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

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

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 Internet Security

Ausgehend von den utilitaristischen Prinzipien lässt sich auf diesen Bereich sehr gut das Konsequenzprinzip anwenden. Das bedeutet, dass bei der Beurteilung einer Handlung stets deren Folgen beachtet werden. Sind die Folgen einer Handlung überwiegend positiv, wird auch die Handlung als positiv bewertet. Ist jedoch voraussehbar, dass die Folgen überwiegend negativ ausfallen, ist die Handlung zu unterlassen oder eine andere Handlungsalternative zu wählen.

- Bin ich selber schuld, wenn ich durch illegales Herunterladen des neuesten PC-Spiels gleichzeitig Trojaner mitinstalliere?

3.3.2 Hacking

Aus der Theorie der Ethik ist vor allem das Whistleblowing zu erwähnen. Die Tätigkeiten von Edward Snowden oder Bradley Manning lassen sich als Hacking mit physischem Zugang beschreiben. Durch Eindringen in Räume mit sicherheitskritischer Hardware und Kopieren der Daten konnten so wichtige Dokumente der Weltöffentlichkeit zugänglich gemacht werden. Sie haben das Gesetz gebrochen für eine (vermeintlich?) gute Handlung, dieser Vorgang wird als eine klassische Güterabwägung in Gewissensentscheidungen bewertet.

- Bin ich als ausreichend abgesicherte Firma direkt verantwortlich für durch Datendiebstahl entstandenen Schaden? (Ja: Ich bin verantwortlich für alle Daten, die bei mir gespeichert werden, Nein: Ich habe genügend Vorsorge getroffen, Geldtransporter ist bei Raub auch nicht als Täter angesehen)
- Ist es vertretbar, dass der Staat mithilfe von ‚Bundestrojanern' bei Personen Online- Durchsuchungen durchzuführen (Ja: Sie haben einen richterlichen Beschluss dazu, dürften ja auch die Wohnung durchsuchen, Nein: Haben in den meisten Fällen keinen direkten Beschluss dazu, Einbruch in die Privatsphäre, Überwachung, unbefugter Zugriff, was ist, wenn ich unschuldig bin?)

3.3.3 Cyber Crime

An sich sind hier die gleichen Gegebenheiten beheimatet wie bereits beim Hacking. Bei illegalen Handlungen ist im Konsens meist keine ethische Urteilsfindung nötig. Im Sinne, wenn ich einen raubkopierten Film herunterlade und auch selbst verteile sollte es klar sein, dass Diebstahl eine ethisch falsche Handlung ist, und dass ich einem Unternehmen (wirtschaftlichen) Schaden zufüge. Eine ethische Urteilsfindung bei dieser strafbaren Handlung wird wohl nur bei groben Missständen mit persönlicher Relevanz infrage kommen, die auch für die größte Zahl der Menschen relevant ist.

- Bin ich als ausschließlicher technischer Bereitsteller einer Filesharing-Plattform verantwortlich für den Inhalt, den meine User hochladen? (Ja: Nährboden für Raubkopien, zahlreiche Betreiber festgenommen und rechtskräftig verurteilt, Nein: Haftet der Inhaber, wenn in seinem Lokal ein Taschendiebstahl geschieht? Rechtslage in manchen Ländern unklar [Grauzone], Zensur des freien Internets)
- Ist eine Vorratsdatenspeicherung für den späteren gerichtlichen Beweis zur Eindämmung der Internetkriminalität gerechtfertigt? (Ja: Wer nichts zu verbergen hat ...., Schutz und Sicherheit für alle, Senkung der Kriminalitätsrate, Nein: Nicht jeder ist ein Terrorist, massive Beschneidung der Privatsphäre, Überwachungsstaat, gläserner Mensch, Speicherkosten, Missbrauch der Daten)

3.3.4 Ethische Urteilsfindung

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

- Sachverhaltsdarstellung
  Der Staat Österreich beschließt, die Vorratsdatenspeicherung wiedereinzuführen. Es soll die Kriminalität eingedämmt werden, und als neutrales 'Nachschlagewerk' für Internet- und Telefonaktivitäten bei Gerichtsverhandlungen verwendet werden.
- Problemfeststellung
  Ist eine Vorratsdatenspeicherung für den späteren gerichtlichen Beweis zur Eindämmung der Internetkriminalität gerechtfertigt?
- Situationsanalyse
  Die Vorratsdatenspeicherung hat womöglich einen abschreckenden Effekt. Doch es gibt Mittel und Wege, diese zu umgehen, es ist mehr eine Verdrängung des Problems. Ein stichhaltiges Beweismittel vor Gericht ist ein großer Vorteil, doch es ist unverhältnismäßig, unbescholtene Bürger rund um die Uhr zu überwachen, 'weil sie ja etwas kriminelles machen können'. Ganz zu schweigen vom Kosten- und Datenaufwand.

- Prüfung der Verhaltensalternativen
  Die Vorratsdatenspeicherung kippen! Es gibt andere Wege zur Kriminalitätsprävention, und am Beispiel Frankreichs, wo der Geheimdienst die weitesten Rechte in ganz Europa hat, konnte der Terror bekanntlich nicht verhindert werden. Die Massenüberwachung in Relation zum aktiven Zugriff auf die Daten steht in keinem Verhältnis, sie wurde nur spärlich verwendet für andere Gerichtsurteile, die allesamt eher der Kleinkriminalität einzuordnen waren. Ist es nicht sinnvoller, nur diejenigen Personen zu überwachen, wenn ein dringender Tatverdacht besteht? Man könnte wieder argumentieren bezüglich Fehlbeschuldigungen.

- Normenprüfung
  Das Prinzip des Utilitarismus: Größtes Glück für die größte Anzahl von Menschen, geringstes Leid für die geringste Anzahl von Menschen? Das muss den Nationalratsabgeordneten durch den Kopf gegangen sein. Aber wenn man es umdreht: Ist die Freiheit und Privatsphäre der Menschen nicht wichtiger, als die Massendatensammlung, die einem Bruchteil der Bevölkerung einen Vorteil verschafft?

- Entscheidung
  Meine Antwort lautet: Nein. Es hat sich gezeigt, dass die totale Überwachung der Internetaktivitäten in keiner Relation zum tatsächlichen Nutzen steht.

4 Authentication, Authorization, Accounting

4.1 Einführung

Authentication ist die Vorgabe einer Identität. Man gibt vor, die Person zu sein, die auf dem Ausweis steht, oder durch Angabe eines Benutzernamens. Authorization ist die Bestätigung dieser Identität durch eine vertrauenswürdige Stelle, auf Basis eines gemeinsamen Schlüssels. Das kann im Internet beispielweise Benutzername und Passwort sein, die die Stelle mit seinen Daten abgleicht und bestätigt im Normalfall. Accounting beschreibt grob die Verwaltung der (Anmelde-) Daten. Die drei AAAs helfen, die Identität zu bestätigen und diese zu wahren. [5]

4.2 Bedenken

Ein großer Punkt besonders im Internet ist der damit verbundene Wegfall der Anonymität. Jede Tätigkeit kann eindeutig einer Person im System zugeordnet werden. Um wieder auf Hacking Bezug zu nehmen, im Sinne der Authentifikation ist bspw. ein unsicheres Passwort sehr einfach zu knacken. Besonders bedenklich ist hier der Identitätsdiebstahl, wo ich durch Vorgabe einer falschen Persönlichkeit etwa durch Social Engineering sehr einfach an sensible Daten gelangen kann.

4.3 Formulierung ethischer Fragestellungen

Das Prinzip AAA spiegelt sich sehr gut im Begriff Verantwortung wider. Ein authentifizierter Account ist die Zuständigkeit von Personen für übernommene Aufgaben bzw. für das eigene Tun und Lassen vor einer Instanz, die Rechenschaft fordert. Hier hat man natürlich retrospektive und prospektive Verantwortung 'von jemandem - für etwas - vor einer Instanz'. Auch die juristische Verwertbarkeit der eigenen Taten ist ein Faktor.

- Hafte ich als User einer Website für den Schaden, den ein Hacker mit meiner Identität am Server angerichtet hat?

4.3.1 Ethische Urteilsfindung

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

- Sachverhaltsdarstellung
  Ein Hacker hat mein User-Passwort (mit Adminrechten ausgestattet) geknackt, und hat damit einen Ausfall der Dienste herbeigeführt. Wer haftet für den entstandenen Schaden?
- Problemfeststellung
  Hafte ich als User einer Website für den Schaden, den ein Hacker mit meiner Identität am Server angerichtet hat?
- Situationsanalyse
  Als Unbeteiligter sollte ich davon ausgehen, dass ich nicht verantwortlich bin für den entstandenen Schaden. Ich hätte aber auch mein Passwort besser absichern können, oder kritische Sicherheitslücken bei der Authentifizierung beheben.

- Prüfung der Verhaltensalternativen
  Als Bevollmächtigter, das System zu verändern habe ich auch ein gewisses Risiko. Ich bin schuld, weil ein unbekannter Täter sich nicht festmachen lässt.

- Normenprüfung
  Hier werden die Grenzen der Verantwortungsfähigkeit aufgezeigt. Ich habe individuelle Verantwortung, meinen Account abzusichern, aber keine Handlungsmacht, wenn jemand anderes (als Straftat) darauf zugreift.

- Entscheidung
  Meine Antwort lautet: Nein. Täter und Opfer umzukehren ist der falsche Ansatz. In so einem Fall bleibt zu überdenken, etwaige Sicherheitsbestimmungen noch weiter zu verschärfen, um einem ähnlichen Fall vorzubeugen.

5 Disaster Recovery

5.1 Einführung

Disaster Recovery (dt. auch Katastrophenwiederherstellung) beschreibt die Vorbereitung und Reaktion auf sogenannte Katastrophen, die abgespeicherte Daten und Lauffähigkeit eines IT-Systems betreffen. In diesem Bereich der Sicherheitsplanung ist mit negativen Ereignissen all das gemeint, was den Betrieb eines Unternehmens gefährdet. Hierzu gehören Cyberattacken, Infrastrukturausfälle ebenso wie Naturkatastrophen. Ein geeignetes Maß an Fehlertoleranz ist zu wählen, damit das System nicht beim kleinsten Problem ausfällt.
Oft können sich Firmen, deren Fokus auf Hochverfügbarkeit liegt, keinen Ausfall leisten. Jeder Ausfall ist auch ein Kostenausfall, ein Nichtausliefern des Produktes. Ein gutes Level an Disaster Recovery ist jedoch auch mit sehr hohen Kosten verbunden (Cluster-Lösung). Wo es das Budget nicht anders erlaubt, muss mit (mehr oder weniger langen) Ausfällen rechnen. Das bringt wie angesprochen Finanzierungsprobleme mit sich, jedoch ist Datenverlust auch ein großer Faktor. [6]

5.2 Bedenken

Ein typisches Disaster kann aber auch nicht technisch verursacht sein. Sogenannte Leaks oder Whistleblowing ist in den letzten Jahren ein großes Thema. Whistleblowing ist der Verrat von innerbetrieblichen Missständen. Bei diesen Missstanden handelt es sich um sensible Informationen deren Veröffentlichung zu Rufschädigung führt. Es wird zwischen internen und externen Whistleblowing unterschieden. Bei internen Whistleblowing hat der Adressat das Recht, die Informationen zu kennen. Beim externen Whistleblowing kommen als Adressanten Personen oder Organisationen in Betracht.
Beispielsweise WikiLeaks ist eine Website auf der Dokumente anonym veröffentlicht werden, die wegen Geheimhaltung, Zensur oder einem sonstigen Grund nicht so einfach zugänglich sind. 2009 hatte sich WikiLeaks inzwischen zu einer zentralen Sammelstelle mit 1,2 Millionen Dokumenten von Regimekritikern und anonymen Quellen entwickelt. Der Kerngedanke ist die Idee des freien Zugangs zu Informationen, die öffentliche Angelegenheiten betreffen. Für große Aufregung sorgte 2010 die Veröffentlichung von Geheimdokumenten des US-Militärs. Die als 'Afghan War Diarys' und 'Iraq War Logs' genannten Dokumente zeigten zahlreiche Verbrechen und Missstände des US-Kriegs im Nahen Osten auf. WikiLeaks ist weiterhin sehr von Spendengeldern abhängig, was die Veröffentlichung weiterer Dokumente erschwert.
Ebenso erwähnenswert ist Edward Snowden, der ehemalige NSA-Mitarbeiter Edward Snowden deckte 2013 auf, wie die USA und GB in großem Umfang und seit mehreren Jahren die Telekommunikation und besonders das Internet global und verdachtsunabhängig überwachen. Auch Gebäude und Vertretungen der Europäischen Union sowie die Vereinten Nationen sollen mit Hilfe von Wanzen ausspioniert worden sein. Die Geheimdienste begründen die umfassende Überwachung damit, dass man dadurch terroristischen Anschlägen vorbeuge. Edward Snowden, der von zahlreichen NGOs ausgezeichnet und für den Friedensnobelpreis nominiert wurde, hat inzwischen Asyl in Russland bekommen.
Disaster Recovery beschreibt eigentlich im Grunde genommen, wie man sich vor Whistleblowing schützen kann, oder was man tun kann, um den Schaden möglichst gering zu halten. Aber ist es so schlecht, Missstände aufzudecken? [7]

5.3 Formulierung ethischer Fragestellungen

Diese Argumentation bezüglich Whistleblowing wurde bereits im Bereich 'Hacking' erklärt. Whistleblowing ist eine Güterabwägung in Gewissensentscheidungen. Sie handeln utilitaristisch, wollen der größten Anzahl der Menschen das größte Glück bringen.

- Hat Snowden mit seinen Taten wirklich das größte Glück für die größte Anzahl der Menschen gebracht, oder sind sie nur noch mehr verunsichert?
- Sind Whistleblower Verräter oder Helden?

5.3.1 Ethische Urteilsfindung

- Sachverhaltsdarstellung
  Edward Snowden deutet durch seine Arbeit auf grobe Missstände hin, die die ganze Welt betreffen. Snowden durfte auf diese Informationen zugreifen, jedoch ist eine Veröffentlichung verständlicherweise untersagt und illegal.
- Problemfeststellung
  Ist Snowden nun ein Verbrecher und gehört vor ein Gericht, oder ist er der Held des einfachen Bürgers?
- Situationsanalyse
  An sich hat sich an der Weltlage seitem nicht sehr viel verändert. Die USA und Großbritannien führen ihre Praxis fort, unter vom Parlament nachträglich legalisierten Rahmenbedingungen. Das Bewusstsein der Bürger ist jedoch gestiegen, vermehrt darauf zu achten, im Internet sicherer unterwegs zu sein.
- Prüfung der Verhaltensalternativen
  Die veröffentlichten Daten sind wahr, das ist nicht zu leugnen und wurde von vielen Seiten bestätigt. Nach geltendem Recht ist Snowden jedoch ein gesuchter Verbrecher, der sich bei Bruch eines Gesetzes wie jeder andere Bürger auch vor einem Strafgericht verantworten soll.
- Normenprüfung
  Das Prinzip des Utilitarismus findet Anwendung: Der Vorteil der Weltbevölkerung ist gewichtiger als die blanken Interessen weniger Regierungsbeamten. Es wäre ein Verbrechen, ein anderes Verbrechen nicht anzuzeigen.
- Entscheidung
  Meine Antwort lautet: Snowden ist ein Held, wenn auch ein zweifelhafter in vielen Augen. Er hat sein Leben aufs Spiel gesetzt und seinen Wohlstand aufgegeben, um anderen Menschen die Augen zu öffnen.

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.

[5] authentifizierung.org. Authentifizierung. `http://authentifizierung.org/`. zuletzt besucht: 01. 06. 2016.

[6] Weinberger. *SYT-Ausarbeitung DezSys*. TGM Sj. 2015/16, 2016.

[7] Stedronsky Karic, Adler. *Ethik-Ausarbeitung Leaks*. TGM Sj. 2015/16, 2016.

Listings

Abbildungsverzeichnis