**Wissenschaftlich Angeleitete Berufspraxis 3**

Studiengang Wirtschaftsinformatik  
Prof. Dr. U.Pielot

## Betr.: Überarbeitete präzisierte Aufgabenstellung vom 20.05.2014

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 in der Regel unverschlüsselt und im Klartext übertragen. Somit wird es Dritten ermöglicht, an den Inhalt dieser E-Mails zu gelangen. Diese wissenschaftliche Arbeit setzt sich damit auseinander, welche Sicherheitsvorkehrungen eine private Person treffen kann, damit Dritten der Inhalt ihrer Mails verwahrt bleibt und damit der Empfänger sicherstellen kann, dass er die Mail vollständig und unverändert erhalten hat und darüber hinaus deren Funktionsweise näher erläutert. Zusätzlich wird auf den Aspekt der Authentizität eingegangen, d. h. ob der Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt. 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 soll nicht jeder Zugriff auf den E-Mail Inhalt haben. Nur der rechtmäßige Empfänger soll in der Lage sein, den Inhalt der Mail zu erfahren. 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 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 mit grundlegenden IT-Kenntnissen, die ein gesteigertes Bedürfnis an gesicherter Kommunikation per E-Mail 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 |
| 19-22 | 19.05.14-01.06.14 | Erarbeitung der Themen:  Grundlagen Kryptografie  Web of Trust  Informationsverschlüsselung  Public-Key-Infrastruktur – PKI  Sicherheitsniveaus  Schlüsselaustausch  Transportwegverschlüsselung  DNSSEC  DANE/TLSA | Chi Cong  Florian  Daniel  Pascal |
| 23 | 02.06.14-08.06.14 | Untersuchung gängiger und alternativer E-Mail Provider hinsichtlich bereitgestellter Konfigurationsmöglichkeiten für eine sichere E-Mail Kommunikation   * Big-Player * E-Mail made in Germany - EmiG * Underdogs | Chi Cong, Florian  Pascal  Daniel |
| 24 | 09.06.14-15.06.14 | Einleitung  Datenschutz 1-mal-1  Zusammenfassung  Ausblick  Zusammenstellen aller bisherigen Zwischenergebnisse zu einem Projektbericht  Erstellung der Nutzerbroschüre | Florian  Chi Cong  Daniel  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. Entwurf einer Gliederung

Deckblatt

1. Eidesstaatliche Erklärung
2. Inhaltsverzeichnis
3. Abbildungsverzeichnis
4. Abkürzungsverzeichnis
5. Einleitung
   1. Motivation (Warum ist das so ein brisantes Thema) (Vergleich Datendiebstahl vs. Datenüberwachung kurz anreißen)
   2. Zielsetzung und Zielperspektive/Abgrenzung
   3. Abgrenzung (evtl. unnötig wenn Zielsetzung klar formuliert wird!)
6. Datenschutz 1-mal-1
   1. Verfügbarkeit
   2. Integrität
   3. Authentizität
   4. Vertraulichkeit
7. Sicherheitsniveaus (Unsere Kategorien, mit Beispielen)
   1. Wozu E-Mail Inhalt schützen? (Kapiteltitel nicht final)
8. Kryptografie (nicht zu sehr in die Tiefe gehen)
   1. Grundlagen (Chico)
      1. symmetrische Verschlüsselung
      2. asymmetrische verschlüsselung
      3. Zertifikate
         1. Certificate Authority - CA
      4. Signaturen
   2. Schlüsselaustausch (Pascal)
      1. Perfect Forward Secrecy - PFS
   3. Transportwegverschlüsselung (Daniel)
      1. Secure Sockets Layer / Transport Layer Security **-** SSL/TLS
   4. Informationsverschlüsselung (Florian)
      1. Pretty Good Privacy - PGP
      2. Secure / Mulitpurpose Internet Mail Extensions - S/MIME
   5. Web of Trust - WOT (Chico)
   6. Public-Key-Infrastruktur - PKI (Florian)
9. Dienste
   1. DNS (Daniel und Pascal)
      1. DNSSEC
      2. DANE/TLSA
10. Mail-Provider
    1. Big-Player
       1. Googlemail
       2. Hotmail - Windows Live
       3. Yahoo mail
    2. E-Mail made in Germany - EmiG
    3. Underdogs
       1. posteo
       2. mailbox.org
       3. startmail (by ixquick)
11. Zusammenfassung (Könnte man evtl. noch irgendwie "frischer" nennen?)
12. Ausblick (Trends/Fazit/Schlusswort)

Da das Thema noch aktuell ist, und ständig *weiter lebt* macht es vll Sinn genau nochmal drauf aufmerksam zu machen das es nur um eine Moment-Aufnahme handelt.

1. Literaturverzeichnis
2. Anhang: Infografik

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)