Das Recht auf Privatsphäre im Digitalen Zeitalter, 24. November 2015

Aus der Sicht Informationssicherheit

SIK

Die Schweizerische Informatikkonferenz (SIK) ist eine interkantonale gesamtschweizerische Organisation mit folgenden Mitgliedergruppen:

- Öffentliche Verwaltungen der Schweiz und des Fürstentums Liechtenstein
- Öffentlich-rechtliche Betriebe z.B. Hochschulen (ETH, Universitäten, Fachhochschulen)
- Körperschaften mit Mehrheitsbeteiligung (>50%) der öffentlichen Hand

Ziel der Schweizerischen Informatikkonferenz ist, die Zusammenarbeit auf dem Gebiet der Informatik und Telekommunikation (ICT) zu fördern.

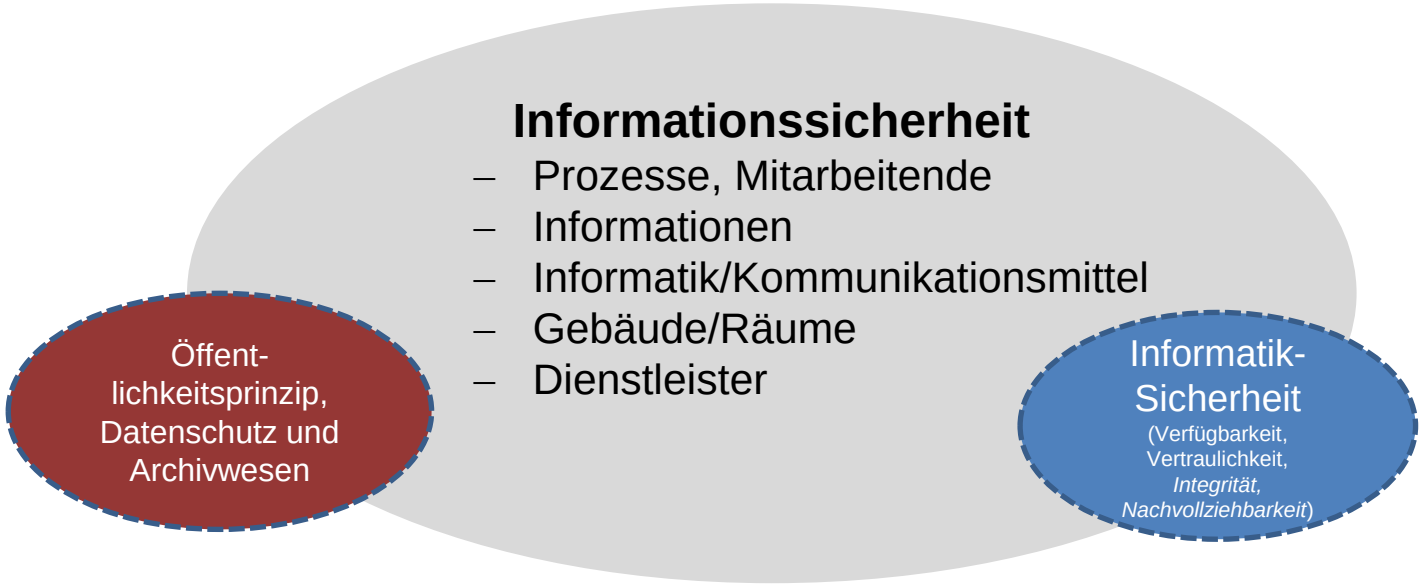
SIK Arbeitsgruppe Informatiksicherheit

Spezialisten der Informations- und Informatiksicherheit sowie der Informatikrevision, die den offenen Erfahrungsaustausch pflegen.
Sie vertreten Bundesstellen, die Kantone und das Fürstentum Lichtenstein.

Zusammenhang Informations- und Informatiksicherheit

- Die enge Verknüpfung der Kundenbedürfnisse (Leistungsbezüger) und die Leistungserbringung mit der Informatik (Leistungserbringer) erfordert eine Fokussierung auf die Sicherheit der Information und der resultierenden Risiken.

- Die Informatiksicherheit ist Teil der Informationssicherheit, ebenso der Datenschutz und das Öffentlichkeitsprinzip/Archivwesen.



Was ist Big Data?

Big Data bezeichnet Datenmengen,
die zu **gross** oder zu **komplex** sind oder
sich zu **schnell ändern**, um sie mit klassischen
Methoden der Datenverarbeitung auszuwerten zu können.

Auszug aus Wikipedia Definition

Mögliche Einsatzgebiete

- Webstatistiken und Marktforschungsergebnisse
- Erhebung in der Energieversorgung
- Die Stellengesuche und Stellenangebote
- Fitnessdaten
- Die Grippemeldungen
- Fernwartung von Steuerungssystemen
- Geheimdienstliche Informationen
- Feststellung von Unregelmässigkeiten beim elektronischem Zahlungsverkehr
- Gewinn durch den Verkauf von Daten

Bequemlichkeit versus Sicherheit

Folgende Erkenntnisse:

- Wir **wissen** dass:
- die Rechtslage unklar und verworren ist
- wir eventuell erpressbar werden
- das «Netz» nichts vergisst und die Löschung der Daten eher schwierig ist

- Wir **wissen nicht**:
- was über uns gespeichert wird (Personendaten und besonders schützens-wert Personendaten, z.B. unsere Schwächen…)
- wer diese Informationen, lesen bearbeiten oder ungewollt weiter leiten kann

- Wir **vertrauen** (blind) darauf, dass die Daten sorgfältig bearbeitet, gespeichert und bei Nichtgebrauch sicher vernichtet werden

- Wir **akzeptieren**, dass:
- sich ev. der Kühlschrank mit dem Auto abspricht
- Das Auto ohne manuelle Eingriffsmöglichkeiten (Lenkrad, Bremsen…) fährt

Wir sind vorsichtig

Folgende offenen Frage sollten beantwortet werden können:

- Ist das Betriebssystem und der Virenschutz aktuell?
- Was teilen wir in den sozialen sozialen Medien wie z.B. Facebook mit?
- Warum und an wen geben wir Personen- oder besonders schützenswerte Informationen preis?
- Wissen wir was mit unseren Daten geschieht?
- Warum erledigen wir unsere eBanking-Geschäfte nicht auf einem separaten System?

Was ist eine Cloud

Der Begriff "Cloud-Computing" umschreibt den folgenden Ansatz:
IKT-Dienste (z. B. Anwendungen, Rechen- oder Speicherkapazität u. ä.) werden dynamisch und an den Bedarf angepasst über ein Netzwerk zur Verfügung zu gestellt.

- Zeitnahe, automatisierte Beschaffung
- Zugang über Netzwerke
- Ressourcen-Pooling
- Elastizität
- Abrechnung

Grobklassifizierung von Anwendungsgruppen und Organisationsform

Cloud-Dienste für Einzelpersonen (Endanwender)
Für die Speicherung von Daten jeglicher Art wie zum Beispiel Dokumente, Fotos, Videos Musik etc. stehen heute Cloud-Dienste wie zum Beispiel Dropbox oder iCloud rund um die Uhr und mit weltweitem Zugriff zur Verfügung.

Cloud-Dienste für die Organisation
- Zum Beispiel wird von einem Cloud-Dienstleister zusätzlicher Speicherplatz bezogen
- Die Daten werden in sehr grossen Mengen gespeichert und im Bedarfsfall weiteren berechtigten Benutzern zum Lesen oder zur Bearbeitung zur Verfügung gestellt

Organisationsform der Cloud
- Private-Cloud
- Community-Cloud
- Public-Cloud
- Hybrid-Cloud

Services der Cloud

- **Software**
  Bereitstellung von Anwendungen (z.B. Geschäfts-, Kollaborations- und Kommunikations-anwendungen)
- **Infrastructure**
  Die Services (zum Beispiel Bereitstellung von Datenspeicher)
  sind via Internet zugänglich, prinzipiell ist weltweit eine Nutzung mit unterschiedlichen Endgeräten möglich (z.B. Smartphones, Laptops)
- **Plattform**
  Bereitstellung von Services, die für die Entwicklung, die Integration und den Betrieb von Anwendungskomponenten benötigt werden.
- **Business process**
  Bereitstellung von ganzen Geschäftsprozessen

Sicherheitsanforderungen an einen Cloudanbieter

- Service Level Agreement (SLA) und/oder schriftlicher Vertrag
- Einhaltung gängiger Standards
- Verschlüsselung Dokumente, Ordner, Client und Transport
- Zugriff Datenherr und Datenbenutzer
- Datenstandort
- Logging der Zugriffe
- Starke Authentifizierung
- Business Continuity Management (BCM)

Informatiksicherheit

Vertraulichkeit der Daten
- Vertraulichkeit der Informationen kann nicht sichergestellt werden
- Unberechtigte können unter Umständen die Informationen lesen, bearbeiten oder löschen

Verfügbarkeit der Daten
- Durch einen unerwarteten Einstellung des Betriebs sind die Daten nicht mehr verfügbar.
- Der Cloud-Betreiber kann den Benutzer erpressen, da er physisch die Daten „besitzt“

Integrität der Daten
- Die Integrität der Daten kann nicht gewährleistet werden
- Sowohl Mitarbeitende des Cloud-Anbieters als auch Hacker können Daten verändern

Compliance
- Nichteinhaltung der rechtlichen Vorgaben und ungeeignete Verträge
- Das Auditingrecht wird in den Verträgen nicht oder ungenügend definiert und kann nur schwer eingefordert werden

Risiken für den Benutzer

Abhängigkeit vom Anbieter
- Man ist an den gewählten Anbieter («Vendor Lock-in») gebunden
- Anbieterwechsel ist anspruchsvoll und kostspielig
- Man muss dem Anbieter vertrauen, dass er die (Sicherheits-)vorgaben einhält

Unvorhergesehener Service-Stop
- Der Services sind im schlimmsten Fall ohne Vorwarnung nicht mehr oder nur noch unter stark veränderten Bedingungen verfügbar

Kontrollverlust
- Einhaltung von Sicherheitsvorgaben können nur schwer vorgegeben werden
- Audits können nur schwer durchgeführt werden
- Eigene Anforderungen können nur bedingt durchgesetzt werden

Fehlendes Wissen des Benutzers
- Das Wissen und die Erfahrungen im Umgang mit Cloud-Computing fehlen
- Ungeeignete Anbieter können ausgewählt gewählt werden
- Ungeeignete Verträge können abgeschlossen werden

Empfehlung

Benutzen sie nach Möglichkeit einen Schweizer Cloud-Anbieter,

welcher die Daten ausschliesslich in der Schweiz speichert