Kanton St.Gallen
Gewerbliches Berufs- und Weiterbildungszentrum St.Gallen

Grundbildung

gbssg.ch

Informatik - Modul 231.

Datenschutz und Datensicherheit anwenden

Datensicherheit – Eine Einführung

1 Einführung Datensicherheit. 2

1.1 Einführungsauftrag 2

1.2 Definition von Datensicherheit 2

1.3 Business Challenges 3

2 Aspekte und Methoden der Datensicherheit. 5

2.1 Encryption 5

2.2 Datenlöschung 6

2.3 Data masking 6

2.4 Data resiliency 7

3 Lösungen zur Datensicherheit. 8

3.1 Data discovery und classification tools 8

3.2 Data and file activity monitoring 8

3.3 Vulnerability assessment sowie risk analysis tools 8

3.4 Automated compliance reporting 8

4 Datensicherheits-Strategien. 10

4.1 Physische Sicherheit von Servern und Endgeräten 10

4.2 Access management 10

4.3 Unterschied von Authentifizierung und Autorisierung 11

4.4 Passwort Manager und Passwortverwaltung 11

4.5 Softwareaktualisierung 11

4.6 Backups 12

4.7 Sensibilisierung der Mitarbeiter 14

4.8 Network and endpoint security monitoring 15

5 Data security trends. 16

5.1 AI / cognitive computung / quantum computung 16

6 Datensicherheit im breiteren Sichtfeld der IT Landschaft. 17

6.1 Datensicherheit auf der cloud implementieren 17

6.2 Multicloud security 17

6.3 Datensicherheit und BYOD 18

6.4 IoT und Datensicherheit 18

7 Datenschutz in der Schweiz. 19

1 Einführung Datensicherheit.

1.1 Einführungsauftrag

Sie haben sich auf den Seiten 16-19 im bereits bearbeiteten Datenschutz-Skript mit der Gegenüberstellung von Datenschutz vs. Datensicherheit auseinandergesetzt. Es wurde eine grobe Einführung über die Definition und den wesentlichen Inhalt von Datenschutz gegeben.

Arbeitsauftrag «Mindmap Datensicherheit»

Erledigen Sie den folgenden Auftrag zu zwei:
Erstellen Sie auf einem A3 Blatt ein Mindmap über die wesentlichen Aspekte von Datensicherheit. Was wissen Sie alles bereits über Datensicherheit?

Die Gegenüberstellung von Datenschutz vs. Datensicherheit darf auch behandelt werden.

Informationen zu Datensicherheit finden Sie unter:
https://www.ibm.com/topics/data-security

1.2 Definition von Datensicherheit

Unter Datensicherheit versteht man den Schutz digitaler Information vor unautorisiertem Zugriff, Datenkorruption sowie Diebstahl während dem ganzen Lifecycle der Daten!

Wenn ein Datenschutzsystem aufgebaut wurde, sollte dieses nicht nur gegen Cyberangriffe, sondern auch gegen insider data breaches sowie menschliches Fehlverhalten schützen. Denn dies sind nach wie vor die häufigsten Fälle von Datenschutzverletzungen.

Datensicherheit bedeutet unter anderem Systeme und Tools bereitzustellen, mit welchen klar sichtbar gemacht werden kann, wo sich geschützte Daten befinden und wie diese genutzt werden. Diese Tools sollten idealerweise data encryption sowie data redaction (z.B. Kreditkarten-Nr. bei SQL Datenbank) bereitstellen. Weiter müssen diese Tools mit den aktuellen Gesetzen konform sein.

Spannende Links zu diesem Thema:

data redaction:

- https://www.imperva.com/learn/data-security/data-masking/
- https://www.oracle.com/technetwork/database/options/data-masking-subsetting/learnmore/faq-security-asdr-external-3215961.pdf

cloud adoption:

- https://www.hcltech.com/technology-qa/what-is-compliance-assessment-for-cloud-adoption#:~:text=Cloud%20Adoption%20is%20a%20strategic,scalability%20of%20data%20base%20capabilities.&text=In%20fact%20the%20depth%20of,enterprise%2Dready%20cloud%20services%20availability.

1.3 Business Challenges

In der Praxis ist Datensicherheit doch sehr schwierig zu implementieren. Dies hat verschiedene Gründe:

- Die Datenmengen die durch Unternehmen generiert werden, verwaltet und verarbeitet werden müssen sind riesig und nehmen stets zu.
- Die Rechnerumgebungen sind heutzutage komplexer als früher. So sind heute Daten häufig auf der öffentlichen cloud, enterprise data center sowie vermehrt auch auf Internet-of-Everthing devices und Sensoren verteilt.
  Dies ermöglicht einem potentiellen Angreifer eine viel grössere Angriffsfläche (attack surface), was einen komplexen Datenschutz erfordert.
- Die Konsumenten sind vermehrt auf das Thema Datenschutz sensibilisiert. Dies zeigte sich z.B. bei einer Abstimmung in der Schweiz, wo sich die Bevölkerung gegen eine digitale ID aussprach, welche von privaten Unternehmen verwaltet worden wäre. (https://www.e-id-referendum.ch/)
- Es gibt immer mehr politische Vorstösse und neue Gesetze welche mehr Datensicherheit fordern, z.B.:
  - Europe's General Data Protection Regulation (GDPR)
  - California Consumer Protection Act (CCPA).
  - Health Insurance Portability and Accountability Act (HIPAA), für den Schutz elektronischer Patientendaten
  - Sarbanes-Oxley Act (SOX), welche Aktionäre von öffentlichen Firmen vor Abrechnungsfehlern und Finanzbetrug mit Bussen von Millionen Dollar schützen soll.

Wenn es um Datensicherheit geht, sind wir alle im selben Boot. Denn jeder von uns hat digitale Daten welche es zu schützen gilt.

Arbeitsauftrag «Persönliche Auswirkungen data breach»

Schreiben sie auf, wo überall Daten von Ihnen gespeichert sind.
Was sind das für Daten ?
Was hätte ein data breach für Sie für Folgen ?

2 Aspekte und Methoden der Datensicherheit.

2.1 Encryption

Durch die Verschlüsselung kann ein wirksamer Schutz der Daten erreicht werden. Dabei kommen verschiedene kryptographische Werkzeuge zum Einsatz. Für den Datenaustausch werden in der Regel andere Algorithmen verwendet, zum Beispiel für die langzeitliche Einlagerung der Daten.

Verschlüsselung ist so ein zentrales Werkzeug für die Datensicherheit, dass wir hier eine kurze Einführung über AES, RSA, sowie Diffie-Hellmann machen wollen. Zuerst jedoch, was ist symmetrische / asymmetrische Verschlüsselung?:

- https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/
- AES:https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- RSA: https://www.comparitech.com/blog/information-security/rsa-encryption/
- Diffie-Hellmann: https://www.youtube.com/watch?v=NmM9HA2MQGI

Weiter ist das Key Managment (security key management) natürlich von essentieller Bedeutung, da mit dem Key natürlich die ganze Sicherheit der kryptographischen Algorithmen steht oder fällt. Siehe dazu:

- https://info.townsendsecurity.com/definitive-guide-to-encryption-key-management-fundamentals

Arbeitsauftrag «Storage»

Wie meine Daten verschlüsselt sind, im storage als auch bei der Übertragung.
- Wie sind die Daten dorthin gelangt (wie wurde verschlüsselt)?
- Wie liegen die Daten auf dem storage? Wie sind diese verschlüsselt?.

Eine wichtige Anmerkung zu encryption Algorithmen. Mathematiker kennen ausser quantum computing und anderen ‹Tricks› keine Mittel zum Knacken der Algorithmen. Aber ist die *Implementierung* dieser Algorithmen vielleicht mit Hintertürchen bestückt? (Man denke z.B. an die NSA, CIA usw…) Sehen Sie das Problem hier?
Leider bleibt das Risiko, dass z.B. whatsapp seine End-to-End Encryption Algorithmen nicht *ehrlich* implementiert. So könnten dann gewisse Individuen Ihren ganzen traffic mithören und entschlüsseln. Deshalb gilt in der Kryptographie: Die Verschlüsselungsalgorithmen müssen

bekannt gemacht werden. Dies sind sie auch! Nur vertrauen Sie facebook usw. ob sie *Ihre* Algorithmen auch sauber implementieren?

Verschlüsselung von Daten in der Praxis

Für den Praxiseinsatz gibt es verschiedene Tools, welche für verschiedene Betriebssysteme betrieben werden können.

Siehe dazu

- https://www.tecmint.com/file-and-disk-encryption-tools-for-linux/
- https://www.tecmint.com/linux-hard-disk-encryption-using-luks/

und für MS Windows:

- https://uk.pcmag.com/encryption/83976/the-best-encryption-software-for-2020

2.2 Datenlöschung

Wenn Daten gelöscht sind, so können sie auch nicht mehr kompromittiert werden. Daher ist dies ein zentrales Werkzeug eines Datenschutz Management Systems.
Jedoch gibt es zwei Arten wie Daten gelöscht werden können.

- Wenn nicht spezifisch verlangt, gibt man mit einem Löschbefehlt den Speicher einfach wieder frei. Dies wird durch geeignete Einträge in das filsystem (z.B. FAT 32, ext4, NTFS) erreicht. Dabei ist das Problem das Folgende: Wurde in der Zeit von der Löschung mit jetzt der betroffene Datenspeicher nicht wieder benötigt und somit überschrieben, so liegen die Daten immer noch im Speicher vor!
- Wenn gründlich gearbeitet werden soll, dann müssen bei einer Löschung die Daten die Daten auch SOFORT überschrieben werden. Am einfachsten können einfach überall Nullen hineingeschrieben werden. Dies garantiert eine vollständige Löschung.

2.3 Data masking

Diese Technik ermöglicht vor allem einen guten Workflow und realistische Arbeit mit Daten in der Entwicklung oder zu Testzwecken. Dabei werden mit echten Datensätzen gearbeitet. Nur werden eben personally identifiable data (persönliche Daten) maskiert. Dies kann durch vertauschen dieser Daten, verschlüsseln der Daten, oder einfach durch Ersetzen mit Werten aus Zufallsgeneratoren erreicht werden.

2.4 Data resiliency

Unter Resilienz beschreibt im Wesentlichen Widerstandsfähigkeit. Unter data resiliency versteht man also die Fähigkeit des IT Systems auf jegliche Form der Störung reagieren zu können.

- Ausfall der Hardware (Redudanz)
- Atomarer Unfall oder Angriff / Krieg oder ähnliches
- Hochwasser Erdbeben oder ähnliche Umweltkatastrophen
- Stromausfälle (ink. UPS!)
- Internet blackouts
- DDOS und ähnliche Angriffe
- Zero-Days attacks

Arbeitsauftrag «Sind meine Daten vor allen Threats geschützt»?

Im Anschluss an die letzten beiden Arbeitsaufträge sollten sie sich jetzt für jeden der oben notierten Daten folgende Fragen beantworten:
Wie resilient sind meine Daten? Wo besteht Verbesserungsbedarf?

3 Lösungen zur Datensicherheit.

Datensicherheitstools und dessen Technologien sollten die immer wachsenden Anforderungen in den heutigen komplexen, verteilten, auf multi-cloud basierten Rechnersystemen adressieren. Weiter sollten diese Tools die Überwachung sowie die policy inforcement zentralisiert ermöglichen. Nur so kann die Datensicherheit effizient bewältigt werden, vor allem in Hinblick auf die oben erwähnte wachsende Komplexität der heutigen Rechnerlandschaften.

3.1 Data discovery und classification tools

Bekannterweise sind heutzutage Daten über ein weites Spektrum von unterschiedlichen Datenspeichern verteilt. So sind diese z.B. auf lokalen Speicher, structured und unstructured data repositories, databases, data warehouses, big data platforms (AI training) und natürlich cloud Umgebungen zu finden.
Bei so einer Streuung sind Tools für die effiziente Erkennung und Klassifizierung dieser Daten wichtige automatisierende Hilfsmittel.
Ebenso sollten mit diesen gleichen Tools ein Erkennen, sowie das Stopfen von Sicherheitslücken machbar sein.

3.2 Data and file activity monitoring

Mit dieser Technik sollte der Zugriff auf Daten überwacht werden. Dies mit dem Ziel Abnormalitäten zu erkennen, riskante Zugriffe aufzuzeichnen und gegebenenfalls sanktionierende Massnahmen einzuleiten.

3.3 Vulnerability assessment sowie risk analysis tools

Mit diesen Tools sollte das Erkennen von out-of-date software, schwachen Passwörtern, misconfigurations sowie Daten welche besonders von exposure bedroht sind ermöglicht werden.

3.4 Automated compliance reporting

Was wenn ein data breach passiert ist, diese Tatsache aber niemals vom betroffenen Unternehmen bemerkt wird? Das wäre sehr schlecht.
In grossen Geschäften werden sogenannte enterprise-wide compliance audit reports gemacht. Dies ist nichts anders ein geschäftsweiter Sicherheitsrapport, in welchen alle Ereignisse aufgelistet und in Bezug auf Gefährdung diskutiert werden. Gute Tools ermöglichen eine automatisierte und zeitechte Generierung solcher Rapporte.

Arbeitsauftrag «Situation Lehrbetrieb»?

Als Hausaufgabe sollten sie sich über den Einsatz von oben erwähnten Software Tools in ihrem Lehrbetrieb schlau machen.

Verwenden Sie bereits solche Tools in ihrem Lehrbetrieb? Welche? Welche Prozesse müssen die Mitarbeiten lernen / einhalten?

4 Datensicherheits-Strategien.

Data security strategies beinhalten immer folgende Aspekte

- People
- Processes
- technologies (software)

Jeder dieser Aspekte ist gleich wichtig. Denn ist einer gebrochen, so bricht die ganze Sicherheit zusammen. Wie bei einer Fahrradkette.

So müssen also alle Teilbereiche (Standorte, Räume, Abteilungen) in einem Unternehmen immer alle drei oben genannte Aspkete implementieren. Die konsequente Implementation von geeigneten Massnahmen in alle Teilbereichen muss eine hohe Poriorität haben.
In der Praxis ist dies eine Frage der Organisation (QS) und der Anwendung und Einbindung der passenden oben besprochenen Tools.

4.1 Physische Sicherheit von Servern und Endgeräten

Egal wo Ihre Daten sind, on-premise (also auf lokalen drives), in corperate data centers oder auf der öffentlichen cloud sie müssen für folgende Punkte sorgen:

- Einbruchsicherheit; d.h. niemand darf ohne geeignete Autorisierung physischen Zugang zum Rechner oder zum storage area network (SAN) haben, wo die Daten gespeichert sind.
- Sind die Daten auch vor Feuer geschützt? Zum Beispiel müsste ein nitrogen fire suppression systems oder ähnliches installiert sein.
- Es muss ebenso dafür gesorgt werden, dass die Klimabedingungen im Serverraum nicht die limits übersteigen (climate control system).

Im Falle, dass ihre Daten in der cloud sind, ist in der Regel der cloud provider für alle diese Punkte verantwortlich. Sie müssen dies jedoch sicherstellen, dass dies so ist!

4.2 Access management

Über ihre gesamte IT Landschaft sollten sie unbedingt die «least-privilege access» Strategie konsenquent verfogen!

Das bedeutet, dass Sie immer nur diejenigen access Rechte vergeben, welche unbedingt benötigt werden, damit ein Mitarbeiter oder ein Prozess seine Aufgabe erfüllen kann. NIEMALS mehr.

Es gibt in der Praxis zahlreiche verschiedene Lösungn von access management. Eine ihnen bekannte ist sicherlich die Lösung mit active directories und domain controllern.
Siehe dazu : https://www.pcwdld.com/access-management

4.3 Unterschied von Authentifizierung und Autorisierung

Im Zusammenhang von access management spielen sicherlich die beiden Begriffe von Authentifizierung und Autorisierung mit.

Doch was bedeuten die beiden Begriff genau?

Hier sind die wichtigsten Antworten:

Was tut es ?

Authentifizierung überprüft credentials, dies könnte sein: username und password.
Somit wird hier überprüft, ob Sie wirklich derjenige sind welcher Sie ausgeben zu sein.

Autorisierung gibt oder verweigert Rechte, z.B. ein file lesen zu können.

Wie funktioniert es ?

Authentifizierung funktioniert über username und password, Fingerabdrücke, Augen-iris-Images, Stimm-/ Gesichtserkennung, Apps, 2FA codes (two step authentification)

Autorisierung funktioniert über settings, welche durch ein Team gemangt wird.
(PS: Dieses Team könnte bestechlich / korrupt sein ?)

Genaueres finden Sie unter:
https://www.okta.com/identity-101/authentication-vs-authorization/#:~:text=Authentication%20and%20authorization%20might%20sound,permission%20to%20access%20a%20resource.

4.4 Passwort Manager und Passwortverwaltung

Ihnen sollte sicherlich bekannt sein, dass man auf unterschiedlichen Plattformen immer unterschiedliche Passwörter verwenden muss !
Dies hängt natürlich damit zusammen, dass wenn ein Passwort erraten wurde, so ein Angreifer nun auf einen Schlag access auf alle ihre Daten hat.
Damit man sich nicht so viele Passswörter merken muss, kann man einen Passwort Manager verwenden. Ist man bei diesem eingeloggt, so setzt dieser bei einem beliebigen Login die für dieses Login nötige credentials ein.

Siehe dazu:

- https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/#:~:text=Password%20managers%20store%20your%20login,one%20you%20have%20to%20remember.
- https://itsfoss.com/password-managers-linux/

4.5 Softwareaktualisierung

Natürlich, wie sie sicher bereits wissen, ist das Patchen von security holes von höchster Wichtigkeit! Sobald updates und patches verfügbar sind, müssen diese innerhalb von Stunden installiert werden.

Wieso am liebsten innerhalb von einer Stunde?
Ganz einfach, wenn ein patch rauskommt, welcher eine gewisse Sicherheitslücke schliessen soll, weiss jeder über die Existenz der Sicherheitslücke.
Alle potentiellen Angreifer haben davon Kenntnis, auch wenn sie vor der Veröffentlichung des patches dieses security hole noch nicht kannten. Jetzt kennen Sie es, es wird ja sogar auf der öffentlichen Seite des Software-Herausgebers publiziert!

Also sind nicht gepatchte Systeme gefundenes Fressen für Hacker.

4.6 Backups

Regelmässige und vollständige Backups von allen kritischen Daten gehört zu jeder gesunden data seucurity strategy.

Dabei sind die folgenden Punkt zu beachten:

- Die Backups müssen auf ihre Brauchbarkeit überprüft werden. (sonst nutzlos)
- Alle Backups müssen denselben physischen und logischen Sicherheitsmassnahmen unterstehen wie die primary databases ! (sonst nutzlos oder die Backup sind einer zu grossen Gefahr ausgesetzt und sind daher angreifbar!).

In der Praxis gibt es viele verschieden Lösung für die Umsetzung von backups.
Siehe dazu:

- https://www.techadvisor.com/test-centre/software/best-backup-software-3647678/
- https://linuxhint.com/11_best_backup_tools_linux/

Arbeitsauftrag «Backups»

Wie realisieren Sie in Ihrem Betrieb Backups? Welche tools setzen sie dafür ein? Auf welchen storages werden die Backups gespeichert? Wo sind diese gelagert? Was passiert bei einem Grossbrand?
Wie gehen Sie persönlich mit Ihren Daten mit dem Thema Backup um?

4.7 Sensibilisierung der Mitarbeiter

Wie bereits oben erwähnt sind die insider data breaches oder breaches aufgrund von menschlichem Fehlverhalten nach wie vor die häufigsten Fälle von Verstössen gegen die Datensicherheit.

Weiter ist der folgende Punkt ein «alter Fisch»:

Sie sind Hacker und wollen Zugang zu einer database der CreditSuisse. Wie ist das einfachste Vorgehen?

Die Antwort ist fast immer dieselbe: Eine social engineering attack !

Warum? Tja, Mathematik ist und bleibt Mathematik. Will heissen die kryptographischen Verfahren zu knacken ist mit hoher Wahrscheinlichkeit nur mit sehr sehr teuren technischen Mitteln (supercomputing, quntum computing) machbar.

Menschen zu knacken ist easy ! Wie im richtigen Leben.

Daher gehört zu einer Sensibilisierung der ganzen Belegschaft klar auch eine fundierte data security Ausbildung und Weiterbildungen der Mitarbeiter in diesen Angelegenheiten.
So sollten alle Mitarbeiter wissen, wie ein sicherer Umgang mit Passwörtern aussieht. Aber auch social engingeering attacks und phising attacks müssen SOFORT erkannt werden können.

Sie müssen ihre Mitarbeiter in *human firewalls* verwandeln!

4.8 Network and endpoint security monitoring

Durch die Implementation geeigneter Tools welche Threats (Gefahren / Angriffe) erkennen können, kann das Risiko und die Wahrscheinlichkeit von einem data breach reduziert werden. Dabei ist auch wieder darauf Acht zu geben, dass diese Software-Pakete auf dem gesamten on-premise network sowie auch auf der gesamten cloud (multi-cloud) Umgebung umgesetzt und unterhalten werden. Sonst ist die Schutzwirkung stark eingeschränkt und gar unwirksam.

Arbeitsauftrag «Datensicherheitsstrategie»

Erstellen Sie auf dieser A4 Seite ein Mindmap, welches klar die data security stragety ihres Lehrbetriebs deutlich macht.
Dabei sollten Sie folgendes Vorgehen verfolgen:

1. Stellen sie alle (besonders) gefährdeten Daten übersichtlich im Mindmap dar.
2. Was für Mechanismen und Techniken werden für deren Schutz eingesetzt? Stellen sie diese mit einer anderen Farbe ebenfalls im Mindmap dar.
3. Wo besteht Ihrer Meinung nach Handlungs- / Verbesserungsbedarf? Zeichnen Sie dies ebenfalls in einer dritten Farbe ins Mindmap ein.

5 Data security trends.

Die Entwicklung im IT Umfeld in gewaltig (exponentielles / logistisches Wachstum).
Natürlich spielt dies auch in einem so schnell wachsenden Feld wie data security ein Rolle.

5.1 AI / cognitive computung / quantum computung

Künstliche Intelligenz wird die Datensicherheit aufgrund der Tatsache verbessern, dass AI die Fähigkeit hat riesige Datenmengen in kurzer Zeit zu verarbeiten (GPU based processing / large input sets / linear algebra).
Cognitive computing, ein Teilgebiet von AI, kann grundsätzlich dieselben Aufgaben erfüllen wie konventionelle AI. Jedoch werden dabei die menschlichen Gedankengänge simuliert. Daher kann cognitive computing vermehrt zur Detektion von security leaks und im allgemeinen Umfeld von data security eingesetzt werden.

Es ist ganz klar das quantum computing vor allem im Bereich der Kryptographie viel verändern wird. RSA und andere werden unsicher! Kann easy geknackt werden. Man beachte hier den ganzen lifecycle der Daten! Alte Daten können dann entschlüsselt werden.
Jedoch ermöglich quantum mechanics auch neue Verfahren, welche unter dem Namen *quantum cryptography* zusammengefasst werden.

6 Datensicherheit im breiteren Sichtfeld der IT Landschaft.

Um Datensicherheit erfolgreich zu implementieren ist es notwendig dies vollumfänglich im ganzen Unternehmen zu tun.
Wenn zu Beginn eine Strategie entwickelt wird, sollte schon von Anfang Wert darauf gelegt werden, dass Firmenziele sowie gesetzliche Vorschriften miteinbezogen werden.
Ein guter möglicher Start wäre dass man ein oder zwei Datenquellen identifiziert, welche besonders schützenswert und gefährdet sind.
Um diese zu schützen können jetzt Strategien und software suites implementiert werden.
Nachdem klare, strenge und präzise Regeln zum Schutz dieser höchstgefährdeten Daten aufgestellt wruden, können diese policies weiter auf die rechstlichen data assets in einer prioritisierten Weise ausgedehnt werden.
Durch automatisierte data monitoring software kann dieser Prozess der Skalierung über ein gesamtes Firmennetzwerk stark vereinfacht werden.

6.1 Datensicherheit auf der cloud implementieren

In Gegensatz zur Implementierung von on-premise data security unterscheidet sich cloud data security doch grundsätzlich. Dies liegt vor allem daran, dass die Daten nicht on-premise sind, sonder viel mehr auf meheren Standorten verteilt liegt.

Um einen wirksamen Datenschutz in der cloud aufzuauen sind tools wie *cloud data discovery and classification* software umabdingbar. Eine konkrete Implementierung von cloud monitoring tools könnte so aussehen, dass diese Software zwischen cloud und der database (database as a service DbaaS) liegt. So kann diese Daten bei der Übertragung überwachen oder diese über eine im Unternehmen bereits vorhandene security platform leiten.
Die zweite Variante hat den klaren Vorteil, dass so alle Daten denselben policies genügen müssen, da sie alle von derselben security suite verwaltet werden.

Was ist database as a service? Siehe dazu:

- https://www.stratoscale.com/blog/dbaas/what-is-database-as-a-service/

6.2 Multicloud security

Zum Start, ein refresher zur multicloud:

- https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud

Je mehr ein Unternehmen auf cloud services zurückgreift, umso komplexer wird die Thematik und die software suits zur Aufrechterhaltung der data security.

Dies hat mehere Gründe:

- Häufig werden mehere cloud paltformen oder provider verwendet, welche hoffentlich dieselben service-level-agreements (SLA) haben. Trotzdem führt dies zu einem erhöhten data security Aufwand.
- Daten sind auf vielen Standorten (Länder / Kontinente) verteilt (alle müssen sicher sein)
- Es müssen nicht nur Daten sondern z.B. auch proprietary business processes vor unbefugtem Zugruff geschützt werden. Diese Prozesse laufen häufig auch auf der cloud.

6.3 Datensicherheit und BYOD

Durch den vermehrten Einsatz privater Geräte in enterprise computing environments steigt das Risiko eines data breaches und Verletzung gegen Datenschutz und Datensicherheit sehr stark!

Was sind die Gründe:

- Die privaten Geräte sind ev nicht upgraded (security holes)
- Auf den privates Geräten läuft vielleicht bereits malware (worms, viruses, trojant horses etc) ohne dass der Besitzer dies weiss
- Weiter sind verschiedene Betriebssysteme mit verschiedener Software darauf zu finden, was die Implementierung geeignetes Datensicherheits-massnahmen ungemein erschwert.
- Vielleicht wurde Ihr BYOD Gerät von einem «Freund» manipuliert. Dies mit dem spezifischen Ziel ihr Unternehmen auszuspionieren und deren IT Landschaft zu schädigen.

Um diese Risikofaktoren abzudecken können Mitarbeiter verpflichtet werden security software of ihren BYOD devices laufen zu lassen, um so wieder die Kontrolle über den Zugriff auf Daten zu erhalten.
Weiter können durch geeignete Schulung der Mitarbeiter diese zur multi-step-authetication, Verwendung von starken Passwörtern und regelmässigen software updates angewiesen werden.

6.4 IoT und Datensicherheit

Internet of Things devices sind immer wieder Gegenstand aktueller Problemstellungen. So werden sie gehackt, werden für sog. Botnets verwendet, oder dienen als Mittel zum Zweck andere Teilnehmer eines Netzwerk anzugreifen oder zu knacken.
Siehe dazu:

- https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

7 Datenschutz in der Schweiz.

In der Schweiz wurde 2008 ein Gesetz neu eingeführt, welches klar regelt, was ein Datenschutzmanagementsystem (DSMS) alles können muss.
Es ist eigentlich ein follow-up vom Art. 4 Abs. 3 der Verordnung vom 28. Sep. 2007 über die Zertifizierung von Datenschutzsystemen, genannt VDSZ, Verordnung über Datenschutzzertifizierung.

Arbeitsauftrag «Datenschutzmanagementsystem»

Wir werden die Gesetzesartikel in Gruppen bearbeiten.
Für die gründliche Bearbeitung, sowie das Finden von praxisnahen Beispielen und das Erarbeiten von einer gut strukturierten Präsentation, sollen 3 Lektionen aufgewandt werden.

Wir beginnen heute. Nächste Woche haben Sie nochmals 2 Lektionen Zeit während des Unterrichts um sich tiefgründig mit der Thematik des schweizerischen Datenschutzmanagements sowie dessen Zertifizierung zu beschäftigen.

In 2 Wochen wollen wir die Präsentationen dazu abhalten.

Zusätzlich zur Präsentation muss jede Gruppe ein Factsheet (1-3 A4 Seiten) bereitstellen, wo die wichtigsten Inhalte sauber zusammengefasst sind.
Zudem sollte ein Fokus darauf gelegt werden, dass die Sachverhalte mit *zahlreichen* gut gewählten Praxisbeispielen ausgeschmückt werden. Pro Vortragsgruppe müssen mindestens 2 passende Praxisbeispiele besprochen werden.

Wir werden 2 verschiedene Dokumente bearbeiten. Es sind dies

- Richtlinien über die Mindestanforderungen an ein DSMS
- Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS

In diesen Dokumenten wird immer wieder auf andere Normen und Gesetze, z.B. das Schweizer Datenschutzgesetz (DSG), verwiesen.
Es ist klar die Erwartungshaltung, dass bei solchen Verweisen auf diese eingegangen wird, indem die zitierten Artikel sauber dargelegt werden.

Die Gruppeneinteilung erfolgt wie folgt:

- Gruppe 1: Richtlinien über die Mindestanforderungen, Art. 1-3
- Gruppe 2: Richtlinien über die Mindestanforderungen, Art. 4-5
- Gruppe 3: Anhang zu den Richtlinien über die Mindestanforderungen a. b. c.
- Gruppe 4: Anhang zu den Richtlinien über die Mindestanforderungen d. e. f.
- Gruppe 5: Anhang zu den Richtlinien über die Mindestanforderungen g. h. i.