Aufgabenbeschreibung 4

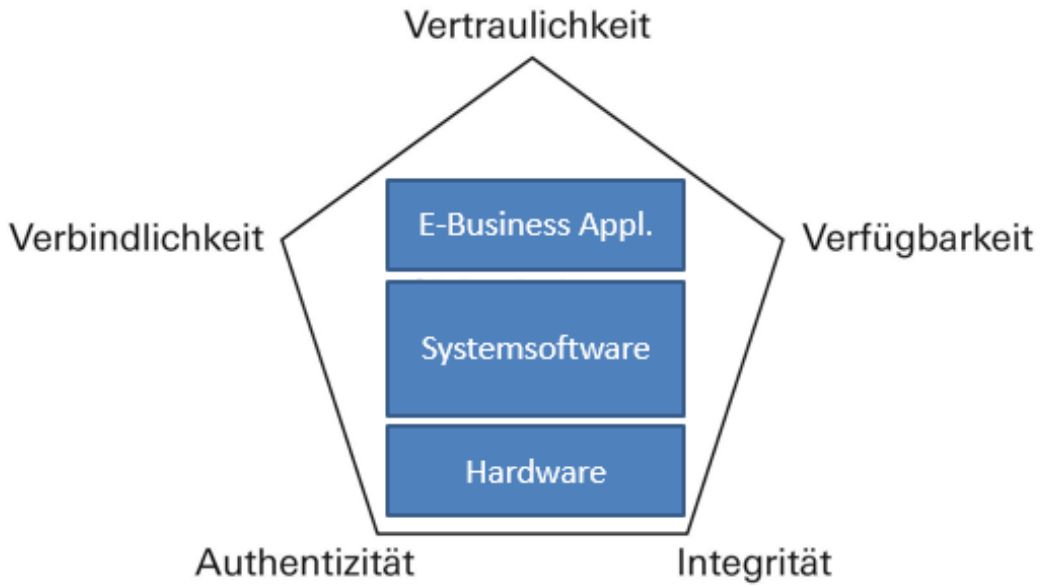
Kompetenzfeld und Handlungsziel

Diese Aufgabe behandelt:
- das Handlungsziel 3
- Handlungsnotwendige Kenntnisse 3.1, 3.2

Thema

Was für Vorgaben aus dem Bereich Datenschutz sind bei E-Business Anwendungen zu beachten. Was hilft Verschlüsselung und was bedeutet das.

Dieses Thema ist eingebettet im ganzen Fragenkomplex von Sicherheit und Nachvollziehbarkeit und umfasst so die Themen Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit und Verfügbarkeit.



Datenschutzes: Bestimmungen und deren Bedeutung auf E-Business-Anwendungen

Grundlagen:
- Bundesgesetz über den Datenschutz (DSG 235.1)
- Datenschutzgesetz (KDSG) des Kt Bern (BSG 152.04)
- Die Gesetze der Schweiz und der EU

Sicherheit: Datenverschlüsselung und Authentizität

Die Verschlüsselung von Informationen und Daten kann aus verschiedenen Gründen sinnvoll sein:

- gemeinsam genutzten Computer, Daten für die Mitbenutzer unlesbar
- unberechtigt Zugang zu einem Computer
- Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien
- eMail werden über unsichere Pfade verteilt
- Nutzung von unsicheren WLAN in öffentlichen Bereichen -> Verschlüsselt kommunizieren

Die Möglichkeiten wie Daten auf einem Gerät verschlüsselt werden können, variieren abhängig vom verwendeten Betriebssystem und dessen Version. Die Qualität der Datenverschlüsselung in neueren Plattformen und Produkte-Versionen ist gestiegen.

Die Verschlüsselung im Internet dient grundsätzlich drei Zielen:

- **Vertraulichkeit**: Die Nachricht ist nur für denjenigen lesbar, für den sie bestimmt ist.
- **Authentizität**: Die Echtheit des Absenders wird gewahrt. Der Absender ist die Person (oder das System), welche als Absender angegeben wird.
- **Integrität**: Die Information wird auf dem Weg zwischen Absender und Empfänger nicht verändert.

Die Verschlüsselung auf mobilen Geräten macht grundsätzlich Sinn, ist aber im Zusammenhang mit E-Business-Anwendungen ebenfalls wichtig. (User, Passwort, Kreditkarte, …)

Auf dem Weg zur Arbeit, auf Reisen oder auch Im Büro und daheim sind digitale Endgeräte (Smartphones, Tablets) immer dabei. Mit den mobilen Geräten werden private und geschäftliche sowie persönliche und vertrauliche Informationen ausgetauscht und Daten direkt gespeichert.

Für Anwenderinnen und Anwender ist es sinnvoll, das gesamte mobile System oder nur einzelne Daten zu verschlüsseln.

Die Frage der Authentizität ist sowohl in der digitalen wie auch der physischen «realen» Welt ein Thema. Über Jahrhunderte hinweg konnte die Identität einer Person mit einem analogen Ausweis nachgewiesen werden (Pass, Empfehlungsschreiben oder Identitätskarte, Personalausweis). In der digitalen Welt ist ein ähnliches Vorgehen für Personen und Systeme / Dinge möglich. Dazu werden häufig sogenannte Zertifikate verwendet. Ein digitales Zertifikat ist an und für sich ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Systemen / Dingen (Objekten) bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Elektronische Zertifikate und die daraus erstellten digitalen Signaturen sind die Basis zur Sicherstellung von Sicherheit und Vertrauen in der digitalen Welt des WEB und der darin operierenden e-Business Anwendungen.

Eine digitale Signatur verbindet die Identität des Unterzeichnenden (WER) unveränderbar mit dem Inhalt einer Transaktion (WAS) und dem Zeitpunkt der Signierung (WANN). Dazu braucht es international anerkannte und akkreditierter Zertifizierungsdienstanbieter (CSP Certification Service Provider). In der Schweiz sind mehrere solcher Anbieter mit weltweiter Anerkennung (WebTrust) aktiv und bieten elektronische Zertifikate nach Schweizerischer (ZertES) und europäischer Gesetzgebung (ETSI) an.

Ziele

Die Lernenden setzen sich mit der Anwendungs-Architektur sowie dem Umfeld / ICT-Infrastruktur von E-Business Anwendungen auseinander. Sie können die ausgewählte Anwendung in der Unternehmensarchitektur einordnen. Die Themen Sicherheit, Performance, Verfügbarkeit, Stabilität und Durchsatz können sie erläutern.

Arbeitsform

Dies ist eine Partnerarbeit (zu zweien).

Jedes Team behandelt beide Themenbereiche.

Zeitbudget

4 Lektionen plus Hausaufgabe

Aufgabe für die Lernenden

Aufgabe 1

Studium der Datenschutzbestimmungen und erstellen einer Zusammenfassung der für eine e-Business Anwendung relevanten Bestimmungen in einem Dokument.

Aufgabe 2

Analyse der Ansatzpunkte für den Einsatz von Verschlüsselung. Wo in der ganzen Kette kann uns die Verschlüsselung helfen? Was für Möglichkeiten gibt es? Die Ergebnisse und Schlussfolgerungen Aufzeigen in einer Präsentation.

Arbeitsergebnis (Werkstück) Kompetenznachweis

Aufgabe 1: Textdokument der LP abgegeben.
Namenskonvention: Klasse_Module_A4-1_Name1_Name2.pdf

Aufgabe 2: Kurz-Präsentation vor der Klasse vorbereiten sowie der LP abgeben:
Namenskonvention: Klasse_Module_A4-1_Name1_Name2.PPT

Lesestoff

DSG https://www.admin.ch/opc/de/classified-compilation/19920153/index.html
KDSG https://www.belex.sites.be.ch/frontend/versions/7
Auskunftsrecht https://www.edoeb.admin.ch/datenschutz/00618/00802/00813/

E-Shop Analytics und Erfolgsoptimierung (abgelegt in Folder 05_Diverses)