits dabei, zumindest Teile einer Smart Factory in der Herstellung und Konstruktion von Fahrzeugen zu verwenden. Besonders in der Robotik ist die Industrie schon recht weit gekommen.

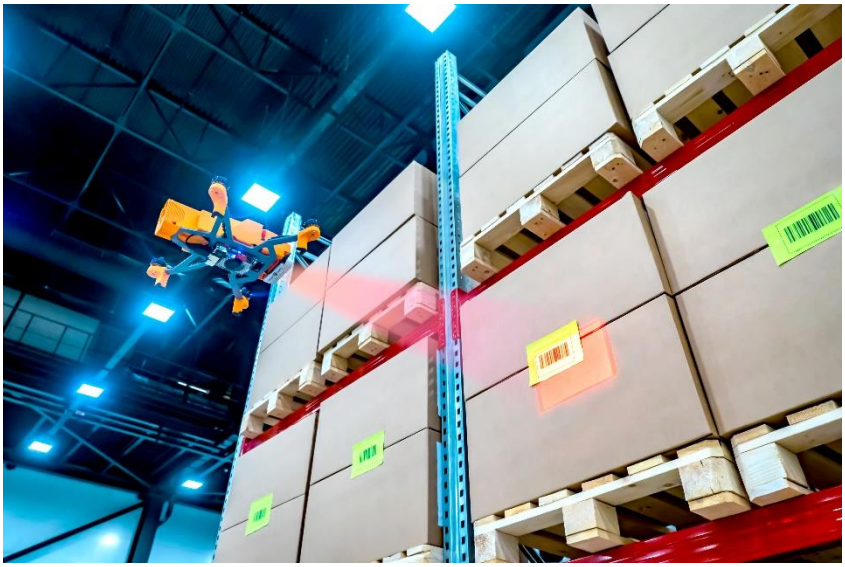
Audi verwendet derzeit beispielsweise das **System *PART4you*.** Dabei handelt es sich um einen Roboter, der mithilfe von integrierten Kameras und Saugnäpfen einzelne Bauteile aufnehmen kann und diese in der Fabrik eigenständig zur richtigen Position bewegt. Dabei werden zusätzlich Sensoren und Chips verwendet, um die Sicherheitsstandards in der Produktionsumgebung einhalten zu können.

Bei BMW werden vermehrt **Smartwatches** eingesetzt, als virtuelle Schnittstelle von Mensch und Fabrik. Die an der Produktion beteiligten Personen werden so über die Anforderungen (z. B. Ausstattungslinie, Schraubenanzahl etc.) informiert – in Echtzeit über die smarten Produktteile selbst. Dazu werden beispielsweise auch am Handgelenk getragene Barcode-Scanner verwendet. Audi testet hier bereits Augmented-Reality Brillen, was vor allem für kürzere Einarbeitungszeiten sorgt.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Auch Drohnen werden bereits eingesetzt. Manche Hersteller verwenden diese beispielsweise für die Inventur ihrer Lagerbestände. Im Prinzip handelt es sich bei einer solchen **„Inventurdrohne“** um einen fliegenden Barcodescanner, der jeden Stellplatz und jedes Produkt anhand von Barcodes identifizieren und zuordnen kann. Die Informationen werden danach an die betrieblichen Systeme weitergeleitet – ziemlich genial, oder?



Auch die **Agrarindustrie** erfreut sich bereits einiger Teilbereiche von Smart Factory. Hier spielen ebenfalls Drohnen eine große Rolle. Diese werden hauptsächlich zur Risikofindung eingesetzt (z. B. Auffinden von Tiernestern). Die Drohnen kommunizieren dabei mit den Erntefahrzeugen und sorgen für eine verbesserte Navigation.

Sie sehen, Smart Factory wird in Teilbereichen schon kräftig eingesetzt und getestet – bis zur tatsächlichen Umsetzung ist es aber noch ein langer Weg. Außerdem gilt es noch **einige offene Fragen und Problemstellung** zu klären:

- **Standards und Normen**
  Wie bereits erwähnt: In einer vernetzten (Industrie-)Welt sollen möglichst alle Computer dieselbe Sprache sprechen. Das ist bei individueller Innovationsforschung einzelner Unternehmen schwierig.

Co-funded by the Erasmus+ Programme of the European Union

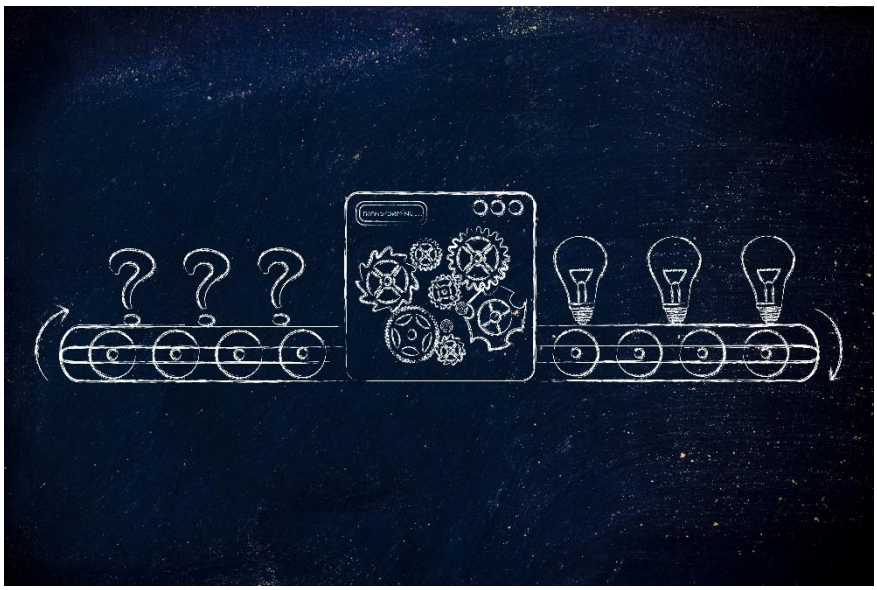
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Recht und Datenschutz**
  Wer ist schuld, wenn die Maschine einen Fehler macht? Das nutzende Unternehmen? Der Hersteller? Der oder die Schichtverantwortliche? Das ist noch nicht wirklich geklärt. Außerdem offen ist die Frage nach der Geheimhaltung von Daten – schließlich will kein Unternehmen, dass eigene Patente oder Forschungsergebnisse nach außen dringen. Das ist bei einer kompletten Vernetzung allerdings ebenfalls schwierig.

- **Sicherheit und Hacking**
  Computer und mit dem Internet vernetzte Systeme sind anfällig für Cyber-Angriffe von außen. Cyber-Kriegsführung oder -Spionage wird ein immer ernsteres Thema. Was passiert, wenn eine Smart-Factory „gehackt“ wird?

- **Abhängigkeit**
  Ein total vernetztes System muss auch funktionieren, wenn einzelne Teile ausfallen. Wenn vereinzelte Anlagen im System nicht korrekt funktionieren, muss gewährleistet sein, dass die Fabrik auch nach Möglichkeit ohne diese weiterläuft – Produktionsausfälle könnten sonst ernste wirtschaftliche Konsequenzen für das Unternehmen bedeuten.

- **Wird der Mensch dümmer?**
  Und wie immer stellt sich die Frage, wenn es um moderne, intelligente Technologien geht – wird der Mensch dümmer, wenn die Maschine intelligenter wird? Eher nicht. Durchaus berechtigt ist aber folgender Gedanke: wenn der Mensch im Produktionsprozess nur mehr als kontrollierendes Organ wirkt, ist er dann in der Lage, bei Ausfällen „einzuspringen“? Geht hier unter Umständen Know-How verloren, wenn stets die Anlage selbst angibt, was zu tun ist?



Merken
Smart Factory wird in Teilbereichen bereits in verschiedenen Branchen eingesetzt – die fortschrittlichste davon ist die Autoindustrie. Hier werden u. a. bereits folgende Techniken eingesetzt: • Smarte Robotik • Drohnen • Smartwatches als Mensch-Fabrik-Interface

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Es gibt allerdings noch einige offene Fragen und Problemstellungen:

- Standards vs. Innovation
- Recht und Datenschutz
- Sicherheit und Hacking
- Abhängigkeit von einem System
- Know-how-Verlust des Menschen

Bis zu einem ganzheitlichen Einsatz von Smart Factories ist es noch ein weiter Weg. Unternehmen forschen, testen und entwickeln zwar schon auf Hochdruck, bis zu einer Zusammenführung aller Teilbereiche müssen allerdings noch einige **technische, sicherheitsrelevante und rechtliche** Problemstellungen gelöst werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.5 Zusammenfassung

Die Smart Factory ist ein **essenzieller Bestandteil der Digitalisierung in der Industrie**. Dabei sollen Fertigungsanlagen, Logistiksysteme und Produkte miteinander selbstständig Informationen austauschen, damit sich die **Produktionsumgebung möglichst selbst organisiert**.

Dazu benötigen die beteiligten Maschinen und Produkte eine Verbindung der mechanischen und elektronischen Komponenten mit einer Software bzw. Informationseinheit, um an einem **Netzwerk an Datenaustausch** teilnehmen zu können.

Der Mensch ist nicht mehr Teil der Produktion, sondern kontrolliert und optimiert die Produktionsprozesse.

Damit wird erreicht, dass Produktion und Logistik **in Echtzeit nach Bedarf gesteuert** wird, Ressourcen effizienter verwaltet und die Produktionskosten verringert werden.

Eine Smart Factory bedarf **einiger betrieblicher und technischer Voraussetzungen**, um die angestrebte Vernetzung und den Datenaustausch in Echtzeit zu ermöglichen.

Die wichtigsten technologischen Bausteine sind schnelles Breitband Internet, Big-Data-Anwendungen und Cloud-Computing, Human-Machine-Interfaces und Cyber-Physical-Systems.

Smart Factory wird in **Teilbereichen bereits in verschiedenen Branchen** eingesetzt – die fortschrittlichste davon ist die Autoindustrie. Vor allem smarte Robotik, Drohnen und Smartwatches (als Mensch-Fabrik-Interface) werden bereits erfolgreich verwendet.

Es gibt allerdings noch einige **offene Fragen und Problemstellungen**. Dazu gehören rechtliche Themen sowie Datenschutz, die Verwendung von standardisierten Technologien, Sicherheitsbedenken und Systemanfälligkeit.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.6 ÜBUNGEN

1. **Die Industrie durchläuft einen weltweiten Prozess der Digitalisierung, dieser Prozess hat viele Namen, aber der wichtigste ist…**
   a. Industrielles Internet
   b. Internet of things
   c. Industry 4.0
   d. Internet of services

2. **Die Industrie 4.0 umfasst viele verschiedene Technologiefelder, darunter auch der/die/das sogenannte …**
   a. Cloud
   b. Carpet
   c. Management
   d. Netzwerk

3. **Produktionsanlagen sollten autonom und möglichst ohne menschliches Einwirken funktionieren. Eine Produktionsumgebung dieser Art umfasst:**
   a. Alle Antworten sind richtig
   b. Produktionsanlagen
   c. Logistiksysteme
   d. Produkte

4. **Die REFA (Deutsche Vereinigung für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung) definiert den Begriff "Smart Factory" als " Produktionsumgebung, die sich _____ organisiert."**
   a. ständig
   b. mit externer Hilfe
   c. selbst
   d. monatlich

5. **Die Übertragung von Daten in der Industrie 4.0 erfolgt durch _____ und _____**
   a. Buse und Computer
   b. Kabel und Knoten
   c. Handys und Satelliten
   d. Chips und Sensoren

6. **Eine Smart Factory tauscht eine große Menge an Informationen aus. Dieser Datenaustausch erfolgt nach folgenden Grundregeln:**

1. Horizontale und vertikale Datenübertragung	a) Der Informationsaustausch funktioniert in beide Richtungen (sowohl beim Senden als auch beim Empfangen von Informationen).
2. Bidirektionaler Datentransfer	b. Informationen werden sowohl vertikal zwischen verschiedenen Abteilungen (z.B.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	Kundenauftragsverwaltung, Produktionshalle, Produkt) als auch horizontal (Maschine A zu Maschine B in der Produktionshalle) ausgetauscht.

7. Mit dem Ziel, wichtige Prozessdaten in der Produktion in Echtzeit zu erfassen, müssen Betriebsleitsysteme in den Datenaustausch integriert werden. Bei diesen Betriebsleitsystemen handelt es sich um Konzepte, die helfen, Unternehmen im Produktionsbereich zu verwalten, zu überwachen und zu steuern. Folgende Elemente müssen einbezogen werden.

1. Enterprise-Resource-Planning	a. Ein Konzept, das sich mit dem Lebenszyklus (vom Entwurf, der Konstruktion und der Produktion bis zum Verkauf, der Nutzung und der Entsorgung) und der Verwaltung der dabei erzeugten Informationen befasst.
2. Manufacturing-Execution	b. Das Management und die Verbesserung der Versorgungskette, d.h. die Lieferung und der Empfang von Produktions- und Dienstleistungsgütern.
3. Product-Lifecycle-Management	c. Hier werden Ressourcen, wie Material und Betriebsmittel, aber auch Personal, Kapital und allgemeine Informationstechnologie geplant, kontrolliert und verwaltet.
4. Supply-Chain-Management	d. Dies bezieht sich auf die Steuerung und Überwachung der Produktion in Echtzeit (im Deutschen auch als Produktionskontrollsystem bezeichnet).

8. Eins nach dem anderen: CPS sind der technische Eckpfeiler jeder Smart Factory. Auch als eingebettete Systeme bezeichnet, bezieht sich dies auf jede elektronische und informationstechnische Ausstattung von Objekten in der Produktionsumgebung. Diese können sein:

1. Sensoren	a. Chips, die Daten analysieren und die nächsten Schritte bestimmen.
2. Identifikatoren	b. Bewegen das Objekt aktiv (z.B. Hebel)
3. Aktoren	c. Zur eindeutigen Identifizierung und Zuordnung von Objekten z.B. Strichcode
4. Kommunikationssysteme	d. Für das direkte Umfeld des Objektes
5. Mikrocontroller	e. System, das den Zugang zum Netzwerk über Kabel oder Funk ermöglicht

9. Eine weitere Grundlage für die Entwicklung der Smart Factory ist ein neues Internet-Protokoll. Ein solches Protokoll kann einen ausreichend großen sogenannten "Adressraum" gewährleisten. Je mehr intelligente Objekte miteinander verbunden sind, desto mehr Internet-Adressen werden benötigt, um sie eindeutig zu adressieren.

a. IPv6 Protokoll
b. MTV
c. IPv4 Protokoll
d. DNS

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

10.Die wichtigsten technologischen Elemente in Industrie 4.0 sind:

a. Pneumatische, hydraulische und mechanische Systeme
b. Sensoren, Aktoren, Identifikatoren und Mikrocontroller
c. Keine Antwort ist korrekt
d. Cyber-physikalische Systeme, große Datenmengen und Cloud Computing, Breitband und ausreichender Adressraum, maschinell-menschliche Schnittstellen und Integration des betrieblichen Produktionssteuerungssystems

11. In der Industrie 4.0 werden bereits folgende Techniken eingesetzt:

a. Selbstreinigende Autos, Eindringlingsschutzsysteme und Smartwatches
b. Intelligente Robotik, Drohnen und Smartwatches als Mensch-Maschine-Schnittstellen (HMI)
c. a und b sind korrekt
d. Autonome Förderbänder, programmierte Produktionsalarme und Analyseroboter

12.Aber in der Industrie 4.0 ist nicht alles perfekt. Es gibt noch einige offene Fragen und Probleme, die geklärt werden müssen.

1. Standards und Normen	a. Wessen Fehler ist es, wenn die Maschinen einen Fehler machen? Die Firma, die sie benutzt? Der Hersteller? Die für die Schicht verantwortliche Person? Das ist noch nicht wirklich geklärt. Auch die Frage des Datengeheimnisses bleibt unbeantwortet - schließlich will kein Unternehmen, dass sein eigenes Patent oder seine eigene Forschung offengelegt wird.
2. Abhängigkeit	b. In einer vernetzten industriellen Welt sollten möglichst alle Computer die gleiche Sprache sprechen. Dies ist bei der individuellen Innovationsforschung einzelner Unternehmen schwierig.
3. Lernen	c. Mit dem Internet vernetzte Computer und Systeme sind anfällig für Cyberangriffe von außen. Cyber-Kriegsführung oder Spionage wird zu einem immer ernsteren Thema. Was passiert, wenn eine Smart Factory gehackt wird?
4. Datenschutzgesetz	d. Wenn der Mensch im Produktionsprozess nur als Kontrollorgan fungiert, wird er dann im Falle von Fehlschlägen "einspringen" können? Ist es denkbar, dass hier Know-how verloren geht, wenn die Anlage selbst immer aufzeigt, was genau zu tun ist?
5. Sicherheit und Hacking	e. Ein vollständig vernetztes System muss auch dann funktionieren, wenn einzelne Teile ausfallen. Wenn einzelne Einheiten im System nicht richtig funktionieren, muss sichergestellt werden, dass die Fabrik, wenn möglich, auch ohne sie weiterarbeitet, da sonst Produktionsausfälle schwerwiegende wirtschaftliche Folgen für das Unternehmen haben könnten.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5. IT-SECURITY

Co-funded by the Erasmus+ Programme of the European Union

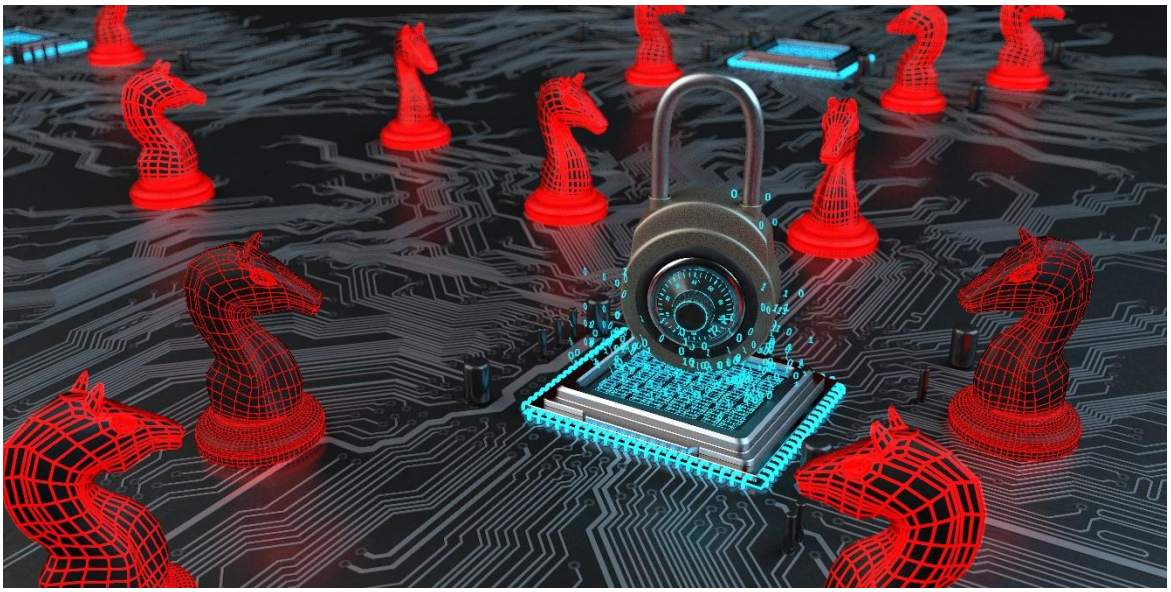
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.1 Das Thema

Die erste Einführung

Das Sichern von Daten war schon einmal leichter. Früher wurden wichtige Dokumente, wie beispielsweise Verträge oder Sparbücher, meistens in Safes versperrt oder schlicht versteckt. Damit war sichergestellt, dass Unbefugte sich gar nicht oder nur sehr schwer Zugang verschaffen konnten.

Heute ist das nicht mehr so simpel. Dokumente und Daten sind nun digitalisiert und oft physisch gar nicht mehr vorhanden. Denken Sie beispielsweise an Ihr Online-Banking, an wichtige Verträge, die elektronisch unterzeichnet und per E-Mail verschickt werden oder private Daten wie Fotos. So wie früher analoge Dokumente „weggesperrt" wurden, müssen heutzutage Daten auch digital gesichert werden. Denn potentieller Datendiebstahl oder ein widerrechtliches Verarbeiten bzw. das Manipulieren von Daten kann hohe Risiken und ernste Konsequenzen mit sich tragen – sowohl für Privatpersonen als auch für ganze Unternehmen und Organisationen.



IT-Security ist als Thema zwar nicht sonderlich neu – aufgrund der rasanten digitalen Entwicklungen in den letzten Jahren gewinnt sie allerdings enorm an Wichtigkeit. Wir sollten uns damit auskennen, denn digitale Informationen sind, ob uns das bewusst ist oder nicht, schlicht die Grundlage des modernen Lebens.

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Vom Privatleben bis hin zum Beruf, vom Einzelunternehmen bis zum globalen Konzern – Daten und Informationen sind in allen Lebensbereichen präsent und ein wertvolles Gut. Ob es um Internetkriminalität, Datenverlust oder Datenfälschung geht – IT-Security sollte wirklich jeden etwas angehen. Diese Lerneinheit wird Ihnen helfen, für die Sicherheit Ihrer privaten Daten zu sorgen und in Ihrem Unternehmen einen wertvollen Beitrag zur Datensicherheit leisten zu können. Somit werden Sie für IT-Sicherheit sensibilisiert und können diesbezüglich selbstsicher auftreten.

Lernziele und Kompetenzen im Überblick

In diesem Kapitel lernen Sie den Begriff IT-Sicherheit in seinen wichtigsten Facetten kennen. Sie erfahren Näheres über Bedeutung und Ziele, aber auch welche Bedrohungen und Maßnahmen es im Bereich der IT-Sicherheit derzeit gibt. Sie werden lernen, wie Sie persönlich zu einer sichereren Informationsumgebung beitragen können – sowohl privat als auch beruflich.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Lernziele
Die allgemeinen Begriffsbestimmungen und Einsatzgebiete von IT-Security kennen und verstehen.
Die Ziele und Aufgaben der IT-Security benennen und erklären können.
Aktuelle IT-Bedrohungen kennenlernen und in den Einsatzbereichen der IT-Security zuordnen können.
Maßnahmen und Verteidigungsmechanismen der IT-Security in der Anwendung kennen.

5.2 Begriffsbestimmungen und Einsatzgebiete

Gleich vorweg: **IT-Security ist nicht gleich Informationssicherheit** – obwohl oft beide Bezeichnungen gleich verwendet werden (vor allem wenn nicht genau vom Englischen in eine andere Sprache übersetzt wurde), gibt es einen feinen Unterschied, der Ihnen auch bei der Definition des Begriffs weiterhelfen wird.

Dieser Unterschied ist im Prinzip das „T“ im Namen – denn IT-Security steht für „Information Technology Security“, also eigentlich „Informationstechniksicherheit.“ Das klingt aber ziemlich sperrig – deshalb bleibt man lieber bei „IT-Security“.

Definition

Informationssicherheit vs. IT-Security

Der Begriff **Informationssicherheit** meint Schutzmaßnahmen für ALLE Systeme, die in irgendeiner Art und Weise Informationen verarbeiten oder lagern. Dabei ist es egal, ob diese digital oder „analog“ sind. Damit ist also der Computer genauso gemeint wie ein Stapel handgeschriebener, vertraulicher Dokumente.

IT-Security ist ein Teilbereich der Informationssicherheit. Hier werden tatsächlich nur die Schutzmaßnahmen von sog. „soziotechnischen“ Systemen gemeint. Soziotechnische Systeme sind nichts anderes als Systeme, in denen der Mensch Informationstechnik verwendet, um Daten zu speichern und zu verarbeiten.

Informationstechnik wird laut Duden übrigens definiert als „Technik der Erfassung, Übermittlung, Verarbeitung und Speicherung von Informationen durch Computer und Telekommunikationseinrichtungen.“

So weit so klar. Da heutzutage aber nur mehr in sehr wenigen Ausnahmesituationen überhaupt keine IT in irgendeiner Art und Weise verwendet wird, deckt die IT-Security einen sehr großen Teil der Informationssicherheit ab.
Ein Beispiel für eine IT-lose Anwendung von Informationssicherheit wäre vielleicht das mit Hand geschriebene Geheimrezept im Safe ihres Lieblings-Restaurants. Darum soll es in dieser Lerneinheit jedoch nicht gehen.
Der Begriff „IT-Security“ umfasst im Wesentlichen folgende vier Faktoren:

- **Computersicherheit:** Hier sind im Speziellen die Sicherheitsvorkehrungen von lokalen und vernetzten Computersystemen selbst gemeint. Wie sicher ist ein Computer vor fremdem Zugriff oder Manipulation? Was passiert, wenn ein Computer „abstürzt“?

- **Datenschutz:** Der Begriff ist momentan in aller Munde – aber zurecht, denn „Datenschutz ist Personenschutz“. Dieser Aspekt ist für die Privatperson der wesentlichste, denn hier geht es um den Schutz der eigenen, personenbezogenen Daten vor Missbrauch. Privatsphäre und Anonymität sind ein heikles Thema in einer digitalisierten Welt.

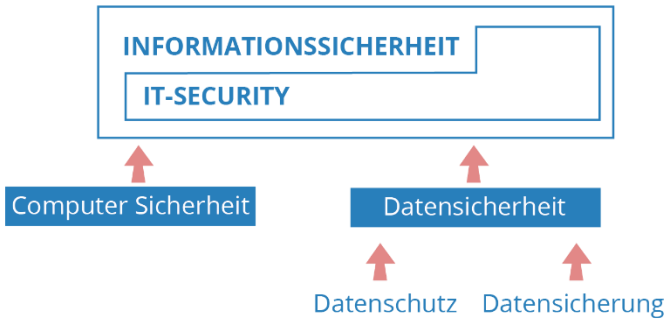
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Datensicherheit:** Das ist wiederum eher technischer Natur. Hier geht es weniger um rechtliche Fragen, sondern eher einfach darum, wie man Daten vor Manipulation oder Verlust schützt. Datensicherheit kann als die technische Vorstufe für erfolgreichen Datenschutz verstanden werden.

- **Datensicherung:** Hier geht es speziell um die (mehrfache) Sicherung der Daten – Sie kennen das höchstwahrscheinlich unter dem Begriff „Backup“. Und nichts anderes ist die Datensicherung auch: die richtige Vervielfältigung von Daten, um gegen deren Verlust vorzubeugen.

Die folgende Grafik macht den Zusammenhang aller gelernten Begriffe etwas verständlicher:



IT-Security macht einen Großteil der Informationssicherheit aus und besteht im Wesentlichen aus Computersicherheit und Datensicherheit. Datensicherheit ist dabei die Grundlage von erfolgreichem Datenschutz und Datensicherung.

Wichtig

Daten und Informationen

Jetzt haben Sie schon so oft die Begriffe „Daten“ und „Informationen“ gelesen, da möchten Sie doch sicher auch den Unterschied wissen:

- Daten sind eigentlich nutzlose Zeichen und Symbole – ohne Kontext bleiben diese Daten inhaltsleer und es ist nichts damit anzufangen. Nehmen wir zum Beispiel einfach die Ziffernfolge 19081974.

- Informationen sind Daten, die in einen Kontext gesetzt werden. Dann werden diese Daten aussagekräftig und transportieren eine Information, z. B.: Geburtsdatum 19.08.1974 – schon ist klar, was mit der Ziffernfolge gemeint war.

Das ist übrigens auch der Grundgedanke hinter Verschlüsselungen, egal ob diese am Computer oder mit der Hand vorgenommen werden. Man lässt Daten ohne Kontext, würfelt diese vielleicht sogar durcheinander. Nur jemand, der auch den Kontext versteht, versteht den Sinn der Ziffernfolge.

Für wen ist die Umsetzung von IT-Security nun wichtig?
Eigentlich für jede und jeden mit einem Computer – ob als Einzelperson oder in einer Organisation. Trotzdem hilft es, die Umsetzungsbereiche von IT-Security etwas präziser einzuordnen, auch, um später die Bedrohungen und entsprechenden Maßnahmen in das richtige Einsatzgebiet zuordnen zu können.

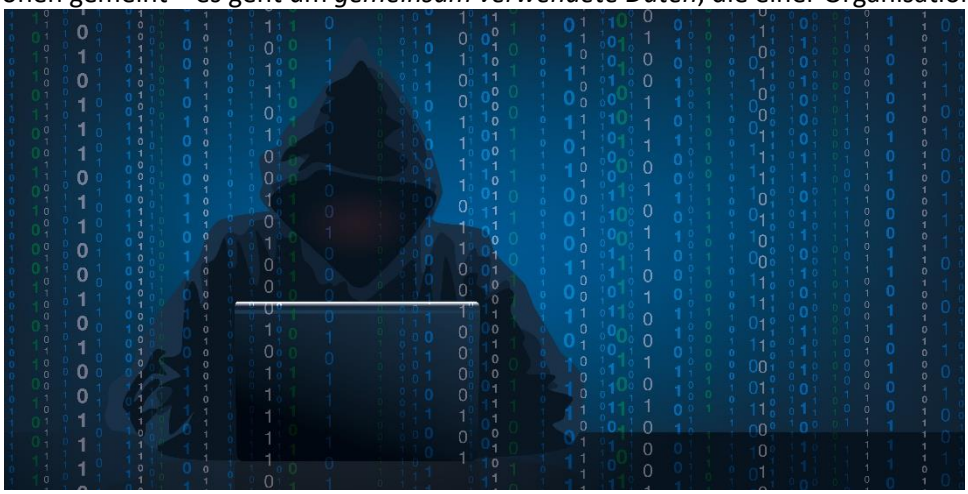
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Im Wesentlichen unterscheidet man, ob Geräte und Daten privat oder innerhalb einer Organisation genutzt werden.

Privater Bereich: Dies betrifft Einzelpersonen und Geräte, die privat genutzt werden. Dazu gehört zum Beispiel Ihr eigener Laptop oder Ihr Smartphone. Ob Sie diesen öffentlich nutzen, also zum Beispiel im WLAN einer Universität ist dabei zweitrangig – wesentlich ist, dass Sie das Gerät zur *Verwaltung Ihrer privaten Daten* verwenden.

Unternehmen und Organisationen: Hier geht es um Geräte, mit denen auf die Daten von Unternehmen oder Organisationen zugegriffen werden kann – beispielsweise Firmenlaptops oder Firmentelefone. Damit sind sowohl wirtschaftliche Unternehmen als auch staatliche Betriebe und Organisationen gemeint – es geht um *gemeinsam verwendete Daten*, die einer Organisation gehören.



Welche Unterschiede gibt es nun konkret in diesen beiden Einsatzbereichen?

- **Privater Bereich**
  So gut wie jede Software hat immer in irgendeiner Art und Weise Programmierfehler. Das kann aufgrund von Ungenauigkeit aber auch ganz einfach aus Unwissenheit geschehen sein – denn niemand kann wissen, über welche „Hintertür“ oder durch welche Besonderheit im Software-Code ungebetener Zugang erlangt werden kann.

  Das ist vor allem deshalb problematisch, weil die meisten Geräte ständig mit dem Internet verbunden sind. Dazu zählen der private Computer, das Smartphone, die Smartwatch, aber eben auch der Fernseher oder der Sprachassistent. Über das Internet führt dann auch meistens der „Einbruch“ bzw. der unautorisierte Zugang zu den persönlichen Daten. Ein Datendiebstahl kann aber auch physisch erfolgen, z. B. durch Einbruch und entwenden des Computers.
  Festzuhalten ist: es kann schnell passiert sein und schon sind Passwörter des Online-Bankings gestohlen, wichtige Dokumente verloren oder private Fotos öffentlich.

  IT Security ist im Privatbereich ein wichtiges Thema – dennoch sind die angewandten Mittel der IT-Security in diesem Bereich weniger ausgeprägt – sei es aufgrund von fehlendem Bewusstsein der nutzenden Personen oder auch aufgrund geringerer technischer Möglichkeiten.

- **Unternehmen und Organisationen**
  Geht es in Unternehmen um IT Security, stehen dabei natürlich hauptsächlich wirtschaftliche Interessen im Vordergrund. Die technische Umsetzung der IT-Security ist zwar meist besser als

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

im privaten Bereich, dafür ist aber die kriminelle Energie hinter möglichen IT-Angriffen bei weitem höher.

Man denke dabei an Banken und Versicherungen, die viel Geld verwalten. Oder technische High-Tech-Betriebe, die ihre Prototypen und Ideen vor der Konkurrenz sichern möchten.
Auch hier sind mittlerweile die IT-Systeme über das Internet verbunden. Ein Beispiel dafür wäre die Nutzung eines Cloud-Services von mehreren Firmenstandorten: Ein Cloud-Server stellt hier Speicherplatz für Dokumente zur Verfügung, die von allen Standorten aus über das Internet gelesen und bearbeitet werden können. Hier muss vor allem sichergestellt werden, dass nur befugte Personen auf diese Dokumente zugreifen können.

Große Unternehmen haben mittlerweile eigene Abteilungen, die sich nur mit der IT-Security beschäftigen und investieren viel Geld, um immer am neuesten Stand zu bleiben. Denn auch hier gilt: WIE ein IT-Angriff passiert, weiß man vorher nicht – deshalb muss hauptsächlich schnell reagiert werden können, WENN ein Angriff erfolgt.

Es gibt übrigens standardisierte Dokumente für IT-Security, sog. Grundschutz-Kataloge, die detailliert IT-Security Modelle vorstellen. Die IT entwickelt sich jedoch so schnell, dass die Befolgung dieser Kataloge alleine nicht ausreicht und sie teilweise schnell veraltet sind.

Merken
IT-Security ist ein Teilgebiet der Informationssicherheit und meint alle Schutzmaßnahmen in der Verarbeitung und Speicherung von Daten mit Hilfe von Systemen der Informationstechnik. Damit sind sowohl Computer als auch alle sonstigen Telekommunikationsmittel im privaten und unternehmerischen Umfeld miteingeschlossen. IT-Security lässt sich auch in Teilgebieten definieren, die miteinander verknüpft sind: • Computersicherheit • Datenschutz • Datensicherung • Datensicherheit Die Einsatzgebiete von IT-Security können dem privaten sowie unternehmerischen und dem öffentlichen Bereich zugeordnet werden. Da die meisten Geräte mit dem Internet verbunden sind, sind die Gefahren von IT-Angriffen und die Maßnahmen für IT-Security in allen Bereichen recht ähnlich – Unterschiede sind im persönlichen Bewusstsein und den technologischen Faktoren zu finden.

5.3 Ziele und Aufgaben der IT-Security

Die oberste Aufgabe in der IT-Security ist es, **den technischen Entwicklungen zu folgen.** Die sich digitalisierende und vernetzende Welt schreitet technologisch sehr rasch voran. Neue Technologien erfordern neue Software, neue Einsatzgebiete erfordern neue Sicherheitsmaßnahmen.

Während früher einfach ein paar wenige, große Computer Aufgaben für ganze Firmen übernommen haben und von ein paar Personen bedient wurden, sind es heute eine Unzahl an kleinen Geräten, die alle miteinander verbunden sind.

Da kann es ganz schön knifflig werden, überhaupt zu erklären, was genau gerade wovor zu schützen ist, welche Bedrohungen es gibt und welche Lücken in Sicherheitssystemen ausgenutzt werden könnten.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Es sind aber sogenannte **Schutzziele** definiert – diese gelten als „Hauptziele“ jeder IT-Security. Diese sind:

Vertraulichkeit – Integrität – Verfügbarkeit

Wenn Sie sich diese drei Schutzziele bewusst zu Herzen nehmen, haben Sie schon die halbe IT-Security umgesetzt! Bei weiteren Recherchen helfen Ihnen übrigens die englischen Begriffe – diese sind deshalb auch in Klammer beigefügt. So sehen diese im Detail aus:

- **Vertraulichkeit** (engl. Confidentiality)
  Daten, Informationen und daraus resultierendes Wissen soll vor Personen, die kein Recht auf die Sichtung dieser haben, verborgen werden.

- **Integrität** (engl. Integritiy)
  Daten, Informationen und daraus resultierendes Wissen sollen vor unerlaubten Veränderungen und Manipulationen geschützt werden.

- **Verfügbarkeit** (engl. Availability)
  Daten, Informationen und daraus resultierendes Wissen sollen jenen, die erlaubten Zugang haben, bei Bedarf auch zugänglich sein.

Diese drei Ziele sind deshalb so wichtig und zentral, da sie im privaten sowie im unternehmerischen Kontext gleich bedeutend sind. Schauen Sie sich dazu folgende Beispiele an:

Beispiele

Die drei Schutzziele im privaten Kontext am Beispiel „Online-Banking“
Sie nutzen den Online-Zugang Ihres Bankkontos. Das ist ein heikles Thema, denn es geht hier um Ihr Geld. Wie sind die Schutzziele hier erfüllt?

- Vertraulichkeit: Ihre Zugangs- und Kontodaten sowie Passwörter sollen nur Ihnen zugänglich sein.

- Integrität: Niemand außer Ihnen soll unerlaubt Überweisungen online durchführen dürfen.

- Verfügbarkeit: Sie sollen jederzeit und von überall aus unbeschränkt Zugang zu ihrem Konto haben können.

Die drei Schutzziele im unternehmerischen Kontext am Beispiel „Produktentwicklung“
Ein Unternehmen entwickelt ein völlig neues Produkt, das den Markt revolutionieren soll. Das soll natürlich vonstatten gehen, ohne dass die Konkurrenz davon mitprofitiert. Wie könnten hier die Schutzziele erfüllt sein?

- Vertraulichkeit: Alle Informationen über die Entwicklung des neuen Produkts sind nur von befugten Personen einsehbar.
- Integrität: Gewonnene Daten aus der Entwicklung des Produkts sind vor Sabotage und Manipulation von außen geschützt.

- Verfügbarkeit: Alle beteiligten und befugten Personen haben gesicherten Zugriff auf die Entwicklung des neuen Produkts und den daraus resultierenden Daten.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Zusätzlich gibt es auch noch erweiterte Schutzziele, die je nach Bedarf bedacht werden müssen. Diese sind nicht unbedingt in der IT-Security zu verankern und können sich im privaten sowie unternehmerischen Kontext stark unterscheiden.

- **Zurechenbarkeit** (engl. Accountability) oder auch **Anonymität** (engl. Anonymity)
  Eine Handlung in der IT-Umgebung kann einer Person eindeutig zugeordnet werden – oder eben nicht. Im unternehmerischen Kontext kann bei interner Sabotage beispielsweise die verantwortliche Person ausgeforscht werden. Im privaten will man übrigens eher das Gegenteil erreichen, nämlich dass die Person größtmögliche Anonymität im Zusammenhang mit ihren Daten genießt – beispielsweise, wenn im Internet zu gesundheitlichen Themen recherchiert wird.

- **Authentizität** (engl. Authenticity)
  Daten, Informationen und daraus resultierendes Wissen soll auf Echtheit überprüfbar sein, zum Beispiel ob übermittelte Forschungsergebnisse original oder von einer dritten Partei manipuliert worden sind.

- **Verbindlichkeit** (engl. Non Repudiation – übersetzt eigentlich „Nichtabstreitbarkeit“)
  Handlungen in einer IT-Umgebung sollen nicht einfach abgestritten werden können – das ist vor allem bei elektronisch abgewickelten Verträgen wichtig. Hier werden beispielsweise elektronische Unterschriften verwendet.

Wie sollen diese Ziele nun in der Praxis erreicht werden?

Alles dreht sich bei dieser Frage um **Schwachstellen.** Oder besser gesagt um das Herausfinden und Beseitigen von Schwachstellen. Wie Sie bereits gelernt haben, hat bspw. jede Software Schwächen. Diese sind nicht im Vorhinein als solche klar erkennbar. Oft liegt es an der mangelhaften Programmierung der genutzten Software oder Auslegung des IT-Systems. Das muss nicht unbedingt heißen, dass „falsch“ programmiert wurde, sondern dass ganz einfach nicht alle bekannten IT-Bedrohungen in der Programmierung bedacht wurden. Schwachstellen können aber auch der Mensch bzw. der falsche Umgang mit IT-Systemen sein.

Wichtig
Natürlich kann IT-Security **auch über die Hardware umgangen** werden, nicht nur über die Software. Das ist aber „unpraktischer“ – denn um über die Hardware Daten zu manipulieren oder zu stehlen,

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

muss man schon physisch präsent sein, beispielsweise mit dem USB-Stick in der Hand oder indem gleich der ganze Computer entwendet wird.

Da ist der Zugang über das Internet in die Software schon bequemer – und vor allem auch schwerer nachzuverfolgen, wenn man währenddessen doch erwischt wird.

Um die Schutzziele der IT-Security zu erreichen, ist es also von enormer Wichtigkeit, diese Schwachstellen und mögliche Bedrohungsszenarien zu identifizieren. Und hier wird es schwierig, denn eine 100-prozentige Darstellung aller Schwachstellen ist aufgrund der ständigen Weiterentwicklung der Systeme und der allgemeinen Unfähigkeit, in die Zukunft blicken zu können, gar nicht möglich – man kann sich nur so gut es geht annähern.

Merken

IT-Security hängt **stark von den aktuellen technologischen Entwicklungen ab** – neue Einsatzgebiete von Informationstechnik bergen auch neue Gefahren. Hier muss schnell reagiert werden, um entsprechende Gegenmaßnahmen bieten zu können.

Es gibt **drei Schutzziele**, die in allen Einsatzgebieten erfüllt sein sollen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Es gibt drei zusätzliche Schutzziele, die nach Einsatzgebiet variieren und entsprechend bedacht werden sollen:

- Zurechenbarkeit bzw. Anonymität
- Authentizität
- Verbindlichkeit

Um diese Schutzziele zu erreichen, ist es **die Kernaufgabe der IT-Security, Schwachstellen von Systemen zu identifizieren** und entsprechend zu eliminieren. Das kann auch Hardware, aktuell jedoch eher Software betreffen – hier sind vor allem Programmierfehler oder nicht bedachte Schwächen in der Programmierung gemeint.

Perfekte IT-Security kann nur angenähert, jedoch nicht zu 100 Prozent erfüllt werden. Deshalb muss IT-Security durchgehend behandelt werden.

5.4 Bedrohungen in der IT

Bedrohungen in der IT sind vielfältig und müssen nicht unbedingt vorsätzlicher bzw. krimineller Natur sein. Genauso kann die IT durch „höhere Gewalt“ und/oder technisches Versagen bedroht sein – das könnte beispielsweise ein durch ein Erdbeben ausgelöster Stromausfall sein, bei dem es zu einem Datenverlust kommt.

Aber natürlich sind auch menschliche Fehlhandlungen denkbar. Ein klassisches Beispiel dazu ist: Das Passwort für das Online Banking wurde vergessen – damit wäre dann die Information auch nicht mehr verfügbar.

Sie lernen nun die möglichen IT-Bedrohungen kennen - behalten Sie dabei immer die Schutzziele des vorherigen Kapitels im Hinterkopf.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

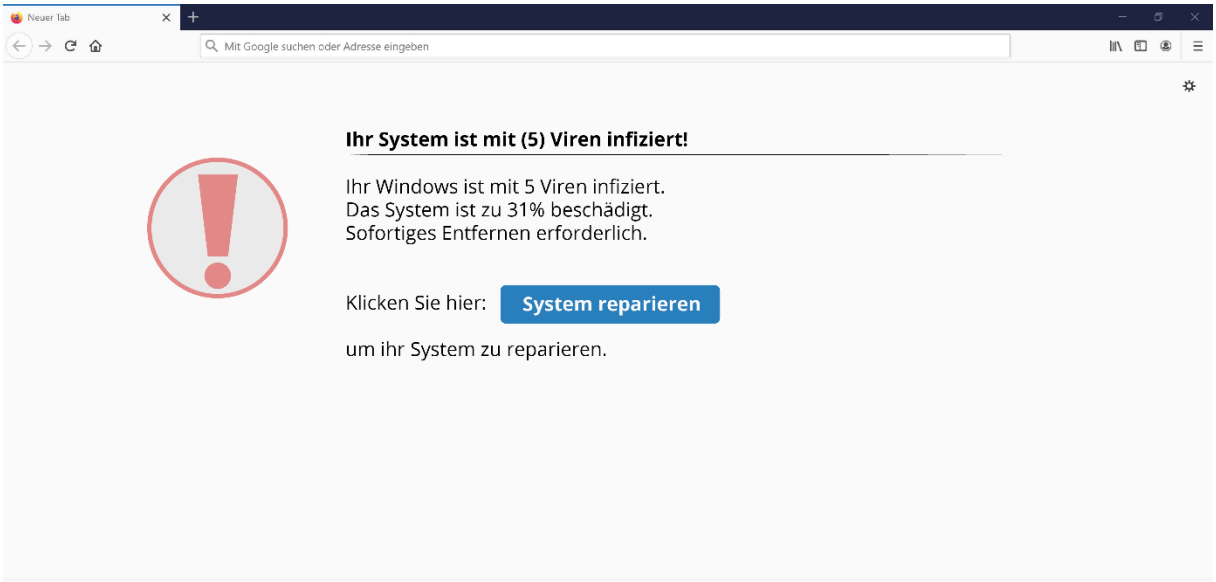
Wichtig
Eine potentielle Bedrohung oder Schwachstelle heißt übrigens nicht gleich automatisch, dass die IT gefährdet ist. Von einer tatsächlichen Gefährdung spricht man erst dann, wenn eine Schwachstelle (z. B. Programmierfehler oder auch leicht zugängliches WLAN) auch auf eine Bedrohung (z. B. Hacker-Angriff) trifft.

Gezielte Angriffe durch Menschen oder Organisationen

In erster Linie sind es natürlich bewusst durchgeführte Angriffe, die von der IT-Security abgewendet werden müssen. Meist als „Hacking“ bezeichnet, verschafft sich eine Einzelperson oder gleich eine ganze Organisation unbefugt Zugang zu fremden Daten und versucht dabei die Schutzziele zu umgehen. Das kann verschiedene Gründe haben: Diebstahl von Geldmittel, Sabotage von Konkurrenzunternehmen, politische Motivation, manchmal auch einfach nur „Spaß“ – immer geht es jedoch darum, sich über das Netzwerk, an dem die Zielgeräte angeschlossen sind, fremde Informationen zu beschaffen, manipulieren oder vernichten.

Die wichtigsten Werkzeuge solcher Hacking-Angriffe kennt man aus Hollywood-Filmen der Jahrtausendwende und haben meist lustige Namen – „Viren“, „Trojaner“, „Würmer“, „Spoofing“, „Phishing“ und weitere. Sehen wir uns einige dieser Beispiele etwas detaillierter an:

- **Virus**
  Computer-Viren sind ganz einfach Programme, die sich in den Zielsystemen automatisch ihrer programmierten Aufgabe widmen: zum Beispiel dem Aufspüren eines Passwortes. Viren brauchen einen sog. Wirten, der sie verbreitet. Das kann eine Massenemail sein oder auch ein sogenanntes „Pop-Up“ – also eine sich selbst öffnende Website, die beispielsweise auf ein angeblich notwendiges Update hinweist.



- **Würmer**
  Das sind Viren, die sich aktiv selbst verbreiten können – das bedeutet, dass sie aktiv Schwachstellen in Systemen und Netzwerken aufspüren und sich dementsprechend selbst weiterleiten, ganz ohne dass ein sogenannter „Wirt“ vorhanden ist.

- **Trojaner**
  Auch als „trojanische Pferde“ bezeichnet, handelt es sich hier um scheinbar nützliche Programme, die das Opfer selbst installiert – im Hintergrund öffnen Trojaner aber

Co-funded by the Erasmus+ Programme of the European Union

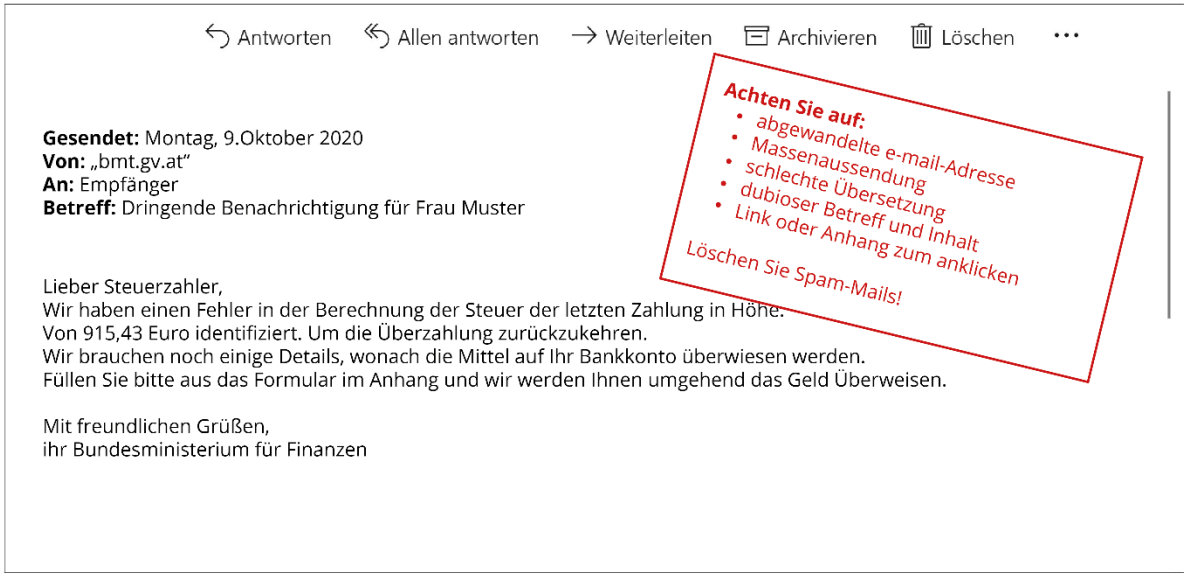
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

selbstständig Hintertüren im System, leiten Daten und Informationen weiter und können beispielsweise Passwörter, die eingegeben werden, aufzeichnen.

- **Denial-of-Service-Attacken**
  Hier will eher die Verfügbarkeit der Daten manipuliert werden – durch gezielte Überlastung des Systems von außen (das kann zum Beispiel durch automatisiert wiederholtes Aufrufen einer Website sein) wird dieses zum Erliegen gebracht. Manchmal passiert dies solange, bis die betroffene Organisation beispielsweise ein Lösegeld bezahlt. Software für erpresserische Methoden wird übrigens auch als „Ransomware“ gezeichnet.

- **Spoofing/Phishing**
  Hier geht es hauptsächlich um Identitätsdiebstahl. Durch gefälschte Websites im Internet und Emails, die auf diese verweisen, wird das Opfer dazu verleitet, aktiv Passwörter oder Kontodaten weiterzugeben. Die finden sich vor allem im privaten Bereich der IT-Security.

- **Spam**
  Der wohl bekannteste Begriff aus der IT-Security bezeichnet übrigens nichts weiter als unerwünscht zugesandte Emails – das können nervige Newsletter sein, aber natürlich auch Wirte von Viren oder Phishing-Versuche.



Oben beschriebene Schadsoftware kann natürlich auch ganz persönlich in das Computersystem „injiziert“ werden – durch einen physischen Einbruch in das Firmengebäude oder in die Wohnung können Informationen gestohlen oder manipuliert werden. Aufgrund der Vernetzung von Computersystemen ist das aber meist gar nicht mehr nötig.

Manchmal passiert eine solche physische Manipulation aber auch ganz einfach intern. Wenn beispielsweise das eigene Firmenpersonal Kundendaten oder Produktgeheimnisse unbefugt entwendet, um diese extern zu verkaufen.

Unbeabsichtigte Bedrohung durch menschliches Fehlverhalten

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bedrohungen der IT-Security müssen aber nicht immer gleich hochkriminell und in voller Absicht geschehen. Manchmal ist es auch einfach Unwissenheit im Umgang mit IT, die eine Gefährdung darstellt:

- **Passwörter**
  Ein gutes Passwort ist am besten schwer zu merken – das ist natürlich unpraktisch. Viele Menschen verwenden deshalb immer noch viel zu schwache Passwörter. *12345* ist beispielsweise ein schwaches Passwort. *UfNS3-?ßsDa-hUdk&* – da sieht es schon ganz anders aus – je mehr verschiedene Symbole, Sonderzeichen, Ziffern und Buchstaben, desto besser. Aber nicht, wenn das Passwort dann erst wieder auf einem Zettel direkt am Bildschirm notiert ist.

  Sie sehen also – das Finden eines geeigneten und sicheren Passwortes, das sich die betreffende Persona auch merken kann, ist gar nicht so einfach. Vor allem da viele Systeme regelmäßig zur Änderung der Passwörter auffordern und es nicht empfohlen ist, dasselbe Passwort mehrmals anzuwenden.

Exkurs
Es gibt sog. **Passwortmanager**, die sowohl privat als auch in Unternehmen genutzt werden können. Das sind Programme, die sichere Passwörter für Webseiten oder Programme generieren und speichern können. Das Programm selbst ist dabei mit einem sog. **Master-Key**, also EINEM Hauptpasswort gesichert. Die Vor- und Nachteile liegen auf der Hand: Man kann eine Vielzahl an verschiedenen, sicheren Passwörtern verwenden und muss sich diese nicht einzeln merken. Wird das Hauptpasswort aber geknackt, kann auch auf alle gespeicherten Passwörter zugegriffen werden. Ein Passwortmanager ist nur dann sicher, wenn das Hauptpasswort stark ist und am besten regelmäßig geändert wird.

  Allerdings ist auch die Weitergabe von Passwörtern ein Problem. Das muss nicht vorsätzlich fahrlässig geschehen. Man will einem Kollegen helfen und gibt ihm schnell den eigenen Zugang zum System. Oder die Systemadministratorin fordert das Passwort für eine Überprüfung an. Das kann zu kritischen Situationen führen – vor allem wenn Personen beteiligt sind, die so absichtlich Passwörter stehlen.

- **Eigene Geräte mitbringen**
  „Bring you own device“ – das bezeichnet keine wilde Weihnachtsfeier im Unternehmen, sondern das Mitnehmen eigener Geräte, beispielsweise externe Festplatten, USB-Sticks, Smartphones und ähnliches. Wenn auf diesen dann firmeninterne Informationen gespeichert oder bearbeitet werden, dann kann die organisationsinterne IT-Security nicht wirklich helfen. Das ist besonders dann kritisch, wenn sogenanntes „Home-Office“ die Praxis ist, also das Arbeiten für eine Organisation von zuhause aus.

  Manchmal werden übrigens Speichermedien von Dritten bewusst mit Schadsoftware „präpariert“ und dann bewusst an Personen, die beispielsweise bei bestimmten Unternehmen arbeiten, verteilt. Das passiert zum Beispiel auf beruflichen Messen, wo gerne USB-Sticks verschenkt werden.

- **Nichtautorisierte Anwendungen installieren**
  Der Firmenlaptop ist zu langsam, also „kümmert man sich selber darum“ indem man Antivirenprogramme und anderes installiert. Oder man zockt auch gern mal in einer freien

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Minute am Arbeitsplatz ein Spiel und lädt sich nebenbei munter, aber unbewusst Schadsoftware auf den Firmen-PC. Auch das kann durch fehlendes Bewusstsein zu Bedrohungen für die IT-Security führen.

Das sind im Wesentlichen die größten Gefahren für die IT-Security. Wie schon erläutert, können natürlich auch gänzlich unvorhersehbare Ereignisse die IT bedrohen – Naturkatastrophen wie Feuer, Blitzeinschläge oder Überschwemmungen können Computersysteme komplett lahmlegen oder zerstören.

Merken
Von einer tatsächlichen Gefährdung im Sinne der IT-Security spricht man, **wenn eine interne Schwachstelle auf eine Bedrohung von außen trifft.** So eine Bedrohung kann ein vorsätzlicher Angriff sein, unbeabsichtigt durch den Menschen oder auch durch „höhere Gewalt“ wie Naturkatastrophen. **Vorsätzliche Angriffe:** • Schadsoftware wie Viren, Würmer und Trojaner • Physischer Einbruch und das Stehlen oder Manipulieren von Informationen oder Computersystemen • Identitätsdiebstahl oder Erpressung durch Phishing, Ransomware und Denial-of-Action-Attacken **Unbeabsichtigte Gefährdung** • Schwache oder weitergegebene Passwörter • Das Verwenden privater Geräte in Firmenumgebungen • Nichtautorisierte Anwendungen installieren **Höhere Gewalt** • Naturkatastrophen • die in weiterer Folge zur Zerstörung oder Lahmlegung der Computersysteme führen.

5.5 Maßnahmen der IT-Security

IT-Security bietet verschiedene Maßnahmen, nicht nur auf technischer Seite. **Menschen im Unternehmen oder auch für ihr Privatleben auf Schadsoftware oder schädliches, unbewusstes Verhalten aufmerksam zu machen**, ist meist schon viel wert.

Dahingehend werden oft Schulungen und Workshops angeboten, die auch im Privatleben das eine oder andere IT-Leid ersparen können. Firmenintern werden manchmal ganze Strategien entworfen, um IT-Security ganzheitlich und möglichst umfassend in Prozesse einzubinden. Ohne eine vorherige Bewusstseinsbildung bei der Belegschaft kann das aber nicht funktionieren.

Trotzdem reichen Investitionen in Information und Bewusstseinsbildung aber natürlich nicht – was macht die IT-Security also noch?

Software
Das Offensichtliche zuerst: Es gibt sog. **Antivirensoftware**, die das eigene IT-System automatisch durchforstet und nach Schadsoftware kontrolliert. Das sollte in kurzen, regelmäßigen Abständen passieren und ist sowohl im privaten als auch unternehmerischen Umfeld von Nutzen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Sicherheitslücken und schädliche Programme, die aus dem Internet geladen werden wollen, können so erkannt und gebannt werden.

Sie wissen es schon, zu 100 Prozent kann man sich trotzdem nicht darauf verlassen. Manchmal wird Schadsoftware ganz einfach nicht als solche erkannt – oder es wird sichere Software als Schadsoftware identifiziert, automatisch entfernt und dann funktioniert der Computer erst recht nicht mehr. Blind einem Antivirenprogramm zu vertrauen ist deshalb nicht ratsam.

Sogenannte **Firewalls** sind ebenfalls beliebte Mittel im privaten wie unternehmerischen Kontext. Diese befassen sich mit den Netzwerkverbindungen der IT – also beispielsweise mit dem WLAN. Hier können unbefugte Zugriffe von außen über das Netzwerk erkannt und unterbunden werden. Meist sind solche Firewalls schon in Antivirensoftware-Produkten integriert.

Sandkästen sind etwas besonders Spannendes, nicht nur für Kinder. In der IT-Security steht ein Sandkasten für ein Programm, das Schadsoftware einsperrt. Dieses relativ neue Konzept ist vor allem bei speziellen Datentypen effektiv. Beispielsweise werden PDF-Dokumente in einem eigenen „Sandkasten", getrennt von anderen Programmen, geöffnet. Ist das PDF schadhaft, wird im schlimmsten Falle nur das Sandkastenprogramm angegriffen – der Rest des Systems bleibt verschont.

Verschiedene Software zu verwenden und auch mal kleineren Anbietern zu vertrauen, kann sich übrigens auszahlen – **je „diverser" die IT aufgestellt ist, desto schwieriger wird es, das System ganzheitlich zu knacken**. Manchmal sind gerade die bekanntesten Antivirensoftwarefirmen besonders von Hackerangriffen betroffen – ganz einfach, weil sie am verbreitetsten sind.

Zugangskontrolle
Zugangskontrolle meint nicht einfach nur ein überlanges Passwort. Unternehmen helfen sich hier mit unterschiedlichen Benutzerrechten. **Nur die wenigsten Personen im Unternehmen haben Zugriff auf alle Daten**, meistens sind diese, je nach Funktion im Unternehmen, beschränkt und aufgeteilt.

Auch kann ein **beschränkter Zugriff auf Internetseiten** oder die Verhinderung von externer Software am Firmencomputer umgesetzt werden. Das Firmen-WLAN kann ebenfalls so ausgelegt sein, dass nur eine sehr beschränkte Auswahl an Applikationen und Programmen heruntergeladen und verwendet werden kann.

Zusätzlich gibt es noch die Möglichkeit, „aktive Inhalte" zu unterbinden – sich selbst ausführende Software (oft sind das Hilfsprogramme) wird so abgestellt. Auch das kann gegen potentielle Schadsoftware wirksam sein. Die hier genannten Maßnahmen werden natürlich eher im unternehmerischen Kontext angewandt.

Unternehmerisch und privat kann man sich allerdings mit der **Kryptografie** behelfen. Das bedeutet nichts anderes als eine Verschlüsselung der Daten. Dabei wird nicht nur der Zugang zu den Daten mit einem Passwort gesichert, sondern die Daten selbst auch noch „verschlüsselt".

Exkurs
Kryptografie von Daten und Informationen – End-to-End End-to-End Verschlüsselung ist ein gängiger Standard in der Datenkryptografie. Hier besitzen Sender und Empfänger einen Übersetzercode. Nachrichten oder Bilder werden vom Sender verschickt. Der Übersetzercode verändert vorher allerdings noch automatisiert die Daten der Nachricht in unverständliche Zahlen- und Symbolfolgen. Der Empfänger erhält diese und kann aufgrund des

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Übersetzers wiederum die Nachricht oder das Bild in seiner Ursprungsform darstellen und verstehen.

Das dient ganz einfach dazu, **dass im Sendeprozess möglicherweise abgefangene Daten nicht in einen Kontext gesetzt werden können** und so als Information unverständlich bleiben.

Backups und Updates

Regelmäßige Updates der Software, um diese aktuell zu halten, hilft natürlich auch. Je älter eine Software ist, desto eher sind deren Fehler bekannt. Vor allem Betriebssysteme und Antivirenprogramme sollten zeitnah auf den neuesten Stand gebracht werden, da hier die größten Bedrohungen im externen Zugriff liegen.

Gegen Datenverlust (wenn z. B. der Computer kaputt oder gestohlen wird) hilft natürlich nur eines: ein regelmäßiges Backup, also das eigene Kopieren der Daten und Informationen – am besten vom IT-System getrennt aufbewahrt auf einer externen Festplatte oder auch in der sog. „Cloud“. Cloud-Systeme sind externe Server und Speicherplätze, die über das Internet verfügbar sind. Hier läuft ein Backup auch automatisierbar ab, allerdings hat man natürlich auch das Risiko, dass der Cloud-Anbieter selbst Opfer eines IT-Angriffes wird.

Merken

Menschen sowohl privat als auch im Unternehmen auf den richtigen Umgang mit IT-Security aufmerksam zu machen ist schon viel wert.

Zusätzlich gibt es eine Reihe an Maßnahmen der IT-Security:

Software

- Antivirenprogramme
- Firewalls
- Sandkästen
- Diverse Aufstellung des IT-Systems

Zugangskontrolle

- Unterschiedliche Benutzerrechte
- Beschränkter Zugang zu Websites und Programmen im Internet
- Kryptografie

Zusätzliche Maßnahmen

- Regelmäßige Backups
- Aktuelle Updates

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.6 Zusammenfassung

IT-Security ist ein Teilgebiet der Informationssicherheit und meint alle Schutzmaßnahmen in der Verarbeitung und Speicherung von Daten in einem IT-System – sowohl im privaten als auch unternehmerischen Bereich. Dabei geht es um **Computersicherheit, Datenschutz, Datensicherung** und **Datensicherheit.**

IT-Security hängt **stark von den aktuellen technologischen Entwicklungen ab**. Es muss vor allem schnell reagiert werden, um entsprechende Gegenmaßnahmen bieten zu können. Dabei gibt es **drei Kernschutzziele**, die in allen Einsatzgebieten erfüllt sein sollen:

Vertraulichkeit - Integrität - Verfügbarkeit

Um diese Schutzziele zu erreichen, ist es **die Kernaufgabe der IT-Security, Schwachstellen von Systemen zu identifizieren** und entsprechend zu eliminieren. Von einer tatsächlichen Gefährdung im Sinne der IT-Security spricht man, wenn eine interne Schwachstelle auf eine Bedrohung von außen trifft.

So eine Bedrohung kann ein **vorsätzlicher Angriff sein**, um Daten zu stehlen oder zu manipulieren (z. B. mit Schadsoftware über das Internet oder durch einen physischen Einbruch in die IT-Abteilung eines Unternehmens).

Aber auch unbeabsichtigt kann ein IT-System bedroht sein (beispielsweise durch ein schwaches Passwort) oder durch Naturkatastrophen, bei denen Computersysteme beschädigt werden.

Menschen sowohl privat als auch im Unternehmen auf den richtigen Umgang mit IT-Security aufmerksam zu machen, kann bereits helfen. Zusätzlich gibt es **Schutzsoftware**, beschränkende **Zugangskontrollen** und weitere Maßnahmen der IT-Security, um potentielle Gefährdungen zu minimieren.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.7 ÜBUNGEN

1. **Wenn Sie sich diese drei Schutzziele bewusst zu Herzen nehmen, haben Sie bereits die Hälfte der IT-Sicherheit umgesetzt! So sehen sie im Einzelnen aus:**

1. Vertraulichkeit	a) Daten, Informationen und daraus resultierendes Wissen sollten vor unbefugten Änderungen und Manipulationen geschützt werden.
2. Integrität	b) Daten, Informationen und daraus resultierendes Wissen sollten, falls erforderlich, denjenigen zugänglich sein, die erlaubten Zugang haben.
3. Verfügbarkeit	c) Daten, Informationen und daraus resultierendes Wissen sollten vor Personen verborgen werden, die kein Recht haben, sie einzusehen.

2. **Es gibt drei zusätzliche Schutzziele, die je nach Anwendungsgebiet unterschiedlich sind und entsprechend berücksichtigt werden sollten:**
   a. Zurechenbarkeit oder Anonymität
   b. Authentizität
   c. Verbindlichkeit
   d. Verantwortlichkeit oder Anonymität
   e. Nachweisbarkeit

3. **Vervollständigen Sie folgende Texte:**

a.

Um diese _____ zu erreichen, ist es die _____ von IT-Security, _____ von Systemen zu erkennen und diese entsprechend zu beseitigen. Dies kann auch die _____ betreffen, derzeit jedoch eher die _____ - es handelt sich dabei vor allem um _____ oder nicht berücksichtigte Schwächen in der Programmierung.

b.

Im Übrigen bedeutet eine potenzielle _____ oder _____ nicht automatisch, dass die IT _____ ist. Eine tatsächliche Bedrohung wird nur dann als Bedrohung angesehen, wenn eine Sicherheitslücke (z.B. Programmierfehler oder leicht _____ WLAN) auch auf eine Bedrohung (z.B. Hackerangriff) trifft.

Man spricht von einer tatsächlichen Bedrohung im Sinne der IT-Sicherheit, wenn eine interne Schwachstelle auf eine externe Bedrohung trifft. Eine solche Bedrohung kann ein absichtlicher Angriff sein oder unbeabsichtigt durch den Menschen oder auch durch „höhere Gewalt“ wie Naturkatastrophen.

4. **Vorsätzliche Angriffe:**
   a. Physisches Eindringen und Diebstahl oder Manipulation von Informationen oder Computersystemen
   b. Identitätsdiebstahl oder Erpressung durch Phishing-, Lösegeld- und Denial-of-Action-Angriffe
   c. Schwache oder weitergegebene Passwörter

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

d. Verwendung privater Geräte in Unternehmensumgebungen
e. Installieren nicht autorisierter Anwendungen
f. Malware wie Viren, Würmer und Trojaner

5. Unbeabsichtigte Gefährdung
a. Schwache oder weitergegebene Passwörter
b. Naturkatastrophen, die in der Folge zur Zerstörung oder zum Stillstand der Computersysteme führen.
c. Verwendung privater Geräte in Unternehmensumgebungen
d. Installieren nicht autorisierter Anwendungen

6. Höhere Gewalt
a. Malware wie Viren, Würmer und Trojaner
b. Physisches Eindringen und Diebstahl oder Manipulation von Informationen oder Computersystemen
c. Naturkatastrophen, die in der Folge zur Zerstörung oder Stilllegung der Computersysteme führen.
d. Identitätsdiebstahl oder Erpressung durch Phishing-, Lösegeld- und Denial-of-Action-Angriffe

7. Vervollständigen sie folgenden Text:

End-to-End _____ ist ein gängiger Standard in der _____. Hier besitzen Sender und Empfänger einen _____. Nachrichten oder Bilder werden vom Sender verschickt. Der Übersetzercode verändert vorher allerdings noch automatisiert die _____ in unverständliche _____ und _____. Der Empfänger erhält diese und kann aufgrund des Übersetzers wiederum die Nachricht oder das Bild in seiner Ursprungsform darstellen und verstehen.

Die Sensibilisierung der Menschen für den richtigen Umgang mit IT-Sicherheit, sowohl privat als auch in Unternehmen, ist bereits sehr wertvoll. Es gibt auch eine Reihe von IT-Sicherheitsmaßnahmen:

8. Software
a. Antiviren-Programme
b. Firewalls
c. Unterschiedliche Benutzerrechte
d. Beschränkter Zugang zu Websites und Programmen im Internet
e. Kryptographie
f. Sandkästen
g. Vielfältiger Einsatz des IT-Systems

9. Zugriffskontrolle
a. Kryptographie
b. Regelmäßige Sicherungen
c. Beschränkter Zugang zu Websites und Programmen im Internet
d. Unterschiedliche Benutzerrechte
e. Regelmäßige Updates

10. Zusätzliche Maßnahmen
a. Antiviren-Programme
b. Regelmäßige Sicherungen
c. Firewalls

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

d. Sandkästen
e. Regelmäßige Updates
f. Vielfältiger Einsatz des IT-Systems

11. IT-Sicherheit ist ein Teilbereich der Informationssicherheit und bezeichnet alle Schutzmaßnahmen bei der Verarbeitung und Speicherung von Daten in einem IT-System - sowohl im privaten als auch im geschäftlichen Bereich. Dazu gehören:

a. Hardware
b. Computersicherheit
c. Software
d. Verschlüsselung
e. Datenschutz
f. Datensicherung
g. Daten-Kryptographie
h. Datensicherheit

12. Die IT-Sicherheit hängt stark von den aktuellen technologischen Entwicklungen ab. Vor allem ist es notwendig, schnell zu reagieren, um geeignete Gegenmaßnahmen ergreifen zu können. Es gibt drei Kernschutzziele:

a. Unterschiedliche Benutzerrechte
b. erwendung privater Geräte in Unternehmensumgebungen
c. Physisches Eindringen und Diebstahl oder Manipulation von Informationen oder Computersystemen
d. Vertraulichkeit
e. Integrität
f. Verfügbarkeit

13. Vervollständigen Sie folgende Texte:

a.

Um diese Schutzziele zu erreichen, ist es die _____ der IT-Security, Schwachstellen_____ von Systemen zu identifizieren und entsprechend zu eliminieren. Von einer tatsächlichen Gefährdung im Sinne der IT-Security spricht man, wenn eine _____ Schwachstelle auf eine _____ Bedrohung trifft.

b.

Aber ein IT-System kann auch _____ bedroht sein, zum Beispiel durch ein schwaches _____ oder durch _____, bei denen Computersysteme beschädigt werden.

Unbeabsichtigt, Passwort, Naturkatastrophen

c.

_____ sowohl privat als auch im Unternehmen auf den richtigen Umgang mit IT-Security aufmerksam zu machen, kann bereits helfen. Zusätzlich gibt es _____, beschränkende Zugangskontrollen und weitere Maßnahmen der IT-Security, um potentielle _____ zu minimieren.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. CYBER PHYSICAL SYSTEMS

Co-funded by the Erasmus+ Programme of the European Union

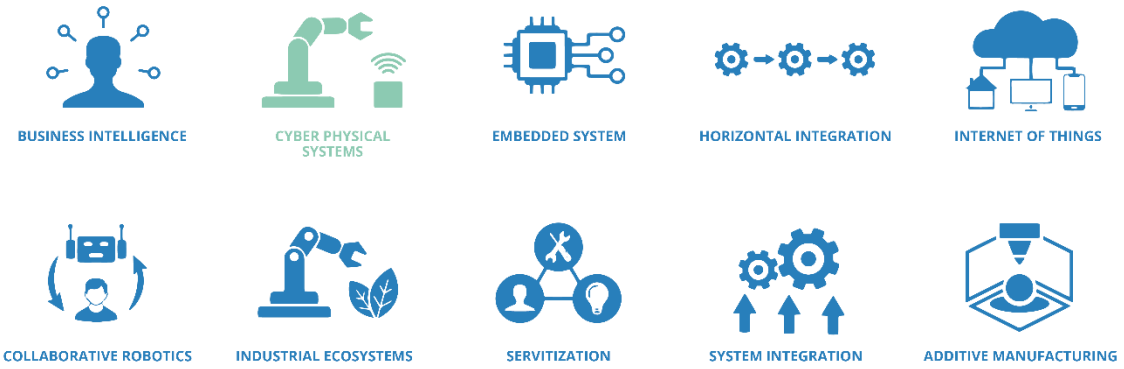
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.1 Das Thema

Die erste Einführung

Big Data ist das Öl der Zukunft – Daten sind gleichzeitig die wichtigste Ressource und das Schmiermittel in der digitalisierten Industrie 4.0, in der die physische Welt mit der digitalen verbunden werden soll. Das klingt ein bisschen wie Science-Fiction – ist aber schon Gegenwart!

Denn der wichtigste Baustein der Industrie 4.0 ist bereits im Einsatz: Cyber Physical Systems sind genau die technischen Wunderwerke, die die Welt, die Sie sehen können, mit der virtuellen Welt der Daten und Informationen verbinden können.



Cyber Physical Systems sind im Wesentlichen die Sinnesorgane der Informationstechnologie, angebracht an zukunftssicheren Maschinen und Produkten. Sie sammeln Eindrücke und Vorgänge ihrer Umgebung und stellen in weiterer Folge genau die Daten zur Verfügung, die den Produktionsprozess immer effizienter und immer besser werden lassen.

Wenn Industrie 4.0 die Zukunft der Fertigungsindustrie ist, dann sind Cyber Physical Systems der Grundbaustein. Genau diesen Grundbaustein lernen Sie in diesem Kapitel kennen.

Der Praxisbezug - Dafür werden Sie das Wissen und die Kompetenzen brauchen

Cyber Physical Systems ist einer der wichtigsten Funktionsträger der Industrie 4.0, mit einem enormen Einsatzgebiet. Das hier erlernte Wissen kann Ihnen in der Industrieproduktion und in der Logistik, aber auch in der Medizin-, Verkehrs-, Verteidigungs-, Umwelttechnik und vielen weiteren weiterhelfen – im Prinzip überall dort, wo Industrie 4.0 anwendbar ist.

Lernziele und Kompetenzen im Überblick

In diesem Kapitel lernen Sie Cyber Physical Systems zu verstehen und in der Industrie 4.0 einzuordnen. Dazu werden Ihnen zuerst die Begriffe und generellen Funktionen nähergebracht. Weiters werden die technologischen Grundlagen erörtert sowie die Anwendungsgebiete und einige konkrete Beispiele in der industriellen Nutzung vorgestellt. Ein Bezug zu aktuellen Problemfeldern runden Ihr Basiswissen zum Thema ab.

Lernziele
Cyber Physical Systems (CPS) als Teil der Industrie 4.0 wahrnehmen und verstehen können.
Die technologischen Voraussetzungen und Komponenten von CPS kennen und miteinander verknüpfen können.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Die Anwendungsgebiete von CPS in der Industrie, der Gesellschaft und individuellen Nutzung kennenlernen.
Die Chancen und Gefahren von CPS kennen und abwägen können.

6.2 Cyber Physical Systems in der Industrie 4.0

In der modernen Welt will alles vernetzt sein. Das Smartphone mit dem Auto, die Kaffeemaschine mit dem Wecker, die Jalousien mit dem Sonnenaufgang, die Smartwatch mit der Gesundheits-App und am besten der Kühlschrank mit der digitalen Einkaufsliste. Warum eigentlich? Damit das Leben komfortabler, besser und ein Stück weit effizienter wird.

Alltagsgeräte tauschen sich untereinander aus, senden Daten und Informationen hin und her und steuern sich so in Echtzeit gegenseitig – eine Art „Automatisierung" des Alltags soll so erreicht werden, der sich automatisch den äußeren Bedürfnissen anpasst.

Diese Vorgänge werden im Wesentlichen „Internet of Things" (IoT), also das „Internet der Dinge" genannt. Geräte sind miteinander verknüpft, tauschen sich aus und steuern sich gegenseitig.

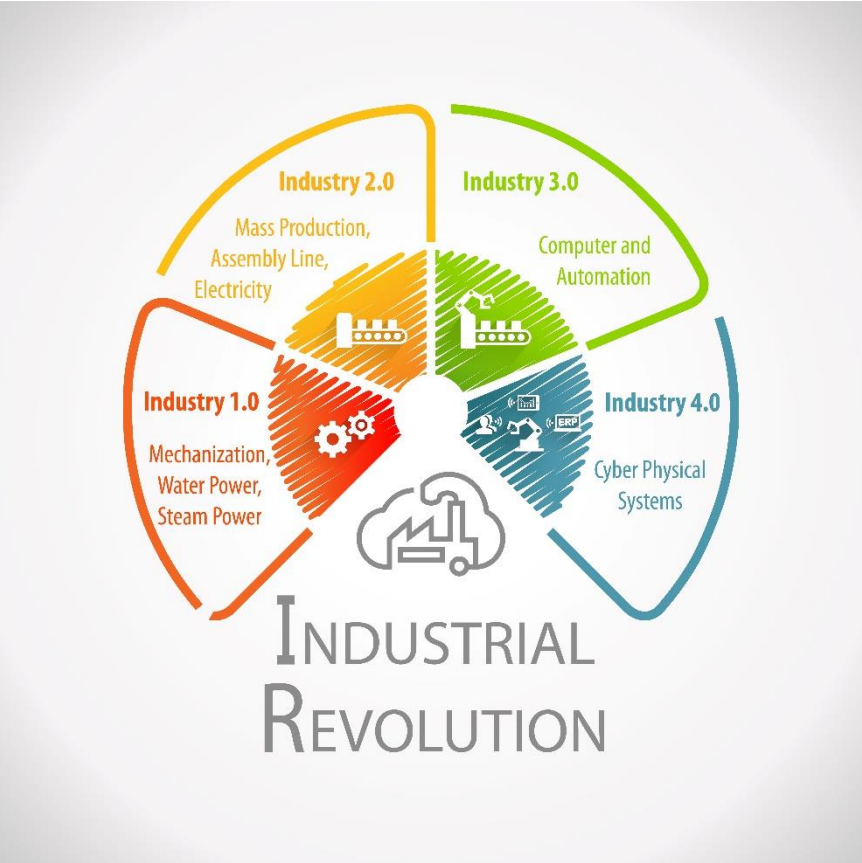
Definition
Internet of Things … die REFA (der deutsche Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung) definiert den Begriff Internet of Things als *„die zunehmende Vernetzung von Geräten, Sensoren und anderen Anlagen mit Hilfe eines IP-Netzes. Dabei wird das Ziel verfolgt, dass physische Dinge, die eigene Zustandsinformationen besitzen, ihre Daten zur Weiterverarbeitung im Netzwerk bereitstellen*."

Genau das will auch die Industrie 4.0 erreichen – vor allem in der Fertigungs- und Logistikindustrie können mit einem richtig umgesetzten Internet of Things wahre Wunder der Effizienz und Kosteneinsparung erreicht werden.

Denn Industrie 4.0 bedeutet simpel gesagt: Alle beteiligten Einheiten einer Produktionsumgebung sind in einem ständigen Austausch über ein Netzwerk in Echtzeit verbunden. Eingeschlossen sind hierbei Fertigungsanlagen und Logistiksysteme aber auch die herzustellenden Produkte (oder dessen Bauteile) sowie der Mensch.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Für diesen Austausch braucht es in erster Linie drei Dinge: Daten, Daten und nochmals Daten. Und damit sind Sie auch wieder bei dem Hauptthema dieses Kapitels angelangt: Cyber Physical Systems (Abkürzung: CPS) –sind nichts weniger als die Grundlage der Industrie 4.0. Denn CPS liefern, Sie haben es erraten: Daten.

Exkurs

Daten, Information und Wissen – die Welt von CPS

Daten sind schön und gut, aber eigentlich nutzlos – wenn diese nicht sinnvoll weiterverarbeitet werden. Denn in einer vernetzten (Industrie-)Welt sind zwar Daten der Rohstoff, die eigentliche nutzbare Ressource ist aber eigentlich erst das aus den Daten erhobene Wissen. Da es bei CPS viel um Daten geht, ist es wichtig, dass Sie hier die Unterschiede verstehen.

Daten sind **einfache Zeichen**, Symbole und Zahlen, die ein System, zum Beispiel eine Maschine, generiert: „1992“ – damit lässt sich noch recht wenig anfangen.

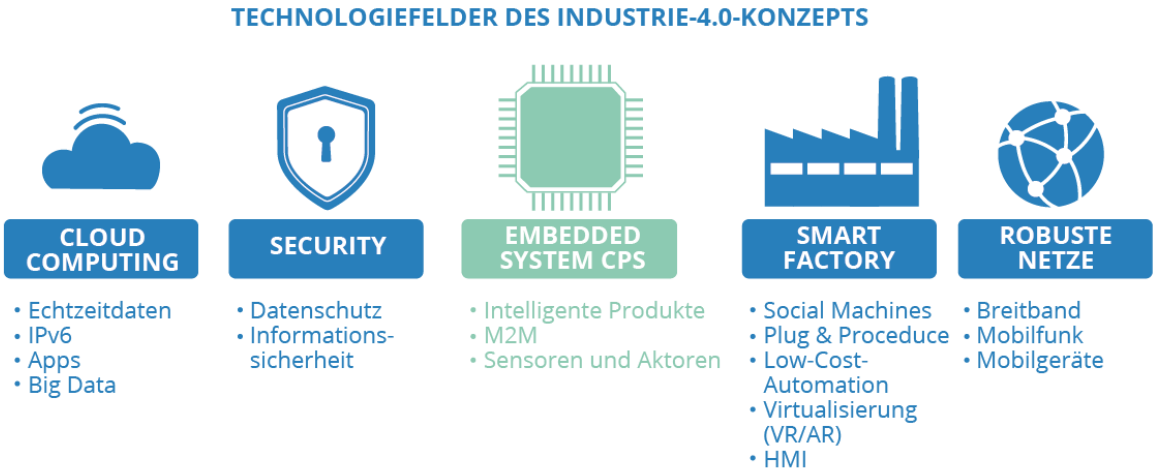
Informationen entstehen, wenn diese **Daten einem Kontext zugeordnet** werden. Dabei entstehen Kenntnisse über einen möglichen Sachverhalt. Eine industrielle Waage gibt beispielsweise eine Einheit aus: „1,992 Gramm“ – somit können Sie schon viel mehr mit dem Wert anfangen. Allerdings hat die Information noch immer recht wenig Wert, denn Sie wissen nicht wohin damit.

Jetzt brauchen Sie noch den **Sachverhalt oder das Produkt**, zu dem Sie die Information zuordnen können: „1,992 Gramm Klebstoff werden für die Verbindung zweier elektronischer Bauteile benötigt.“ Damit wissen Sie erst, was wofür gebraucht wird und können eine fundierte Entscheidung treffen oder ein Problem lösen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Damit Industrie 4.0 funktionieren kann, muss die physische Welt (also die Produktionsumgebung mit allen Maschinen und Produkten) mit der digitalen (Netzwerk und Software) verbunden werden. Genau das ist die Aufgabe von CPS.



Dies geschieht, **indem mechanische und elektronische Komponenten mit informations- bzw. softwaretechnischen Komponenten verbunden werden**. Diese kommunizieren dann über eine Dateninfrastruktur (z. B. Internet). Dabei werden vor allem zwei Grundaufgaben bearbeitet:

- Generierung und Austausch von Daten
- Kontrolle und Steuerung von Infrastruktur

Wichtig

"Embedded Systems" und CPS

Die aufmerksamen Leserinnen und Leser werden es in der Grafik oben erkannt haben. Embedded Systems (zu Deutsch: eingebettete Systeme) sind im selben Atemzug genannt wie CPS. Was ist denn da los?

Embedded Systems sind der technologische Vorgänger von CPS und umfassen klassische Mess-, Steuerungs- und Regelungstechniken. Auch hier wird die digitale („cyber") mit der mechanischen („physical") Welt verbunden – allerdings bliebt jede Einheit für sich. CPS sind nun ein ganzer Verband solcher Gerätschaften, angeschlossen an ein Netzwerk und in ständigem Austausch („Systems" – daher der Name Cyber Physical Systems).

Das Wesentliche von CPS ist allerdings nicht, DASS es diese Aufgaben übernimmt, sondern WIE SCHNELL. Denn in einer nach Industrie 4.0 funktionierenden Produktionsumgebung (auch „Smart Factory" genannt) gibt es nur ein Credo und das heißt: Vollgas voraus. Denn damit eine komplett vernetzte Produktionsumgebung von diesem Netzwerk profitiert, müssen die Daten in Echtzeit ausgelesen, zu Information und Wissen weiterverarbeitet werden und dann der Fertigungsprozess entsprechend angepasst werden.

So werden dann statische und mobile Geräte, Einrichtungen und Maschinen (beispielsweise Förderbänder oder Roboter) und damit vernetzte Gegenstände in Echtzeit angesteuert. Das kann eine

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

immense Steigerung der Produktionseffizienz bewirken, die Kosten senken und komplexe Vorgänge und Prozesse in ihrer Bearbeitungszeit optimieren.

Merken
Cyber Physical Systems (CPS) sind die technologische Grundlage der Industrie 4.0 bzw. des Internet of Things. Dabei geht es um: • die Generierung und Auswertung von Daten im Produktions- und Weiterverarbeitungsprozess, • sowie die Steuerung und Kontrolle der Infrastruktur in einer Produktionsumgebung • in Echtzeit. Dafür wird die physische Welt (Fertigungsanlagen, Logistiksysteme, Maschinen etc.) mit der digitalen (Software) über ein Datennetzwerk (Internet) vereint. Dies geschieht über eine Verbindung von mechanischen bzw. elektronischen Komponenten mit software- bzw. informationstechnischen Komponenten. Diese Verbindungen sind CPS.

6.3 Die Technologien hinter CPS

CPS sind ein Netzwerk vieler verschiedener Technologien, die dazu dienen, die reale mit der virtuellen Welt zu verbinden. Technisch professioneller ausgedrückt ist damit ein Verbund von mechanischen Systemen gemeint, die von einem computerbasierten Ablauf gesteuert und kontrolliert werden.

Die verschiedenen Technologien dienen dazu, **kontextabhängige Prozesse wahrzunehmen**, zu **messen** und zu **benennen** – und daraus die **passende Vorgangsweise abzuleiten und umzusetzen**. Das geschieht maschinenübergreifend über ein Netzwerk.

Da muss natürlich die passende Technologie her – das Schöne ist, diese ist bereits erfunden und im Einsatz! CPS sind insbesondere deshalb das Rückgrat der Industrie 4.0, weil aufgrund ihrer Entwicklungen überhaupt erst eine vernetzte Produktionsumgebung theoretisch denkbar wurde.

Jetzt wird es etwas kompliziert: Die im Einsatz befindlichen Technologien bilden eigentlich selbst schon Systeme. Die oben besprochenen „Embedded Systems“ als Teil von CPS beispielsweise heißen nicht umsonst so – CPS kann man sich also eher als eine Art „Übersystem“ von kleineren Subsystemen vorstellen.

Das folgende Beispiel soll das besser erklären:

Beispiel
Ein System der Systeme Ein Bürogebäude hat in jedem seiner Räume ein eigenes System für den Brandfall installiert. Jedes dieser Systeme besteht aus einem Sensor, der einen Feuerausbruch erkennt, einem Alarm, der im Falle eines Brandes läutet und einem Feuerlöschsystem an der Decke. Angenommen in Raum A beginnt der Mistkübel zu brennen – der Sensor erkennt dies, der Alarm läutet und das Feuerlöschsystem fängt an, Wasser zu versprühen. Raum B im nächsten Stock bekommt davon allerdings noch nichts mit. Sind nun aber die Systeme in Raum A und Raum B miteinander verbunden, kann Sensor A dem Sensor B melden: „Bei uns brennt es!“ Sensor B kann nun zeitnah entscheiden, den Alarm

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

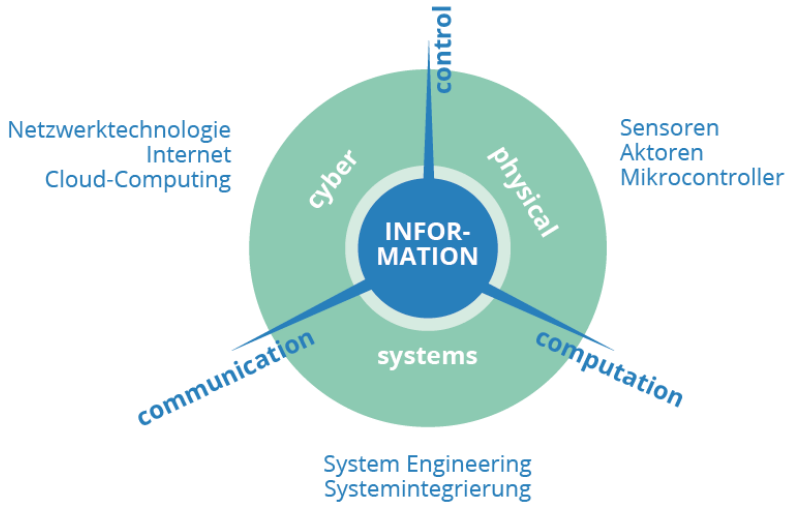
auszulösen, damit auch dieser Raum evakuiert wird, allerdings das Feuerlöschsystem nicht zu aktivieren – denn in Raum B brennt es ja (noch) nicht.

So wurde systemübergreifend eine kontextabhängige Entscheidung automatisiert und in Echtzeit durchgeführt.

Die erforderlichen Technologien lassen sich in drei Kerntechnologien einteilen:

- Kontrolle (Control)
- Kommunikation (Communication)
- Verarbeitung (Computation).

Folgende Grafik zeigt, wie diese zusammenhängen:



Ein solches Modell bringt natürlich herzlich wenig, wenn man nicht auch die einzelnen Bestandteile versteht:

Physische Elemente – zwischen Kontrolle und Verarbeitung

Hier handelt es sich im Wesentlichen um die erwähnten Embedded Systems, also Subsysteme. Diese bestehen aus:

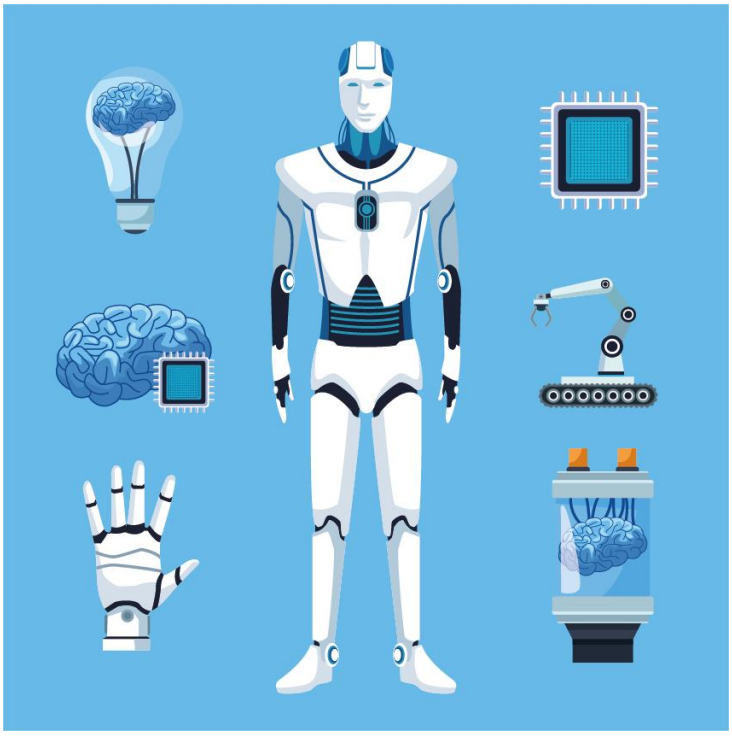
- **Aktoren:** Das sind zumeist Bauteile der Antriebstechnik – damit ist nicht unbedingt gemeint, dass etwas fährt, sondern dass zumindest etwas bewegt wird. Ein Roboterarm, der ein Bauteil umdreht, braucht beispielsweise einen Motor, mit dem er bewegt wird. Wesentlich ist, dass so ein Aktor von einem elektrischen Signal angesteuert werden kann.

- **Sensoren:** Diese sind das Gegenstück zu den Aktoren – sie „erfühlen“ ihre Umgebung nach physikalischen oder chemischen Eigenschaften (z. B. Druck, Wärme, Helligkeit etc.) und stellen diese anhand einer Messgröße dar (Bsp.: Temperatur des Werkstücks = 10 Grad Celsius). Diese Messgröße kann als elektrisches Signal weiterverarbeitet werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Mikrocontroller:** Das Gehirn eines Embedded Systems – auch „Chip“ genannt, übernimmt der Mikrocontroller Rechenaufgaben wie ein Computer. Er überwacht, steuert und transferiert Prozesse automatisch, je nach seiner Programmierung.



Siehe da: eigentlich ist die Kombination der physischen Elemente nichts weiter als ein Roboter! Er erfühlt seine Umgebung mit seinen Sensoren, bewegt und handelt entsprechend mit seinen Aktoren und das genauso, wie es sein Mikrocontroller vorschreibt. Wichtig ist, dass dynamisch auf die Umwelt reagiert werden kann und Aktionen und Messungen parallel ausgeführt werden können.

Cyber Elemente – zwischen Kontrolle und Kommunikation

Die Cyberelemente dienen der virtuellen Welt von Datentransfer und Datenverarbeitung. Hier entsteht aus Daten Information und aus Information Wissen. Dafür wird vor allem eines benötigt – eine ordentliche Netzwerktechnik!

- **Internet:** Bei solchen Datenmengen in Echtzeit muss ein superschnelles Breitband-Internet vorhanden sein. Aber auch neue Mobilfunkstandards wie z. B. 5G können beim Datentransfer helfen.

- **Adressraum:** Jedes Element braucht auch eine eigene Internetadresse. Neue, umfangreichere Internetprotokolle wie IPv6, die viel mehr verschiedene Internetadressen ermöglichen, können dafür sorgen, dass jedes Element seine eigene, unmissverständliche Adresse hat.

- **Cloud-Computing:** Um die Datenmengen schnell weiterzuverarbeiten, braucht man eine große Computerleistung – dabei kann man auf externe Server zugreifen, welche Rechenleistung übernehmen und zusätzlich Speicherplatz für Datenbanken zur Verfügung stellen.

Daten müssen in Echtzeit ankommen, berechnet und in einen Kontext gesetzt werden. Aufgrund dieses Wissens muss nun eine Entscheidung über die weitere Vorgehensweise der Produktionsumgebung

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

getroffen werden (Erinnern Sie sich an das Brandmelder-Beispiel) und diese an die entsprechenden Subsysteme weitergeleitet werden. Diese setzen dann um – und dann geht alles wieder von vorne los.

Systemische Elemente – zwischen Kommunikation und Verarbeitung

Hier geht es schließlich um die Verbindung und Anwendung eines großen Systems – das ist eher theoretischer Natur. Dabei hilft die Disziplin des sog. „Systems Engineering“. Hier werden die Ansprüche an das CPS definiert und dementsprechende Maßnahmen gesetzt:

- **Anforderung:** Was soll überhaupt gemacht werden? Welche Maschinen müssen wie zueinander aufgestellt werden, damit sie miteinander arbeiten können (z. B. in einer Fertigungsstraße)?

- **Systemintegration:** Welche Schnittstellen brauchen die einzelnen Systeme, um in das größere integriert zu werden? Welche Software wird verwendet?

- **Qualitätssicherung:** Wie werden Fehler analysiert? Wie werden diese ausgebessert? Welche Fehlertoleranz hat ein einzelnes Subsystem im Vergleich zum gesamten System?

Merken
CPS generieren Daten, Information und Wissen aus physikalischen Vorgängen. Diese werden in Echtzeit verarbeitet, steuern dynamisch Prozesse und sind über ein Netzwerk miteinander verbunden. Dazu braucht es drei Kerntechnologien: Control, Computation und Communication. Diese werden über folgende technologische Bausteine und Konzepte erfüllt: • Physische Elemente: Aktoren, Sensoren und Mikrocontroller • Cyber Elemente: Netzwerk-Technologien wie das Internet • Systemische Elemente: Eine den Anforderungen entsprechende Konzeptualisierung des Gesamtsystems mit „Systems Engineering“ CPS sind nichts anderes als Übersysteme von verschiedenen Subsystemen mit diesen technologischen Bausteinen.

6.4 Anwendungsbereiche von CPS

Die Anwendungsgebiete von CPS sind eigentlich grenzenlos – neben rein industriellen (aber eher noch in der Zukunft liegenden) Einsatzfeldern wie intelligenter Fertigungs- und Produktionsumgebungen in verschiedenen Branchen („Smart Factories“), werden CPS auch in anderen Feldern bereits jetzt eingesetzt. Dazu gehören intelligente Stromnetze („Smart Grids“), Electronic-Health, altersgerechte Assistenzsysteme aber auch intelligente Verkehrsüberwachungssysteme oder auch automatische Frühwarnsysteme im Katastrophenschutz.

Einige Beispiele sollen Ihnen die bereits stattfindende Integration von CPS in der Welt bewusst machen:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Industrie 4.0 – Smart Factory

Stellen Sie sich vor, es gibt eine Produktionsumgebung, die sich autonom steuert, je nach Produkt und Bauteil selber weiß, was zu tun ist und dabei auch noch selbstständig ihre Prozesse effizienter gestaltet. Das wäre doch was! Dies würde man gleichzeitig sozusagen als das „finale Level der Industrie 4.0“ bezeichnen.

Tatsächlich sind einige Unternehmen bereits fleißig dabei, CPS in ihrer industriellen Herstellung integrieren zu wollen. Vor allem die Autoindustrie verwendet vereinzelt schon CPS, um Arbeitsschritte automatisiert ablaufen zu lassen – von einer kompletten Vernetzung ist die Industrie allerdings noch ein Stück weit entfernt, da einfach noch nicht alle erforderlichen Technologien dafür ausreichend erforscht wurden.

In der Autoindustrie ist Smart Factory bereits ein großes Thema wie Sie an obiger Grafik sehen können. Wer sich in der Autoindustrie also einen Namen machen möchte, weiß, womit er oder sie sich beschäftigen muss!

Beispiel

Wartung von Maschinen

Eine der größten Kostenpunkte in Industriebetrieben ist die Wartung der Maschinen. CPS helfen Industriebetrieben bereits jetzt, hier Kosten zu sparen. Schauen Sie sich dazu folgenden Vergleich an:

Wartung ohne CPS

Hier wird entweder reaktiv oder präventiv gewartet.

Reaktive Wartung: Es wird einfach solange produziert, bis die Maschine nicht mehr funktioniert – das hat zwar äußerst geringe Wartungskosten zu Beginn, man riskiert jedoch lange Ausfallszeiten und hohe Austauschkosten.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

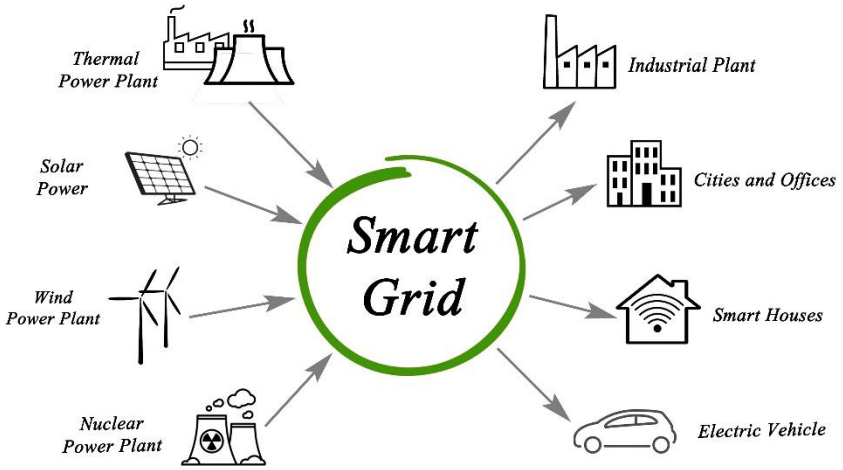
Präventive Wartung: Ungeachtet der tatsächlichen Ausfälle, wird in regelmäßigen Abständen gewartet, also Teile oder ganze Maschinen ausgetauscht – das ist zwar recht sicher, aber auf Dauer teuer.

Wartung mit CPS
Die Maschinen können über ihre Sensoren selbst feststellen, wann eine Wartung fällig werden würde. Verschleiß kann so sehr zeitnah festgestellt und die Wartung viel effizienter durchgeführt werden.

Außerdem können so eventuelle Ausfälle „vorhergesagt“ und entsprechend reagiert bzw. vorgebeugt werden.

Smart Grid – das Internet der Energie

Auch ein Stromnetz kann mit CPS „intelligent“ werden. Warum ist das überhaupt notwendig? Strom wird heutzutage immer dezentraler erzeugt. Das heißt, dass es meist (vor allem in ländlichen Gebieten) keine einzelne, zentrale Quelle mehr gibt, wo der Strom herkommt, sondern viele kleinere Quellen wie z. B. Windkraftanlagen, Photovoltaikanlagen, Biogasanlagen etc.



Das ist komplex und braucht System – vor allem im Bereich der Lastregelung (d. h. welches Gerät gerade wieviel Strom braucht). Gut, dass es CPS gibt. So können sich sämtliche Akteure im Stromnetz (Erzeugung, Speicherung, Lieferung und Verbrauch) untereinander vollautomatisch und in Echtzeit austauschen.

Geräte kommunizieren in Folge dem Stromnetz, wieviel Strom erzeugt und zur Verfügung gestellt werden muss. Diese reagieren, können die Quelle entsprechend auswählen und bei Überlastung auch mal den Strom abriegeln.

Katastrophenschutz, militärische Verteidigung und Verkehr

CPS können auch echte Lebensretter sein. CPS, die über entsprechende Sensoren Naturkatastrophen, wie Tornados oder Erdbeben, schon Tage vorher erkennen und davor warnen können, sind in Evakuierungsfällen unverzichtbar geworden. Auch in Umweltthemen können CPS Hilfestellung bieten

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

– so können beispielsweise Bodenbeschaffenheiten automatisch erkannt und anhand deren Veränderungen Rückschlüsse auf Pflanzen und Tiere in der Umgebung gemacht werden.

Das unterscheidet sich gar nicht so sehr von den industriellen Einsatzgebieten: Schließlich sollen auch hier die Effizienz gesteigert und die benötigte Zeit und die Kosten reduziert werden.

Aber auch militärisch werden CPS eingesetzt. Moderne Flugabwehrsysteme oder auch militärische Drohnen werden mit solchen Systemen untereinander vernetzt, um entsprechend schnell und aufeinander abgestimmt reagieren zu können.

Auch der Verkehr profitiert von CPS und ist eigentlich ein offensichtliches Beispiel für eine Systemregulierung in Echtzeit. Staus, Unfälle und Fahrbahnschäden werden in Echtzeit registriert und entsprechende Umleitungsmaßnahmen oder Straßenabsperrungen durchgeführt – damit wird der Verkehr entlastet und weiteren Staus oder Unfällen vorgebeugt. Auch völlig autonome Fahrzeuge sind so denkbar. Das ist allerdings noch Zukunftsmusik denn hier muss erst auch noch die entsprechende Straßeninfrastruktur gebaut werden.

E-Health

Neben öffentlichen und unternehmerischen Einsatzgebieten kann auch jede einzelne Person ganz individuell von CPS profitieren. Da wäre beispielsweise das Schlagwort E-Health (Electronic Health, also die elektronische Verarbeitung gesundheitlicher Daten) zu nennen.

Dabei können Vorbeugung, Überwachung, Diagnose, Behandlung und Verwaltung miteinander elektronisch verknüpft werden. Die elektronische Gesundheitsakte in Österreich (auch ELGA genannt) ist ein Teil der E-Health, genauso wie Online-Apotheken oder auch Smartwatches und Fitness-Tracker (am Handgelenk getragene Geräte, die gesundheitliche Daten wie bspw. den Pulsschlag erkennen oder Stürze registrieren).

Beispiel
Bei einem Patienten wird Diabetes diagnostiziert. Er bekommt ein digitales Blutabnahmegerät, um den Blutzucker regelmäßig zu überwachen. Dieses ist mit seiner Smartwatch gekoppelt, die aufgrund der übermittelten Daten Handlungsvorschläge in Bezug auf Sport, Ernährung und Medikamente bringt.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Im Notfall reagiert die Smartwatch und kann eigenständig die Rettung alarmieren. Trifft diese ein, wird dem Rettungssanitäter über die Smartwatch mitgeteilt, dass es sich um einen Diabetiker handelt. Dieser kann so die richtigen Maßnahmen schnell einleiten.

Ein weiteres Anwendungsgebiet ist die (Altersgerechte) technologische Unterstützung – Ambient Assisted Living

Hier geht es im Wesentlichen um Menschen, die in irgendeiner Art und Weise Unterstützung für ein selbstbestimmtes Leben benötigen – sei es aufgrund von altersbedingten Problemen oder körperlicher Einschränkungen.

CPS werden hier eingesetzt, um Technologien zu erschaffen, die auf die jeweiligen Bedürfnisse der Menschen eingehen können. Dabei werden nicht nur diese unterstützt, sondern beispielsweise auch Pflegepersonal und Angehörige.

Wohnungen können beispielsweise so gestaltet werden, dass mithilfe von Sprache Heizungen gesteuert, Rollos bedient oder Beleuchtungen aktiviert werden können. Dies wäre auch automatisiert denkbar, z. B. indem immer, wenn die Person die Wohnung verlässt das Licht sowie der Herd ausgeht. So würden älteren Menschen einige manuelle Schritte erspart werden. Bei Brandgefahr kann zusätzlich zu einem Alarm auch die Feuerwehr automatisch verständigt werden.

Ein Kritikpunkt: Die Bedienung solcher Systeme muss allerdings vorher neu gelernt werden – z. B. welche Sprachkommandos verwendet werden müssen. Das kann für beeinträchtigte oder ältere Menschen schwierig sein. Es muss also besonderes Augenmerk auf die Einfachheit und Benutzerfreundlichkeit dieser Systeme gelegt werden.

Merken

CPS bietet eine Reihe von Anwendungsgebieten, manche davon sind bereits umgesetzt, andere sind für die Zukunft geplant.

Einige Beispiele sind:

Industrie 4.0

- Smart Factories und vollautomatisierte Produktionsumgebungen
- Wartungs- und Logistiksysteme

Gesellschaftliche Einsatzgebiete

- Smart Grid
- Katastrophenschutz
- Umweltschutz
- Militärische Verteidigung
- Verkehr

Individuell

- E-Health
- Ambient Assisted Living

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.5 Chancen und Gefahren von CPS

Wie Sie bereits gelernt haben, sind CPS vor allem da, um komplexe Systeme schneller und effizienter zu machen. Dabei gibt es verschiedenste Vor- und Nachteile.

Wie sieht es mit den **Vorteilen** aus? Einige kennen Sie aus dem vorherigen Kapitel sicher schon:

- **Effizienzsteigerung und Kosteneinsparung**

Systeme können viel effizienter ablaufen. Aufgrund einer ständigen Selbstkontrolle und Nachregelung werden Themen wie Wartung, Verschleiß, Ressourcenverbrauch und Produktionsausfälle minimiert, in Echtzeit wahrgenommen und entsprechend reagiert.

Z. B. können Logistiksysteme Lagerbestand und Bedarf automatisch feststellen und entsprechende Bestellungen aufgeben.

- **Anpassungsfähigkeit**

CPS ermöglichen es der vernetzten Umgebung, extrem schnell zu reagieren, sich anzupassen und Prozesse selbst zu steuern. Dabei kann beispielsweise in der gleichen Produktionsumgebung sowohl in Massenfertigung produziert als auch an einzelnen Prototypen gearbeitet werden. Das ist in herkömmlichen Fabriken meist nicht ohne hohe Zusatzkosten möglich.

Verschiedenste Systeme können unter einem großem System vereint werden. So werden Zukunftskonzepte wie selbstfahrende Autos und vernetzte Straßensysteme überhaupt erst möglich.

- **Arbeitssicherheit**

Der Mensch wird in vielen gefährlichen Situationen nicht mehr direkt vor Ort benötigt. Katastrophenschutz, militärische Einsätze oder auch Fertigungsverfahren werden von CPS Einheiten ausgeführt. Der Mensch hat lediglich eine Kontroll- und Steuerungsfunktion.

Und die Nachteile? Nun, da ist es schon schwieriger. Es gibt aber tatsächlich einige Gefahren, die beachtet werden müssen und aktuell noch große Fragezeichen aufwerfen:

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Komplexe Technik**

Sie haben es schon erkannt – in CPS steckt jede Menge Technik. Die muss funktionieren, nicht nur allein, sondern eben vor allem zusammen. Wenn ein Subsystem defekt ist, dann kann unter Umständen das große Ganze betroffen sein. Aufgrund der vielen technischen Elemente, die alle miteinander verbunden sind, gelten CPS als recht anfällig für Störfälle. Je komplexer die Technik, desto mehr Möglichkeiten für Fehler gibt es.

Das kann so weit gehen, dass einzelne kleine Fehler das ganze System lahmlegen. Die Fehlersuche gestaltet sich dann dementsprechend langwierig und schwierig.

- **Programmierte Entscheidungen**

CPS sollen so autonom wie möglich agieren. Da kann aufgrund eines Softwarefehlers oder auch aufgrund eines unvorhergesehenen Ereignisses auch einmal eine „falsche“ Entscheidung getroffen werden. Eine Maschine kann nur soweit „denken“, wie sie programmiert wurde. Für manche Situationen könnte dies zu wenig sein, vor allem bei Bedienfehler durch den Menschen.

- **Hacking und Sicherheit**

Wie Sie gelernt haben, werden CPS auch in gesellschaftlichen Themen eine große Integration erfahren. Technische Systeme könnten jedoch auch gehackt und damit sabotiert oder manipuliert werden. Das ist besonders bei Einsatzgebieten wie der Energieversorgung oder militärischen Anwendungen kritisch.

Dabei müssen absolut hohe Sicherheitsbestimmungen ständig neu erfüllt werden. Hier liegt einer der größten Nachteile von vernetzten Systemen.

- **Datenschutz und persönliche Rechte**

Wir leben in einer Welt in der vieles miteinander verbunden ist und unzählige Informationen im Netz vorhanden sind. Hier stellt sich natürlich auch die Frage, welche Daten wohin gesendet und von wem genutzt werden.

Das geht über Unternehmensdaten bis hin zu höchst privaten Daten. Die Energienutzung im eigenen Haushalt kann Aufschluss über Lebensgewohnheiten bieten, Gesundheitsdaten können in Versicherungsfragen Nachteile bringen oder Unternehmen können wichtige Daten an die Konkurrenz verlieren.

Auch hier gilt es, nicht nur informationstechnische, sondern auch rechtliche Fragen zu klären und neue Standards einzuführen.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Merken
CPS haben eine Reihe von Vor- und Nachteilen. Vorteile: • Effizienzsteigerung und Kostenersparnis • Anpassungsfähigkeit • Arbeitssicherheit Nachteile • Anfällige Technik • Fehlentscheidungen • Hacking • Datenschutz

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.6 Zusammenfassung

Cyber Physical Systems (CPS) sind die technologische Grundlage der Industrie 4.0 bzw. des Internet of Things. Dabei geht es um die **Generierung und Auswertung von Daten, um in Echtzeit Prozesse steuern und anpassen zu können.**

Dafür wird die **physische Welt mit der digitalen über ein Datennetzwerk vereint.** Dies geschieht über die Verbindung von mechanischen bzw. elektronischen Komponenten mit software- bzw. informationstechnischen Komponenten.

CPS ist ein Übersystem verschiedener Subsysteme. Diese Subsysteme enthalten Embedded Systems, mechatronische Konzepte wie Roboter und Netzwerksysteme wie Internet und Cloud-Computing.

Die wichtigsten technologischen Bausteine und Konzepte dafür sind **Aktoren, Sensoren, Mikrocontroller, moderne Datennetzwerke** und **System Engineering.**

CPS bietet eine Reihe von modernen Anwendungsmöglichkeiten. Diese sind industriell von Nutzen (z.B. durch Smart Factory Konzepte), gesellschaftlich (z. B. im Katastrophenschutz, in der Verteidigung, Smart Grid oder im Verkehr) und individuell (z. B. durch E-Health oder ambient assisted living)

Die Vorteile von CPS sind hohe Effizienz, Anpassungsfähigkeit, Arbeitssicherheit und Kostenersparnis. Nachteile liegen in anfälliger Technik, möglichen Fehlentscheidungen der Systeme, der Gefahr von Hacking und in der Herausforderung des Datenschutz im Zusammenhang mit solchen Systemen gerecht zu werden.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.7 ÜBUNGEN

1. Vervollständigen Sie den folgenden Text:

CPS ist ein _____ vieler verschiedener _____ die dazu dienen, die reale Welt mit der virtuellen Welt zu verbinden. In professionelleren technischen _____ bezieht sich dies auf ein Netzwerk mechanischer _____, die durch einen computergestützten _____ gesteuert und überwacht werden.

2. Subsysteme bestehen aus:

1. Aktuatoren	a) Das Gehirn eines eingebetteten Systems - auch als "Chip" bezeichnet - Der Mikrocontroller führt Computeraufgaben wie ein Computer aus. Es überwacht, steuert und überträgt Prozesse je nach Programmierung automatisch
2. Sensoren	b) Dies sind hauptsächlich Komponenten der Antriebstechnik - dies bedeutet nicht unbedingt, dass sich etwas bewegt, sondern dass sich zumindest etwas bewegt. Zum Beispiel benötigt ein Roboterarm, der eine Komponente umdreht, einen Motor, um sie zu bewegen. Es ist wichtig, dass ein solcher Aktuator durch ein elektrisches Signal gesteuert werden kann.
3. Mikrocontroller	c) Dies sind die Gegenstücke zu den Aktuatoren - sie "erfassen" ihre Umgebung anhand physikalischer oder chemischer Eigenschaften (z. B. Druck, Wärme, Helligkeit usw.) und stellen diese anhand einer Messgröße dar (z. B.: Temperatur des Werkstücks = 10 Grad Celsius). Diese Messgröße kann als elektrisches Signal weiterverarbeitet werden

3. CPS generiert Daten, Informationen und Wissen aus physischen Prozessen. Diese werden in Echtzeit verarbeitet, steuern Prozesse dynamisch und sind über ein Netzwerk verbunden. Dies erfordert drei Kerntechnologien: Steuerung, Berechnung und Kommunikation. Diese werden durch folgende technologische Module und Konzepte erfüllt:

	Wahr	**Falsch**
Physikalische Elemente: Aktoren, Sensoren und Mikrocontroller		
Industrie 4.0		
Systemische Elemente: Eine Konzeptualisierung des Gesamtsystems gemäß den Anforderungen mit "Systems Engineering"		
Cyber elements: Network technologies like the Internet		
Soziale Anwendungsbereiche		
Individuell		

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Vervollständigen Sie den folgenden Text:

Die Einsatzmöglichkeiten von CPS sind eigentlich grenzenlos - neben rein _____ (aber eher zukunftsorientierten) Anwendungsfeldern wie _____ Fertigungs- und Produktionsumgebungen in _____ Branchen ("Smart Factories") werden CPS bereits in anderen Bereichen eingesetzt. Dazu gehören intelligente Stromnetze ("Smart Grids"), _____ Gesundheit, _____ Assistenzsysteme, aber auch _____ Verkehrsüberwachungssysteme oder _____ Frühwarnsysteme im Katastrophenschutz.

5. CPS bietet eine Reihe von Anwendungsbereichen an, von denen einige bereits implementiert wurden, andere für die Zukunft geplant sind.
Einige Beispiele sind:

1. Industrie 4.0	a. • Elektronische Gesundheitsdienste • Altersgerechte technologische Unterstützung (Ambient Assisted Living)
2. Soziale Anwendungsbereiche	b. • Intelligente Fabriken und vollautomatisierte Produktionsumgebungen • Wartungs- und Logistiksysteme
3. Individuell	c. • Intelligentes Stromnetz • Zivilschutz • Umweltschutz • Militärische Verteidigung • Verkehr

6. Wie Sie bereits erfahren haben, dient CPS in erster Linie dazu, komplexe Systeme schneller und effizienter zu machen. Es gibt verschiedene Vor- und Nachteile.
Was sind die Vorteile?

a. Erhöhte Effizienz und Kosteneinsparungen

Systeme können viel effizienter laufen. Durch ständige Selbstkontrolle und Neueinstellung werden Probleme wie Wartung, Verschleiß, Ressourcenverbrauch und Produktionsausfallzeiten minimiert, in Echtzeit wahrgenommen und entsprechend reagiert.
Beispielsweise können Logistiksysteme Lagerbestände und Nachfrage automatisch ermitteln und entsprechende Bestellungen aufgeben.

☐ Richtig ☐ Falsch

b. Anpassungsfähigkeit

Mit CPS kann die Netzwerkumgebung extrem schnell reagieren, Prozesse selbst anpassen und steuern. Beispielsweise kann dieselbe Produktionsumgebung sowohl für die Massenproduktion als auch für die Arbeit an einzelnen Prototypen verwendet werden. Dies ist in herkömmlichen Fabriken ohne hohe Zusatzkosten in der Regel nicht möglich.
Verschiedene Systeme können unter einem großen System kombiniert werden. Auf diese Weise werden in erster Linie zukünftige Konzepte wie selbstfahrende Autos und vernetzte Straßensysteme möglich.

☐ Richtig ☐ Falsch

c. Betriebssicherheit

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

In vielen gefährlichen Situationen werden Menschen vor Ort nicht mehr benötigt. Katastrophenschutz, militärische Operationen oder sogar Herstellungsprozesse werden von CPS-Einheiten durchgeführt. Der Mensch hat nur eine Überwachungs- und Kontrollfunktion

☐ Richtig ☐ Falsch

7. **Wie Sie bereits erfahren haben, dient CPS in erster Linie dazu, komplexe Systeme schneller und effizienter zu machen. Es gibt verschiedene Vor- und Nachteile. Was ist der Nachteil? Nun, dort wird es schwieriger. Aber es gibt tatsächlich einige Gefahren, die berücksichtigt werden müssen und derzeit noch große Fragezeichen aufwerfen:**

   a. **Komplexe Technologie**

   Sie haben es bereits erkannt - in CPS steckt viel Technologie. Es muss nicht nur alleine, sondern vor allem zusammen funktionieren. Wenn ein Subsystem defekt ist, kann das gesamte System betroffen sein. Aufgrund der vielen technischen Elemente, die alle miteinander verbunden sind, wird CPS als sehr fehleranfällig angesehen. Je komplexer die Technologie ist, desto mehr Möglichkeiten gibt es für Fehler. Dies kann zu einzelnen kleinen Fehlern führen, die das gesamte System lähmen. Die Fehlerbehebung ist dann entsprechend langwierig und schwierig.

   ☐ Richtig ☐ Falsch

   b. **Programmierte Entscheidungen**

   CPS sollten so autonom wie möglich handeln. Eine "falsche" Entscheidung kann aufgrund eines Softwarefehlers oder eines unvorhergesehenen Ereignisses getroffen werden. Eine Maschine kann nur so weit "denken", wie sie programmiert wurde. In einigen Situationen kann dies zu wenig sein, insbesondere bei Betriebsfehlern durch Menschen.

   ☐ Richtig ☐ Falsch

   c. **Hacking und Sicherheit**

   Wir leben in einer Welt, in der viele Dinge miteinander verbunden sind und unzählige Informationen im Internet verfügbar sind. Hier stellt sich natürlich auch die Frage, welche Daten wohin gesendet werden und von wem sie verwendet werden. Dies reicht von Unternehmensdaten bis zu sehr privaten Daten. Der Einsatz von Energie im eigenen Haushalt kann Aufschluss über die Lebensgewohnheiten geben, Gesundheitsdaten können in Versicherungsangelegenheiten Nachteile mit sich bringen oder Unternehmen können wichtige Daten an Wettbewerber verlieren. Auch hier ist es notwendig, nicht nur die Informationstechnologie, sondern auch rechtliche Fragen zu klären und neue Standards einzuführen.

   ☐ Richtig ☐ Falsch

   d. **Datenschutz und Persönlichkeitsrechte**

   Wie Sie gelernt haben, wird CPS auch eine starke Integration in soziale Fragen erfahren. Technische Systeme könnten jedoch auch gehackt und damit sabotiert oder manipuliert werden. Dies ist besonders wichtig in Bereichen wie der Energieversorgung oder militärischen Anwendungen.
   Absolut hohe Sicherheitsvorschriften müssen ständig eingehalten werden. Dies ist einer der größten Nachteile vernetzter Systeme.

   ☐ Richtig ☐ Falsch

8. **Vervollständigen Sie folgende Texte:**

   a.

Cyber Physical Systems (CPS) sind die _____ Basis von Industrie 4.0 oder dem Internet der Dinge. Dies _____ die Erzeugung und Auswertung von Daten, um Prozesse in Echtzeit zu _____und _____.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

b.

Zu diesem Zweck wird die _____ über ein Datennetz mit der _____ kombiniert. Dies erfolgt durch _____ mechanischer oder elektronischer _____ mit Software- oder Informationstechnologiekomponenten.

c.

CPS ist ein _____ verschiedener Subsysteme. Diese _____ umfassen eingebettete Systeme, _____ wie Roboter und _____ wie das Internet und Cloud-Computing.

9. Was sind die wichtigsten technologischen Bausteine und Konzepte für die CPS?

a. Microkontroller
b. Hardware
c. Aktuatoren
d. Sensoren
e. Software
f. moderne Datennetze
g. Systemtechnik
h. Programmierfehler

10. CPS bietet eine Reihe moderner Anwendungsmöglichkeiten.

1. Industrieller Nutzen	a. Smart-Factory-Konzepte
2. Sozialer Nutzen	b. E-Health, umgebungsunterstütztes Wohnen
3. Individueller Nutzen	c. Zivilschutz, Verteidigung, Smart Grid, Verkehr

11. Die Vor- und Nachteile von CPS sind:

	Vorteil	**Nachteil**
Anfällige Technologie		
Gefahr von Hacking		
Arbeitssicherheit		
Kosteneinsparungen		
Hone Effizienz		
Mögliche Fehlentscheidungen der Systeme		
Anpassungsfähigkeit		

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7. LÖSUNGEN ZU DEN ÜBUNGEN

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7.1 Basics Digitalisierung und Arbeitswelt 4.0

1. 5, 2, 4, 1, 3
2. c
3. a
4. b
5. c
6. d
7. 4, 6, 3, 5, 1, 2
8. R, F, R, F, F,
9. 2, 5, 3, 4, 1

7.2 Cloud Computing

1. F, R, R, F, R
2. 4, 1, 3, 2, 5
3. 1c, 2a, 3a, 4b, 5c, 6b, 7b, 8c, 9c, 10a
4. F, R, F, R, R
5. a
6. b
7. c
8. c
9. a

7.3 Big Data

1. a
2. abd
3. Analyse, Datenmengen, Erkenntnisse, Entscheidungen
4. c
5. R, R, R
6. 5, 6, 2, 4, 3, 1
7. R, F, R
8. a
9. 3, 5, 1, 6, 2, 4

7.4 Smart Factory

1. c
2. a
3. a
4. c
5. d
6. 1b, 2a
7. 1c, 2d, 3a, 4b
8. 1d, 2c, 3b, 4e, 5a
9. a
10. d
11. b

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

12. 1b, 2e, 3d, 4a, 5c

7.5 IT-Security

1. 1c, 2a, 3b
2. abc
3. a) Schutzziele, Kernaufgabe, Schwachstellen, Hardware, Software, Programmierfehler
   b) Bedrohung, Schwachstelle, gefährdet, zugängliches
4. abf
5. acd
6. c
7. Verschlüsselung, Datenkryptografie, Übersetzercode, Nachrichtendaten, Zahlen, Symbolen
8. abfg
9. acd
10. be
11. befh
12. def
13. a) Kernaufgabe, Schwachstellen, interne, externe
    b) unbeabsichtigt, Passwort, Naturkatastrophen
    c) Menschen, Schutzsoftware; Gefährdungen

7.6 Cyber Physical Systems

1. Netzwerk, Technologien, Begriffen, Systeme, Prozess
2. 1b, 2c, 3a
3. R, F, R, R, F, F
4. Industriellen, intelligenten, verschiedenen, elektronische, altersgerechte, intelligente, automatische
5. 1b, 2c, 3a
6. aR, bR, cR
7. aR, bR, cF, dF
8. a) technologische, beinhaltet, steuern, anzupassen
   b) physiche Welt, digitalen Welt, Verbinden, Komponenten
   c) Supersystem, Subsysteme, mechatronische Konzepte, Netzwerksysteme
9. acdfg
10. 1a, 2c, 3b
11. N, N, V, V, V, N, V

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.