**Wissenschaftlich Angeleitete Berufspraxis 3**

Studiengang Wirtschaftsinformatik  
Prof. Dr. U.Pielot

## Betr.: Überarbeitete präzisierte Aufgabenstellung vom 30.04.2014

Gruppe 13

Thema: Analyse und Bewertung technischer Verfahren zur Absicherung der E-Mail Kommunikation im Privat-Anwenderbereich.

1. Welches Problem soll behandelt werden?

E-Mails werden wie Postkarten versendet. Jeder, der sie in die Hände bekommt, kann deren Inhalt ~~erfahren~~ lesen~~, sofern er dies möchte~~. E-Mails werden zwar elektronisch, aber in der Regel genauso ungeschützt versandt. ~~Außerdem gibt es im E-Mail Verkehr kein Äquivalent zum Postgeheimnis, welches das unerlaubte Öffnen oder Lesen von Briefen strafbar macht.~~ Diese wissenschaftliche Arbeit setzt sich damit auseinander~~soll sich damit auseinandersetzen~~, welche Sicherheitsvorkehrungen eine private Person (bspw. ein Student) treffen kann, um seine E-Mails sicher (vor Veränderungen; Integrität) und geschützt (vor dem Mitlesen durch Dritte; Verschlüsselung) zu versenden. Zusätzlich wird noch der Aspekt der Echtheit (d. h. ist der Absender/ Empfänger wirklich derjenige, für den er sich ausgibt; Authentizität) beleuchtet. Des Weiteren wird die Funktionsweise dieser Verfahren erläutert. Als Anlage zu dieser Arbeit soll außerdem eine Broschüre erstellt werden, welche dem Leser eine Zusammenfassung über die derzeitige Lage und Möglichkeit sicherer E-Mail Kommunikation gibt.

1. Warum ist das Problem von Interesse?

Hierfür existieren zwei verschiedene Gründe. Zum einen werden durch das Mitlesen von E-Mails ~~der Datenschutz und~~ die Privatsphäre des Menschen verletzt. Wie beim Brief soll nur der Absender und der rechtmäßige Empfänger auf den Inhalt der Mail erhalten. Dieses ist im Mailverkehr nicht gewährleistet, weswegen andere Methoden zurückgegriffen werden muss, um die Vertraulichkeit zu garantieren. Zum anderen ist das Thema durch die derzeitigen Medienberichte über die Programme der NSA sehr aktuell. Vielen Privatpersonen ist es einerseits mitunter unklar, was überhaupt „von außen“ alles mitgelesen werden kann und andererseits kennt nur eine geringe Anzahl der ~~zu untersuchenden Zielgruppe~~ betroffenen Personen die verschiedenen Möglichkeiten zum Schutz beim Versenden von E-Mails. Genau auf diese verschiedenen technischen Möglichkeiten soll in dieser wissenschaftlichen Arbeit eingegangen werden, sodass nicht nur die Autoren, sondern auch alle Leser ein besseres Verständnis für diese Thematik erlangen können.

1. Für wen ist das Problem von Interesse (Zielgruppe)?

Von Interesse ist die oben genannte Problemstellung insbesondere für Privatpersonen, die ein gesteigertes Bedürfnis an gesicherter Kommunikation per E-Mail haben ~~und grundlegenden IT-Kenntnissen.~~

Für Privatpersonen mit grundlegenden IT-Kenntnissen, die ein erhöhtes Bedürfnis an sicherer (E-Mail) Kommunikation haben.

1. Welche Fragen sollen mit dem schriftlichen Bericht beantwortet werden? Formulieren Sie mindestens eine Leitfrage!

Welche Verfahren, Methoden und Protokolle sind für eine sichere E-Mail Kommunikation notwendig und wie sehen deren Funktionsweisen aus?

Welche unterschiedlichen Sicherheitsbedürfnisse gibt es in der privaten E-Mail Kommunikation und wie kann man diese hinsichtlich praxisorientierter Anwendungsfälle beschreiben und in Sicherheitsstufen kategorisieren?

Wie ist eine Zuordnung zwischen beschriebenen Sicherheitsstufen und Verfahren zu entwickeln, um entsprechend den Anwendungsfällen optimale technische Konzepte für sichere E-Mail Kommunikation zu empfehlen?

Welche Möglichkeiten hat der private Endanwender um mit den E-Mail-Angeboten von gängigen und alternativen Providern seine Kommunikation sicher zu gestalten, bzw. bis zu welcher Sicherheitsstufe ist dies möglich?

Wie kann eine Zusammenfassung der Ergebnisse aussehen, die der Zielgruppe in kurzer Zeit über die derzeitige Lage und Möglichkeit sicherer E-Mail Kommunikation informiert?

### Gründe für die Verschlüsselung

* Mailserver, die Mitlesen und nach Schlagworten filtern
  + Schwierig an diese Infos ranzukommen?!
  + Nicht ins Detail drauf eingehen
  + Als Grund aufnehmen für eine Verschlüsselung

### Kategorien/Vertraulichkeitsstufen

1. Wie kann man verschiedene Sicherheitsbedürfnisse der Zielgruppe kategorisieren?
2. Wie viele Stufen der Vertraulichkeit sind für die Zielgruppe sinnvoll?

* Verschiedene Sicherheitsbedürfnisse in einer Kategorisierung aufstellen
  1. Unsicher (z.B. E-Cards zu Weihnachten)
  2. Halbwegs sicher (z.B. Telefonnummer, Adresse)
  3. Drei viertel sicher (z.B. Passwörter)
  4. Vollkommen sicher (z.B. Anwalt, Versicherung, Arzt, Banking)
  5. 🡪 Welche Verschlüsselungsstufe dahinter ist sinnvoll (Aufwand/Nutzen)

### Technische Möglichkeiten/Verfahren

1. Welche technischen Verfahren gibt es zur Verschlüsselung von E-Mails, in welchen Punkten unterscheiden sich diese?
2. Welche Zuordnung zwischen den untersuchten technischen Verfahren und den zuvor aufgestellten Vertraulichkeitsstufen kann aufgestellt werden?

* PGP, sMiMe -> End to End
* SSL
* Authentizität, Integrität, Verschlüsselung (CIA)
* Funktionsweise der Verschlüsselung und die Technologien dahinter in Projektbericht beschreiben

### DE-Mail

1. Worin setzt sich DE-Mail von der gängigen E-Mail Kommunikation hinsichtlich Verschlüsselung ab und welche technischen Unterschiede sind vorhanden?

### Ergebnis: Anwenderhandbuch

1. Bieten gängige Provider von E-Mail Diensten (z.B. 1&1, t-online, aber auch kleine/jüngere Anbieter (Start Ups)) den Schutz, um die entsprechenden Vertraulichkeitsstufen abzudecken?
2. Was für ein Hilfsmittel könnte man der Zielgruppe bereitstellen um einen schnellen Überblick über die Möglichkeiten für sichere E-Mail Kommunikation zu geben?

* Anwenderhandbuch als Ergebnis
  1. Verschiedene Anbieter von E-Mail Diensten (GMX, WEB.de, T-Online) untersuchen, vergleichen und bewerten, welche Möglichkeiten zur Verschlüsselung diese schon von Haus aus mitbringen
     1. Verschlüsselung auf Weg
        1. Von mir zum Server
        2. Evtl. zwischen den Servern
     2. Problem: Entweder sie verschlüsseln voll oder gar nicht
     3. Kein Anbieter macht eine Ende zu Ende Verschlüsselung?!
     4. Ist DE-Mail vielleicht besser
     5. Sind kleine Start Ups ggf. besser (4-5 kleine Anbieter ermitteln und deren Technologien untersuchen)?
     6. Was müsste man tun, damit die E-Mail Kommunikation durchweg sicher ist
     7. Auf unsere Matrix eingehen
  2. Klick-Anleitung für Outlook und andere E-Mail Clients (z.B. Thunderbird)

Optional:

1. Wie sicher sind Apps auf dem Markt zum Versenden von E-Mails
   * Mobile Endgeräte und vorhandene Apps betrachten
   * Sorge, ob es nicht zu sehr in die Breite geht
2. Welche Literatur wurde bisher herangezogen?

* Schwenk, Jörg, 2010. *Sicherheit und Kryptographie im Internet. Von Sicherer E-Mail bis zu IP-Verschlüsselung*, 3. Aufl., Berlin: Vieweg+Teubner
* Eckert, Claudia, 2013. *IT-Sicherheit. Konzepte – Verfahren – Protokolle*, München: Oldenbourg

1. Projektplanung:

Allgemeine Regeln:

* Wöchentliche Statusmeetings zum gegenseitigen Austausch der aktuellen Arbeitsstände und Klären von Problemen
* Kommunikation via Mail; alternativ kann auch WhatsApp für schnelle Rückfragen genommen werden
* Benutzung von Trello für das Projekt-Controlling

|  |  |  |  |
| --- | --- | --- | --- |
| KW | Woche | Aufgaben | verantwortlich |
| 16 -18 | 14.04.14-04.05.14 | Erarbeitung der präzisierten Aufgabenstellung | Florian |
| 19 | 05.05.14-09.05.14 | Verfahren, Methoden, Protokolle sowie deren Funktionsweisen erarbeiten   * Brainstorming zu möglichen Verfahren, Methoden, Protokolle   Brainstorming zu möglichen Sicherheitsbedürfnissen und einer entsprechenden Klassifizierung | Florian |
| 19-20 |  | Erarbeitung Methode/Protokoll/Verfahren Nr. 1 aus Brainstorming in KW 19  Erarbeitung Methode/Protokoll/Verfahren Nr. 2 aus Brainstorming in KW 19  Erarbeitung Methode/Protokoll/Verfahren Nr. 3 aus Brainstorming in KW 19  Erarbeitung Methode/Protokoll/Verfahren Nr. 4 aus Brainstorming in KW 19 | Pascal  Daniel  Chi Cong  Florian |
| 21-22 | 19.05.14-01.06.14 | Untersuchung gängiger und alternativer E-Mail Provider hinsichtlich bereitgestellter Konfigurationsmöglichkeiten für eine sichere E-Mail Kommunikation   * t-online * 1&1 * Alternativer Anbieter/Start Up 1 * Alternativer Anbieter/Start Up 2   Betrachtung der Thematik DE-Mail   * Was ist DE-Mail? * Welches technische Konzept der Sicherheit steckt dahinter * Welche Vorteile gibt es gegenüber der gängigen Kommunikation | Chi Cong  Florian  Pascal  Daniel  Florian  Daniel  Chi Cong |
| 23 | 02.06.14-08.06.14 | Brainstorming zu Sicherheitsbedürfnisse mit Hilfe von Erkenntnissen der letzten Woche finalisieren  Erarbeitung der Kategorisierung der Vertraulichkeitsstufen  Zuordnung der Kategorien und Verfahren  Zusammenstellen aller bisherigen Zwischenergebnisse zu einem Projektbericht | Chi Cong  Chi Cong  Chi Cong  Daniel |
| 24 | 09.06.14-15.06.14 | Erstellung der Nutzerbroschüre | Pascal |
| 25 | 16.06.14-22.06.14 | Erstellung der Präsentation | Pascal |
| 26 | 23.06.14-28.06.14 | Review Projektbericht und Finalisieren der Präsentation | Florian |
| 26 | 28.06.14 | Abgabe Projektbericht, Abgabe Präsentation | Florian |

1. Offene Fragen für das TT:

* Frage: nur Beschreibung von Techniken oder auch Anleitungen möglich (ähnlich Anwenderhandbuch)?
* Frage: Wie können wir die Zielgruppe weiter spezialisieren? (durch Anwendung verschiedener Geräte -> Geräteklasse?)
* Frage: Sind Netzplan, Vorgangsplan, etc. abzuliefern
* Frage: Können wir auch tex Dateien statt word abgeben oder gibt es eine andere Lösung?
* Frage: Dürfen wir Prezi benutzen?
* Frage: Vergleich zu Unternehmen (interne Frage 8)