FH Salzburg

VO Web-Technologien

Einheit 9, Oliver Jung

Technik
Gesundheit
Medien

Die Entwicklung des WWW

Zentrale Frage:

Das Web ist aus der modernen Gesellschaft nicht mehr wegzudenken. Welche Auswirkungen hat diese tiefgehende Durchdringung eigentlich und worauf müssen wir achtgeben?

Beschäftigen uns in dieser Woche mit:

- Kurzem Überblick über Entwicklungsstadien des Webs
- **Social Web**: Soziale Netzwerk, Social Media und deren Verankerung in der Gesellschaft
- **Semantic Web**: Webseiten werden Maschinen-lesbar und -verstehbar
- **Service Web**: Technologische Grundlagen der digitalen Transformation der Gesellschaft und deren besondere Herausforderungen bei Datenschutz und Sicherheit

Das Web heute und morgen

Seit seiner Einführung vor 25 Jahren unterlag das World Wide Web einem stetigen Entwicklungs- und Veränderungsprozess:

- **Web 1.0: Lesbar und statisch** (vor 2000)
  - Nur einige (professionelle) Autoren konnten Inhalte veröffentlichen
  - Web-Ressourcen waren ganz überwiegend statisch
- **Web 2.0: Kollaborativ und mitwirkend** (bis heute)
  - Nutzer (auch Laien) können eigene Inhalte veröffentlichen dank Anwendungen im Bereich ➔ **Social Web**
  - Viele Webseiten werden dynamisch erzeugt und immer komplexer
  - Neue Technologien und Frameworks ermöglichen es Entwicklern, immer komplexere Web-basierte Anwendungen zu bauen

Das Web heute und morgen

- **Web 3.0: Semantisch und ausführbar** (noch im Entstehen)
  - Informationen werden maschinell lesbar und verständlich
    - Heutige Suchmaschinen nutzen Schlüsselwortbasierte Mechanismen
    - Such-Algorithmen vergleichen und zählen Zeichenketten, verstehen Bedeutung der Suchbegriffe und Dokumente nicht
  - **semantisches Web** bietet nicht länger nur Dokumente, sondern auch **Dinge** (Menschen, Orte, Ereignisse, ...), setzt sie in **Beziehung**
  - Web-Anwendungen können miteinander verwoben werden durch Web Services ➔ **Service Web**

Das Web heute und morgen

- **Web 4.0: Mobil** (heute)
  - parallele, alternative Version des existierenden Webs
  - misst dem lokalen Kontext größere Bedeutung zu
  - nutzt stark das ➔ **Service Web** (Server-seitiger Teil von Apps)

- **Und darüber hinaus?**
  Wie könnte das **Web 5.0** aussehen?

Social, Semantic und Service Web

Fokussieren uns auf drei Aspekte des Webs von heute und morgen:

Social Web

- Ursprung und Anwendungen des Social Web:
  - Blogs und Wikis
  - Social Networks und Social Media
- Meinungsbildung und Manipulation im Social Web
  - Twitter Bots
  - Fake News und Manipulation
  - Filterblasen und Echokammern
- Privatsphäre und Sicherheit im Social Web
  - „Privacy Paradoxon"
  - Gefahren durch Social Engineering

Social, **Semantic** und Service **Web**

Semantic Web

- Web bietet nicht mehr nur Sammlung von Dokumenten sondern von Entitäten (Personen, Orte, Ereignisse, ...) und setzt diese in Beziehung zueinander
- Maschinen „verstehen" Bedeutung der Informationen im Web
- Anwendungsszenarien:
  - Semantik-unterstützte Suche
  - intelligente Agenten
- Technische Grundlagen des Semantic Web
- Linked Open Data als praktikabler Ansatz

Social, Semantic und **Service Web**

Service Web

- Web Services sind eine grundlegende Technologie für das **Internet der Dinge** (**IoT**)
- IoT Visionen: Smart Factory, Smart Home, Smart World
  - Industrie 4.0 – Ausprägung von IoT in Industrie und Wirtschaft
- Spektakuläre Sicherheitsvorfälle
- Sicherheit und Datenschutz als zentrale Herausforderung in einer hochvernetzten Welt

Entstehung des Social Web

Wahrnehmung und Nutzung des Internets änderte sich seit 2005:

- **Mitwirkungs-Prinzip** des Web 2.0
  - Nutzer sind Bearbeiter von Webseiten und nicht nur Leser von statischen Web Informationen
  - Nutzer teilen ihre Daten im Web, z.B. Lesezeichen, Fotos, berufliche Informationen, Videos, ...
  - Es entsteht ein (virtuelles) Gemeinschaftsgefühl
- Zunehmende Nutzung des Webs als Kommunikationsplattform, Grenzen zwischen Web Anwendungen und lokalen Anwendungen auf dem Rechner verwischen, z.B.
  - Nutzung von *Gmail* im Browser anstatt eines lokalen Mail Clients

Formen des Social Webs: Wikis

Wikis sind frühe Form von Anwendungen des Social Web

- „Wiki" ist hawaiisch für kurz, schnell
- verwirklichen Idee einer kollaborativen Textverarbeitung und Kommentierung von Beiträge im WWW

- Erste Wiki-Installationen wurden bereits 1995 veröffentlicht (WikiWikiWeb)
- **Wikipedia** wurde 2001 gestartet und erhöhte Popularität und Verbreitung des Konzepts
  - Wikipedia ist unter den 10 populärsten Webseiten gelistet
- Wikis wurden auch bekannt durch eine Nutzung als Wissensdatenbanken in Unternehmen und Organisationen
  - Mitarbeiter können ihr Wissen teilen und speichern

Formen des Social Webs: Blogs

Web-Blogs, oder kurz **Blogs**, verbreiten sich Ende der 1990er Jahre und bieten weitere wichtige Form des Social Webs

- **Blogs** sind öffentliche persönliche Tagebücher bzw. Journale im Web
- Ein oder mehrere Autoren – die Web-Logger, kurz **Blogger**, veröffentlichen Beiträge (**Posts**) über ihr Leben oder ein spezielles Thema
- Blog-Leser können sich aktiv beteiligen durch Feedback in Form von Kommentaren, Bewertungen, ...
- Nutzer können Blogs abonnieren durch **Feeds** (z.B. RSS, Atom)
- Technisch sind Blogs realisiert durch
  - Blog Hosting Dienste, z.B. **Blogger**, **tumblr**, ...
  - Hosting auf eigenem Server, z.B. **WordPress**

tumblr.

Formen des Social Webs: Microblogging

Microblogging wurde für gelegentliche kurze persönliche oder unternehmerische Status-Updates eingeführt

- Posts haben meist Länge von nur 200 Zeichen oder weniger
- Für Microblogs wurde Konzept der **Asynchronen Follower** eingeführt: User erhalten Status-Updates von Microbloggern denen sie „folgen“, aber nicht umgekehrt

- Um aufkommende Themen zu identifizieren, werden **#Hashtags** im Social Web benutzt

- Derzeit ist **X (ehem. Twitter)** bekanntester Microblogging-Anbieter
  - □ wurde 2006 gestartet und ist heute wichtiger Mediankanal für öffentliche Personen, politische Aktivisten, ...

Formen des Social Webs: Soziale Netzwerke

Soziale Netzwerkedienste, oder kurz **Soziale Netzwerke** entstanden zusammen mit dem Microblogging

- Soziale Netzwerke kombinieren Blogging / Microblogging mit Liste weiterer verbreiteter Funktionen (Features):
  - persönliches Profil
  - Freundesliste (im Gegensatz zum Follower-Konzept legen Soziale Netzwerke bidirektionale Nutzerbeziehungen an)
  - Aktivitäten-Verlauf (kombiniert Status-Updates der Freunde eines Nutzers und erlaubt Kommentare)
  - Privater Nachrichtenaustausch mit anderen Nutzern und Nutzergruppen
  - Ausdruck persönlicher Interessen, z.B. durch „likes"
  - Soziale Anwendungen (z.B. Spiele) ➔ Soziale Netzwerke werden Plattform für eigene Anwendungen

LinkedIn

facebook

Formen des Social Webs: Soziale Medien

Durch stark fallende Preise für Speicher und hohe Bandbreiten entstanden seit 2005 zahlreiche Portale für Soziale Medien

- Soziale Medien bieten Nutzern Möglichkeit, Medien-Ressourcen wie Fotos, Videos oder Audios mit Freunden oder der Öffentlichkeit zu teilen
  - Autoren können Feedback für ihre Medien erhalten
  - Autoren können ihre Medien speichern, um sie z.B. in ihre persönliche Webseite einzubetten, ohne sich Gedanken um Speicherplatz zu machen
- Bekannte Plattformen für Soziale Medien sind heute:
  - Fotos – **Instagram**, **flickr**, ...
  - Video – **YouTube**, **Vimeo**, ...
  - Audio – **Soundcloud**, ...

Kritik an Sozialen Medien

Privatsphäre (Privacy)

- Anbieter Sozialer Netzwerke fordern oft weitgehende Nutzungsrechte für von Nutzern bereitgestellte Inhalte
- Persönliche Informationen können genutzt werden für personalisierte Werbung und Verkauf an Werbetreibende zur Zielgruppenbestimmung

Vertrauenswürdigkeit

- Jeder kann wahrheitsgetreue oder falsche Inhalte erstellen, z.B. „Edit Wars" auf Wikipedia oder die Diskussion um „**Fake News**"
- Unechte Accounts mit falschem Namen können erstellt werden

Verlässlichkeit

- Dienste können von Staaten geblockt werden, um den Zugriff auf Informationen zu beschränken

Bedeutung Sozialer Netzwerke

Soziale Netzwerke sind sehr populär und werden von immer mehr Menschen genutzt, z.B.:

- **Facebook**: 2,96 Milliarden aktive Nutzer pro Monat (Jan. 2023)

- Für **Verbreitung von Nachrichten und Informationen** ist die Bedeutung sozialer Netzwerke enorm gestiegen
- **Quelle** und **Korrektheit** von Informationen lassen sich für Nutzer nur **schwer überprüfen** ➔ Stichwort ***Fake-News***
- Jeder Nutzer, ob Mensch oder Maschine, kann Inhalte erstellen und verbreiten
- Potenzial der Manipulation der öffentlichen Meinung ist durch soziale Netzwerke dramatisch gestiegen

Twitter-Bots

Ein **Bot**, kurz für Roboter, ist Programm, das weitgehend automatisiert eine Aufgabe abarbeitet

- Twitter-Bots täuschen gezielt **menschliches Verhalten** vor mithilfe von Machine Learning Technologien
- Erste Generation wurde zum Aufbau der Reichweite des eigenen Profils eingesetzt, heute geht es vermehrt um **Beeinflussung**
- Bots folgen dabei vorher festgelegten Interessen und twittern nur gelegentlich, um nicht automatisch als Spam erkannt zu werden
- Durch Tweets und Retweets (teilen von fremden Tweets) wird öffentliche Aufmerksamkeit für bestimmte Inhalte verstärkt
- Es existieren aber auch „gute" Bots, die nützliche Automatisierungen durchführen, z.B.
  - Chat-Bots im Facebook Messenger

Twitter-Bots

Aktuelle Beispiele der Meinungsbeeinflussung durch Bots:

- **Brexit**
  - Untersuchung von 1,5 Millionen Tweets von mehr als 300.000 Twitter-Accounts zum Thema Brexit
    - Bedeutender Anteil der Tweets wurde von Bots verfasst
    - Großteil der Bots sprach sich für Brexit aus
- **US-Präsidentenwahl**
  - Mehr als ein Drittel der Pro-Trump Tweets und fast ein Fünftel der Pro-Clinton Tweets zwischen erstem und zweitem Fernsehduell wurden von Bots abgesetzt
  - Insgesamt mehr als 1 Million Tweets von Bots

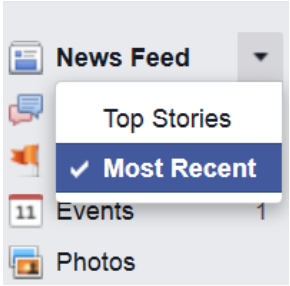
➔ Wieviel Beeinflussung Bots tatsächlich erreichen, lässt sich schwer messen, aber Bots spielen starke Rolle vor allem in politischen Diskussionen

Filterblasen

- Soziale Netzwerke versuchen mithilfe von Algorithmen vorauszusagen, welche Informationen einen Nutzer besonders interessieren
- Diese Inhalte werden dann prominent platziert, als uninteressant eingestufte Inhalte werden teilweise sogar ausgeblendet mit dem Ziel, das Nutzer länger auf Plattform verweilt und sich wohlfühlt
- Nutzern werden so allerdings auch Informationen vorenthalten, die vermeintlich nicht seinen Interessen und Standpunkten entsprechen
- Verstärkend wirkt hierbei noch das ***Echokammern***-Phänomen:
  - Nutzer vernetzen sich im virtuellen Raum verstärkt mit Gleichgesinnten
  - Dies kann zu einer fatalen Verengung der Weltsicht führen

Filterblasen

- **Beispiele**:
  - Personalisierte Suche von Google
  - Personalisierter Aktivitäts-Feed von Facebook und Instagram



- Diese Informationsblasen können in verschiedenen Themenbereichen Auswirkungen auf den öffentlichen Diskurs haben
- Aber auch hier gilt: Tatsächliche Beeinflussung ist bisher nicht einwandfrei nachgewiesen …

Fake-News

- Ob Twitter-Bots oder echte Menschen, jeder kann online Beiträge erstellen und verbreiten
- Zurzeit ist Diskussion um Fake-News in aller Munde, also absichtlich über das Internet verbreitete Falschmeldungen zur Beeinflussung der öffentlichen Meinung zu bestimmten Themen
- Im Europäischen Auswärtigen Dienst (EAD) in Brüssel arbeiten inzwischen 11 Beamte ganztags daran, Fake-News zu enttarnen und Gegendarstellungen zu veröffentlichen
- Dazu durchforstet ein Netzwerk aus rund 400 Journalisten, Universitätsangestellten, Beamten, NGO-Mitarbeitern und Einzelpersonen in 30 Ländern das Internet nach Fake-News

Fake-News

- Nachdem Politik Druck auf Facebook ausgeübt hat, hat Facebook neue Netzwerkfunktionen einführen, um gegen Fake-News vorzugehen
  - Nutzer erhalten die Möglichkeit, einen Beitrag als potenzielle Falschmeldung zu melden
  - Externes Recherchezentrum prüft die gemeldeten Inhalte und markiert gegebenenfalls als zweifelhaft
  - Am Ende soll neben Beitrag mit falschen Informationen ein Warnhinweis erscheinen sowie Link zu einem Artikel mit den tatsächlichen Fakten

Kann man Fake-News erkennen?

Wie kann man selbst Fake-News identifizieren?

- Seriosität der Quelle:
  - Sind Impressum und Kontaktmöglichkeiten vorhanden?
  - Wie lange existiert Seite schon?
  - Was verbreitet Quelle ansonsten für Nachrichten?
- Handelt es sich um Satire?
- In welchem Kontext steht die Seite? Veröffentlicht Seite ansonsten viele Quatschmeldungen und Unsinn?
- Was steht im Artikel und was nur in Vorschau?
  - Auf Facebook können Titel eines verlinkten Artikels einfach geändert werden

Kann man Fake-News erkennen?

- Wo kommen Informationen ursprünglich her? Seriöse Journalisten nennen und verlinken Informationen eines Artikels, Meldungen von Nachrichtenagenturen enden mit Kürzeln wie
  „dpa“, „Reuters“ oder „AFP“
- Wurde Quelle richtig wiedergegeben? Bei Fake-News werden verlinkte Quellen oft veraltet oder falsch wiedergegeben
- Zeigt Foto/Video wirklich beschriebene Situation, oder wurde einfach ein altes genommen und als Augenzeugen- oder Skandalclip inszeniert? (Lässt sich leider nur schwer nachvollziehen für Laien)

Macht der Algorithmen und Big Data

- Unternehmen setzen zunehmend auf das Sammeln, Verknüpfen und Auswerten (persönlicher) Daten
- Über Smartphone oder Browser können permanent Daten über Nutzungsverhalten gesammelt und auch an Dritte weitergegeben werden
- Auf Basis dieser Daten wird personalisierte Werbung geschaltet
- Analyse dieser „Big Data" bringt Unternehmen starken Wettbewerbsvorteil:
  - Kunden können besser verstanden und bedient werden
  - interne Prozesse können effizienter gestaltet werden
- Diese Praxis bietet allerdings auch viel Potenzial für Missbrauch!

Macht der Algorithmen und Big Data

Beispiele für Nutzung von Big Data:

- US-Supermarktkette Target: Analyse des Einkaufsverhaltens kann schwangere Frauen identifizieren und deren Geburtstermine hochrechnen
- Facebook-Likes: Persönliche Eigenschaften wie Alter, Geschlecht, sexuelle Orientierung, ethnische Zugehörigkeit, politische Einstellung, Beziehungsstatus oder Alkoholkonsum lassen sich mit hoher Treffsicherheit erschließen
- ZestFinance: Berechnung der Kreditwürdigkeit von Kunden
- Predictive Policing: Steuerung des Einsatzes von Polizeikräften nach Wahrscheinlichkeit, wo und wann zukünftig Straftaten stattfinden, auf Basis der Daten von Fallakten

Macht der Algorithmen und Big Data

- Wie kann man sich vor der ungewollter Datensammelei schützen?
  - AdBlocker/ScriptBlocker für Browser installieren
  - Berechtigungen in Apps kontrollieren und ggf. entziehen
- Vollständige Abschottung jedoch nicht möglich
- Gesellschaftlicher und politischer Diskurs ist nötig, was Algorithmen dürfen und was nicht
- Algorithmen der Unternehmen müssen transparenter werden

Das „Privacy Paradoxon“

- Soziale Netzwerke ermutigen Nutzer, **private Informationen preiszugeben**
  - Profilinformationen: Voller Name, Wohnort, Telefonnummer, Geburtsdatum, Arbeitgeber, Schulabschlüsse, Foto, ...
  - Interessen: Facebook „Likes“
  - Freunde und Familienmitglieder
  - Persönliche Meinungen („Timeline“)
- **Privacy Paradoxon**
  - Nutzer sozialer Netzwerke geben **bereitwillig** ihre private Informationen preis („**Selbstoffenbarung**“)
  - Dennoch haben diese Nutzer **gleiches (hohes!) Bedürfnis nach Privatsphäre**, wie diejenigen, die soziale Netzwerke ablehnen

Das „Privacy Paradoxon“

Gründe für Privacy Paradoxon bei Nutzung sozialer Netzwerke

- Gefühlt viele Vorteile, Nachteile nicht offensichtlich
  - Nutzer sozialer Netzwerke machen überwiegend Erfahrung, dass Preisgabe privater Informationen fast immer ohne (direkte) negative Konsequenzen bleibt
  - Veröffentlichte Details aus Privatleben führen oft zu positivem Feedback („Likes“), Zuspruch oder Anteilnahme aus der Community
- Mangelndes Problembewusstsein
  - Nutzer wissen oft nicht, was mit ihren Daten geschieht
  - Bewusstsein, dass mit Daten für „kostenlose“ Leistung bezahlt wird, ist oft nicht vorhanden

Verletzung der Privatsphäre durch Dritte

Soziale Netzwerke erlauben oft Einschränkung der Sichtbarkeit preisgegebener Informationen auf bestimmte Empfängergruppen

- Aber: Durch Interaktion berechtigter Empfänger mit geteilten Inhalten können auch weitere Personen Zugriff erlangen
  - Beispiel:
    - Nutzer X teilt Information mit seinen Freunden
    - Nutzer Y aus Freundesliste kommentiert Information
    - Nutzer Z ist mit Y bekannt aber nicht mit X
    - Nutzer Z sieht: Y hat Information von X kommentiert
    - Z erlangt so Zugriff auf Information auch von X (X ➔ Y ➔ Z)
- **Vorsicht:** häufig nicht einfach zu durchschauen, wer auf welche preisgegeben Information Zugriff erhält

Mögliche Nachteile durch Selbstoffenbarung

Preisgabe privater Informationen kann **handfeste Nachteile** haben

- Zugang „unerwünschter" Personen zu privaten Informationen
  - 60% der US-Arbeitgeber recherchieren Bewerber in sozialen Netzwerken
  - 49% dieser Arbeitgeber fanden Informationen, die dazu führten, Bewerber nicht einzustellen

    (Quelle, www.careerbuilder.com, Apr. 2016)
- Informationsressource für Angriffe durch ➔ **Social Engineering**
  - Erraten von Passwörtern (➔ **Passwortsicherheit**)
  - Diebstahl digitaler Identitäten
- Überwachung durch Betreiber des sozialen Netzwerks
  - Betreiber kann Internet-Bewegungsprofil des Nutzers erstellen
  - eventuelle Weitergabe des Bewegungsprofils an Dritte

Social Engineering

Grundidee: Angreifer kontaktiert Opfer, gibt sich als Techniker oder Systemadministrator aus und versucht, Zugangsdaten (Passwörter) zu erlangen

Beispiel: Angreifer erlangten Zugang auf privaten Email-Account von ehemaligem CIA-Direktor John Brennan (Identitätsdiebstahl)

- Hacker kennt Handynummer des Opfers, stellt fest, zu welchem Provider (Verizon) dieser gehört (durch Reverse Lookup)
- Hacker gibt sich bei Verizon-Support erfolgreich als Verizon-Techniker aus, der Kundendaten benötigt – erhält z.B. letzte vier Stellen des Bankkontos
- Hacker gibt bei AOL-Support an, Passwort vergessen zu haben und kann mit Verizon-Daten die Sicherheitsfragen beantworten
- Passwort wird zurückgesetzt
- Angreifer hat 3 Tage lang Zugriff auf Email-Konto

Social Engineering: Phishing und Spear Phishing

Phishing = Password Fishing

- Technik zur betrügerischen Erlangung von sensiblen Informationen
- Typisches Vorgehen: Versand betrügerischer Emails
  - Versand mit vertrauenswürdig wirkender Absenderadresse, z.B. Bank, Unternehmen, Behörde, …
    - Absenderadresse wird ausgewählt nach Information, die erschwindelt werden soll
    - Emailadressen können leicht gefälscht oder vorgetäuscht werden („Email Spoofing“)
  - Mit dem dadurch erlangten Vertrauen wird erwünschte Nutzerreaktion hervorgerufen
    - Herausgabe von Daten, z.B. Benutzernamen und Passwörter
    - Installation von Schadsoftware

Social Engineering: Phishing und Spear Phishing

Gute Nachricht: Diese Art „herkömmlicher" Phishing- Angriffe wird heute von vielen Internetnutzern als solcher erkannt und läuft dadurch ins Leere

Schlechte Nachricht: Personalisierte Phishing-Angriffe, sogenanntes **Spear Phishing** ist auf dem Vormarsch

- Angreifer sammelt detaillierte Informationen über sein Opfer
- Hilfreich für vorgetäuschte Vertrauenswürdigkeit, z.B. Agieren unter Identität einer Person, die Opfer kennt und der es vertraut
- Opfer denkt, dass Email von vorgetäuschtem Absender kommt, weil Nachricht Informationen enthält, die eigentlich nur dieser Absender kennen kann
- Erfolgsaussichten bei dieser Masche sind sehr hoch, aber auch für Angreifer ist Aufwand deutlich höher als beim herkömmlichen Phishing

Social Engineering: Vertrauen und vertrauliche Informationen

Grundidee von Social Engineering-Attacken basiert auf Missbrauch von **Vertrauen**

- Opfer vertraut Angreifer, da dieser **vertrauliche Informationen** hat, die eigentlich nur Mitglieder eines **vertrauenswürdigen Kreises** haben

Wie erlangt Angreifer vertrauliche Informationen?

- Klassische Technik: **Dumpster Crawling** – Angreifer durchsucht Mülltonne des Opfers nach Briefen, Abrechnungen, Kontoauszügen, …
- Informationstechnischer Ansatz: Hacken des Computers eines Opfers
- **Viel einfacher:** Einsammeln der freiwillig preisgegebenen Informationen aus den sozialen Netzwerken

Passwortsicherheit

Auch **Angriffe auf Passwörter** können durch persönliche Informationen aus Social-Media-Profilen erleichtert werden

- Verbreitet: **Password Guessing** – Erraten von Passwörtern
  - Angreifer probiert wahrscheinliche Passwörter zu einem Account durch
  - Angriffstools arbeiten mit Wortlisten und Wörterbüchern
- **Problem**: Nutzer wählen gerne (immer gleiche/ähnliche) Passwörter, die sie sich leicht merken können, z.B.
  - Begriffe oder Daten aus persönlichem Umfeld
  - Geburtsdaten, Namen, Begriffe im Zusammenhang mit Interessen (Lieblings-Romanfigur, -Band, -Filmtitel, ...)
  - Persönlich Informationen der Opfer helfen Angreifer, kann z.B. **Wortlisten personalisieren** ➔ Trefferwahrscheinlichkeit steigt

Passwortsicherheit

Beispiel:

- Nutzer gibt auf Facebook an, Fan von „Star Trek" zu sein
- Angreifer kann spezielle (fertig erhältliche) Wortliste mit allen Begriffen aus Star Trek-Universum verwenden
- Ähnliche Wortlisten auch verfügbar z.B. für „Herr der Ringe", „Game of Thrones", Monty Python-Filme und -Serien, ...

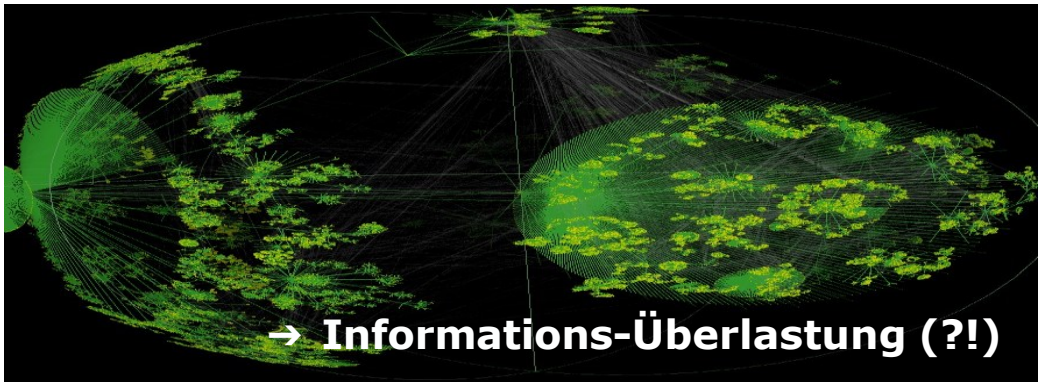
Informationen aus Social Networks nicht nur hilfreich beim Knacken (Raten) von Passwörtern, sondern insbesondere auch für sogenannte **Sicherheitsfragen** zum Zurücksetzen von Passwörtern, z.B.

- Mädchenname der Mutter
- Erstes Automodell
- Straße der ersten Wohnung
- Teile von Kreditkarten- oder Kontonummern

Beschränkungen des World Wide Web

Erinnerung: Das WWW erlaubt Zugriff auf enorme Menge an Informationen

- Es gibt Milliarden von WWW-Dokumenten – allerdings ist nur ein kleiner Teil von Suchmaschinen indexiert
- Außerdem können Milliarden von Dokumenten im *Deep Web* gefunden werden
- Die Menge der Dokumente im WWW verdoppelt sich alle 6 Monate



Beschränkungen des World Wide Web

Relevante Informationen?

- Was ist **wichtig**, was nicht?
- Was ist **Information**, was ist Werbung?
- Was ist **Bedeutung** der Information?
- Wie **glaubwürdig** ist die Information?
- Was gehört **zusammen**?
- Welche Teile sind eigentlich **überflüssig**?

Beschränkungen des World Wide Web

- Menschliche Nutzer haben **kontextuelles Wissen / Allgemeinwissen** und können daher die (meisten) Informationen korrekt interpretieren
- Ein **Roboter** (Programm) kann nicht zwischen wichtigen und unbedeutenden Informationen unterscheiden, da es **Bedeutung nicht versteht**
- Roboter braucht Informationen über Bedeutung eines Dokuments und seiner verschiedenen Teile (**Metadaten**)

- WWW wurde ursprünglich **für Menschen entwickelt**
- Technologie hinter dem WWW ist Markup-Sprache HTML
- HTML und CSS beschreiben
  - wie Informationen **strukturiert** und **dargestellt** sind
  - wie Informationen **verlinkt** werden können
  - aber **nicht Bedeutung** der Informationen (**Semantik**)

Semantik

Semantik ist Teilgebiet der **Linguistik**, dass sich mit

- **Sinn** und
- **Bedeutung**

von **Sprachen** und **linguistischen Symbolen** beschäftigt Semantik

versucht Frage zu beantworten, wie

- Sinn und Bedeutung von komplexen Begriffen abgeleitet werden können von Sinn und Bedeutung einfacher Begriffe

Semantik baut auf **Syntax** auf

- **Kommunikation** benötigt ein allgemeines Verständnis von **Syntax** und **Semantik** der ausgetauschten Sprachsymbole und Zeichenketten

➔ Gegenseitiges **Verständnis** ist nur möglich, wenn Sender und Empfänger die **identische Semantik** vereinbart haben

Problembereich 1: Suche nach Informationen

Schlüsselwort-basierte Suche

- Ruft viele **irrelevante** Ergebnisse ab
  - verschiedene Bedeutungen (Homonyme)
  - anderer Kontext
- Kann nicht **alle relevanten** Ergebnisse finden
  - Synonyme
  - Mangel an präzisem Kontext

Anforderung:

➔ Einführung einer formalen Terminologie / **Ontologie** (Explizite formale Spezifikation einer gemeinsamen Konzeptualisierung)

Eine Ontologie besteht aus:

- Taxonomie, d.h. eine Hierarchie von Konzepten
- sprachlichen Beschreibungen, z.B. OWL

Problembereich 2: Informationsextraktion

- Nur Menschen können Informationen korrekt extrahieren
- Software (Roboter) fehlt
  - kontextuelles Wissen
  - Allgemeinwissen

  wird benötigt, um Informationen aus ihrer Text- oder Bild-basierten Darstellung zu extrahieren

Anforderung:

➔ **Aggregation und Integration von Informationen** aus verschiedenen Quellen

Vision für das Semantic Web

Tim Berners-Lee – Erfinder des WWW – im September 1998:

- „Das Web war als Informationsraum entworfen worden, mit dem Ziel nicht nur für Mensch-zu-Mensch Kommunikation nützlich zu sein, sondern auch, dass es Maschinen möglich ist, sich zu beteiligen und zu helfen."

- **HTML** als Sprache zur Strukturierung von Informationen im WWW fehlt es an Möglichkeiten, die Bedeutung der Informationen auszudrücken

Potenziale des Semantic Web

Beispiel 1: Suchmaschinen heute

Suchanfrage: „Golf von 2015“

Nutzer muss Anfrage verfeinern, da Ergebnisse mehrdeutig sind

- Anfrage zu „Golf“:
  - Auto oder Sport oder sonstiges? ➔ Verfeinerung: Auto
- Anfrage zu „2015“:
  - Jahr der Konstruktion oder technischer Parameter?
    ➔ Verfeinerung: Jahr der Konstruktion
- Anfrage zu „Golf von 2015“:
  - Verkaufsangebot, Handbuch oder sonstiges?
    ➔ Verfeinerung: Handbuch
- ...

Suchmaschine muss Nutzer nach Bedeutung der Anfrage fragen

Potenziale des Semantic Web

Beispiel 1: Suchmaschinen von morgen

Suchanfrage: „Golf von 2015"

Suchmaschine „kennt" den Nutzer

- Nutzer überprüft in letzter Zeit regelmäßig Ergebnisse von professionellen Golf-Turnieren
- Nutzer hat online im letzten Jahr Golfschläger gekauft
- Nutzer hat News-Gruppe „en.rec.golf.balls" abonniert
- Nutzer hat Bildschirmhintergrund „PGA Tour 2014" gewählt
- Nutzer besitzt die Domain www.thegolffanatic.com
- …

Suchmaschine kann anhand dieses Wissens Bedeutung der Anfrage erschließen und richtig beantworten ...

Ziele des Semantic Web

- Automatische Organisation von Wissen in der jeweiligen Domäne
- Bereitstellung automatisierter Werkzeuge für Wartung, Entfernung von Inkonsistenzen oder Extraktion von neuem Wissen
- Ersetzung der Schlüsselwort-basierten Suche durch Inhalts-basierte Suche mit „intelligenten“ Frage- und Antwort-Zyklen
- Nutzerfreundliche Suche
- Extraktion und Darstellung von Wissen
- Beantwortung von Fragen zu über verschiedenen Dokumente verteilte Informationen
- Exakte Bestimmung, wer auf welche Teile einer bestimmten Information zugreifen kann

Technische Realisierung des Semantic Web

- Realisierung des Semantic Web benötigt Anzahl von Technologien für jeweils verschiedene Zwecke:

- Jede Informations-Quelle im Semantic Web benötigt eine eindeutige Kennung
  ➔ **URI**
- Informationen im Semantic Web müssen formal ausgedrückt werden, um automatisiert verarbeitet werden zu können; dazu wird einheitliche Syntax gebraucht
  ➔ **XML, XMLSchema**
- Einfache semantische Beziehungen zwischen Informations- Entitäten müssen ausgedrückt werden können
  ➔ **RDF (Resource Description Framework), RDFSchema**

Technische Realisierung des Semantic Web

- Verschiedene Semantiken müssen beschreib- und erklärbar sein, um auch scheinbar inkonsistente Informationen kombinieren zu können

  ➔ **Ontologien**

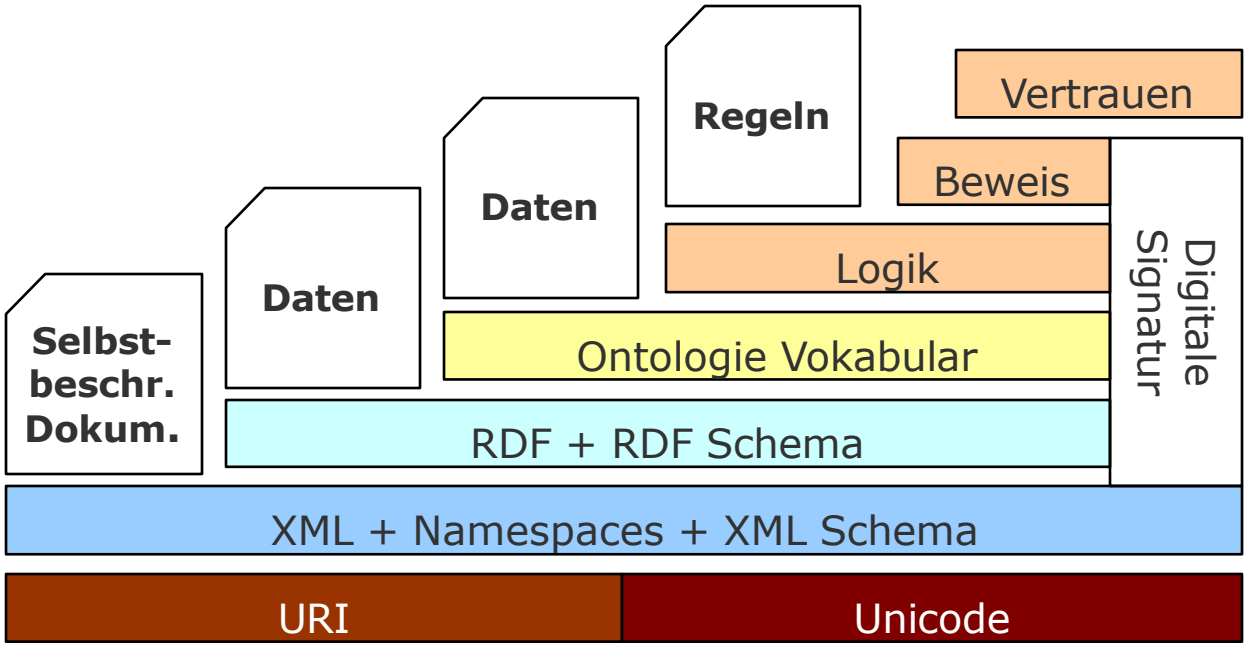
- Neue Information (Wissen) muss aus vorhandenen Informationen abgeleitet werden können

  ➔ **Inferenz-Mechanismen**

- Datenschutz (in Bezug auf Vertraulichkeit und Integrität) muss gewährleistet werden können

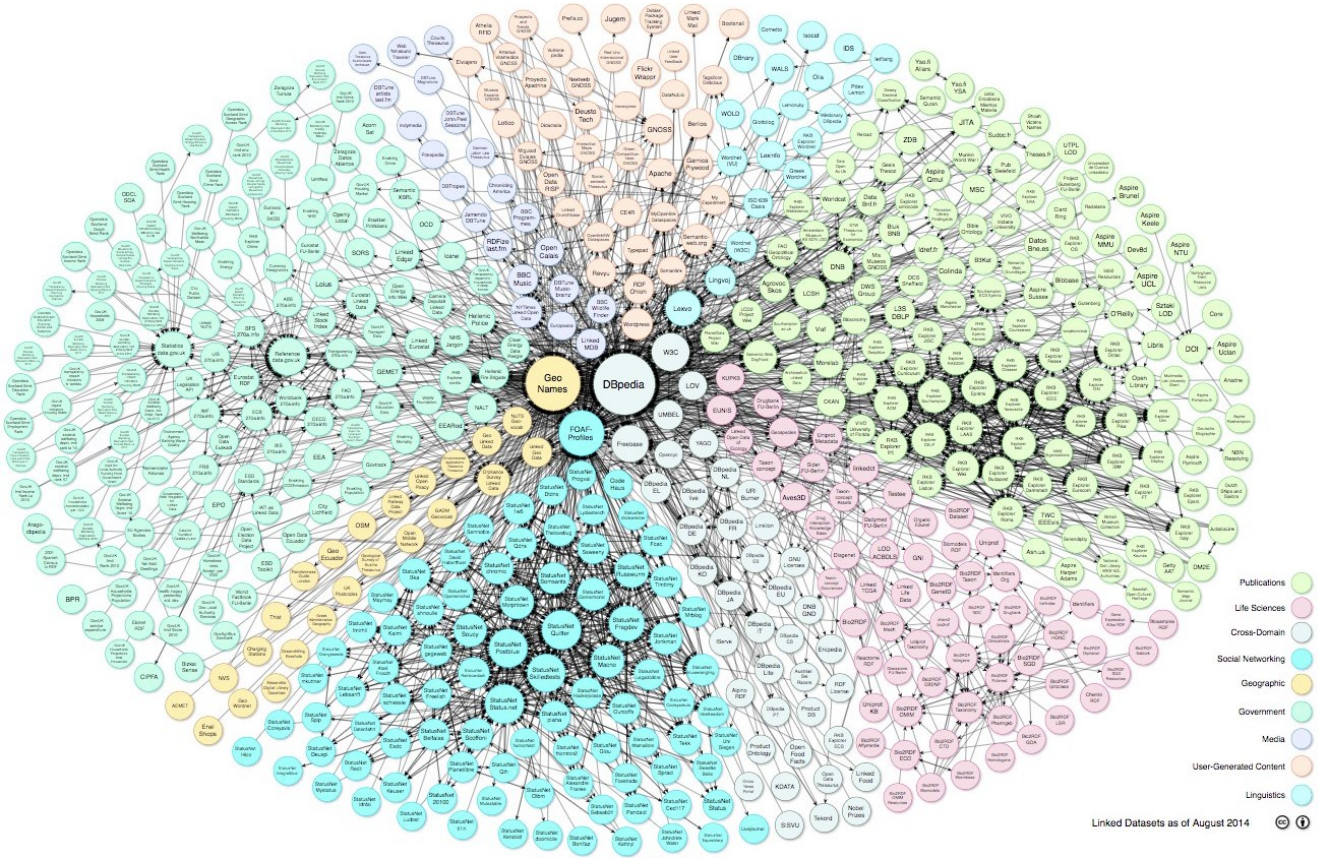
  ➔ **XMLEncryption and XMLSignature**

Semantic Web – Technology Stack



Linked Open Data

- Weltweites Netzwerk im Web frei verfügbarer Daten, die automatisiert von Programmen verarbeitet werden können
- Werden per URI und HTTP abgefragt
- Meist per RDF beschrieben und verlinkt, semantisch abfragbar per SPARQL
- Damit auch Teil des Semantic Web
- Bekannte Datensätze:
  - DBpedia: Extrahierte Informationen aus Wikipedia
  - FOAF: Datensatz über Personen und ihre Beziehungen
  - GeoNames: Informationen über Orte und deren Position


Geo Names
DBpedia
FOAF-Profiles
Publications
Life Sciences
Cross-Domain
Social Networking
Geographic
Government
Media
User-Generated Content
Linguistics
Linked Datasets as of August 2014

Digitale Transformation

Entwicklung der digitalen Technologien – „Digitale Revolution" – treibt **digitale Transformation** in allen Bereichen unserer Gesellschaft

- **Digitale Technologien** sind charakterisiert durch
  - breite Verfügbarkeit von Computern, Smartphones, Tablets, Programmierbaren Controllers und vielen neuen Smart Devices
  - **Internet** – als universelle globale Kommunikationsplattform
- Internet entwickelt sich immer mehr zum **Internet der Dinge – IoT**, in dem nicht nur Menschen sondern auch Dinge angesprochen und untereinander interagieren können
  - **Dinge werden smart** – bekommen digitale Hülle –, so dass sich neben der physikalischen Interaktionsebene eine neue, digitale Interaktionsebene etabliert

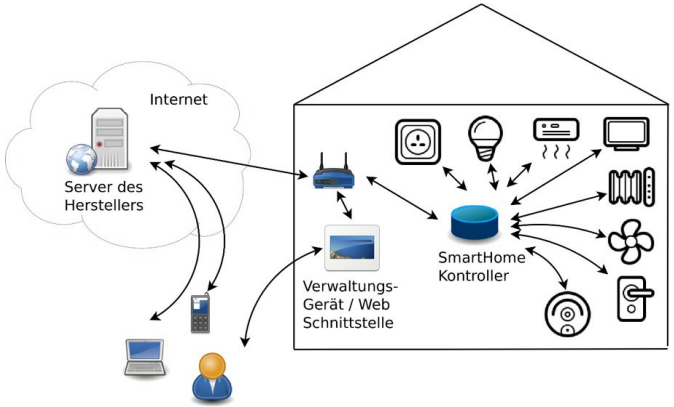
Digitale Transformation in der Wirtschaft: Trends und Herausforderungen

- **Trends**
  - Verbindung von industriellen Netzwerken mit dem Internet
  - Zusätzliche, oft drahtlose, Sensoren und Aktuatoren
- **Herausforderungen**
  - Umgang mit Ressourcenbeschränkungen
  - um Größenordnungen unterschiedliche Reaktionszeiten
  - Sicherheit in alles Aspekten
  - Kombination von Informatik mit Elektrotechnik, Maschinenbau, Automatisierungstechnik, …
- Interaktion mit industrieller Technik (genauer: deren digitaler Hülle) erfordert Schnittstellen, auf die über Internet zugegriffen werden kann ➔ **Webservices** als mögliche Technologie

Digitale Transformation: Smart Home

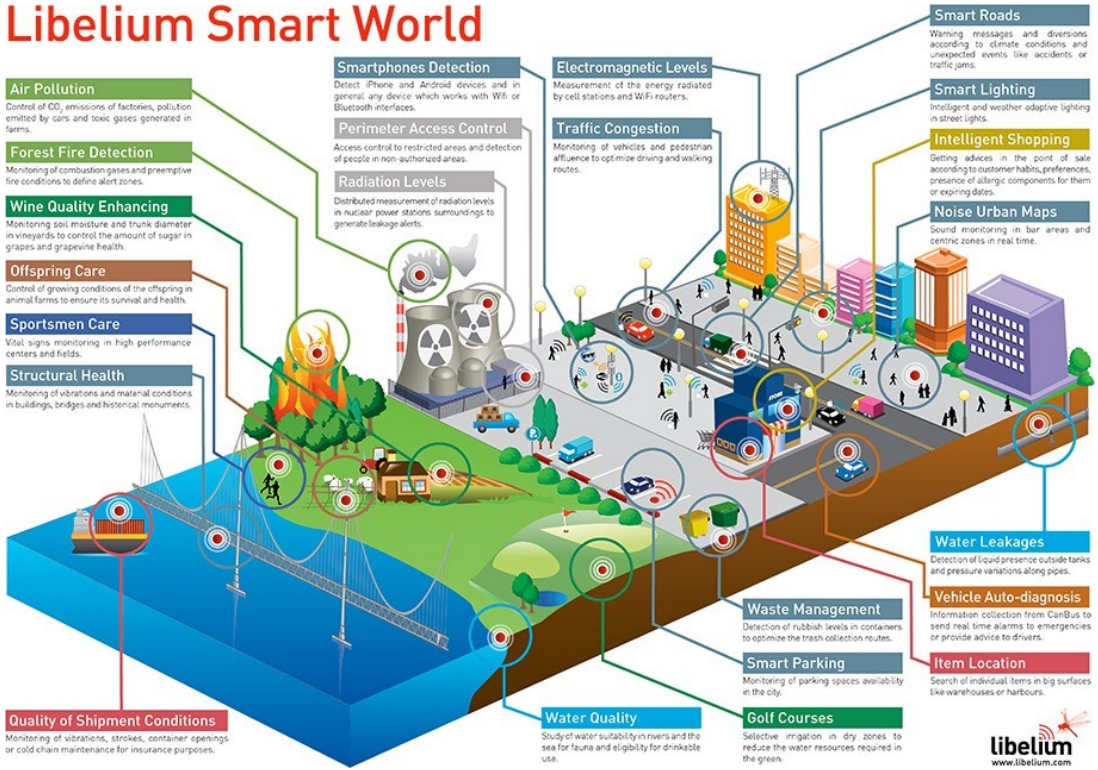
Smart Home – weiterer Anwendungsfall für Internet der Dinge: Steuerung von vernetzter Haustechnik mithilfe von Controllern

- Physikalische Systeme in Häusern / Wohnungen erhalten digitale Hülle
  - Licht- und Unterhaltselektronik
  - Heizung und Klimaanlagen
  - Fenster und Türen
  - Alarmanlage
  - Jalousien



- Viele Smart Home Lösungen nutzen Cloud-Technologie, um Verwaltung der Haustechnik für Nutzer zu erleichtern

Digitale Transformation:
Alles mündet in die Vision einer Smart World



http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking

Internet der Dinge und Webservices

Ressourcen im Web sind nicht mehr nur Dokumente, sondern verstärkt auch **physische Geräte**, die über **Webservice** Technologien **digitale Schnittstellen** anbieten

- Menschen können über (Web-)Anwendungen mit Geräten interagieren, z.B. Steuerung der Heizung im Smart Home
- Maschinen interagieren auch untereinander, z.B. kann Jalousiensteuerung im Smart Home den Webservice eines Wetterdienstes nach Vorhersagen abfragen

Digitale Transformation eröffnet **riesige Potenziale** neuer Möglichkeiten, bringt aber auch **Herausforderungen** mit sich

- Kleine Smart Devices (z.B. Sensoren) müssen **energiesparend** gebaut werden ➔ **schlanke Kommunikationsprotokolle**
- Nachdenken über **Sicherheit** und **Schutz der Privatsphäre** muss vor Hintergrund der Smart World noch mehr in den Fokus rücken

Smart Cars – ein spektakulärer Angriff: Der „Chrysler Hack“

Sicherheitsforscher Miller und Valasek demonstrieren für WIRED Magazin Übernahme eines modernen SUV

1. Angreifer können Internet-Adresse des Autos feststellen und verbinden sich damit über dessen Internetanbindung
2. Über verschiedene Sicherheitslücken und Schwächen im Design gelingt es ihnen, das Car Entertainment System zu übernehmen und von dort auf internes Bordnetzwerk zuzugreifen
3. Weitergehende Manipulation der Software des Fahrzeugs erlaubt umfassende

   „Fernsteuerung“

Smart Cars – ein spektakulärer Angriff: Der „Chrysler Hack“

Den Angreifern war es möglich:

- Klimaanlage zu manipulieren
- Soundsystem zu bedienen
- Wischer, Lichter, etc. zu steuern
- GPS-Position und Geschwindigkeit auszulesen
- **Gaspedal und Bremse zu bedienen**
- Motor abzuwürgen
- Lenkung teilweise zu bedienen (derzeit nur im Rückwärtsgang)

(Vernetzte) Computersysteme haben Schwachstellen und können über das Internet massiv manipuliert werden!

IoT und Smart World – Angriffe auch auf die physikalische Welt

- Früher zielten Hacker-Angriffe meist auf rein digitale Systeme oder auf Nutzer des Webs ab
- Integration digitaler Komponenten in physikalische Systeme (etwa bei Smart Factory oder im Smart Home) macht auch Cyberangriffe auf physikalische Systeme möglich
  - unberechtigtes An-/Abschalten
  - Auslesen von Daten oder Veränderung von Konfigurationen
  - Beschädigung oder Zerstörung der Systeme
- Angriffe können nicht mehr „nur" Daten, Reputation oder finanzielle Ressourcen treffen, sondern auch Maschinen oder gar die Unversehrtheit von Menschen – wie im Fall des Auto-Hacks – werden zu direkten oder mittelbaren Zielen von Cyberattacken

Risiken für das Smart Home – Smart Meter

Smart Meter sind Verbrauchsmesser („Meter“) für Strom, Gas, Wasser mit Netzanschluss

- Analoge Verbrauchsmesser werden 1-2 mal pro Jahr abgelesen
- Smart Meter sind ständig mit Energie-Anbieter verbunden und schicken ihm Messwerte zu
- Anbieter erkennt zeitnah Energiebedarf und kann diesen z.B. über Tarifgestaltung optimieren (Strom in der Nacht günstiger, …)
- Bilanzierungsprozesse, Prognosen, Rechnungserstellung, … werden erleichtert
- Typischerweise eröffnen Smart-Tarife dem Verbraucher auch Sparmöglichkeiten
- Detaillierte Informationen über Energie-Nutzung in einem Haushalt sagt viel über Bewohner aus (Schlafzeiten, Waschzeiten, Personen im Haus, Kochzeiten, …)
- Smart Meter ermöglicht dem Energie-Anbieter – und damit auch Angreifern – auch Fernabschaltung der Energieversorgung

Risiken für Smart Factory und Industrie 4.0

Industrielle Anlagen waren bisher **isolierte Systeme**

- Steuerungsanlagen (PLCs) für physikalische Maschinen und industrielle Netzwerke auf Zuverlässigkeit und sicheren Betrieb ausgelegt
- Keine Verbindung mit anderen Unternehmensnetzwerken und dem Internet

Industrie 4.0 und Smart Factory bedingen **hochvernetzte Anlagen**
➔ dadurch **anfälliger für Cyberattacken**

- Datendiebstahl
- Spionage
- DoS-Attacken (Denial of Service – Ziel: Betriebsschädigung und Außerbetriebnahme von Anlagen)
- Malware (Viren, Würmer, Trojaner)

Zusammenfassung

- IoT, Smart World, hochgradige Vernetzung und weitergehende Durchdringung unserer Gesellschaft mit (Web-)Anwendungen läuten **neues technologisches Zeitalter** ein (4. industrielle Revolution)
- Digitale Transformation birgt aber gleichzeitig **hohes Gefahrenpotential** für Industrie und Gesellschaft
  - neue Arten von Angriffen, nicht nur auf digitale Systeme
  - inhärent Verletzung der (digitalen) Privatsphäre, bis hin zu deren faktischer Abschaffung
- Sicherheit und Datenschutz sind **zentrale Herausforderungen**, denen sich Forschung, Politik, Wirtschaft – aber auch **jeder einzelne** – stellen muss
  - Schaffung geeigneter politischer Rahmenbedingungen
  - Bereitstellung technischer Hilfsmittel
  - Sicherheitsbewusstsein

Rückblick

1. Einführung, URIs und HTTP(S)
2. Markup Languages (XML, SGML, HTML)
3. Cascading Stylesheets und RWD Basics
4. AWD/RWD in-depth, CSS Framework und Präprozessoren
5. Erste Einheit clientseitige Web-Programmierung (DOM, JavaScript, ECMA, Datenstrukturen, Event, Bedingungen, Schleifen)
6. Zweite Einheit clientseitige Programmierung (AJAX, WebSockets, JSON) und Grundkonzepte serverseitige Programmierung (Ansätze, Frameworks, Datenhaltung)
7. Ausgewählte Frameworks und Bibliotheken, Serverseitige Programmierung mit PHP
8. Best Practices der Front-End Entwicklung, Codeoptimierung, Usability&UX Testing
9. Das Web von Morgen

Kursresumé
URI und HTTP(S)

World Wide Web ist **verteiltes Hypermedia-System**, untereinander verlinkte Web-Dokumente liegen weltweit auf verschiedenen Servern

- Zum Abruf der Dokumente wird eindeutiges Adressierungsschema benötigt
  - Jedes Dokument braucht (mindestens) einen **Uniform Resource Identifier – URI**
  - URI meist als **Uniform Resource Locator – URL** – realisiert, Identifikation von Ressourcen erfolgt über deren „Adresse" (Domain Name des Server, Pfad auf dem Server, Dateiname)
- Anforderung und Übertragung der Dokumente erfolgt mit **Hypertext Transfer Protocol – HTTP**
  - HTTP bietet einfaches Frage-Antwort-Schema (Request / Response), mit dem Clients (Browser) bei Servern Dokumente anfordern können

Kursresumé
URI und HTTP(S)

- Erweiterungen für HTTP verbessern Performance:
  - **Persistente Verbindungen** und Pipelining
  - **Kompression**
  - **Caching** (in Clients, Servern und Zwischensystemen – Proxies)
- Überwindung der Zustandslosigkeit von HTTP mittels **Sessions und Cookies** für Web-Anwendungen möglich
- Browser und Server können Auslieferung von Content-Varianten aushandeln – **Content Negotiation**
- Nach über 25 Jahren wird mit **HTTP/2** derzeit Nachfolger für das zentrale Web-Protokoll eingeführt

Kursresumé
HTML, CSS und XML

Dokumente im WWW werden mit HTML und CSS beschrieben

- Trennung von Struktur und Gestaltung
  - **Hypertext Markup Language – HTML** – für strukturierte Aufbereitung des Dokumenteninhalts
  - **Cascading Stylesheets – CSS** – für Gestaltung der Darstellung von Dokumenten auf verschiedenen Ausgabegeräten
- HTML führt **Hyperlink**-Konzept ein
- HTML-Dokumente bestehen aus
  - Head: Informationen *über* den Inhalt (Metainformationen)
  - Body: eigentlicher Inhalte
- HTML ist **Markup-Sprache**: Strukturgebende Markups („Tags“) sind Teil des Dokumenteninhalt und werden durch Markup-Trenner (<. . .>) gekennzeichnet

Kursresumé
HTML, CSS und XML

- Aktuelle Version **HTML 5** führt „sprechende" Strukturelemente, Multimedia-Tags, neue Formular-Funktionen und Zeichenfläche (Canvas) ein
- CSS-Regeln legen fest, welche HTML-Elemente wie gestaltet werden sollen
  - **Selektoren** wählen zu gestaltendes Element aus
  - **Deklarationen** weisen bestimmten Gestaltungsmerkmalen einen Wert zu
- **Responsives Webdesign** sorgt dafür, dass Webseiten automatisch an spezifische Anforderungen der verschiedenen Endgeräte (Desktop, Smartphone, Tablet, ...) angepasst werden
- **Extensible Markup Language – XML** ist (wie SGML) Meta-Markupsprache, also Sprache zur Beschreibung von Sprachen

Kursresumé
Web-Programmierung

Komplexere Nutzerinteraktion im Web und Web-Anwendungen werden mittels Web-Programmierung realisiert

- Wir unterscheiden **clientseitige** und **serverseitige** Web-Programmierung
- Bei clientseitiger Web-Programmierung wird Programmcode mit Webseite ausgeliefert und dann **im Browser ausgeführt**
- **Document Object Model – DOM** – bietet Schnittstelle für die Manipulation von HTML-Elementen
- Bei serverseitiger Web-Programmierung wird **Programm auf dem Server ausgeführt** und Ausgabe (z.B. HTML-Dokument) an Browser zur Anzeige ausgeliefert
- Für **Kodierung von Informationen** (Text, Grafik, Multimedia) zur Übermittlung im Web gibt es spezifische Anforderungen und Formate

Kursresumé
Clientseitige Web-Programmierung

JavaScript ist das wichtigste Werkzeug für clientseitige Web-Programmierung

- JavaScript (standardisiert als ECMAScript) ist Skriptsprache zur Manipulation von HTML-Elementen
- Für viele gängige Anwendungsfälle gibt es umfangreiche **Bibliotheken** und **Frameworks**, z.B. jQuery oder D3
- Auch für CSS gibt es Reihe an Frameworks, die wiederkehrende Aufgaben vereinfachen
  - **CSS-Präprozessoren** erweitern CSS-Syntax, z.B. um Variablen und Funktionen
- **AJAX** – **Asynchronous JavaScript and XML –** erlaubt Kommunikation zwischen clientseitiger Web-Anwendung und Servern, z.B. zur hintergründigen Anfrage zusätzlicher Ressourcen

Kursresumé
Serverseitige Web-Programmierung

Viele Aufgaben der Web-Programmierung – insbesondere solche, bei denen große Datenmengen zu verarbeiten sind – werden auf dem Server gelöst

- Webserver ruft **serverseitiges Programm** auf (z.B. über **CGI-Schnittstelle**) und übergibt Anfrageparameter aus dem HTTP-Request
- Programm auf dem Server wird ausgeführt, erzeugt **parameterabhängige Ausgabe**, z.B. als **HTML** oder **JSON**, und gibt diese an Webserver zurück (der diese als HTTP-Response an Client ausliefert)
- Serverseitige Web-Programmierung basiert heute fast immer auf mächtigen **Web-Frameworks**, z.B. Ruby on Rails oder Django

Kursresumé
Serverseitige Web-Programmierung

- Daten auf dem Server werden **in Datenbanken persistiert** und über Web-Framework mit **Object Relational Mapper – ORM** – abgefragt
  - **Relationale Datenbanken:** Fixe Datenstruktur (Tabellen), hohe Datenkonsistenz
  - **NoSQL-Datenbanken:** Flexible Datenstruktur, leichter zu skalieren, Konsistenz schwieriger zu gewährleisten
- **Web Services** ermöglichen **Kommunikation zwischen** unterschiedlichen **Web-Anwendungen** und erlauben so Realisierung verteilter Applikationen

Kursresumé
Best Practices, Codeoptimierung, Testing

- Ziel ist es ein technisches Optimum anzustreben, die größtmögliche Benutzerzahl zu erreichen, einen Wettbewerbsvorteil zu schaffen und zukunftsorientiert zu entwickeln
- Umsetzung durch Einhaltung von Best Practices (**Web Standards, Progressive Enhancement, Responsive Web Design**) und **iterativer Entwicklungsprozesse**
- Große Teile von Codeoptimierung werden durch Engine, Frameworks und (JIT) Compiler übernommen, dennoch gilt es einige Details zu beachten: **Critical Rendering Path, Garbage Collection, Repaints & Reflows, Memory Leaks, Animationen**, …
- **Unmoderated Remote Usability Testing** erhebt zusätzlich zu qualitativen Daten auch quantitative Messdaten, ist kostengünstig/agil/skalierbar und erreicht Nutzer in ihrem natürlichen Kontext

Kursresumé
Social, Semantic und Service Web

Soziale Netzwerke, das Semantic Web und Anwendungen für Web Services (z.B. im IoT Bereich) sind wichtige Themen für das Web von heute und morgen

- **Soziale Netzwerke** und **Social Media** sind aktuelle Killer-Applikationen des Webs
- Kritisch zu betrachten sind trotz oder gerade wegen der weitgehenden Verbreitung
  - Manipulationsmöglichkeiten bei der Meinungsbildung
  - Implikationen für Datenschutz und Sicherheit
- **Semantisches Web** verknüpft nicht länger nur Dokumente, sondern auch **Dinge** (Menschen, Orten, Ereignissen, ...) und setzt sie in **Beziehung**
  - **Bedeutung** einer Information wird auch erkennbar für Maschine

Kursresumé
Social, Semantic und Service Web

- **Internet of Things:** „Dinge" (physikalische Geräte, Sensoren, ...) erhalten „digitale Hülle" – können über Entfernung angesprochen werden oder auch miteinander kommunizieren
- **Smart Home, Smart Factory, Smart Traffic, ...** zeigen Visionen auf für mögliche Veränderungen dank digitaler Technologien
- **Sicherheit** und **Datenschutz** sind zentrale Herausforderungen für tiefergehende Verankerung der Smart-Technologien in der Gesellschaft

FH Salzburg

VO Web-Technologien

Einheit 9, Oliver Jung

Technik
Gesundheit
Medien