

Inhaltsverzeichnis

| | |
|--|------------|
| AUTORENTEAM | iii |
| EINLEITUNG | v |
| SEMINARZIELE | vi |
| INHALTSVERZEICHNIS | vii |
| Kapitel I Verschlüsselung | 1 |
| 1. Kryptografie | 2 |
| 1.1. Was ist Verschlüsselung..... | 2 |
| Substitution..... | 2 |
| Transposition..... | 2 |
| Frequenzanalyse..... | 2 |
| 1.2. Verwendung von Verschlüsselung..... | 2 |
| Authentifizierung und Zugriffssteuerung..... | 2 |
| Integrität..... | 2 |
| 2. Verschlüsselungstechnologien | 3 |
| 2.1. Kryptische Hash-Funktionen..... | 3 |
| 2.2. Symmetrische Verschlüsselung..... | 3 |
| 2.3. Asymmetrische Verschlüsselung..... | 4 |
| 2.4. Vergleich von Symmetrischer und asymmetrischer Verschlüsselung..... | 5 |
| 2.5. Schlüssellängen und ihre Bedeutung..... | 5 |
| Schlüssellängen bei symmetrischen und asymmetrischen Verfahren..... | 5 |
| 2.6. Digitale Signaturen..... | 7 |
| 3. Kryptografische Angriffe | 9 |
| Brute Force Angriff..... | 9 |
| Schwache Schlüssel Angriffe..... | 9 |
| Man-in-the-Middle und Replay Angriffe..... | 9 |
| Kapitel II E-Mail Kommunikation | 11 |
| 4. E-Mail | 12 |
| 4.1. E-Mail Standards..... | 12 |
| Zugriff auf E-Mails..... | 12 |
| Mailserver..... | 12 |
| MTA (Mail Transfer Agent)..... | 13 |
| MDA (Mail Delivery Agent)..... | 14 |
| Mailfilter..... | 14 |
| MRA (Mail Retrieval Agent)..... | 14 |
| Relay Server..... | 14 |
| SMTP-Protokoll..... | 14 |
| POP-Protokoll..... | 15 |
| IMAP-Protokoll..... | 15 |
| IMAPS-Protokoll..... | 17 |



| | | |
|------|--|----|
| | POP3S-Protokoll | 17 |
| 4.2. | Aufbau einer E-Mail | 17 |
| | Aufbau einer E-Mail | 17 |
| | Header – der Kopf der E-Mail | 17 |
| | Body – der Inhalt der E-Mail | 18 |
| | Signatur – die Unterschrift unter der E-Mail | 18 |
| | Mailfooter | 19 |
| | Dateianhänge | 19 |
| | E-Mail Formate | 19 |
| | Plain-Text | 19 |
| | Rich-Text | 19 |
| | HTML | 19 |
| | Die E-Mail Adresse | 20 |
| 4.3. | Die E-Mail Zustellung | 21 |
| | Kommunikation mit POP | 26 |
| 4.4. | Hilfreiche Tools für die Headeranalyse | 29 |
| 4.5. | E-Mail Anwendungssicherheit | 30 |
| | POP-Protokoll | 30 |
| | IMAP-Protokoll | 31 |
| 4.6. | E-Mail Anwendungsgefahren und Reaktionen | 32 |
| | Authentizität, Datenschutz und Integrität | 32 |
| | Beweiskraft und Beweiswert von E-Mails | 32 |
| 4.7. | E-Mail Authentifizierung und Vertraulichkeit | 34 |
| | E-Mail-Überwachung | 34 |
| | S/MIME | 34 |
| 4.8. | Gefahren durch E-Mail | 35 |
| | Allgemeine Gefahren | 35 |
| | Verlust von E-Mails | 35 |
| | Unautorisierte Zustellung | 35 |
| | Fehlerhafte Konvertierung | 35 |
| | Fehlende Verschlüsselung | 35 |
| | Keine Absenderauthentifizierung | 36 |
| | Datenmenge | 36 |
| | Umgang / Handhabung | 36 |
| | Unachtsamkeit bei Massenmails | 37 |
| | E-Mail spezifische Gefahren | 38 |
| | Spam Mails | 38 |
| | Viren | 38 |
| | Würmer | 39 |
| | Trojaner | 39 |
| | Rootkits | 39 |
| | Spyware | 40 |
| | Mail Bomben | 40 |
| | Phishing Mails | 40 |
| | Remailer | 42 |
| | Hoax | 42 |
| | Meldungen, die das Mitleid eines Benutzers erwecken: | 42 |
| | Kettenbriefe Glück und Unglück: | 42 |
| | Gewinnspiele: | 42 |
| | Schreckensmeldungen: | 42 |
| 4.9. | E-Mail Sicherheits-Tipps | 43 |
| | Vermeidung von Malware | 43 |

| | |
|--|-----------|
| Technische Möglichkeiten..... | 43 |
| Vermeidung von SPAMs..... | 43 |
| Bessere Organisation am Arbeitsplatz..... | 44 |
| Mitarbeiter | 44 |
| Administrator | 44 |
| 4.10. Beschwerden über unerwünschte Massen-E-Mails..... | 45 |
| 4.11. Einmal E-Mail Adressen..... | 45 |
| 5. PKI (Public Key Infrastructure)..... | 46 |
| 5.1. DE-Mail..... | 46 |
| Sicherheitsmerkmale..... | 47 |
| Nachweise und Versandmöglichkeiten | 48 |
| Ende-zu-Ende-Verschlüsselung und elektronische Signatur..... | 48 |
| Kriterienkatalog für den Datenschutznachweis..... | 48 |
| Rechtsverbindlichkeit | 49 |
| 5.2. Was ist PKI?..... | 49 |
| 5.3. Digitale Zertifikate | 49 |
| 5.4. Qualifizierte Digitale Signatur..... | 53 |
| Der Weg zur Qualifizierten Digitalen Signatur | 56 |
| 6. GDPdU-Konforme Archivierung | 58 |
| Widerspruch zwischen Anforderungen der GDPdU und dem Postgeheimnis.. | |
| | 63 |
| 7. Praktische Übungen | 65 |
| 7.1. Gpg4win | 65 |
| 7.2. OpenLimit CC Sign | 65 |
| Signierung | 66 |
| Ablauf des Einrichtens in Outlook mit den Kontoeinstellungen in Outlook... | 69 |
| 7.3. DigiSeal Reader | 69 |
| 7.4. PGP..... | 73 |
| Notizen | 73 |
| Literaturverzeichnis | 74 |
| Abbildungsverzeichnis | 75 |
| Stichwortverzeichnis..... | 76 |