JUST DO IT
HÖHERE ABTEILUNG FÜR
INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

Ausarbeitung

Ethik

Systemtechnik-Matura
5BHIT 2015/16

Michael Weinberger

Version 1.0
Begonnen am 21. April 2016
Beendet am 01. Juni 2016

Betreuer: Graf/Borko

Inhaltsverzeichnis

1 Cloud Computing und Internet of Things **2**

1.1 Einführung . . . 2

1.2 Bedenken . . . 2

1.3 Formulierung ethischer Fragestellungen . . . 3

1.3.1 Versuch einer ethischen Urteilsfindung . . . 3

2 Automatisierung, Regelung und Steuerung **5**

3 Security, Safety, Availability **6**

3.1 Einführung . . . 6

3.1.1 Internet Security . . . 6

3.1.2 Hacking . . . 6

3.1.3 Cyber Crime . . . 7

3.1.4 Availability . . . 7

3.2 Bedenken . . . 7

3.3 Formulierung ethischer Fragestellungen . . . 8

3.3.1 Ethische Urteilsfindung . . . 8

4 Authentication, Authorization, Accounting **9**

4.1 Einführung . . . 9

4.2 Bedenken . . . 9

4.3 Formulierung ethischer Fragestellungen . . . 9

5 Disaster Recovery **10**

5.1 Einführung . . . 10

5.2 Bedenken . . . 10

5.3 Formulierung ethischer Fragestellungen . . . 10

6 Algorithmen und Protokolle **11**

6.1 Einführung . . . 11

6.2 Bedenken . . . 11

6.3 Formulierung ethischer Fragestellungen . . . 11

7 Konsistenz und Datenhaltung **12**

7.1 Einführung 12
7.2 Bedenken 12
7.3 Formulierung ethischer Fragestellungen 12

Kompetenzen für den Teilbereich 'Ethische Aspekte, Rechtliche Grundlagen und Gesellschaftliche Auswirkungen der Informationstechnologie'

- können die Interaktion zwischen Informationstechnik, Gesellschaft und Politik analysieren und in ihrer Arbeit beachten
- kennen rechtliche Grundlagen der Informationstechnologe und reflektieren Auswirkungen des Missbrauchs von Informationstechnologien
- beachten ethische Standards bei Datensicherheit, Datenschutz und Privatsphäre
- beachten ethische Grundwerte in der Sicherheits- und Überwachungstechnik

Diese Ausarbeitung orientiert sich auf der Theorie der Dokumente 'SYT Unterlagen Graf 1. Teil' und 'SYT Unterlagen Graf 2. Teil', und genannte werden folglich nicht weiter zitiert.

1 Cloud Computing und Internet of Things

1.1 Einführung

In den letzten Jahren geht der Trend immer mehr in Richtung Cloud Computing, dem Anbieten von verschiedensten IT-Dienstleistungen über das Netzwerk. Dieser Prozess funktioniert dynamisch und an den Bedarf des Nutzers angepasst. Die Grundlage der Cloud bietet das Internet als Plattform. Darüber werden Verbindungen zu externen Servern hergestellt, um Anwendungen bereitzustellen. Damit ist auch die Möglichkeit zur Datenspeicherung mit inbegriffen.
Der Benutzer muss die verschiedenen IT-Services (Software, Plattformleistungen, Infrastrukturleistungen) nicht mehr selber bereitstellen, sondern mietet diese kurzerhand. Die Anbieter bieten hier ein flexibles und dienstbasiertes Geschäftsmodell (Everything as a Service). Dieser Service ist nicht nur besser skalierbar und ausfallsicherer, sondern im Zweifelsfall auch billiger als ein großer Server-Verbund im eigenen Netzwerk.
Man unterscheidet zwischen öffentlichen und privaten Clouds. Die Public Cloud wird von der breiten Öffentlichkeit genutzt, sprich verschiedene Kunden. Die Private Cloud ist hiervon das Gegenteil, das Angebot ist auf einen bestimmten Kunden ausgerichtet und auf dessen interne Anwendungen beschränkt.
Als zweiter großer Bereich dieses Pools ist Internet of Things definiert. Internet of Things bezeichnet die Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgabe für den Besitzer erledigen können. Der Anwendungsbereich erstreckt sich dabei von einer allgemeinen Informationsversorgung über automatische Bestellungen bis hin zu Warn- und Notfallfunktionen. Als Beispiel, die Waschmaschine stellt fest, dass zu wenig Waschmittel im Haus ist, und bestellt dieses von selbst nach. Oder auch selbstfahrende Autos, die untereinander kommunizieren und so Staubildungen bestmöglich verhindern sollen. [1, 2]

1.2 Bedenken

Es ist zu bedenken, dass hier die (persönlichen) Daten auf fremden Servern liegen. Der Begriff Cloud ist für viele sehr abstrakt, und nicht näher definiert, wo die Daten schlussendlich landen. Es ist jedoch so, dass diese lediglich auf einem anderen Server landen, der von fremden Personen bzw. Unternehmen verwaltet wird und deren Handlungsspielraum unterliegt. Die Privatsphäre kann durch diese Vollmacht sehr einfach gebrochen werden, was auch zu einem Missbrauch der Daten führen kann. Ebenso ist fraglich (in AGBs meist definiert, aber für User unbekannt), ob die Daten in der Cloud auch an Dritte weitergegeben werden, beispielsweise zu Werbezwecken.
Durch Internet of Things kann ein besonders gutes Profil über einen Menschen erstellt werden. Diese Gegenstände, beispielsweise Fitnessarmbänder, können ständig den Gesundheitszustand mitloggen. Der gläserne Mensch wird dadurch immer mehr Realität, da, wie vorhin besprochen, nie restlos sichergestellt werden kann, wo diese Daten dann schlussendlich landen. Hier ist der sogenannte Begriff 'Data Mining' eine gute Erklärung, möglichst viele Daten generieren über einen Benutzer, um durch Algorithmen Zusammenhänge zu finden und Rückschlüsse auf das Verhalten zu ziehen.

1.3 Formulierung ethischer Fragestellungen

Wie zu sehen ist, gibt es hier vor allem einige Bedenken hinsichtlich des Datenschutzes und der Wahrung der Privatsphäre. Auch wenn den allgemeinen Geschäftsbedingungen zugestimmt wird (Statistiken zeigen, dass diese wirklich nur in Ausnahmefällen tatsächlich gelesen werden), räumt das dem Unternehmen aufgrund dieses Missstandes erweiterte Rechte ein? Natürlich stellt sich auch die Finanzierungsfrage, da (vor allem Internet-) Unternehmen meistens von personalisierter Werbung leben. So sollte eine Auswertung der Userdaten ethischen und auch allgemein gesetzlich gültigen, österreichischen Normen (Datenschutzgesetz 2000) entsprechen. Dies kann anonymisiert geschehen, ist jedoch immer eindeutig einer Person zuteilbar.
Auslegbar ist hier der Kategorische Imperativ: 'Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könnte'. Jeder Mensch soll als Zweck behandelt werden, und nicht als Mittel (zu Geld, Expansion, als Ressource). Ein ethisch orientiertes Unternehmen sollte die Menschenwürde weit über den Profit stellen. Denn moralisch zu handeln, bedeutet auch vernünftig zu handeln.
Im Bereich des Internet of Thing gilt ganz klar das Hedonismusprinzip. Die Tracking-Geräte, smarten Fernseher und Kühlschränke bieten Antworten auf Probleme, die es in dem Sinne eigentlich gar nicht gab. Diese befriedigen menschliche Bedürfnisse und Interessen, und erzeugen so ein quantitatives (nicht messbares) Glücksgefühl. Grundsätzlich gilt: Die Vernetzung von immer mehr Gegenständen ist praktisch, aber nicht allgemeinhin nötig. [3]

- Dürfen IT-Unternehmen die gesetzlichen Rahmenbedingungen vollständig ausnutzen, und den Verwender seiner Anwendungen immer mehr zum 'gläsernen' Menschen werden lassen?
- Dürfen IT-Unternehmen gesammelte Gesundheitsdaten (allgemein: sehr sensible persönliche Daten) mit Versicherungen, Regierungsbehörden, usw. austauschen?

1.3.1 Versuch einer ethischen Urteilsfindung

Hier wird versucht, zur zweiten oben genannten Frage kurz und bündig ein entsprechendes Urteil zu finden.

- Sachverhaltsdarstellung
  Der IT-Unternehmer stellt dem Benutzer einen Fitness-Tracker zur Verfügung, unter Zustimmung der AGB. Diese synchronisiert die gesammelten Daten mit den firmeneigenen Servern (Cloud), und liefert dem Benutzer täglich aktuelle Ergebnisse in Hinblick auf seinen Trainingsfortschritt. Der Benutzer leidet unter den Vorzeichen einiger gesundheitlicher Probleme, die in Zukunft mit etlichen Behandlungen tragend werden. Der Tracker registriert dies im Gesamtbild.
- Problemfeststellung
  Dürfen IT-Unternehmen (die Datenhoheit über die Daten besitzen) gesammelte Gesundheitsdaten mit Krankenkassen, Hausärzten oder Bankinstituten austauschen?
- Situationsanalyse
  Das Unternehmen kann durch die rechtlich legale Weitergabe seinen Erhalt finanzieren und

den Mehrwert für den Kunden aufrecht erhalten. Der Kunde jedoch könnte von seiner Versicherung schlechter eingestuft werden, und vielleicht auf Basis falscher Messungen mehr bezahlen. Möglich ist, dass der Benutzer keinen Kredit bewilligt bekommt, wenn ihn auch seine Bank schlechter einstuft.

- Prüfung der Verhaltensalternativen
  Ganz klar: Die Daten anonymisiert weitergeben, und eher mit anderen Unternehmen zusammenarbeiten. Auf Basis der Messungen könnte Werbung für Nahrungsergänzungsmittel, Vitamine, Fitnesscenter in der Nähe generiert werde. Dies würde ebenso den Erhalt finanzieren, und für den Kunden zu keinem Problem werden.

- Normenprüfung
  Als gut und richtig würde nur gelten, dass der Benutzer nicht für seinen Abstieg auch noch Geld bezahlt. Der oben erwähnte Kategorische Imperativ sollte Anwendung finden, um einen wirklich fairen Ablauf zu gewährleisten.

- Entscheidung
  Meine Antwort lautet: Nein. In dieser Form soll das Unternehmen nicht zu sehr auf seine Rechte pochen und dem Benutzer laufend Nachteile verschaffen.

2 Automatisierung, Regelung und Steuerung

Themengebiet wird ausgelassen (1 von 1)

3 Security, Safety, Availability

3.1 Einführung

3.1.1 Internet Security

Internet Security ist ein breiter Begriff, der zusammenfassend bedeutet seine persönlichen, sensiblen Daten im Internet möglichst gut zu schützen. Dieses Thema betrifft jede Aktion, die im Internet getätigt wird. Wie allseits bekannt birgt das World Wide Web auch gewisse Risiken, dessen wir uns in manchen Fällen nicht bewusst sind, entweder aus Leichtgläubigkeit oder Unwissenheit. Als Gegenmittel sind eine verschlüsselte Kommunikation oder komplexere Passwörter die ersten Ansätze für einen sicheren Umgang mit dem Internet.
Ein sorgsamer Umgang mit den eigenen Stammdaten ist heute mehr denn je gefragt. Wohnadresse, Handynummer oder ähnlich sensible Daten, die auf die eigene Identität Rückschlüsse zulassen sollten nicht achtlos jedem bekanntgegeben werden. Das Internet vergisst nicht, getätigte Schritte sind nur schwer wieder zu entfernen, wenn nicht gar unmöglich. Außerdem sollte beachtet werden, dass nicht alle Meldungen, die angezeigt auch tatsächlich der Wahrheit entsprechen. Sofern nicht fundierte Quellen vorliegen, sollte die sensationelle Mitteilung eher mit einer gewissen Skepsis betrachtet werden. Auch Gewinnspiele, vermeintliche Erbschaften aus Ghana und sonstige Spam-Mails führen in den meisten Fällen in die Betrugsfalle. Nicht jede Webseite ist vertrauenswürdig, auch wenn auf den ersten Blick nicht eindeutig, so ist es vergleichsweise einfach einem Cyber-Crime zum Opfer zu fallen, wenn beispielsweise gefälschte Bankseiten nahezu perfekt imitiert werden und währenddessen die Zugangsdaten mitspeichern. [4]

3.1.2 Hacking

Als Hacker wird allgemein jemand bezeichnet, der in Computersysteme eindringt. Sie beschäftigen sich vorrangig mit Sicherheitsmechanismen und deren Schwachstellen. Während der Begriff auch diejenigen beinhaltet, die Sicherheitslücken suchen, um sie aufzuzeigen oder zu korrigieren, wird er in der allgemeinen Öffentlichkeit häufiger für Personen benutzt, die unerlaubt in fremden Systemen solche Lücken ausnutzen. Dementsprechend ist dieser Begriff stark negativ belegt.
Es gibt einige technische Begriffe, die hier im Zuge relevant sind. Diese populären Techniken zielen vor allem auf schlecht abgesicherte Systeme ab, jeder zusätzliche Schutz erschwert das Leben eines jeden Hackers. Die einfachste Methodik ist das sogenannte Social Engineering, wo mit persönlichem Kontakt und zwischenmenschlicher Beeinflussung Personen zur Preisgabe von vertraulichen Informationen bewegt werden, der Mensch ist bekanntlich die größte Schwachstelle eines jeden Computersystems. Wie im vorherigen Kapitel beschrieben, ist das womöglich nützliche Gratis-Programm ein ‚Trojanisches Pferd', das im Hintergrund aber eine andere Funktion erfüllt, ohne Wissen des Anwenders. Ebenso gefährlich sind Backdoors, die es (oft vom Hersteller eingebaut) ermöglichen Zugang zu wichtigen Funktionen oder zu sonst nur geschützten Bereichen zu erhalten. Das klassische Computervirus von damals ist heute weitaus komplexer und kann nicht mehr als Einzelbegriff angesehen werden, da er sich wie beschrieben in viele Unterkategorien aufspaltet. An sich ist darunter ein Schadprogramm zu verstehen, dass sich selbst reproduziert wenn einmal ausgeführt, mit dem Ziel auf möglichst rasche Verbreitung, wie zum Beispiel auch auf Wechseldatenträger, die jenes auch auf andere Systeme ausbreiten lassen können. Eine andere Art ohne Ziel der Informationsbeschaffung ist das ‚destruktive' Hacking, etwa eine Denial of Service- Attacke, die durch Überlastung eines Servers mit Anfragen auf dessen rasche Außerstandsetzung abzielt.

[4]

3.1.3 Cyber Crime

Cyber Crime allgemein umfasst im Groben alle Straftaten, die unter Ausnutzung der Informationstechnik oder gegen diese begangen werden. Es gibt die Unterscheidung zwischen zwei Arten, die *Computerkriminalität*, welche einen Computer mit oder ohne Internetnutzung als Tatwaffe beinhalten sowie die *Internetkriminalität*, die mithilfe der Techniken des Internets durchgeführt wird. Hacking ist ein Paradebeispiel für ein Cyber-Crime, der Begriff Internet Security beschreibt, wie man sich möglichst gut davor schützen kann.
Das genaue Spektrum ist wie auch bei Kriminalfällen außerhalb der IT sehr weitläufig und lässt sich nur grob bzw. vereinzelt zu bestimmten Kategorien zuordnen, da es keinen festen Handlungsrahmen gibt, jedoch mit dem großen Unterschied, dass Menschen nicht körperlich, sondern höchstens psychisch beeinträchtigt werden können. Im Bereich Hacking genannte Praktiken sind allesamt (wenn unbefugt) hier zuzuordnen, nämlich illegal und strafbar. Immer wieder stoßen Gesetze an ihre Grenzen, dank des rasanten Fortschritts der Technologien müssen Gesetzestexte nicht selten um gewisse erweitert werden. Eines der Keywords in diesem Bereich ist etwa Phishing, wo mit täuschend echten Nachbauten von realen Webseiten Daten abgefangen werden können, die User eingeben. Spamming ist bereits seit Aufkommen der E-Mails ein anhaltendes Problem. Mithilfe von Schadcode-Attachments oder betrügerischen Absichten, etwa der Aufforderung einer Echtgeldüberweisung zum Erhalten einer Erbschaft, treiben Kriminelle seit Mitte der 90er ihr Unwesen. Mit Aufkommen der ersten Videostreamingplattformen finden auch sogenannte ‚Hate Crimes' immer mehr Anwendung mit dem Hochladen von Videos, die nur darauf abzielen eine Person öffentlich zu denunzieren. Dieses ist mit dem Begriff Cyberbullying zu beschreiben, der erst in diesem Jahrtausend erfunden werden musste. Eine ebenso verabscheuungswürdige Tat ist die Verbreitung von Kinderpornografie, die auch Ermittler zwecks Verfolgung vor große Herausforderungen stellt. [4]

3.1.4 Availability

Availability bedeutet: Ein Server, eine Anwendung soll immer und überall verfügbar sein. Durch Downtime, etwa verursacht durch Hacking auch mit den verbundenen Datenverlust, entsteht ein meist enormer wirtschaftlicher Schaden. Man ist gewohnt, dass Suchmaschinen oder soziale Netzwerke immer da sind, wenn man sie braucht. Eine weniger zuverlässige Anwendung hat ein großes Vertrauensproblem seitens der Nutzer. [4]

3.2 Bedenken

sammeln von fakten
datendiebstahl, hacking, ... sicherheits- und überwachungstechnik (auch kameras, massenüberwachung, vorratsdatenspeicherung), verlust der privatsphäre durch totale sicherheit, wie viele daten darf ein unternehmen von mir sammeln, social engineering als zugang zu sensiblen daten, mensch = schwachstelle

Wieder gibt es ein essentielles Problem mit dem Datenschutz und der Privatsphäre, wie so oft in der Informationstechnologie. Ein Mindestmaß an Vorsorge ist immer nötig, aber man kann keineswegs kollektiv ausschließen, dass man einem Internetverbrechen zum Opfer fällt. Kann man jedoch ein

'gutes' von einem 'bösen' Hacking unterscheiden?
Auch die Sicherheits- und Überwachungstechnik wird in letzter Zeit immer mehr zum Thema. Viele Staaten setzen auf Kameras zur Massenüberwachung. Sämtliches Material live auszuwerten ist nicht möglich, nur ein Einblick retrospektiv ist möglich. Macht das dann Sinn, den gesamten öffentlichen Raum aufzunehmen? Was, wenn die Rohdaten in falsche Hände gelangen? Fraglich ist, ob der Verlust der Privatsphäre die totale Sicherheit mit sich bringt. Wie viele Daten darf ein Unternehmen oder der Staat von mir sammeln? Social Engineering ist bekanntlich die einfachste Art, um an Informationen zu kommen. Der Mensch ist die größte Schwachstelle, und das sollte in der Überwachungstechnik bei der Planung bedacht werden.

3.3 Formulierung ethischer Fragestellungen

3.3.1 Ethische Urteilsfindung

4 Authentication, Authorization, Accounting

4.1 Einführung

begriffserklärungen, anwendungsfälle, beispiel, hilft die identität zu bestätigen und zu wahren

4.2 Bedenken

sammeln von fakten
wegfallen der anonymität, wie unsicher ist mein passwort, hacking, identitätsdiebstahl, wie sicher ist mein system / sicherheitslücken

4.3 Formulierung ethischer Fragestellungen

diskutieren anhand der bedenken auf grundlage der theorie
aufstellen einiger wichtiger fragen und versuch einer ethischen urteilsfindung

5 Disaster Recovery

5.1 Einführung

begriffserklärungen, anwendungsfälle, beispiel, notwendigkeit hervorheben, gutes level mit hohen kosten verbunden

5.2 Bedenken

sammeln von fakten
leaks, whistleblowing bis hin zu wikileaks, panama papers als folge schlechter disasterplanung oder übersehen von sicherheitslücken, datenverlust für unternehmen nicht tragbar, wie weit hafte ich für datenverlust

5.3 Formulierung ethischer Fragestellungen

diskutieren anhand der bedenken auf grundlage der theorie
aufstellen einiger wichtiger fragen und versuch einer ethischen urteilsfindung

6 Algorithmen und Protokolle

6.1 Einführung

begriffserklärungen, anwendungsfälle, beispiel, notwendigkeit hervorheben, verschlüsselung, sicherheitszertifizierungen, was ist standard in der it, vertrauensproblem bei ungesicherten verbindungen, rechtslage bis von zu gesetzen zum verbot von verschlüsselung

6.2 Bedenken

sammeln von fakten
sicherheitslücken in verschlüsselungsalgorithmen, unverschlüsselte kommunikation kann abgefangen werden, schüre ich durch verschlüsselung terrorismus? wenn alle daten verschlüsselt sind, können verbrechen geplant werden und behörden haben keine handhabe.

6.3 Formulierung ethischer Fragestellungen

diskutieren anhand der bedenken auf grundlage der theorie
aufstellen einiger wichtiger fragen und versuch einer ethischen urteilsfindung

7 Konsistenz und Datenhaltung

7.1 Einführung

begriffserklärungen, anwendungsfälle, beispiel, notwendigkeit hervorheben, erklärung inkonsistenzen, wieso datenbanken, kundendaten konsisten sein sollen, fehlertoleranz, schutz vor missbrauch oder verlust (lost update bei bankdaten?)

7.2 Bedenken

sammeln von fakten
wo liegt die verantwortung? kunde, der daten freigibt oder unternehmer, der daten ablegt. was passiert bei datendiebstählen? habe ich die vollständige einsicht, was auf den servern abgelegt ist?

7.3 Formulierung ethischer Fragestellungen

diskutieren anhand der bedenken auf grundlage der theorie
aufstellen einiger wichtiger fragen und versuch einer ethischen urteilsfindung

Literatur

[1] Toni Agudo. Cloud-computing. `http://www.gruenderszene.de/lexikon/begriffe/cloud-computing`. zuletzt besucht: 01. 06. 2016.

[2] Dr. Markus Siepermann. Internet der dinge. `http://wirtschaftslexikon.gabler.de/Definition/internet-der-dinge.html`. zuletzt besucht: 01. 06. 2016.

[3] Republik Österreich. Bundesrecht konsolidiert: Gesamte rechtsvorschrift für datenschutzgesetz 2000, fassung vom 01.06.2016. `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597`. zuletzt besucht: 01. 06. 2016.

[4] Polydor Weinberger, Taschner. *Internet Security, Hacking, Cyber-Crime*. TGM Sj. 2015/16, 2016.

Listings

Abbildungsverzeichnis