STADT WIL

Datenschutz und Datensicherheit
in der öffentlichen Verwaltung

Workshop St. Galler Ortsgemeinden - VSGOG
Montag, 19. September 2022, in Rapperswil

Kurt Hanselmann

Leiter Informatik-Dienste
bis Ende Januar 2022

Projektleiter Abacus Wil
bis Ende September 2022

kurt.hanselmann@leunet.ch | 079 411 25 88

Agenda

- Informatik Stadt Wil in Zahlen
- Datenschutz
- Datensicherheit
- Technische Massnahmen
- Sensibilisierung der Mitarbeitenden
- Bearbeitung von Personendaten
- Datenverarbeitung durch Dritte

Agenda

- Microsoft 365 (früher Office 365)
- Fachstellen im Kanton St. Gallen
- Rechtliche Grundlagen, Links, Merkblätter
- Fragen

Informatik Stadt Wil in Zahlen

Infrastruktur für die Stadtverwaltung, Volksschule und externe Kunden:

- 4635 AD-Konti
- 100 Server (20 physisch, 80 virtuell)
- 1260 PC/Notebook mit Windows 10
- 1600 iPad's (mehrheitlich im Schulbereich)
- 453 Drucker
  davon 63 Multifunktionsgeräte
- 1327 Telefonapparate
  davon 70 Handy
- 174 Beamer
- 338 WLAN-Sender
- 145 Netzwerkkomponenten (Switches)
- 68 Glasfaserstandorte

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 als Schutz vor **missbräuchlicher Datenverarbeitung**, Schutz des **Rechts auf informationelle Selbstbestimmung**, Schutz des **Persönlichkeitsrechts bei der Datenverarbeitung** und auch **Schutz der Privatsphäre** verstanden. Datenschutz wird häufig als Recht verstanden, dass jeder Mensch grundsätzlich selbst darüber entscheiden darf, wem wann welche seiner persönlichen Daten zugänglich sein sollen.

Datensicherheit

- **Vertraulichkeit**
  Nur autorisierte Benutzer haben Zugang zu übertragenen und gespeicherten Daten
- **Integrität**
  Schutz vor beabsichtigten oder unbeabsichtigten Veränderungen
- **Verfügbarkeit**
  Gewährleistung des ständigen Zugriffs auf die Daten
- **Kontrollierbarkeit**
  Prüfung der Massnahmen durch Protokollierung

Datensicherheit

Datensicherheit hat also zum Ziel, beliebige Daten vor Schäden wie **Manipulation** und **Nicht-Verfügbarkeit** schützen. Hierzu zählen unter anderem Aspekte wie die physische Sicherheit, der Schutz vor Fremdzugriffen, der Schutz vor internen Zugriffen, die Verschlüsselung der Kommunikation, die Datensicherung wie auch Updates und Patches.

Datenschutz und Datensicherheit

Eine (Sicherheits-) Kette ist bekanntlich so stark, wie deren schwächstes Glied.

Es gilt, das schwächste Glied, bzw. die schwächsten Glieder zu eruieren und entsprechende Massnahmen zu ergreifen.

Massnahmen

Eine starke Sicherheitskette wird im wesentlichen erreicht durch:

- **die Implementierung von technischen Massnahmen**
- **die Sensibilisierung der Mitarbeitenden**

Technische Massnahmen

Auf technischer Ebene gilt es eine Vielzahl von Massnahmen zu treffen:

- Virenschutz
- Patches (Betriebssystem und Anwendungssoftware)
- SPAM-Filter / Sandbox
- Starke Passwörter
- Zwei-Stufen-Authentifizierung
- Aktuell-gehaltene Benutzerverwaltung
- Regelmässige, zuverlässige Backups

Technische Massnahmen

- **Serverräume**
  abgeschlossen, Einbruchsicherung, Videoüberwachung, Protokollierung der Zutritte, Klimatisierung (max. 25 Grad), Feuer- und Wasseralarm, Löschanlage
- **Switches**
  sind nicht öffentlich zugänglich, regelmässig mit aktueller Firmware ausgestattet
- **Netzwerke**
  mit VLAN’s abgeschottet
- **Freie Anschlussdosen in Büros und frei zugänglichen Räumen (z.B. Sitzungszimmer, etc.)**
  sind nicht mit dem Netzwerk verbunden

Technische Massnahmen

- **USB-Devices**
  Handhabung von USB-Sticks und externen Festplatten regeln
- **Zugriffsrechte**
  restriktive Zuteilung (nur was zur Erfüllung des Tagesgeschäftes nötig)
- **Datenhaltung**
  wenn immer möglich zentral auf einem Server; falls auf einem PC/Notebook sind die Daten verschlüsselt
- **E-Mail Verkehr**
  besonders schützenswerte Daten dürfen nur verschlüsselt versandt werden.

Technische Massnahmen

- **Firewall-Systeme**
  nachvollziehbare Regeln; regelmässige Wartung
- **Überwachung / Alarmierung**
  wichtige Geräte und Dienste sind über ein Alarmsystem proaktiv zu überwachen
  z.B. mit PRTG
- **Geordnete Ausserbetriebnahme alter Geräte**
  Festplatten/SSD-Speicher sind „richtig“ zu löschen, oder zu zerstören
- SLA mit Hard- und Software-Lieferanten
- Filter für anstössige und rassistische Web-Inhalte (besonders im Schulbereich)

Sensibilisierung der Mitarbeitenden

„Das grösste Risiko befindet sich zwischen der Stuhllehne und der Tischkante“

Durch gezielte Instruktion und Ausbildung der Mitarbeitenden kann ein hoher Sicherheitsstandard erreicht werden.

Sensibilisierung der Mitarbeitenden

- **Vertrauenskultur schaffen**
  Mitarbeitende melden Unregelmässigkeiten oder allfällig eigenes Fehlverhalten unverzüglich an eine bekannte Stelle
- **wachsam sein**
  keine dubiosen Websites oder E-Mails öffnen/beantworten
- **Awareness-Schulungen**
  regelmässig Schulungen i.S. IT Sicherheit durchführen

Sensibilisierung der Mitarbeitenden

- **Phishing**
  keine (persönlichen) Daten an Unbekannte preisgeben (insbesondere Zugangsinformationen)
- **Passwort**
  mindestens 12-stellig, Gross-/Kleinbuchstaben und Sonderzeichen, regelmässig wechseln, für verschiedene Dienste unterschiedliche Passwörter verwenden
- **Bildschirm sperren**
  beim Verlassen des Arbeitsplatzes

Sensibilisierung der Mitarbeitenden

- **Homeoffice**
  Regeln für die Arbeit im Homeoffice aufstellen
- **Administratoren-Rechte**
  liegen beim Administrator, nicht beim Benutzer
- **Social Engineering**
  keinen unbekannten (hilfsbereiten) Personen vertrauen
- **Überprüfung**
  die vereinbarten Regeln werden regelmässig und unangemeldet überprüft

Bearbeitung von Personendaten (Art. 4 DSG)

- Nach Massgabe des Zwecks in der Rechtsgrundlage
- Für die betroffenen Personen erkennbar, und nach Massgabe der Verwendung vollständig und richtig
- Organisatorische und technische Massnahmen vor Verlust, Entwendung, sowie unbefugter Kenntnisnahme

- Anonymisierung der Personendaten für Statistik, Planung und Forschung (Art. 7 DSG)

Besonders schützenswerte Personendaten (Art. 1.b DSG)

- Religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten. Ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation oder einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert
- Gesundheit, Intimsphäre und ethnische Zugehörigkeit
- Genetische Daten
- Biometrische Daten, die eine natürliche Person eindeutig identifizieren
- Leistungen und Massnahmen der sozialen Hilfe
- Strafrechtliche sowie disziplinarische Verfahren und Sanktionen

Datenverarbeitung durch Dritte
Art. 9 Datenschutzgesetz SG (DSG)

- Die Datenbearbeitung durch Dritte darf nicht durch Gesetz oder Verordnung ausgeschlossen sein.
- Der Dritte bietet Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung
- Der Dritte darf die Daten nur so bearbeiten, wie es das öffentliche Organ selbst darf
- Die Daten müssen vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden.
- Das öffentliche Organ muss mit regelmässigen Kontrollen prüfen, ob der Datenschutz eingehalten wird.

Datenverarbeitung durch Dritte

Art. 9 Datenschutzgesetz SG (DSG)

- Es muss Schweizer Recht anwendbar und der Gerichtsstand in der Schweiz sein.
- Der Ort der Datenbearbeitung (Serverstandort) soll in der Schweiz, bzw. in einem Staat mit gleichwertigem Datenschutzniveau, sein. Durch den CLOUD-Act haben US-Behörden Zugriff auf Daten, welche nicht in den USA gespeichert sind.
- Vertraulichkeitserklärungen einholen

Cloud-Dienste

Microsoft 365, Web-Applikationen, Cloud-Speicher

Microsoft 365 - Datenschutz-Folgenabschätzung, Vorabkonsultation

Art. 8 Datenschutzgesetz SG (DSG)

- Bevor Microsoft 365 eingesetzt werden darf, muss eine **Datenschutz-Folgenabschätzung** (Risikoanalyse) durchgeführt werden.
- Ergibt diese Analyse für die betroffenen Personen ein hohes Risiko, ist das Projekt der kantonalen Fachstelle oder der zuständigen Gemeindefachstelle zur **Vorabkonsultation** zu unterbreiten.

Kritische Punkte: wer ist Vertragspartner; nur zulässige Unterauftragsnehmer; Services in der Schweiz; Auditrecht; Zugriffsbegehren ausländischer Behörden

Microsoft schliesst ein Zugriff auf Personendaten für „legitime Geschäftstätigkeiten“ nicht aus. Deshalb kommt MS365 für sensible Personendaten nicht in Frage.

Fachstellen für Datenschutz im Kanton St. Gallen

Fachstelle für Datenschutz des Kantons St. Gallen
Regierungsgebäude, 9001 St. Gallen
datenschutz@sg.ch | 058 229 14 14

Gemeindefachstellen

- **Stadt St. Gallen** - Petra Rüttimann, Rathaus, 9001 St. Gallen
  petra.ruettimann@stadt.sg.ch | 071 224 53 83
- **Region Oberuzwil** - Manuela Staub, Flawilerstrasse 3, 9242 Oberuzwil
  manuela.staub@oberuzwil.ch | 071 955 77 46

Fachstellen für Datenschutz im Kanton St. Gallen

- **Region Rapperswil-Jona -** Armin Blöchlinger, Zürcherstrasse 65, 9501 Wil
  info@bl-au.ch | 071 912 30 44
- **Rheintal Werdenberg Sarganserland** - Claire-Lise Lippuner
  Grünaustrasse 8, 9470 Buchs SG
  claire-lise.lippuner@innovatis.net | 081 300 14 40

Die Zuständigkeit für Ihre Ortsgemeinde kann auf dieser Website abgerufen werden:
https://www.sg.ch/sicherheit/datenschutz/kontakt-weitere-datenschutzbehoerden/adressen-gemeindefachstellen.html

Rechtliche Grundlagen

- **Bundesgesetz über den Datenschutz**
  (DSG) 01.03.2019
- **Kantonales Datenschutzgesetz**
  (DSG) 25.06.2019
- **Merkblätter und Arbeitshilfen**
  Kanton St. Gallen
- **Merkblatt Cloud-spezifische Risiken und Massnahmen**
  V3.0 / 03.02.2022
- **Checkliste Microsoft 365 in der Verwaltung**
  März 2021 | Fachstelle für Datenschutz

Übrigens …..

….. auch analog geführte Daten unterliegen der Datensicherheit und dem Datenschutz!


Herzlichen Dank
für Ihre
Aufmerksamkeit