**Wissenschaftlich Angeleitete Berufspraxis 3**

Studiengang Wirtschaftsinformatik

## Betr.: Überarbeitete präzisierte Aufgabenstellung vom 28.05.2014

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 der Zielgruppe 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 und es der Zielgruppe als Ergebnis ermöglichen ein besseres Verständnis für diese Thematik erlangen zu 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 Form ihre Fragen hinsichtlich der Möglichkeit sicherer E-Mail Kommunikation beantwortet?

1. Welche Literatur wurde bisher herangezogen?

* SCHWENK, J.: Sicherheit und Kryptographie im Internet. Von Sicherer E-Mail bis zu IP-Verschlüsselung: Vieweg+Teubner., 2010
* ECKERT, C.: IT-Sicherheit / Konzepte - Verfahren - Protokolle, Offline: Oldenbourg., 2013
* SORGE, C.; GRUSCHKA, N. & IACONO, L. L.: Sicherheit in Kommunikationsnetzen: Oldenbourg., 2013
* ERTEL, W.: Angewandte Kryptographie: Carl Hanser Verlag., 2012
* SCHMEH, K.: Kryptographie - Verfahren, Protokolle, Infrastrukturen: dpunkt.verlag., 2013
* SPITZ, S.; PRAMATEFTAKIS, M.; SWOBODA, J.: Kryptographie und IT-Sicherheit - Grundlagen und Anwendungen: Vieweg+Teubner Verlag., 2011
* BÖCK, H.: Perfect Forward Secrecy: Zukunftssicher per Schlüsselaustausch, GOLEM.DE - Klaß & Ihlenfeld Verlag GmbH, Online, Klaß & Ihlenfeld Verlag GmbHOranienstr. 16410969 Berlin, 2013
* Bundesamt für Sicherheit in der Informationstechnik: Glossar und Begriffsdefinitionen (2009), URL: https:/www.bsi.bund.de/DE/Themen/ITGrundschutz/

ITGrundschutzKataloge/Inhalt/Glossar/glossar\_node.html (Stand 28.05.2014)

* Berliner Beauftragter für Datenschutz und Informationsfreiheit: Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität (2008), URL: http://www.datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet (Stand 28.05.2014)

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
   2. Zielsetzung
   3. Abgrenzung
6. Datenschutz 1-mal-1
   1. Verfügbarkeit
   2. Integrität
   3. Authentizität
   4. Vertraulichkeit
7. Sicherheitsniveaus
8. Kryptografie
   1. Grundlagen
      1. symmetrische Verschlüsselung
      2. asymmetrische verschlüsselung
      3. Zertifikate - Certificate Authority - CA
      4. Signaturen
   2. Schlüsselaustausch (Perfect Forward Secrecy – PFS)
   3. Transportwegverschlüsselung (Secure Sockets Layer / Transport Layer Security **-** SSL/TLS)
   4. Informationsverschlüsselung
      1. Pretty Good Privacy - PGP
      2. Secure / Mulitpurpose Internet Mail Extensions - S/MIME
   5. Web of Trust - WOT
   6. Public-Key-Infrastruktur - PKI
9. Dienste
10. DNSSEC
11. DANE/TLSA
12. 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)
13. Zusammenfassung
14. Ausblick
15. Literaturverzeichnis
16. Anhang: Infografik