Sicherheit und Schutzwürdigkeit von Informationen, Testdaten, ITIL 4 – 7 Leitprinzipien

Inf 2020d, Sashauna Wray, Valentin Ehinger

Datenschutzbestimmungen

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

13. Bundesverfassungsartikel [1]

Auf dieser Grundlage wurden diverse Gesetzte erlassen, um die Einhaltung der Privatsphäre der privaten Person zu gewährleisten, welche im Bundesgesetz von 1992 definiert sind. Dabei wird der Begriff besonders schützenswerte Daten definiert und was darunter zu verstehen ist.

1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen;

In den Modulunterlagen (AB_4) wird zudem zwischen langfristiger und kurzzeitiger Aufbewahrung unterschieden. Die Langfristigen müssen besonders gut gepflegt werden, da diese personenbezogenen Daten bis zu 10 Jahre nach deren Tod aufbewahrt werden können.
Nebst dem Definitionsbereich der Verfassung gibt es noch diverse Ergänzungen. Kantonale Gesetze sowie EU-Gesetze.
Bei den von uns betrachteten Applikationen, welche mit personenbezogenen Daten in Berührung kommen, sind überschaubar. Lediglich die API-Applikation (Mulesoft), SAP und Salesforce kommen mit diesen Daten in Berührung.
Seit einem Jahr ist der Verlauf, wer die Daten gesammelt hat, zu dokumentieren. Die grössten Anstrengungen bezüglich des Datenschutzes übernimmt die API-Applikation, welche die Daten verschlüsselt und nur den Applikationen zur Verfügung stellt, welche diese auch benötigen.
SAP, Salesforce und Personen aus dem UX (User Xperience) verwenden personenbezogene Daten zur Analyse. Dies geschieht jedoch in anonymisierter Form. Die Daten werden bei den Applikationen auch verschlüsselt angezeigt, damit kein Rückschluss auf tatsächliche Personen gemacht werden kann. Die Personendaten werden von der API-Applikation an die Datenbankservices übergeben, welche von Google verwaltet wird. Google unterstütz unsere anderen Applikationen in der Analyse der anonymisierten Daten.

[1] https://www.fedlex.admin.ch/eli/cc/1999/404/de#a13 08.09.2022

Die Applikationen verwenden diese Daten, wie beschrieben, nur zur Analyse des Kundenverhaltens. Die Kunden müssen sich bezüglich des Schutzes ihrer Daten keine Sorge machen, da diese nur zu darstellungszwecken entschlüsselt werden (Rechnung, Lieferschein, Darstellung im Web-Shop nach Registrierung) zu jedem anderen Zeitpunkt, ist es weder für Mensch noch Maschine möglich, Daten einer gewissen Person zu zuordnen.

Authentifikation

Die Authentisierung ist für das Nachweisen der Identität zuständig. Das Nachweisen der Identität ist eine Authentifizierung. Dies führt zur Autorisierung von Zugang zu Privilegierten Informationen.

Authentifizierungs-Methoden

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

Implementierte Sicherheitsmechanismen und Massnahmen

In der Interdiscount werden hauptsächlich **Software-Token** verwendet. Ein Software-Token ist ein Teil von einer Zwei-Faktor-Authentifizierungssicherheitsvorrichtung. Es wird verwendet, um die Nutzung von Computerdiensten zu autorisieren.
Die Applikationen kommunizieren über APIs. Sie verwenden dafür Access **Keys**, die auf der Instanz gespeichert werden. **SMS** wird bei dem Mitarbeiter als eine Authentifizierung Methode verwendet. Dabei wird ein Zeitsensibler einmaliger Code verwendet, der an den Mitarbeiter gesendet wird. Auf dieser Weise können sich Hacker nicht anmelden, wenn sie das Passwort geknackt haben. Zusätzlich wird mit dem regelmässigen Wechseln vom Password und den Passwortregel für zusätzliche Sicherheit garantiert.

Verschlüsselung

Verschlüsselung Beispiele

Gemeinsam genutzte Computer bei dem die Daten des Benutzers nicht einsehbar sind für Mitbenutzer. Bei unberechtigtem Zugang zu den Daten von einem Computer. Es wird für Informationen auf mobilen Geräten und Speichermedien verwendet. Für die Nutzung von unsicheren WLAN in öffentlichen Bereichen.

Es gibt verschiedene Möglichkeiten die Daten auf einem Gerät zu verschlüsseln. Die Verschlüsslung Art ist abhängig vom Betriebssystem. Des do neuer die Plattform oder Productversion, des do besser ist die Qualität der Datenverschlüsselung.

Verschlüsselung Ziele

Vertraulichkeit: Nur Personen, für welche die Daten bestimmt sind, könne sie lesen/einsehen.

Authentizität: Sowohl der Absender als auch der Empfänger werden auf ihre Echtheit überprüft.

Integrität: Auf dem Weg vom Sender zum Empfänger werden die Informationen nicht verändert.

Die Datenverschlüsselung ist in E-Business-Anwendungen wichtig für den User, Password, Kreditkarte usw.

Symmetrische und asymmetrische Verschlüsselung

Beim **symmetrischen Verfahren** wird derselbe Schlüssel verwendet zum ver- und entschlüsseln. Im **asymmetrischen Verfahren** werden zwei verschiedene Schlüssel verwendet. Ein öffentlicher Schlüssel und ein privater Schlüssel. Der **öffentliche Schlüssel** ist zum Verschlüsseln der Daten und ist für jeden zugänglich. Der **private Schlüssel** ist zum Entschlüsseln und muss geheim gehalten werden.

Einsatzbereiche der Verschlüsselung

Auf dem Client

Verschiedene Verschlüsselungsmöglichkeiten existieren für den Desktop. Mit Data-Cloud Lösungen werden sie mitgeliefert. Es ist dabei möglich sie wie bei **SecureSafe** zu machen. Um

die ganze Festplatte oder einzelne File-Share zu verschlüsseln, kann **Symantec** verwendet werden. Möglich ist es auch eMails zu verschlüsseln und Passwörter zu Verwalten.

WEB-Anwendungen

Eine Verschlüsslung ist hier empfehlenswert für einen Client, der am WEB angeschlossen ist. Klassifizierte Informationen werden ausgetauscht. Remote-Zugriffe auf einen Server als privilegierter User gehören auch dazu.

Speicherung

Die Daten vom E-Business Anwendung werden nach Situation und Einstufung der Schutzwürdigkeit und Bedrohung verschlüsselt abgelegt. Nur bei der Verarbeitung sind sie unverschlüsselt im System.

Testdaten Management

Testing ist ein wichtiger Posten und gehört zu jedem Change dazu. Bei Interdiscount wurde deshalb ein eigenes Team gegründet, welches sich nur um Testabwicklungen kümmert. Da je nach dem Change verschiedene Testdaten in Anspruch genommen werden müssen, werden die Testdaten nicht von tatsächlichen Benutzern verwendet. Die Anonymisierung und das Absichern vor Fremdzugriff wäre ein zu grosser Aufwand. Alle Testdaten werden synthetisch hergestellt, das heisst, sie werden generiert. Kunden müssen sich deshalb auch keine Sorgen machen, dass durch Fehler im Testing ihre Daten durchsickern könnten.
Die Testdaten werden mittels eines Testdatengenerators erstellt. Der angekommene Change wird mit den Testdaten durch eine Pipeline laufen gelassen. Die Pipeline ist so konfiguriert, dass diese zudem Auswirkungen auf andere Applikationen feststellen kann und bei einem erfolgreichen Durchlauf, wird der Change automatisch auf die produktionsnahe Umgebung gepusht.

Zusammenfassung

Die Zusammenfassung/Präsentation befindet sich im Verzeichnis:
EhingerWray/AB3/präsi.pptx .

ITIL4 7 Leitprinzipien

Die Leitprinzipien sind grundlegend generell gehalten und anhaltend geltend. Das heisst, dass die Prinzipien auch in mehreren Jahren noch dieselbe Gültigkeit haben. Hierfür eine Zusammenstellung der Leitprinzipien.

Focus on Value

Das heisst, dass sich die Organisation sich auf Wertgenerierung konzentrieren sollte. Es sollte immer ein Wert produziert werden. Eine Bäckerei hat als Value (Wert) Brot und nicht Mehl.

Mehl wäre keine zusätzliche Wertgenerierung, sondern den erhaltenen Wert (unverfeinert und somit ohne Wertsteigerung) eins zu eins zurückgegeben. Wird keine Wertsteigerung erzielt, verschwendet man Zeit, Geld und Ressourcen.

Start where you are
Das bedeutet, dass man sich nicht bei jeder Idee neu erfinden sollte. Ein Bäcker, der nun eine neue Variante hat, Brot herzustellen, sollte nicht aufhören Brote herzustellen und von Neuem beginnen. Sondern er sollte diese neue Methode auf gleichbleibende Prozesse anwenden. Dampfbacken… Alle Prozesse vor dem Backen bleiben gleich. Man muss nur wegen einer neuen Backform nicht den gesamten Prozess neu erfinden. Kneten bleibt, und vielleicht auch die Inhaltsstoffe werden gleichbleiben.

Progress iteratively with Feedback
Durch das Aufteilen einer Aufgabe in kleinere Teilabschnitte, kann mehr, schneller und besser Feedback eingeholt werden. Hier nehme ich als Beispiel eine Schreinerei, welche Stühle produziert. Ein Stuhl zu produzieren kann in mehrere Teilschritte aufgeteilt werden. Dadurch können Fehler, wie ein schiefer Stuhl vermieden werden. Man kann zu jedem produzierten Teilstück Rückmeldung anfordern. Dadurch erhält man Bestätigung, der Kunde oder Chef weiss zusätzlich auch immer, wie weit die Arbeit fortgeschritten ist und es können allfällige Änderungswünsche leichter einfliessen. Die einzelnen Teilschritte bauen aufeinander auf und formen das fertige Produkt.

Collaborate and promote visibility
Um das Beispiel der Schreinerei und dem Stuhl erneut zu verwenden, kann man sagen, dass die Schreinerei, auch wenn es sehr viele Mitarbeiter sind, das gleiche Ziel haben. Sie haben das Ziel, einen Stuhl herzustellen. Dafür wenden sie die vorherigen Punkte an. Sie tauschen sich aus, denn sie können das Ziel nur gemeinsam erreichen. Sie zeigen einander, woran sie arbeiten, wo sie Schwierigkeiten haben. Sie zeigen dies auch in der Dokumentation ihrer Arbeit, damit aussenstehende oder das Personalmanagement ihre Arbeit auch wahrnimmt.

Think and work holistically (Ganzheitlich denken und arbeiten)
Darunter zu verstehen ist, dass man als Team arbeitet, sich Expertenwissen aneignet, dieses im richtigen Ramen einfliessen lässt und sich bei fehlendem Expertenwissen, welches dazu holt. Man soll ein Projekt als eine Einheit sehen. Wenn diese Schreinerei nun einen Thron (andere Form von Stuhl) produzieren soll, weiss vielleicht jemand im Team, wie dies gemacht wird. Hier kann diese Person sein vorhin ungenutztes Wissen einfliessen lassen.

Keep it simple and practical

Wenn man sich an dieses Prinzip hält, kommt man schneller ans Ziel. Möglichst wenig Umwege machen. Dies bedeutet auch, dass die eigene Vorgehensweise dem vorliegenden Fall angepasst und seine Meinung von dem Fall abstrahiert werden muss. Die einfachste Variante ein Problem/Projekt zu verarbeiten, ist oftmals auch die effizienteste.

Optimize and automate

Unter einer Optimierung ist zu verstehen, dass Prozesse beschleunigt werden können, in dem man zum Beispiel eine Fehlertoleranz einbaut. Ein Stuhlbein muss nicht immer denselben Durchmesser haben, oder muss nicht zu 100% glatt sein. Dadurch wird das Teilprodukt (Stuhlbein) schneller fertig. Automatisieren ist, wenn nur menschliche Personen am Produkt arbeiten, eine Arbeitsaufteilung. Oder man kann sich überlegen, einige Schritte an nichtmenschliche Produktionsanlagen zu übergeben. Eine zu starke Automatisierung bei Menschen führt zu monotoner Arbeit. Wenn man dieses Prinzip umsetzen will, sollte man jedoch die anderen Prinzipien zu beachten und nicht zu optimieren, wo schon optimiert wurde.

Anwendung im Betrieb

Viele dieser Prinzipien werden sehr stark gelebt und umgesetzt. Aufteilung in Teams mit differenziertem Fachwissen, was eine schnellere Projektzuteilung erlaubt. Man arbeitet und lebt als Team, welches auch gestärkt wird. Es wird grossen Fokus auf die Generierung von Value gelegt wobei Arbeitsprozesse nicht jedes Mal komplett neu erarbeitet, sondern optimiert werden. Täglicher Austausch wie auch Expertenwissensaustausch werden ernst genommen und den dafür nötigen Raum gegeben.