

So schützt die Gemeinde ihre Daten

Wer kann sich eine wegen eines Totalausfalls der IT-Einrichtung geschlossene Gemeindekanzlei vorstellen? Das kann sich niemand leisten. Und trotzdem – es ist möglich, dass plötzlich nichts mehr läuft. Diejenigen Bürgerinnen und Bürger, die davon betroffen sind, werden sicher kein Verständnis dafür aufbringen. Sie sind überzeugt, dass eine Gemeindeverwaltung ihren IT-Betrieb ähnlich absichern sollte wie zum Beispiel eine Bank.

Die Schweizer Gemeindeverwaltungen sind von grossen, reisserischen Pech- und Pannenberichten bis heute verschont geblieben. Man ist überzeugt, dass es Storys wie «CD mit sämtlichen Sozialhilfeempfängern kam beim Transport abhanden», «offener Webzugang zur aktuellen Einwohnerdatei», «Baugesuche sind aus dem IT-System verschwunden» nur im Ausland gibt. Auf unseren Verwaltungen wird durchs Band verantwortungsbewusst und mit hoher Qualität gearbeitet. Die meisten Mitarbeitenden sind sich jedoch kaum bewusst, wie stark ihre heutige Tätigkeit von einer funktionierenden IT-Umgebung abhängt. Die von den Stimmbürgern eingesetzten «Hüter» und «Garanten» für eine effiziente und bürgerfreundliche Verwaltung können nur hoffen, dass nichts passiert und sie nicht unvorbereitet für erlittene IT-Pannen plötzlich Rede und Antwort stehen müssen.

Von grossen IT-Pannen und latenten Gefahren

Funktioniert die IT nicht, kann an den meisten Verwaltungsarbeitsplätzen nicht weitergearbeitet werden (siehe Tabelle). Und ein Behördengang ohne Resultat löst grosse Verärgerung aus. Für jede Amtshandlung wurde in den letzten drei Jahrzehnten eine IT-Lösung gebaut. Die Mitarbeitenden bedienen diese Instrumente tagtäglich und vertrauen den Ergebnissen vielfach blindlings.

Zu den latenten Gefahren gehören

- die unkümmerte Bedienung: Die grösste und teuerste Gefahr für die IT entsteht gemäss verschiedenen Studien durch Irrtum und Nachlässigkeit der Mitarbeitenden in der Verwaltung. Das Fehlverhalten wird begründet mit fehlenden Regelungen, Unwissenheit, mangelnder Ausbildung und Gleichgültigkeit der Menschen
- der Remote-Support: Heute stehen in den Gemeindeverwaltungen neben



Wer hat Zugang zu welchen Daten? Um die IT-Sicherheit zu erhöhen, müssen auch Verhaltensregeln kommuniziert werden. (Bild: Peter Kirchhoff, Pixelio)

Keine Abfrage möglich	Der Arbeitsfluss ist gestoppt
	Die «Notkarteien» sind nicht mehr vorhanden oder nicht in aktuellem Zustand
	Das Ausweichen auf Papierdossiers ist zeitraubend und für viele ungewohnt
Die Textbearbeitung läuft nicht	Es kann keine Auskunft erteilt werden
	Die Vorlagen fehlen – die «Fallmappe» muss manuell und visuell durchgepflügt werden
Die Drucker funktionieren nicht	Die Schreibmaschinen sind weggeräumt – eine einzige ist geblieben für das Erstellen von Adressetiketten
	Nicht funktionierende Drucker lähmen den Betrieb
Das E-Mail-Programm funktioniert nicht	Bestätigungen, Bewilligungen können nicht ausgefertigt werden
	Der Arbeitsfluss ist gestört
	Beim Griff zum Telefon als E-Mail-Ersatz wird einem bewusst, wie effizient E-Mail ist

Grosse IT-Pannen und ihre Auswirkungen.

(Tabelle: zvg)

Wichtige Schritte zur IT-Sicherheit

- Sensibilisieren: Sicherheit ist Chefsache. Die Verwaltung und die Behörden sind auf die IT-Sicherheit aufmerksam zu machen, beispielsweise indem das Thema auf eine Traktandenliste aufgenommen wird oder entsprechende Unterlagen in Umlauf gebracht werden
- Anstoss geben: Die Verwaltungsleitung steht dahinter. Sie will das Thema IT-Sicherheit aktivieren, indem sie eine Arbeitsgruppe bildet und dafür Geld spricht
- Aufbau Regelwerk: Die IT-Abläufe werden dokumentiert. Wer hat Zugang und Mutationsberechtigung bei welchen Daten und Programmen? Es werden Verhaltensregeln aufgestellt und vermittelt, beispielsweise auch als Anhang zu den Arbeitsverträgen
- Umsetzung: Für die IT-Sicherheit wird ein Ansprechpartner bestimmt und eingesetzt. Die IT-Infrastruktur wird gemäss Massnahmenkatalog angepasst, und die Mitarbeitenden werden geschult
- Kontrolle: Regelmässige Sicherheits-Checks (Stichproben) durchführen

den zentralen Applikationen 20 und mehr Randapplikationen im Einsatz. Diese werden von unterschiedlichen Herstellern meistens über Remote-Support am Laufen gehalten. Die Datenintegrität ist durch den Zugang von aussen gefährdet

Weitere Gefahren sind beispielsweise

- Nachlässigkeiten im Umgang mit Listen bei Transport, Lagerung, Vernichtung und Wiederverwendung (Rückseiten)
- Verlassen von Bildschirmarbeitsplätzen ohne Logout
- Passwort-Handling
- externe DVDs, USB-Sticks, Handys, PDAs oder Notebooks enthalten ein hohes Gefahrenpotenzial
- einfacher Zutritt zu Datenarchiven

Der Spagat zwischen Datenschutz und Auskunftsbereitschaft

Alle Amtsstellen verlangen den Zugang zu Einwohnerdaten wie auch zu Debitoren- und Kreditoreneinformationen. Die Daten sind vorhanden – in einer Form, in der sie sozusagen kostenlos

den Interessenten zur Verfügung gestellt werden können. Der Zugang ist somit nur noch eine Formsache. Die Datenschutzstelle beobachtet im Bereich Personendaten deren korrekte Bearbeitung. Sie kontrolliert, wie die «öffentlichen Organe» – unter anderem Gemeinderäte, Kommissionen und Verwaltungsstellen – mit den Personendaten umgehen. Wird nach den Grundsätzen von Treu und Glauben und der Verhältnismässigkeit gearbeitet? Das bedeutet die Beachtung von Zweckbindung, Zugriffsrechten, Datenvermeidung und Datensparsamkeit. Bei festgestellten Mängeln werden die Verantwortlichen ermahnt – das sind die Gemeindebehörden!

Wie die Nuss geknackt werden kann

IT-Sicherheit ist Chefsache. Wie kriegt die verantwortliche Behörde das Thema in den Griff? Hat sie die Zeit und das Wissen für fundierte Sicherheitsabklärungen, oder soll sie Hilfe von aussen für folgende notwendige Arbeiten beziehen?

- Definition des Schutzbedarfes
 - Der Ausführungsgrad der technischen Sicherheit wird ermittelt aufgrund der Frage: Wie viel Ausfall verträgt die EDV?
 - Wie lange können Sachbearbeiter schlimmstenfalls ohne Verfügbarkeit einer Anwendung auskommen?
 - Eine tabellarische Auflistung sämtlicher Anwendungen dient der Ermittlung des Schutzbedarfes
- Sind die Verwaltungsmitarbeitenden für die IT-Sicherheit sensibilisiert?
 - Die Gefährdung im IT-Betrieb setzt sich zusammen aus Bedrohung und Schwachstellen
 - Die Gefährdungsarten sind grob in höhere Gewalt, technisches Versagen, vorsätzliche Handlung und organisatorische Mängel zu unterteilen
- Wie bekommt die Behörde verlässliche Auskunft über den Sicherheitszustand in ihrer Gemeindeverwaltung?
 - Durch Beiziehen von spezialisierten, unabhängigen Fachleuten
 - Erfassen der Istsituation vor Ort zusammen mit dem IT-Verantwortlichen
 - Gemeinsame Festlegung des Schutzbedarfes
 - Definition der Zugriffsberechtigungen

Ein Bericht über den Sicherheitszustand und ein Massnahmenkatalog zur Sicherstellung der IT-Sicherheit müssen der Behörde vorliegen und laufend bei IT-Entscheiden beigezogen werden. Eine grundsätzliche Abklärung der IT-Sicherheit ist für alle von Nutzen – für die Behörden, das Verwaltungskader, die IT-Verantwortlichen und nicht zuletzt für die Bürgerinnen und Bürger.

Urs Fässler, urs.faessler@tribull.ch

Das Beispiel der Gemeinde Arth

Die IT-Kommission der Gemeinde Arth entschied im Frühling 2008 anlässlich einer Sicherheitspräsentation, eine detaillierte Sicherheitsabklärung in Auftrag zu geben. Diese lief folgendermassen ab:

- Standortbestimmung: Vor Ort wurde anhand eines Kriterienkataloges die Sicherheit rund um den IT-Betrieb abgeklärt. Die Hardware- und Netzwerkkomponenten wurden erfasst. Besonders aufmerksam wurden der Zugang zu den Daten und die Bedienung der Programme durchleuchtet
- Kenntnisnahme Sicherheitsbericht: Der aus den Abklärungen entstandene Sicherheitsbericht wurde aufmerksam zur Kenntnis genommen. Er zeigt die vorhandenen Schwachstellen auf und unterstützt die IT-Kommission mit einem Massnahmenkatalog in ihren zukünftigen Sicherheitsvorkehrungen
- Strategie-Ausarbeitung: Machbarkeit abklären, technisch, organisatorisch. Kostenschätzung pro Schwachstelle
- Prioritäten setzen: Terminierung der Umsetzung
- Umsetzung: Zuerst wurde ein Notfallszenario ausgearbeitet für den Fall, dass an den Bildschirmen in der Gemeindeverwaltung nichts mehr geht. Es soll der Gemeindeleitung ermöglichen, einen Disasterablauf ordnungsgemäss nach Regeln abzuwickeln. Ein Sicherheitshandbuch ist in Arbeit, wird laufend fortgeschrieben und dient den Mitarbeitenden als Nachschlagewerk für alle IT-Sicherheitsbelange. Die IT-Sicherheit ist ab sofort ein fixes Traktandum in den Sitzungen der IT-Kommission. Sicherheitsbericht nachführen