IT Sicherheit – Begriffe und Normen

Ergänzungen

Wintersemester 2017/2018
Prof. Dipl.-Ing. Klaus Knopper

Das Lesen der hier verlinkten Seiten wird empfohlen und kann nützlich sein, um das jeweilige Stichwort und den Zusammenhang mit BVoIT zu verstehen und erklären zu können (“Wofür braucht man das?”).

1 Ergänzung “Verschlüsselung”

1.1 Zertifikat

Ein Zertifikat enthält einen selbst- oder fremdsignierten öffentlichen Schlüssel, *keine privaten Schlüssel*. Zertifikat und privater Schlüssel können zusammen in Form einer PKCS#12-Datei in das Mailprogramm importiert werden.

1.2 Arten von Verschlüsselung

Verschlüsselung auf dem Transportweg: SSL/TLS

Verschlüsselung von Daten in Containern (z.B. Mail-Attachment): S/MIME, PGP, 7zip, TrueCrypt

1.3 Standards und Containerformate für Schlüssel und Signaturen

Standard/Format	Bedeutung
x509	Standard für Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate
S/MIME	(Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail
pkcs7	Containerformat für verschlüsselte oder signierte Teile einer E-Mail bzw. eines Dokuments.
pkcs12	Containerformat mit Passwortschutz zum Import/Export eines öffentlichen/geheimen Schlüsselpaars.
PKI	“Public Key Infrastruktur”, ein System zum Erstellen, Verwalten und Verteilen von digitalen (auch Signierer-)Zertifikaten.

1.4 OpenSSL (Programm)

Der OpenSSL-“Einzeiler” zum Generieren eines 3650 Tage gültigen, selbstsignierten Zertifikats (mit geheimem Schlüssel in separater Datei!):

```
openssl req -new -x509 -days 3650 -nodes -out zertifikat.pem -keyout geheim.pem
```

2 IT-Sicherheitsstandards und Handbücher

Hier ist zwischen technischen Maßnahmen (Verschlüsselung, Firewall, Zugangskontrolle, physikalische Netzwerk- und Systemtrennung etc.) und organisatorischen Maßnahmen (Policy, Konzept) zu unterscheiden, die ineinander greifen müssen, um zum Erfolg zu führen.

Norm	Inhalte
ISO/IEC 15408	Common Criteria
ISO/IEC 27001	Informationssicherheits-Managementsysteme (ISMS)
ISO/IEC 27002	Informationssicherheits-Managementsysteme (ISMS)
BSI-Standard 100-1	Managementsysteme für Informationssicherheit
BSI-Standard 100-2	IT Grundschutz Vorgehensweise [BSI2]
BSI-Standard 100-3	Risikoanalyse auf Basis von IT-Grundschutz [BSI3]

Tabelle 1: Liste von Normen und Empfehlungen zur Informationssicherheit, Auszug aus BITKOM: Kompass der IT-Sicherheitsstandards, http://www.kompass-sicherheitsstandards.de/

Frage: Wird bei diesen Standards tatsächlich ein “hoher Grad von Sicherheit” zertifziert oder gefordert? Was genau wird bei “Common Criteria” (“Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie”) eigentlich betrachtet? (auch Kritik lesen!)