Zusammenfassung Modul 231 2. Prüfung

Nachtrag Datenschutz 🡪 Die wichtigsten juristischen Werke: Einer der wichtigsten juristischen Werke betreffend Thema Datenschutz ist das Datenschutzgesetz (DSG)

**Definition Datensicherheit**

**Das Ziel der Datensicherheit ist der Schutz der Daten vor Verlust & Manipulation. Das primäre Mittel sind technisch-organisatorische Maßnahmen und das sekundäre Mittel ist das Gesetz.** Während beim Datenschutz das Ziel der Schutz der Person ist.

**Schwierigkeiten bei Umsetzung der Datensicherheit**

Die Systeme werden zunehmend komplexer zudem gibt es immer mehr politische Vorstösse und neue Gesetze, welche mehr Datensicherheit fordern. Die Konsumenten sind vermehrt auf das Thema Datenschutz sensibilisiert.

**Konsequenzen eines Datenlecks**

Beispiel: Ein Datenleck kann grosse Unternehmen jedoch auch uns Privatpersonen betreffen. Sagen wir Daten von unserem Handy gelangen an die Öffentlichkeit. Dies könnte verheerende Folgen für uns haben. Schlimmsten Fall könnte dies rufschädigend sein und wir erleben soziale Konsequenzen, beispielsweise verliert eine Person durch ein peinliches Video, das von ihm aufgetaucht ist, seinen Job. Auch für grosse Unternehmen kann dies verheerend sein, Menschen verlieren ihr Vertrauen in das Unternehmen, die Unternehmen verlieren eventuell Kunden und müssen hohe Strafen bezahlen.

**Verschlüsselung (Encryption)**

Durch Verschlüsselung kann ein wirksamer Schutz der Daten erreicht werden. Dabei wird mit Hilfe eines Schlüssels die Daten so verändert, dass sie wie zufällige Bitmuster aussehen (Verschlüsselung). Man unterscheidet grundsätzlich zwei kryptographische Verfahren:

Symmetrische Verschlüsselung z.B. AES

Dieses Verfahren verfügt über einen einzigen Schlüssel zur Ver- und Entschlüsselung. Es ist so konstruiert, dass die Datenveränderung für alle Teilnehmer umkehrbar ist, welche über den Schlüssel verfügen, mit dem die Daten verschlüsselt werden. Alle Teilnehmer haben also Kenntnis vom Schlüssel (Shared Secret) und jeder Teilnehmer, der den Schlüssel kennt, kann Klartext lesen.

Asymmetrische Verschlüsselung z.B. RSA

Dieses Verfahren ist so konstruiert, dass für die Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden. Man spricht von einem sogenannten Public-Key Verfahren. Ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel wird mathematisch so verknüpft, dass nur die Kombination der beiden Schlüssel eine Entschlüsselung erlaubt. Der öffentliche Schlüssel ist wortwörtlich öffentlich, der private Schlüssel bleibt geheim. Daten, die mit dem öffentlichen Schlüsselt verschlüsselt werden, können nur durch den Besitzer des privaten Schlüssels entschlüsselt werden.

Im Gegensatz zu der symmetrischen Verschlüsselung ist die asymmetrische Verschlüsselung deutlich rechenintensiver. Der Vorteil der asymmetrischen Verschlüsselung liegt darin, dass im Gegensatz zum symmetrischen Verfahren kein sicherer Übertragungskanal für den Schlüssel benötigt wird, da das Geheimnis nie den Kommunikationsteilnehmer verlässt. Tatsächlich findet in technischen Lösungen eine hybride Verschlüsselung statt. Bei HTTPS wird beispielsweise symmetrisch verschlüsselt.

Links zu den Verschlüsselungsverfahren: <https://studyflix.de/informatik/symmetrische-verschlusselung-1610>

**Data Resilienz**

Die Widerstandsfähigkeit von Daten beschreibt die Fähigkeit eines IT-Systems, mit Störungen umgehen zu können. Für viele Störungen gibt es Gegenmassnahmen.

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Data Masking

Im Sinne des Datenschutzes, aber auch im Sinne der Datensicherung ergibt es Sinn, Verwendung von Daten auf die Personengruppen einzuschränken, welche die Daten auch tatsächlich benötigen. Um diese Untergruppen dennoch realitätsnahe Datenbasen bieten zu können bedient man sich der Technik des **Maskierens.** Dabei wird grundsätzlich mit der echten Datenbasis gearbeitet. Allerdings werden Personendaten maskiert, indem z.B. Informationen vertauscht werden oder aber gewisse Teile der Information durch Platzhalter <<überschrieben>> werden. (z.B. alle Zahlengruppen der Kreditkartennummer werden bis auf die letzte Gruppe durch <<XXXX>> ersetzt. Informationen werden durch Informationen ersetzt, welche von Zufallsgeneratoren erzeugt wurden.

Datenlöschung

Wenn Daten gelöscht sind, so können sie auch nicht mehr kompromittiert werden. Daher ist die Löschung von Daten ein zentrales Werkzeug eines Datenschutz Management Systems. Doch Löschen ist nicht gleich Löschen. Und je nach dem, wie die Daten gelöscht wurden, können sie mit geeigneten Werkzeugen mehr oder weniger einfach ganz oder zumindest teilweise gelöscht werden

Beispiel: Beim Formatieren einer Festplatte wird nur deren <<Inhaltsverzeichnis>> gelöscht, die eigentlichen Daten bleiben bestehen.

Um sichere Löschung zu gewährleisten, muss daher auf Werkzeuge wie SDelete oder secure delete [Linux] zurückgegriffen werden. Wenn man seine alten Datenträger verkaufen oder wegwerfen will geht man das Risiko ein, dass jemand mit Hilfe von Recovery-Werkzeugen wiederherzustellen versucht. Deshalb muss man vor der Weitergabe sicher gehen, alle Daten definitiv zu löschen!

**Klassen von Software zur Unterstützung von Datensicherheit**

Heutzutage sind Daten über ein weites Spektrum von unterschiedlichen Datenspeichern verteilt. Beispiele dafür sind z.B. Lokale Speicher, Strukturierte Datenablagen, unstrukturierte Datenablagen, Datenbanken und Warehouses…

Bei so vielen Mengen von Daten sind Tools für effiziente, automatisierte Erkennung und Klassifizierung wichtige Hilfsmittel.

Wichtige Hilfsmittel sind:

**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 zu ergreifen.

**Vulnerability assessment und risk analysis tools** -> Mit diesen Tools sollte das Erkennen von veralteter Software, schwachen Passwörtern, Fehlkonfigurationen, sowie von besonders bedrohten Daten ermöglicht werden.

**Automated Compliance Reporting** -> In grossen Unternehmen werden unternehmensweite Berichte zur Einhaltung von Regeln im Umgang mit Daten durchgeführt. Dies ist im Wesentlichen ein unternehmensweiter Sicherheitsbericht, in welchen alle potenziell gefährlichen Ereignisse aufgelistet werden und derer Bedeutung diskutiert werden.

Wie schützt man Endgeräte und Server

Einbruchssicherheit -> Niemand darf ohne geeignete Autorisierung physischen Zugang zu den Geräten (Servern, Storage Area Networks, Network Attached Storages) erlangen

Brandschutz -> Sind die Daten vor Feuer geschützt? Serverräume werden typischerweise mit Halogen, Stickstoff oder CO2 Löschanlagen vor Brand geschützt. Durch Freisetzung dieser Gase wird der Sauerstoff aus dem Raum verdrängt und das Feuer damit erstickt.

Klimatische Bedingungen -> Computerhardware erzeugt Abwärme. Gleichzeitig versagen Halbleiter ab einer gewissen Temperatur ihren Dienst. Es muss daher dafür gesorgt werden, dass die klimatischen Bedingungen in den Serverräumen gewisse Grenzen nicht überstiegen.

Access Management

Die Beschränkung von Zugriff, ist ein wichtiges Mittel zur Reduktion der Angriffsfläche. Aus diesem Grund sollte man für seine gesamte IT-Landschaft eine geeignete Strategie umsetzen, anhand der man Zugriff gestatten oder ablehnen kann. Ein erfolgreiches Grundprinzip stellt dabei die **<<Least Privilege Access>> Strategie** dar. <<Least Privilege Access>> bedeutet, dass der Benutzer der Infrastruktur stets nur gerade jene Berechtigung vergeben, welche das Erfüllen deren Aufgaben unerlässlich sind. In keinem Fall sollten die Benutzer über mehre Rechte verfügen, da dies die Angriffsfläche wieder erhöht. Allen verwendeten Systemen liegts stets das Prinzip der **Authentifizierung und er Autorisierung** zu Grunde.

**Authentifizierung und Autorisierung**

Bei der Authentifizierung ist die Sicherstellung der Identität des Benutzers. In der Regel geschieht dies über geeignete Identitätsnachweise (Credentials).

Autorisierung

Die Autorisierung kümmert sich um die effektiven Berechtigungen. Die Autorisierung erlaubt oder verweigert Operationen auf verschiedenen Ressourcen. Sowohl Authentifizierungsdaten als auch Autorisierungsregeln werden in grossen Organisationen typischerweise von speziellen Teams verwaltet. Natürlich muss die Integrität dieses Teams sichergestellt werden.

Passwort Manager

Passwörter sollten eine möglichst zufällige Kombination von Zeichen sein, was das Merken der Passwörter erheblich erschwert. Dabei kann ein Passwort Manager helfen. Dies sind Sofwarepakete, welche verschiedene Credentials in einem durch ein Masterpasswort geschützten Speicher hinterlegen. Diese Produkte gibt es für verschiedene Plattformen und lassen sich oft über Online-Dienste auf verschiedenen Geräten synchronisieren.

Backups

Ein Backup ist im Wesentlichen eine räumliche Trennung zwischen dem Originaldatenträger und Sicherheitskopien desselben. Die räumliche Trennung spielt insbesondere bei Ereignissen höherer Gewalt eine grosse Rolle. Die Frage ist nicht, ob man ein Backup benötigen wird, viel mehr ist stellt sich die Frage, **wann** es einen treffen wird. Regelmässige und vollständige Backups von allen kritischen Daten sind ein wesentlicher Teil einer Datensicherheitsstrategie. Bei Backups geht es dabei einige wichtige Punkte zu beachten.

Die Backups müssen regelmässig auf ihre Brauchbarkeit überprüft zu werden. Konkret heisst das, ob man das gesicherte System auch die relevanten Daten wiederherstellen kann. Alle Backups müssen denselben physischen und logischen Sicherheitsmassnahmen unterstehen wie die Quelldaten. Das beste Zugrifssicherungssystem ist nutzlos, wenn das Backupmedium unverschlüsselt und zugänglich ist.

Sensibilisierung der Mitarbeiter

Das schwächste Glied ist immer noch der Mensch. (Phishing Mails, Fehlkonfigurationen…) Tatsächlich ist eine ziemlich alte Taktik nach wie vor die Beste, um Zugang zu Datenbestand des Ziels zu erlangen: **<<Social Engineering>>**

Social Engineering bedeutet, man beschäftigt sich so lange mit der Zielperson, bis man genug weiss, um sie entweder zum gewünschten Verhalten zu bringen oder z.B. ein Passwort zu erraten. Warum ist das so? Ein Kryptographisches Verfahren zu knacken ist nur mit sehr teuren technischen Mitteln machbar. Dagegen ist das <<Knacken>> von Menschen wesentlich einfacher.

Daher gehört zu einer Sensibilisierung der ganzen Belegschaft klar auch eine fundierte Ausbildung und Weiterbildung im Bereich Data/Cyber-Security. Mit Hilfe Schulung solle die Mitarbeiter lernen, wie ein sicherer Umgang mit Passwörtern aussieht, aber auch sensibilisiert werden für Social Engineering Angriffe oder Phishing. **Die Mitarbeiter sind die menschlichen Firewalls eines IT-Systems**

**Softwareaktulisierung**

Software ist aus verschiedenen Gründen immer fehlerbehaftet. Die meisten Fehler kommen dabei selten oder nie an die Oberfläche. Falls doch, so kann es sein, dass die Softwarefehler ein Sicherheitsrisiko darstellen. Entsprechend ist das Stopfen (Patchen) von Sicherheitslücken von höchster Wichtigkeit. Ist eine Lücke bekannt werden destruktive Kommunikationsteilnehmer schnell versuchen sich diese zu Nutzen zu machen. Daher sollte man keine Zeit beim Einspielen von Sicherheitspatches verlieren.

**Datensicherheit in der Zukunft**

Zunehmende Verwendung und Vernetzung, aber auch neue Technologien wie Quantencomputer fordern die Datensicherheit immer wieder aufs Neue heraus. Insbesondere für Quantencomputer wird erwartet, dass sie die Kryptographie wie sie heute existiert, aushebeln wird. Gleichzeitig werden Quantencomputer aber auch neue kryptographische Verfahren hervorbringen, welche die Sicherheit der Daten aufs Neue gewährleisten können. Neue Entwicklungen bringen aber nicht nur düstere Aussichten, so bieten Entwicklungen auf dem Gebiet des Machine Learning eine Erleichterung gewisser Aufgaben. Machine Learning zeichnet sich dadurch aus, dass riesige Datenmengen in vergleichsweiser kurzer Zeit verarbeitet werden und nicht offensichtliche Zusammenhänge ermittelt werden können.

**Datensicherheit auf der Cloud implementieren**

Um einen wirksamen Datenschutz in der Cloud zu aufzubauen sind Werkzeuge wie Cloud Data Discovery and Classification unerlässlich. Diese Werkzeuge suchen automatisch nach sensiblen Informationen im Cloud-Datenbestand. Eine konkrete Implementation von Cloud Monitoring Werkzeuge könnte so aussehen, dass diese Software zwischen Cloud und der Datenbank liegt. Diese Zwischenschichten leiten ihre Ergebnisse dann an eine im Unternehmen bereits vorhandene Sicherheitsplattform zur Begutachtung weiter.

Sicherheit in der Multi Cloud

Multi Cloud verfolgt das Ziel die eigenen Dienste bei mehr als einen Cloud Anbieter zu beziehen. Im Prinzip handelt es sich dabei um die konsequent weitergedachte Vermeidung von SPOFs. Sollte ein Cloud-Anbieter angegriffen werden oder die Dienste nicht verfügbar sein, kann mit dem anderen Anbieter weitergearbeitet werden. Desto mehr ein Unternehmen auf Cloud-Dienste zurückgreift, umso komplexer wird die Thematik 🡪 Häufig werden mehrere Cloud Plattformen oder -provider verwendet, welche hoffentlich dieselben service-level-agreements (SLA) haben. Trotzdem führt dies zu einem erhöhten Aufwand in der Datensicherheit, da die effektive Infrastruktur unterschiedlich ausfallen kann. Daten sind auf viele Standorten verteilt und alle müssen dieselben Sicherheitsstandards garantieren. Häufig müssen neben Daten auch firmeneigene Prozesse geschützt werden, welche in der Cloud <<betrieben>> werden. Auch der Diebstahl/Verlust von Prozess-Knowhow kann eine Firma erheblich schädigen.

Datensicherheit beim Einsatz von BYOD und IoT Geräten

Geräte des Internets sind immer wieder Gegenstand von Problemstellungen. Sie werde gehakt, für sogenannte Botnets verwendet oder dienen als Plattform, von der aus anderem Teilnehmer eines Netzwerks angegriffen werden (DDOS-Attacke). Je nach Leistungsfähigkeit des gekaperten Geräts werden diese auch gerne als Ausgangspunkt genommen, um fast unbemerkt in andere Knoten vorzudringen. Risikofaktoren 🡪 Im Gegensatz zu anderen Technologien bieten IoT-Geräte aufgrund ihrer internetgestützten Konnektivität eine besonders grosse Angriffsfläche.