smartlearn
virtual learning. real success.

MODUL 150

E-BUSINESS-APPLIKATIONEN ANPASSEN

ARBEITSBLATT 4

Markus Nufer

Handlungsziele

Dieses Aufgabenblatt behandelt das Handlungsziel 3:

HZ3 «Auswirkungen der Änderungen auf Sicherheit und Schutzwürdigkeit der Informationen bei allen beteiligten Komponenten wie Client, Webserver, Applikationsserver und Datenbankserver überprüfen und dokumentieren».

Die Vorgaben in der Modul-Identifikation geben die Handlungsfähigkeiten für dieses Handlungsziel wie folgt vor:

3.1 Kennt die Bestimmungen des Datenschutzes und der Informationssicherheit und deren Bedeutung für Web-Applikationen.

3.2 Kennt Methoden der Datenverschlüsselung und der Gewährleistung der Authentizität (HTTPS, Zertifikate).

Inhalt

Thema

Das Handlungsziel 3 hat als Objekt die «**Sicherheit und Schutzwürdigkeit von Informationen**» im Zusammenhang mit E-Business Anwendungen. In einem ersten Schritt werden in diesem Arbeitsblatt die Sicherheit und der Schutz von Informationen genauer betrachtet. Ausgehend davon geht es um die Vorgaben aus dem Bereich Datenschutz welche bei E-Business Anwendungen zu beachten sind.

Die Handlungsfähigkeiten sind fokussiert und eingebettet im ganzen Fragenkomplex von Sicherheit, Schutz und Nachvollziehbarkeit und umfassen so die fünf Themen Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit und Verfügbarkeit.

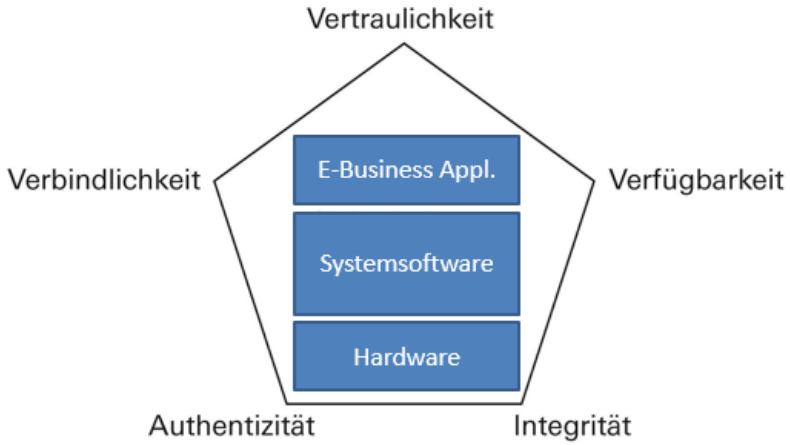

Abb. Informationssicherheit

Daten- / Informationssicherheit

Informationssicherheit beschreibt die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Informationen in unterschiedlichsten Formen und Formaten sind nicht auf digitale Daten beschränkt. Ziel ist es, vor Gefahren und Bedrohungen zu schützen und wirtschaftliche Schäden zu verhindern.

Die Informationssicherheit wird im Rahmen des ICT-Sicherheitsmanagements (Architektur) gewährleistet. Informationssicherheit und IT-Sicherheit können nicht gleichgesetzt werden. Die ICT-Sicherheit behandelt nur einen Teilbereich der Sicherheit von Informationen. Informationen können nicht nur auf IT-Systemen gespeichert sein, sondern auch in Papierform vorliegen oder kann mündlich weitergegeben werden.

Während sich die ICT-Sicherheit hauptsächlich auf den Schutz von in elektronischer Form gespeicherten Daten fokussiert, beschränkt sich die Informationssicherheit grundsätzlich nicht auf digitale Formen von Informationen.

Die allgemeinen Schutzziele von Informationen (und Daten) umfassen die Sicherstellung:

- der **Vertraulichkeit** von Informationen
  welchen Personen Informationen einsehen oder verändern dürfen.
- der **Integrität** von Informationen
  Sicherung, dass Informationen nicht unerkannt bzw. unbemerkt verändert werden.
- der **Verfügbarkeit** von Informationen
  Zeit in denen Informationen verfügbar sind.
- der **Verbindlichkeit** von Informationen
  zweifelsfreie und gegebenenfalls gerichtsverwertbare Zuordnung (Log, Signaturen).
- der **Authentizität** von Informationen
  Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Information.

Schutz von Informationen

Die Schutzwürdigkeit von Informationen wird grundsätzlich vom Owner (Besitzer) oder Ersteller / Lieferant von Informationen festgelegt. Die verschiedenen Gesetze und Verordnungen legen dazu die Grenzen fest.

Art. 13 der Bundesverfassung legt grundlegend fest, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehr sowie auf Schutz vor Missbrauch ihrer persönlichen Daten hat.

Zu den besonders schützenswerten Daten gelten insbesondere die den Intimbereich des Menschen betreffen, so etwa alle Gesundheitsdaten (vgl. Art. 3 des Bundesgesetzes über den Datenschutz DSG). Grundsätzlich können je nach Kontext alle Personendaten als sensibel betrachtet werden.

«Wer schutzwürdige Informationen verfasst oder herausgibt, weist sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu: GEHEIM, VERTRAULICH, INTERN.»[1]

Mit einem **Geheimhaltungsgrad** (auch Geheimhaltungsstufe genannt) werden Informationen entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft. Dabei wird jedes Objekt (Dokument) gemäss seiner Schutzwürdigkeit und Gefährdung einem Schutzgrad (Schutzklasse) zugeordnet.[2]

Datenschutz

Datenschutz ist ein in der zweiten Hälfte des 20. Jahrhunderts entstandener Begriff, der teilweise unterschiedlich definiert und interpretiert wird. Je nach Betrachtungsweise wird Datenschutz verstanden als Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch Schutz der Privatsphäre.[3]

Der **Datenschutz** umfasst aus Sicht der ICT organisatorische und technische Massnahmen gegen den Missbrauch von Daten innerhalb einer Organisation. Ursprünglich wurde unter dem Begriff **Datenschutz** der Schutz der Daten selbst im Sinne der Datensicherung, z. B. vor Verlust, Veränderung oder Diebstahl, verstanden.

---

[1] Zitat aus «Verordnung über den Schutz von Informationen des Bundes» 510.411 Art. 4
[2] Auszug aus WiKi https://de.wikipedia.org/wiki/Geheimhaltungsgrad
[3] https://de.wikipedia.org/wiki/Datenschutz

Datensicherung

Die «**Datensicherung**» ist eine Massnahme zur Sicherstellung der **Verfügbarkeit** im Kontext Informationssicherheit. Die auf einem Speichermedium redundant gesicherten Informationen werden in der ICT als Sicherungskopie bezeichnet. Die Aufbewahrung von Sicherungskopien sollte an einem geographisch anderen Standort erfolgen.

Die Pflicht zur Datensicherung in Unternehmungen basiert auf den gesetzlichen Vorschriften über eine ordnungsgemäße, nachvollziehbare, revisionssichere Buchführung.

Die **kurzzeitige Aufbewahrung** (von einem Tag bis drei oder auch sechs Monate) unterscheidet sich die **langfristige Archivierung**. Die Grundsätze zur Archivierung und Nachprüfbarkeit digitaler Datenbestände sind in verschiedenen Gesetzen und Verordnungen geregelt. So gelten beispielsweise für Gesundheitsdaten Zeiträume von 25 Jahren bis zu lebenslänglich + 10 Jahre.

Die langfristige Archivierung stellt grosse Herausforderungen an die ICT dar. Es geht dabei um die Bearbeitung von Datenformate und Speichermedien. Wie sollen beispielsweise Datenbestände auf flexiblen Trägern (Floppy Disk[4] 8-inch) aus der Zeit von 1975 heute noch eingelesen werden? Oder wie kann eine Lotus SmarteSuite AmiPro[5] Datei aus der Zeit von 1995 heute angezeigt werden?

Abb. Datenträger aus der Vergangenheit

Datenschutz-Bestimmungen und deren Bedeutung für E-Business-Anwendungen

Für den Datenschutz sind sehr viele Gesetze und erlasse vorhanden. In der Schweiz gibt es ein Bundesgesetz mit einer Verordnung, sowie in den meisten Kanton und Städten wieder Gesetze und Verordnungen. Organisatorisch gibt es auf Bundesebene den EDÖB Eidg. Datenschutz- und Öffentlichkeitsbeauftragten mit seinem Team sowie in den meisten Kantonen den Datenschutzbeauftragten.

[4] Weitere Infos: https://en.wikipedia.org/wiki/Floppy_disk
[5] Quelle: https://de.wikipedia.org/wiki/Lotus_SmartSuite

Mit den E-Business Anwendungen, welche via Internet International benutzt werden können, stehen die ICT Branche und ihre Kunden zusätzlich in der Pflicht die Internationalen Gesetze und Verordnungen einzuhalten (EU, USA, etc.).

Gesetzliche Grundlagen

- Bundesgesetz über den Datenschutz (DSG 235.1) und die Verordnung (VDSG 235.11)
- Datenschutzgesetz (KDSG) des Kt Bern (BSG 152.04)
- Die Gesetze der Schweiz und der EU
- Personensicherheitsprüfung VBS[6]
- Europäischen Datenschutzkonvention (mit Bestimmungen zum Schutz des Menschen bei automatischer Verarbeitung von Daten)

Nach europäischem Recht und Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Das Speichern und Verarbeiten von personenbezogenen Daten sind nur unter Zustimmung des Betroffenen zulässig.

Angriffsmethoden bei WEB Anwendungen

Es gibt unzählige Möglichkeiten, Schwachstellen in einer Webanwendung zu finden und diese auszunutzen. Im Modul 183 werden diese vertieft behandelt. Einige Beispiele:

- SQL-Injection
- Cross-Site-Scripting
- Session Hijacking
- Cross-Site-Request-Forgery
- Directory Traversal
- E-Mail-Injection
- Man-In-The-Middle-Angriff
- Man-in-the-Browser
- Denial of Service

Datenverschlüsselung und Authentizität

Verschlüsselung

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

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

[6] https://www.vbs.admin.ch/de/themen/integrale-sicherheit/personensicherheitspruefung.html

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.

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. Deshalb macht die verschlüsselte Speicherung auf mobilen Geräten grundsätzlich Sinn, ist aber im Zusammenhang mit E-Business-Anwendungen noch wichtiger (User, Passwort, Kreditkarte, …).

Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung

Beim symmetrischen Verfahren wird mit demselben Schlüssel ver- und entschlüsselt.
Beim asymmetrischen Verfahren hingegen gibt es nicht nur einen Schlüssel, sondern zwei; nämlich einen öffentlichen Schlüssel, der für jeden zugänglich ist und einen privaten Schlüssel, der geheim gehalten werden muss. Der öffentliche Schlüssel ist dabei für die Verschlüsselung zuständig und der private Schlüssel für die Entschlüsselung.

Einsatzbereich der Verschlüsselung

Auf dem Client
Für den Desktop existieren verschiedene Verschlüsselungsmöglichkeiten. Diese werden entweder mit Daten-Cloud Lösungen mitgeliefert, wie dies bei SecureSafe[7] möglich ist. Zitat: „SecureSafe zeichnet sich durch die mehrfache Verschlüsselung, die dreifache Datensicherung und die Zero-Knowledge-Architektur für höchsten Privatsphärenschutz aus.“

Die Lösung von Symantec[8] bietet wahlweise die Verschlüsselung der ganzen Festplatte oder einzelner File-Share an, die Verschlüsselung von eMails und die Verwaltung von Passwörtern ist ebenfalls im Angebot.

WEB Anwendungen
Eine Verschlüsselung der Verbindungen ist grundsätzlich empfehlenswert für einen Client, der am WEB angeschlossen ist und klassifizierte Informationen austauscht. Dazu gehören auch Remote-Zugriffe auf einen Server als privilegierter User!

Speicherung
Daten von E-Business Anwendungen werden je nach Situation und Einstufung der Schutzwürdigkeit und der Bedrohungslage verschlüsselt abgelegt. Einzig bei der Verarbeitung in der E-Business Anwendung sind diese dann unverschlüsselt im System.

Authentifizierung - Authentizität

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

[7] https://www.securesafe.com/de/
[8] https://www.symantec.com/de/de/products/encryption

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.

OATH Initiative for open authentication

Abb. Hacker sind überall (aus Präsentation oath)

Heute sind verschiedene Authentifizierungs-Methoden übliche:

- Simple Passwörter
- Challenge Response
- One time Psswords
- Public Key Encryption
- Single SignOn
- Adaptive Authentication
- Biometrics
- Push Technologies
- SMS
- Image Recognition
- Hardware Tokens
- Software Tokens

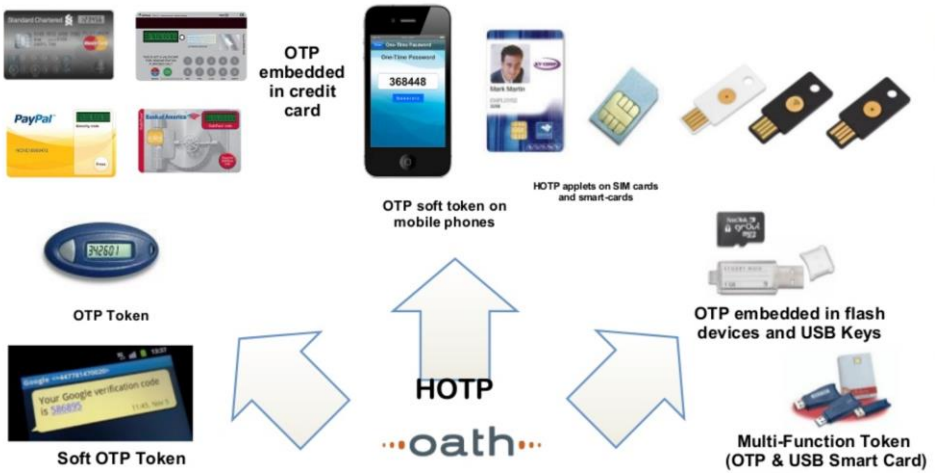

Abb. Token Innovationen (Quelle OATH)

The Open Authentication Initiative (OATH) von führende ICT Unternehmen hat zum Ziel, «Strong Authentication Technology» im Netz und bei Anwendungen.

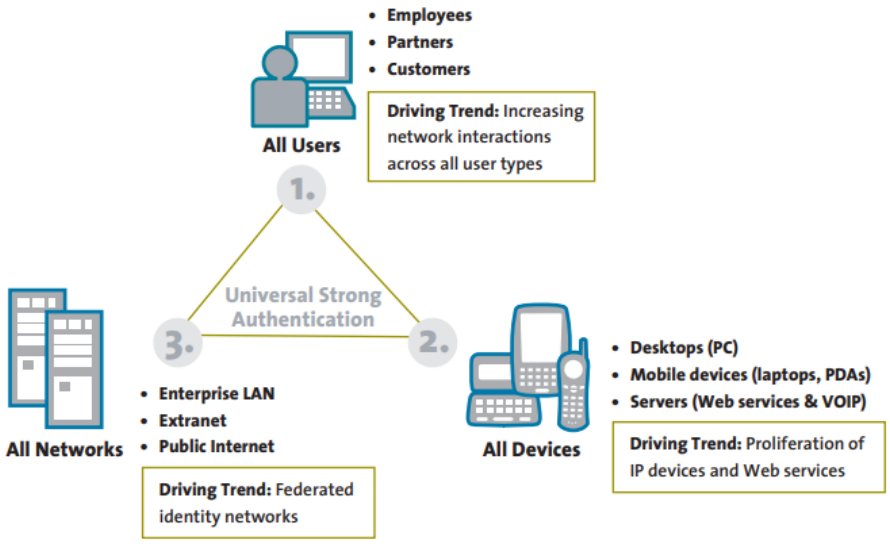

Abb. Strongly Authenticating Everyone and Everything—Everywhere

OHTA Authentication

Um auf geschützte Services/Daten auf dem Resource Server zuzugreifen, muss ein **«Access Token»** vom Client als Repräsentation der Autorisierung übermittelt werden. Mittels des Parameters scope können die mit dem Access Token verbundenen Berechtigungen festgelegt werden. Zum einen kann der Client gewünschte Berechtigungen beim Authorization Server anfragen, zum anderen teilt dieser die gewährten Berechtigungen mit. Das Access Token hat eine zeitlich begrenzte Gültigkeit.

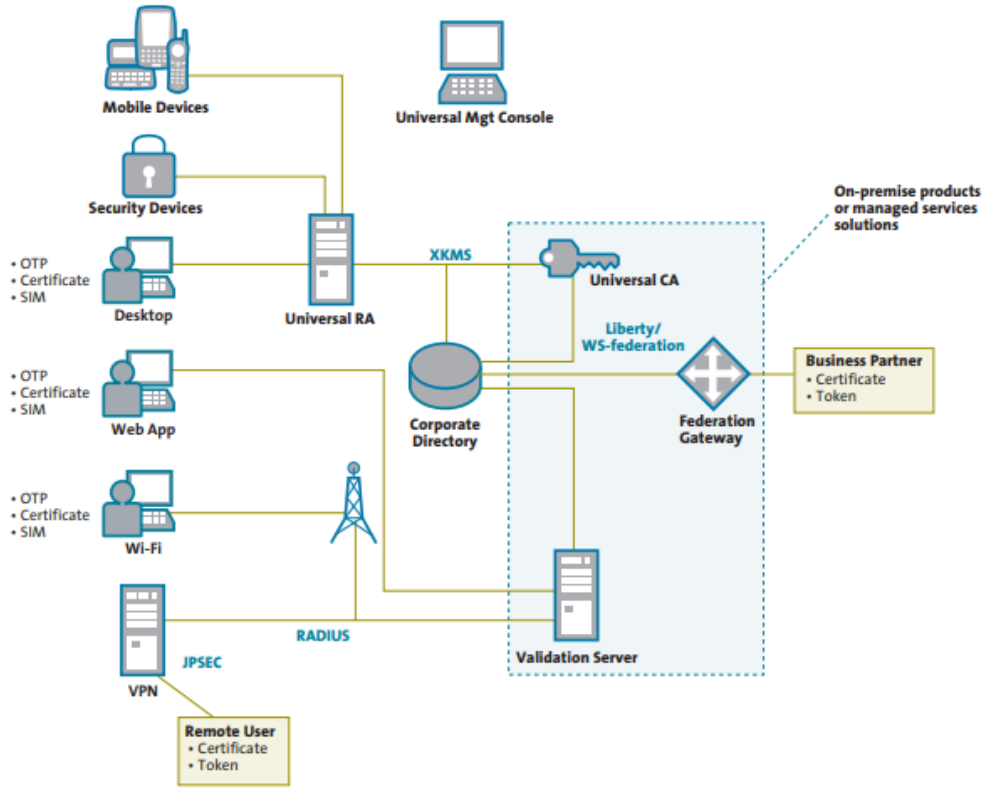

Abb. Universal Strong Authentication

Passwörter und Benutzer-Identifikation

Seit jeher kann durch die Vergabe von persönlichen Benutzer-Identifikationen und Benutzer-Passwörtern ein User identifiziert werden. Die Unsitte in Organisationen, unpersönliche Benutzer (z.B. Abteilungs-Identifikation mit einem trivialen Passwort) zu definieren, sollte der Vergangenheit angehören.

Um die Nachvollziehbarkeit bei E-Business Applikationen gewährleisten zu können, sind persönliche Benutzer-Identifikationen und sichere Passwörter notwendig. Eine Steigerung der Sicherheit bei der Identifikation ist mit dem Einsatz von elektronischen Zertifikaten möglich (vgl. entsprechender Abschnitt).

Einsatz der Authentifizierung auf dem Frontend

Single Sign on
Single-Sign-On („Einmalanmeldung“) bezeichnet in der IT ein für den User einfaches Authentifizierungsverfahren:

1. Ein Benutzer meldet sich einmalig an seinem Arbeitsplatz an.
2. Er erhält dadurch Zugriff auf alle Rechner und Dienste (inklusive der Cloud), für die er lokal autorisiert ist, solange er sich am selben Arbeitsplatz aufhält.
3. Sobald sich der Benutzer von seinem Arbeitsplatz abmeldet, entfallen alle Zugriffsrechte. Dies passiert entweder nach einem vorher festgelegten Zeitraum oder wenn der Benutzer manuell ein Single-Sign-Out bzw. -Off ausführt.

SSO ist ein Zugangsverfahren für mehrere assoziierte, aber voneinander unabhängige Anwendungen. Der Benutzer muss sich nur einmal anmelden und seine Zugangsdaten nicht bei jeder Anwendung einzeln angeben.

Aufgrund ihrer Benutzerfreundlichkeit kommen Single-Sign-On-Verfahren sowohl im privaten (Webanwendungen und private Clouds) als auch im professionellen Bereich (unternehmensintern genutzte Applikationen und Portale im Intranet) zum Einsatz.

2 Faktor Authentisierung
Die **Zwei-Faktor-Authentisierung** (2FA), häufig auch als Zwei-Faktor-Authentifizierung bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden, oder Passphrase und TAN beim Online-Banking. Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung.[9]

Verschiedene E-Business Anwendungen werden heute auch mit dem «Google Authenticator»[10] abgesichert.

Multi-Faktor-Authentifizierung mit Google Authenticator
Der Google Authenticator als Beispiel für eine Zwei-Stufen Authentifizierung ermöglicht die Zwei-Stufen-Authentifizierung mittels Einmalkennwörtern gemäss der branchen-übergreifenden Initiative For Open Authentication (OATH)[11].

TouchID und FaceID
Die Authentifizierung kann auch mit eindeutigen Merkmalen des menschlichen Körpers erfolgen. So sind etwa Iris-Scanner bei der Zutrittskontrolle in Sicherheitsanlagen verbreitet. Die Gesichtserkennung und der Fingerabdruck sind ebenfalls verbreitet.

Beim Vergleich von Face ID und Touch ID funktioniert das Entsperren mittels Touch ID etwas schneller. Einen weiteren Vorteil hat Touch ID mit Face ID gemeinsam: Die Daten für die Authentifizierung werden in einem speziell abgesicherten Bereich des Prozessors sicher und verschlüsselt aufbewahrt.

Cremes oder andere Öle wirken sich im Vergleich von Face ID und Touch ID nachteilig auf das letztere System aus. Falls der Sensor selbst nass oder schmutzig ist, können ebenfalls Probleme bei der Entsperrung auftreten.

Registrierungsvorgang

Es sind grundsätzlich zwei Registrierungsvorgänge zu unterschieden:

- Einfache Zertifikate können übers WEB erstellt werden
- Qualifizierte Zertifikate bedingen eine persönliche Vorsprache ab einer Registrierungsstelle[12] zwecks Überprüfung der Identifikation.

Das elektronische Zertifikat und der dazugehörige persönliche Schlüssel müssen zwingend auf einer sicheren Signaturerstellungseinheit gespeichert werden. Die Standardlaufzeit des Zertifikates beträgt 3 Jahre.

Das **Secure E-Mail Zertifikat** wird auf Personen ausgestellt und kann zum Signieren, Verschlüsseln und Authentisieren verwendet werden. Eine rechtlich bindende Signierung von Dokumenten und Daten kann ebenfalls mit dem Secure E-Mail Zertifikat erfolgen, sofern keine qualifizierte Schriftlichkeit verlangt ist oder zwischen den Parteien vereinbart wurde, dass gegenseitig dieses Zertifikat zur Zeichnung verwendet werden kann.

[9] Quelle: https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung
[10] https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=de
[11] Vergleiche: https://openauthentication.org/
[12] Link auf Registrierungsstellen: https://www.quovadisglobal.ch/Registrierung/RegistrationOffices.aspx

Das Secure E-Mail Zertifikat ist ein Soft-Token Zertifikat (P12 Datei) und nur in Verbindung mit einer lokal installierten E-Mail Anwendung einsetzbar.

Das **fortgeschrittene persönliche Zertifikat** APC oder ACC (Advanced Personal Certificate und Advanced Commercial Certificate) wird auf Personen ausgestellt und kann zum Signieren und Authentisieren verwendet werden. Eine rechtlich bindende Signierung von Dokumenten und Daten kann ebenfalls mit dem fortgeschrittenen persönlichen Zertifikat erfolgen, sofern keine qualifizierte Schriftlichkeit verlangt ist oder zwischen den Parteien vereinbart wurde, dass gegenseitig dieses Zertifikat zur Zeichnung verwendet werden kann. Das Signieren von PDF Dokumenten inkl. automatischer Erkennung in Adobe erfordert als Datenträger zwingend USB Token oder Smartcard. Merkmale Advanced Signature:

1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet.
2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers.
3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.
4. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Das **qualifizierte persönliche Zertifikat** QPC oder QCC (Qualified Personal Certificate und Qualified Commercial Certificate) erfüllt die höchsten Anforderungen des schweizerischen Signaturgesetzes (ZertES) und des europäischen Standards (ETSI). Es dient der Erstellung von rechtlich verbindlichen digitalen Signaturen (gemäss schweizerischem Obligationenrecht OR der Handunterschrift gleichgestellt) und wird zum elektronischen Unterzeichnen von Dokumenten verwendet.

Das **qualifizierte persönliche Zertifikat** kann nur auf natürliche Personen ausgestellt werden. Es besteht auf Wunsch die Möglichkeit, zusätzlich den Namen der Organisation (Unternehmen, Firma, Organisation, Verband, Verein usw.), die firmeninterne Organisationseinheit und/oder die Funktion des Zertifikatsinhabers eintragen zu lassen. Möglich ist auch die Verwendung eines Pseudonyms anstatt des Namens des Zertifikatsinhabers, was auch anonymisierte digitale und rechtsgültige Unterschriftsprozesse ermöglicht.

digitale Signatur

Die digitale Signatur entspricht einer Unterschrift oder einem Siegel. Nur wer den Siegelring (hier den Private-Key) besitzt, kann die Signatur anfertigen. Im Gegensatz zur Geheimhaltung bleibt beim digitalen signieren die Botschaft unverschlüsselt. Es wird lediglich ein Hash-Code der Botschaft **verschlüsselt**; und zwar diesmal mit dem **Private-Key**. Alle sollen die Herkunft der Botschaft überprüfen können. Hierzu wird mit dem Public-Key der verschlüsselte Hash-Code dechiffriert und mit dem Hash-Code der unverschlüsselten Botschaft verglichen. Da der Public-Key öffentlich zugänglich sein soll, ist es für jede Person möglich, die Unterschrift auf Echtheit zu prüfen; vorausgesetzt natürlich, dass bereits dem Public-Key vertraut werden kann ;-)

ICT Infrastruktur Sicherheit

Wie kann man sich optimal vor Datenmissbrauch und Cyberkriminalität schützen?

Bei der Informatik-Sicherheit ist es wie beim Einbruchschutz für Häuser oder beim Diebstahlschutz für Autos: Jede noch so ausgeklügelte Massnahme kann früher oder später von einem Einbrecher überlistet werden. Ziel von Einbrüchen oder Diebstählen sind aber in erster Linie Häuser und Autos mit mangelnden Sicherheitsvorkehrungen.

Netzwerke, Server, Speicher und ICT-Infrastruktur bilden das Nervenzentrum und Rückgrat jedes ICT-Systems und damit die Basis für den Betrieb der E-Business Applikationen. Die ICT-Systeme «leben» von den ein- und ausgehenden Datenströmen und sind so von Natur aus anfällig für Angriffe. Robuste, integrierte Sicherheitsmechanismen können geschäftskritische und persönliche Informationen/Daten gegen unautorisierte Zugriffe und Manipulationen schützen. Eingebettete Sicherheitslösungen -möglicherweise in der Form von Trusted Platform Modules (TPM)- erfüllen die Forderung nach zuverlässiger ICT-Sicherheit.

Weg der Daten

In den heute weit verbreiteten Systemen (Client-Server, WEB Anwendungen etc.) mit einem Anschluss des Clients üblicherweise über ein WLAN sind viele Angriffspunkte möglich.

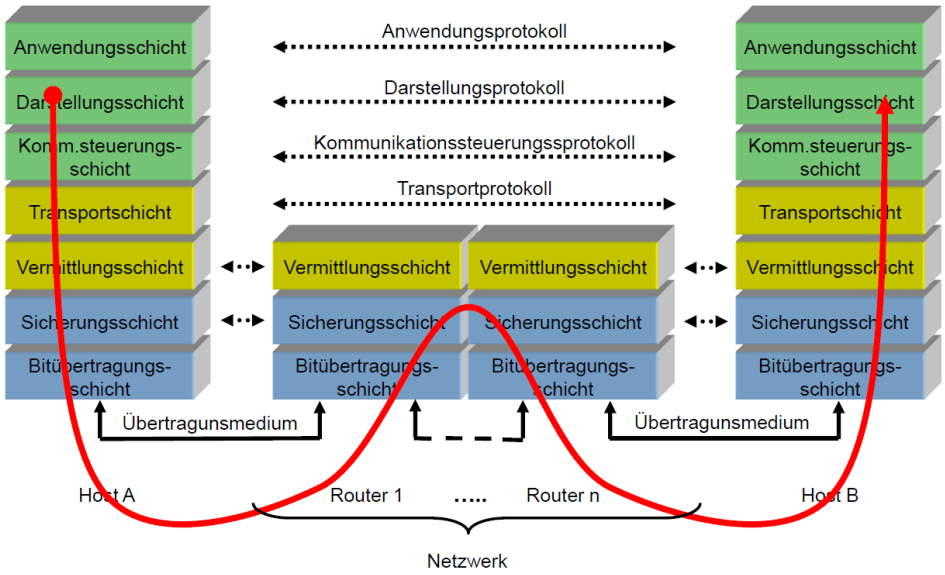

Abb. Kommunikation zwischen zwei Host (Client und Server) über einen Router

Heikle Daten können für die Dauer der Übertragung mit dem Einsatz von Verschlüsselung einfach geschützt werden.

Innerhalb der E-Business Anwendung und bei der Datenübertragung zu einer anderen E-Business Anwendung sind zwar ebenfalls Gefahren vorhanden, aber die Wahrscheinlichkeit eines Angriffes sind deutlich geringer als im Netzwerk. Abhängig von der Ausbreitung des lokalen Netzwerkes und die Form der Datenspeicherung können auch diese Angriffspunkte durch eine Verschlüsselung gesichert werden.

Sicherheit der Backups

Der vollständige oder teilweise Datenverlust kann für eine Organisation verheerende Folgen haben. Ein gutes Backup Konzept sorgt da vor - beinhaltet es doch sowohl die Datensicherung wie auch die Sicherung ganzer Server, um bei Bedarf schnell und vollständig Daten und Server wieder herstellen zu können. Einige Punkte in einem Backup-Konzept:

- Wie viele? Ein Backup ist gut. Zwei und mehr Backups sind besser.
- Wie oft? Wie viele Backups und Snapshots erstellt werden. Einmal täglich, mehrmals täglich, etc. Mittels Generationenprinzip auch auf Daten von vorgestern und von letztem Jahr zugreifen können.
- Wohin? Die Backups sollen örtlich getrennt sein und mindestens ein Backup dezentral (ausser Haus) aufbewahrt sein.
- Was? Klare Definition, welche Daten und welche Server gesichert werden.
- Wie? Mit welchem Backup Programm und auf welches Medium werden die Sicherungen gemacht.
- Restore testen! Überprüfung, ob die Daten und Systeme täglich gesichert werden und ob die Daten zurückgeladen werden können.
- Wer? Festlegen wer zuständig ist für die Durchführung und die Kontrolle.

Abhängig vom Speicherort (wie Beispielsweise in der Cloud) bestehen grosse Risiken bei den Backups. Ein möglicher Diebstahl und ein unerlaubter Zugriff muss abgesichert werden; es muss klar sein, wer auf die Backups zugreifen darf und kann.

Firewall und Antivirusprogramm

Diese Schwelle bildet beim vernetzten digitalen Arbeiten Sicherheitssoftware wie Firewalls und Antivirenprogramme. Sie gehören zum Grundinventar jeder ICT-Infrastruktur. Die teuerste Software nützt aber nichts, wenn sie nicht auf dem neusten Stand gehalten wird. Dafür ist der Systemverantwortliche oder in Kleinfirmen der Unternehmer selber verantwortlich. Die Antivirensoftware und die Firewall müssen ständig aktualisiert werden - bestenfalls werden die neusten Versionen automatisch aus dem Web heruntergeladen. Die Firewall muss zudem auf allen Internetnetzwerkverbindungen aktiviert sein. Schliesslich sollten regelmässig die Updates für das Betriebssystem installiert werden. Ein Softwarefachmann kann den PC so einrichten, dass alle nötigen Aktualisierungen mehr oder weniger automatisch ausgeführt werden.

Passwörter und Benutzer-Identifikation

Zur IT- und Datenschutz-Sicherheit gehört auch die Vergabe von persönlichen Benutzer-Identifikationen und Benutzer-Passwörtern für jeden PC und von Passwörtern bei Bildschirmschonern.

Die persönliche Benutzer-Identifikationen und sichere Passwörter bilden die Basis für die Identifikation von Benutzern. Eine Steigerung der Sicherheit bei der Identifikation ist mit dem Einsatz von Zertifikaten möglich.

Arbeitsblatt

Zielsetzung

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 Einzelarbeit oder eine Partnerarbeit (zu zweien).

Jedes Team behandelt das Thema für sich und liefert die Ergebnisse als Dokument der Lehrperson ab. Die LP kann einzelne Teams auffordern, die Präsentation vor der Klasse zu halten.

Zeitbudget

5 Lektionen plus selbständiges Studium und Arbeitsleistung Aufgaben für die Lernenden

Aufgabe 1

Studium der Datenschutzthematik und der relevanten Bestimmungen. Erstellen einer Zusammenstellung der relevanten juristische Bestimmungen Punkte, welche für die in den bisherigen Arbeitsblättern behandelten E-Business Anwendungen.

Aufgabe 2

Analyse Möglichkeiten für eine sichere Authentifikation. Zusammenstellen der implementierten Sicherheitsmechanismen die in den bisherigen Arbeitsblättern behandelten E-Business Anwendungen. Aufzeigen allfälliger Massnahmen.

Aufgabe 3

Analyse der Möglichkeiten für den Einsatz von Verschlüsselung. Wo in der ganzen Kette kann uns die Verschlüsselung helfen? Was für Möglichkeiten gibt es und was ist zu empfehlen? Aufzeigen allfälliger Massnahmen für die in den bisherigen Arbeitsblättern behandelten E-Business Anwendungen.

Aufgabe 4

Zusammenstellung der Aufgaben 1 bis 3 in einer Management-Präsentation.

Arbeitsergebnis (Werkstück) Kompetenznachweis

Aufgabe 1, 2 und 3:	Textdokument der LP abgegeben. Für LP welche die Unterlagen per Mail einfordern: Namenskonvention: Klasse_Module_A4_Name1_Name2.pdf
Aufgabe 4:	Kurz-Präsentation (8 Minuten) für die Geschäftsleitung vorbereiten sowie der LP abgeben. Für LP welche die Unterlagen per Mail einfordern: Namenskonvention: Klasse_Module_A4_Name1_Name2

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/

Juristische Infos im Internet

- Die DSGVO 2018 vom EDÖB - Auswirkungen auf die Schweiz vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragter - die Berufsbezeichnung schlechthin :-). Hier finden Sie auch ein PDF mit den konkreten Auswirkungen auf die Schweiz - 11 Seiten, also für juristische Verhältnisse ganz ok.
- Recht einmalig sind die Restriktionen in Bezug auf Rechtsberatung in Deutschland. In den 20-ern des letzten Jahrhunderts eigentlich als Schutz vor unqualifizierter Rechtsberatung angedacht, wurden dann 1935 von den Nationalsozialisten zur Ausgrenzung jüdischer Juristen entsprechende Gesetze eingeführt. Die Entstehung dieser Gesetzeslage können sie im Eintrag Rechtsberatungsgesetz auf Wikipedia nachvollziehen.
- e-recht24.de - ist zwar mehr für den deutschsprachigen EU-Raum, aber die Sonderstellung der Schweiz ist im Internet auch nicht mehr das, was es mal war :-)
- drweb.de Linkverzeichnis - viele Informationen zum Thema Abmahnungen. Auch wenn das Thema in der Schweiz (noch?) nicht so dramatisch erscheint, sind ein paar Grundkenntnisse sinnvoll, wenn Sie sich aktiv im Internet bewegen.
- und noch eine Möglichkeit...weitere Informationen zum Thema Abmahnungen
- Der wesentliche Unterschied in der Gesetzgebung zwichen der Schweiz und Deutschland/Österreich besteht darin, dass die Anwaltskosten der Abmahnung außergerichtlich nicht auf den Abgemahnten überwälzt werden können. In der Schweiz muss der Abmahnende die entstehenden Kosten der Abmahnung also selber tragen.
- Ein weiteres Thema ist die Impressumspflicht. Weder in der Schweiz noch in Deutschland müssen private Homepages ein Impressum enthalten - solange sie keine gewerbsmässigen Ziele verfolgen. Spätestens, wenn Sie einen Webauftritt für

Geschäftskunden realisieren sollten Sie sich aber mit dem Thema Impressum beschäftigen.

- Viele Gerüchte gibt es auch zum Thema Disclaimer. Hier geht es um Haftungsausschluss. Sie werden teilweise in E-Mails verwendet (zumeist aber sinnlos) und finden sich auch auf vielen Websites (meistens ebenso sinnlos).
- Sie finden häufig die Begriffe IT-Recht beziehungsweise IP-Recht. IT sollte klar sein: *information technology*. IP ist in diesem Zusammenhang die Abkürzung von *intellectual property* und betrifft das Recht des geistigen Eigentums. Damit beschäftigt sich das **Eidgenössische Institut für Geistiges Eigentum** ige.ch
- Zum Thema Urheberrecht gibt es auf dem educa.ch-Server ein ganzes Dossier: Das Urheberrecht im Bildungsbereich
- Probleme, die beim Einsatz von Fertigwebshops entstehen können und wie man sie vermeidet: e-recht24.de
- Opt-in, Double Opt-In vom Confirmed Opt-In und die Grenzen durch ein Amtsgericht.
- Abschliessend noch ein Link auf die juristische Fäkultät der Uni Basel, die unter anderen das Lugano-Übereinkommen erwähnen. Hier geht es um die rechtlichen Beziehungen auch bezüglich Internetrecht mit der EU.

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