Kanton St.Gallen
Departement des Innern

Amt für Gemeinden und Bürgerrecht
Gemeindeaufsicht

Bericht über die Schwerpunktprüfung 2021: «IT-Sicherheit»

St.Gallen, 9. Mai 2022

Sehr geehrte Verwaltungsratspräsidentinnen und Verwaltungsratspräsidenten
Sehr geehrte Bürgerratspräsidentinnen und Bürgerratspräsidenten
Sehr geehrte Damen und Herren

Das Amt für Gemeinden und Bürgerrecht hat gestützt auf Art. 158 Abs. 1 Bst. a GG als Aufsichtsstelle die Schwerpunktprüfung «IT-Sicherheit» im Rahmen einer Online-Umfrage durchgeführt. Es wurden alle 264 Spezialgemeinden und Zweckverbände angeschrieben, wovon 181 an der Online-Umfrage teilgenommen haben. Zusätzlich dazu wurde bei 18 Spezialgemeinden und Zweckverbänden eine detaillierte Prüfung in Form eines Interviews durchgeführt.

Wir freuen uns, Ihnen diesen Gesamtbericht übergeben zu können und sind überzeugt, dass Sie in diesem Bericht wertvolle Informationen, Anregungen und Tipps für Ihre Spezialgemeinde oder Ihren Zweckverband entnehmen können. Machen Sie von dieser Gelegenheit Gebrauch. Wir bitten Sie, auch die Geschäftsprüfungskommission oder Kontrollstelle als auch das Verwaltungspersonal über den Gesamtbericht zu informieren.

Wir bedanken uns an dieser Stelle ganz herzlich bei den beteiligten Spezialgemeinden und Zweckverbänden dafür, dass sie sich für die Schwerpunktprüfung zur Verfügung gestellt haben sowie für die stets angenehme und konstruktive Zusammenarbeit.

Für Fragen stehen wir den Verwaltungsratsmitgliedern, den Mitgliedern der Geschäftsprüfungskommissionen oder Kontrollstellen sowie dem Verwaltungspersonal gerne zur Verfügung.

Der Abteilungsleiter	Der Revisor
Martin Jeker M.A. HSG	Dejan Janjic dipl. Experte Rechnungslegung und Controlling

Berichtsempfänger	Spezialgemeinden und Zweckverbände des Kantons St.Gallen
Prüfungszeitraum	Juni bis November 2021

Inhaltsverzeichnis

Im Bericht verwendete Abkürzungen

GG	Gemeindegesetz vom 21. April 2009, sGS 151.2
IKS	Internes Kontrollsystem
IT	Informationstechnologie
GPK	Geschäftsprüfungskommission oder Kontrollstelle
KOM SG[1]	Verein Interessensgemeinschaft Kommunikationsnetz St.Gallen
KOMSG	Kantonales Datennetz der KOMSG
Rat	Verwaltungsrat

[1] Mit KOM SG ist der Verein gemeint, mit KOMSG das Netzwerk

1 Ausgangslage

Die Digitalisierung eröffnet den Spezialgemeinden und Zweckverbänden neue Möglichkeiten mit der Bevölkerung in Kontakt zu treten und die Effizienz von Dienstleistungen zu steigern. Zugleich erfordert sie eine Neuorganisation oder Anpassung der Prozesse und führt zu einer grösseren Abhängigkeit von der IT-Infrastruktur und deren Anbietern. Diese Vernetzungen und Abhängigkeiten führen in zunehmendem Umfang zu Datenverlusten und Vermögensschäden. Um diese Cyberrisiken besser in den Griff zu bekommen und sich vor Angriffen zu schützen, haben die Gemeinden und Spezialgemeinden Vorkehrungen zu treffen. Insbesondere bei den Spezialgemeinden ist unklar, inwiefern ausreichend Vorkehrungen durch die Verantwortlichen zur Risikominimierung von Cyberangriffen getroffen werden. Diese Schwerpunktprüfung soll aufzeigen, wo Schwachstellen im Umgang mit IT-Risiken bestehen und Empfehlungen für die verantwortlichen Entscheidungsträger liefern.

2 Relevante Rahmenbedingungen

Die Verwaltungsstellen der politischen Gemeinden und des Kantons St.Gallen unterhalten eine gemeinsame Kommunikationsinfrastruktur, die KOM SG (KOM SG). Die KOM SG definiert interne Sicherheitsvorschriften um die notwendigen Rahmenbedingungen und ein sicheres Umfeld zu gewährleisten. Die definierten Mindestanforderungen gelten für alle angeschlossenen Institutionen innerhalb des KOM SG-Verbundes und für Dienstanbieter und Netzbetreiber die Übergänge ins KOMSG betreuen. Zur Sicherstellung der Sicherheit im KOMSG-Netz führt die KOM SG periodische Überprüfungen durch. Die angeschlossenen Gemeinden werden mittels eines Auditberichts auf missbräuchliche Verwendung der Informatikmittel und sicherheitsrelevante Risiken hingewiesen.

Alle Gemeinden des Wahlbezirks Sarganserland haben sich für den operativen Betrieb der ICT-Dienste auf dem KOMSG-Netz zusammengeschlossen. Dies beinhaltet die Harmonisierung des Einkaufs und Betriebs der ICT-Dienstleistungen (Kopierer, Drucker, Support), der Sicherheit, der Berichterstattung usw. durch die Informatikdienste Sarganserland (IDSL). Andere Gemeinden organisieren den IT-Support selbst oder mit einer externen Firma.

Viele Spezialgemeinden (Ortsgemeinden, Schulgemeinden, Korporationen) und Zweckverbände sind nicht Mitglied der KOM SG und unterliegen daher nicht den Sicherheitsvorschriften und der Überwachung durch die KOM SG. Dies führt unweigerlich zu einer grösseren Verantwortung der jeweiligen Räte, die IT-Sicherheit bei der Risikobeurteilung höher zu gewichten und sicherzustellen. Die IT-Sicherheit ist ausreichend und der Grösse der Gemeinde entsprechend zu gewährleisten.

3 Gesetzliche Grundlagen

Für die politischen Gemeinden besteht mit dem Gesetz über E-Government in Art.7 die gesetzliche Grundlage, dass angemessene Massnahmen zum Schutz der Integrität und Verfügbarkeit von Daten bestehen müssen. Die Massnahmen sind regelmässig zu überprüfen und haben dem Stand der Technik zu entsprechen.

Der Rat der Spezialgemeinde ist gemäss Art. 89 GG das oberste Leitungs- und Verwaltungsorgan der Gemeinde. Er führt und plant Ihre Tätigkeiten. Zudem ist er gemäss Art. 123 GG für die Existenz eines IKS verantwortlich. Es ist davon auszugehen, dass mit steigenden Abhängigkeiten der Informatikmittel die IT-Risiken im IKS berücksichtigt werden müssen.

4 Projektziele

Mit der Schwerpunktprüfung 2021 soll festgestellt werden, ob die Spezialgemeinden angemessene Massnahmen zum Schutz der Integrität und Verfügbarkeit der von ihnen eingesetzten IT-Services sowie zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit der von ihnen gespeicherten, verarbeiteten und übertragenen Daten treffen. Ebenso soll geprüft werden, ob dies dem zu erwartenden Stand der Technik entspricht.

Ein besonderes Augenmerk soll dabei auf der Tätigkeit des Rates bezüglich Organisation und Verantwortlichkeiten, Awareness (Bewusstsein) und IKS liegen.

Folgende Themen sind in der Zielsetzung im Prüfprogramm berücksichtigt:

Themen und Ziele	**Aussage der Prüfung**
Rat (Führung und Planung)	Bewusstsein für Cyberrisiken sind im Rat vorhanden.
	Risiken aus dem Umgang mit Informatikmitteln sind dem Rat bekannt.
	Organisatorische Massnahmen zum Umgang mit Cyberrisiken sind definiert und schriftlich festgehalten.
	Sensibilisierung der Mitarbeitenden durch den Rat
	Externe Sicherheitsservices sind bekannt und aktualisiert.
IKS (Vollständigkeit der Risiken und Kontrollen)	Risiken und Schlüsselkontrollen betreffend IT-Sicherheit sind im IKS berücksichtigt.
	Festlegung der Verantwortlichkeiten der Kontrollen
	Überprüfung der Wirksamkeit der Kontrollen

Aus den Zielen und den Prüfungshandlungen sollen nach der Prüfungsdurchführung Empfehlungen zur Minderung der Risiken an die Gemeinden formuliert werden.

5 Ergebnisse Schwerpunktprüfung IT-Sicherheit

Die Ergebnisse beruhen auf der Auswertung der Online-Umfrage sowie der Interviews. Aufgrund des Prüfungsumfangs wird in den Feststellungen der Fokus auf jene Antworten gelegt, die zu einem grossen Teil ähnlich beantwortet wurden.

5.1 Organisation

Die Organisation der IT variiert je nach Grösse der teilnehmenden Spezialgemeinde oder des teilnehmenden Zweckverbandes und muss differenziert betrachtet werden. Generell gilt, dass die Organisation der Grösse und dem Risiko angepasst sein sollte.

5.1.1 IT-Struktur

Definition einer verantwortlichen Person, Zusammenarbeit mit externen Partnern, Systemadministrator, Übersicht der IT-Organisation (Mappe), Notfallkonzept

Feststellungen:
Bei mehr als zwei Drittel der teilnehmenden Spezialgemeinden ist eine für die IT verantwortliche Person definiert. Die übrigen Spezialgemeinden sind jeweils am Netzwerk der politischen Gemeinde angeschlossen, haben die Betreuung der IT an einen externen Partner delegiert oder haben aufgrund der Grösse keine verantwortliche Person. Die Fachkunde der zuständigen Personen variiert teilweise stark.

Mehr als zwei Drittel der Teilnehmenden arbeiten mit einem externen IT-Dienstleister zusammen. Die meisten Spezialgemeinden verstehen darunter Wartungsverträge und Support von betriebsnotwendiger Software. Die Funktion des Systemadministrators[2] ist bei den meisten Teilnehmenden nicht definiert oder wird durch die IT-verantwortliche Person wahrgenommen. Vereinzelt übernimmt der Ratspräsident die Funktion des Systemadministrators. Die Applikationen oder Berechtigungen werden vom Systemadministrator oder dem jeweiligen Anwender freigegeben. Bei mehreren Spezialgemeinden besteht hierzu keine Regelung, da aufgrund derer Grösse mit privaten Einzelgeräten gearbeitet wird.

Positiv ist zu werten, dass mehr als die Hälfte aller Teilnehmenden über eine Übersicht der IT verfügt. Die Spezialgemeinden ohne IT-Übersicht sind mit privaten Geräten organisiert oder der politischen Gemeinde angeschlossen.

Die wenigsten Spezialgemeinden verfügen über einen Notfallplan. Wo vorhanden, gilt der Notfallplan für die Steuerungssoftware (z.B. Leitsystem bei einer Wasserversorgung oder einer Abwasserreinigungsanlage) oder es wird auf die Datensicherung verwiesen.

Hinweise und Empfehlungen:
- Wir empfehlen die Definition eines IT-Verantwortlichen, auch falls die IT vollständig durch einen externen Partner betreut wird. So ist sichergestellt, dass die strategische Ausrichtung und die Verantwortlichkeit durch den Rat wahrgenommen werden kann.
- Stellen Sie sicher, dass der Zugriff der Anwender auf die für sie notwendigen Daten und Software begrenzt ist. Ausnahmen bilden hier private Geräte, mit denen autonom gearbeitet wird.

[2] Person mit Administratorenrechten auf Geräte als auch auf Software und Website

- Stellen Sie sicher, dass die Anwender mit Administratorenrechten einen eigenen User-Account haben und nicht mit dem Administrator-Benutzer arbeiten.
- Sollte eine Software durch mehrere Anwender genutzt werden, empfehlen wir die Berechtigungen anhand eines Berechtigungskonzepts zu erteilen. Die Erteilung der Berechtigungen sollte, nach Möglichkeit im Vieraugenprinzip erfolgen. Ein Berechtigungskonzept dient als technische Unterstützung des Vieraugenprinzips der Geschäftsprozesse.
- Der Ernstfall kann aufgrund einer technischen Störung oder Softwarestörung als auch durch einen externen Angriff eintreten. Ein Notfallkonzept kann die Reaktionszeit im Ernstfall verkürzen und die Sicherstellung des Geschäftsbetriebs gewährleisten.

5.1.2 Datensicherungen

Regelmässige Datensicherung

Feststellungen:
Den meisten Spezialgemeinden ist das Risiko eines Datenverlusts bewusst und es werden täglich Datensicherungen vorgenommen. Vereinzelte Spezialgemeinden haben keine konsequente Datensicherung, da sporadisch und teilweise mit Privatgeräten gearbeitet wird. Auch sind mehrere Spezialgemeinden nicht in einem Netzwerk verbunden und arbeiten mit autonomen Einzelgeräten. Die Datensicherung ist bei diesen Spezialgemeinden individuell organisiert.

Hinweise und Empfehlungen:
- Wir empfehlen, die Datensicherung konsequent und regelmässig durchzuführen. In den vergangenen Monaten haben Cyberangriffe zugenommen: Daten wurden verschlüsselt und der Geschäftsbetrieb konnte nicht mehr gewährleistet werden. Als Datensicherung eignen sich, abhängig von der Grösse der Infrastruktur, externe Festplatten, Bandlaufwerke oder ein separater Server (physisch oder virtuell). Eine Kopie der Datensicherung unabhängig vom Netzwerk (offline) erhöht die Datensicherheit zusätzlich.
- Sollte für die Datensicherung eine Cloud-Lösung angedacht sein oder im Einsatz sein, gilt zu beachten, dass die Daten ebenfalls durch die Schadsoftware verschlüsselt werden können. Gewisse Dienstleister bieten hierfür einen Schutz. Bitte beachten Sie das bei der Auswahl des Cloud-Dienstes für die Datensicherung.
- Bei Spezialgemeinden, welche mit Einzelgeräten arbeiten, empfehlen wir dem Rat, die Datensicherung der einzelnen Nutzer in einem Merkblatt/einer Empfehlung festzuhalten und in einer Ratssitzung zu thematisieren.

5.1.3 Beschaffung und Entsorgung von Hard- und Software

Beschaffung Hard- & Software, Entsorgung

Feststellungen:
Die Beschaffung von neuen Geräten und Software hängt stark von der Grösse der Organisation ab. Mehrere kleinere Spezialgemeinden zahlen den Anwendern eine pauschale Entschädigung für die Benützung privater Geräte. Vereinzelt wurde von den Teilnehmenden gemeldet, dass keine Regelung vorhanden ist und die Anwenderinnen und Anwender im Rahmen der Finanzkompetenzen individuell neue Geräte oder Software beschaffen können. Bei den übrigen zwei Drittel der Spezialgemeinden ist die Beschaffung von Hard- und Software organisiert. Der Bedarf wird im Rat behandelt und entsprechend

budgetiert. Die Beschaffung erfolgt dann entweder durch die IT-Verantwortlichen oder durch den externen Partner.

Bei der Detailprüfung wurde die Entsorgung alter Geräte hinterfragt. Es ist erfreulich, dass das Risiko von Datendiebstahl auch bei der Entsorgung von Geräten grossmehrheitlich beachtet wird. Die Geräte werden zusätzlich zur normalen Datenlöschung nochmals formatiert oder die fachgerechte Entsorgung wird durch den externen IT-Partner gewährleistet. Vereinzelt wird die Festplatte entfernt und weiterhin aufbewahrt oder sogar zerstört.

Hinweise und Empfehlungen:
- Im Sinn einer einheitlichen Organisation und Sicherstellung der Kompatibilität der einzelnen Geräte und Software empfehlen wir, die Beschaffung im Rat zu behandeln und die Ausgaben zu budgetieren. Die für die IT verantwortliche Person kann die Beschaffung im Rahmen der Finanzkompetenzen erledigen. Von einer individuellen Beschaffung raten wir – ausser bei Kleinstgemeinden – ab.
- Achten Sie auf eine fachgerechte Entsorgung. Für eine vollständige Löschung der Daten kann eine Software heruntergeladen werden wie zum Beispiel DBAN. Eine Beschreibung der Funktionsweise sowie den Download der Software finden Sie auf giga.de/downloads/dban/. Um die Wiederverwertung der Daten zu vermeiden, empfehlen wir die physische Zerstörung der Festplatte oder des Datenträgers.

5.1.4 Sensibilisierung der Anwender

Benutzerrichtlinien, Sensibilisierung auf Risiken, Hinweis auf Website zur Prüfung von E-Mail-Missbrauch und Warnmeldungen

Feststellungen:
Die Hälfte aller Spezialgemeinden hat Nutzungsrichtlinien für die IT. Bei vereinzelten Spezialgemeinden wird die Nutzungsvereinbarung unterschrieben im Personaldossier abgelegt. Eine verbreitete Form ist ein Merkblatt mit Hinweisen oder auch nur eine mündliche Instruktion der Anwenderinnen und Anwender. Die Spezialgemeinden ohne Benutzerrichtlinien geben an, dass dies aufgrund der Grösse der Organisation unnötig oder überflüssig ist.

Eine Sensibilisierung auf aktuelle Sicherheitsrisiken findet bei den meisten Spezialgemeinden nicht statt. Es wird darauf vertraut, dass die Anwenderinnen und Anwender durch ihren Arbeitgeber (Grossteil der Spezialgemeinden funktioniert im Miliz-System) informiert wurden oder sich selbst über aktuelle Risiken und Gefahren erkundigt haben. Spezialgemeinden, welche die Anwenderinnen und Anwender informieren, tun dies vorwiegend im Rahmen von periodischen Sitzungen/Schulungen oder Informations-E-Mails mit Hinweis auf aktuelle Gefahren.

Hinweise und Empfehlungen:
- Benutzerrichtlinien dienen den anwendenden Personen als Information, für welche Zwecke sie die Geräte der Spezialgemeinde einsetzen dürfen und was es bei der Verwendung privater Geräte zu beachten gilt. Zusätzlich wird in den Richtlinien als vorbeugende Schutzmassnahme auf Risiken durch unsachgemässe oder unaufmerksame Handhabung hingewiesen. Nutzen Sie die Chance, die Anwenderinnen und Anwender als beste Präventivmassnahme einzusetzen. Wir empfehlen dem Rat, allen Anwende-

rinnen und Anwendern ein Merkblatt mit den Nutzungsrichtlinien zur Verfügung zu stellen. Im Internet lassen sich diverse Muster solcher Benutzerrichtlinien finden. Es kann auch auf die Vorgaben der Sicherheitsvorkehrungen der KOM SG[3] zurückgegriffen werden.
- Tagtäglich ist in den Zeitungen von neuen Hacker-Angriffen zu lesen, die ganze Unternehmen stilllegen. Meistens handelt es sich um eine kleine Unaufmerksamkeit der Anwenderin oder des Anwenders, welche das Problem ausgelöst hat. Wir empfehlen, die Anwenderinnen und Anwender regelmässig auf eventuelle Risiken hinzuweisen. Insbesondere den Ratspräsidentinnen und Ratspräsidenten empfehlen wir eine aktive Informationspolitik und das Thema regelmässig an einer Ratssitzung zu behandeln. Der Aufwand hierfür ist bedeutend geringer als nachträglich den Schaden zu beheben.
- Folgende Websites bieten sich für aktuelle Warnmeldungen im Bereich IT-Risiken an:
  - Hinweis zu Phishing-Mails: https://www.swisscom.ch/de/b2bmag/sicherheit/phishing-entlarven-melden-loeschen/
  - aktuelle Gefahren: NCSC Startseite (admin.ch)
  - aktuelle Gefahren: cybercrimepolice.ch

  Im Link der Swisscom mit Hinweisen zu Phishing-Mails ist am Ende des Theorieteils ein E-Learning aufgeschaltet, welches zusätzlich der Sensibilisierung der Anwenderinnen und Anwender dient.

5.2 Technik

Die Art der Infrastruktur ist den Spezialgemeinden und Zweckverbänden nicht vorgeschrieben. Je nach Komplexität der Aufgaben und Grösse der Organisation sollte die optimalste Variante gewählt werden. Unter Umständen kann die effizienteste Variante die Verwendung von privaten Einzelgeräten sein.

5.2.1 Netzwerk

Netzwerk oder Einzelstationen, Cloud

Feststellungen:
Vereinzelte Spezialgemeinden sind am Netzwerk der politischen Gemeinde angeschlossen. Der Grossteil der Gemeinden ist aber mit autonomen Einzelgeräten unterwegs, ohne Anbindung an ein internes Netzwerk.

Mehr als die Hälfte der Teilnehmerinnen und Teilnehmer hat keinen webbasierten Dienst (Cloud) im Einsatz. Die genutzten Cloud-Lösungen werden von diversen Anbietern zur Verfügung gestellt und unterscheiden sich hauptsächlich in den Kosten und dem Server-Standort. Teilweise werden auch webbasierte Programme (zum Beispiel Abacus) genutzt. Der Standort der Server ist aufgrund der lokal geltenden Datenschutzgesetze ein nicht zu unterschätzendes Risiko bezüglich Datenschutz.

Hinweise und Empfehlungen:
- Ob mit Einzelgeräten oder in einem Netzwerk gearbeitet wird, ist den Spezialgemeinden überlassen. Wir empfehlen eine periodische Überprüfung, ob mit einer Reduktion oder Ausweitung der Infrastruktur effizienter und sicherer gearbeitet werden kann.

[3] https://komsg.ch/Sicherheit/

- Daten der Spezialgemeinde sind vertraulich, was bei der Auswahl des Cloud-Dienstes berücksichtigt werden sollte. Die Serverstandorte der jeweiligen Cloud-Dienste unterstehen den lokalen Datenschutzgesetzen, welche teilweise nicht so streng ausgelegt sind wie das Schweizer Datenschutzgesetz. Wir empfehlen aufgrund des Datenschutzes eine europäische oder schweizerische Lösung zu verwenden.

5.3 Sicherheit

Die beste Infrastruktur ist nur mit einem konsequenten Schutz sinnvoll einsetzbar. Der Schutz kann präventiv durch Zugriffsbeschränkungen auf einzelne Applikationen oder die Anmeldung am Gerät gewährleistet werden. Ein weiterer präventiver Aspekt sind die Firewall und Virenschutzprogramme, welche gegen einen unbefugten Fernzugriff oder die Abwehr von Schadprogrammen unabdingbar sind. Der konsequente Schutz der Infrastruktur und der Daten dient der Gewährleistung der Aufgabenerfüllung der Spezialgemeinde.

5.3.1 Sicherheitsprogramme

Firewall und Virenschutz, Cyberangriffe

Feststellungen:
Es ist erfreulich, dass sich praktisch alle Spezialgemeinden des Risikos bewusst sind und ein Virenschutzprogramm im Einsatz haben. Eine Firewall ist bei praktisch allen Spezialgemeinden mit einer Netzwerkstruktur vorhanden. Die Zuverlässigkeit der Firewall kann aufgrund fehlender Informationen zur Konfiguration nicht beurteilt werden. Vereinzelte kleinere Spezialgemeinden überlassen die Verantwortung, wie die Geräte geschützt werden, den Anwenderinnen und Anwendern. Teilweise handelt es sich um Privatgeräte, die aber mindestens im Eigeninteresse der Eigentümerin oder des Eigentümers geschützt werden sollten. Die Qualität des Schutzes auf Privatgeräten ist äusserst ungewiss und wird normalerweise nicht von der Spezialgemeinde überwacht.

Einen grösseren oder folgenschweren Cyberangriff hatte bisher keine der teilnehmenden Spezialgemeinden. In wie vielen Fällen der Angriff bereits durch die Firewall oder das Virenschutzprogramm abgewehrt wurde, konnte nicht eruiert werden. Bei einem Teilnehmenden gab es einen Angriff auf die Website und bei einem weiteren einen Angriff auf das Netzwerk. Beide Angriffe konnten schnell abgewehrt werden.

Hinweise und Empfehlungen:
- Die Sicherheit der Daten liegt im Interesse der Spezialgemeinde. Auch wenn der Virenschutz an die anwendenden Personen delegiert ist, sollten gewisse Vorgaben vorhanden und umgesetzt sein. Es besteht ein erhöhtes Risiko eines Datendiebstahls oder -verlustes durch mangelhaften Schutz der Privatgeräte. Ein aktuelles Virenschutzprogramm muss zwingend auf allen Systemen installiert sein. Der Rat hat weitere Präventivmassnahmen sicherzustellen, damit das Risiko einer grösseren Kostenfolge und eines Reputationsschaden im Fall eines Cyberangriffs reduziert wird.

5.3.2 Updates

laufende Updates auf alle Software

Feststellungen:
Regelmässige und zeitnahe Updates haben einen hohen Stellenwert und tragen aktiv zur Sicherheit bei. Sei es ein Windows-Update, welches Sicherheitslücken schliesst, das Update der Buchhaltungssoftware oder das Update des Virenschutzprogramms. Der Grossteil der Spezialgemeinden ist sich des Risikos bewusst und führt regelmässig Aktualisierungen von Windows durch. Vereinzelte Spezialgemeinden führen nur für einzelne Bereiche oder keine regelmässigen Windows-Updates durch. Begründet wird dies mit der Aussage, dass die Anwenderin oder der Anwender selbst verantwortlich ist.

Wie aktuell die übrige Software gehalten wird, wurde bei der Detailprüfung hinterfragt. Ein Trend kann hier nicht abgebildet werden, da je nach Tätigkeitsgebiet die Risiken individuell beurteilt werden müssen. Bei einem Teil der befragten Spezialgemeinden ist die Aktualisierung der Programme an den externen IT-Partner delegiert oder es wird nur für vereinzelte Software ein Update durchgeführt. Die übrigen Spezialgemeinden führen regelmässig Updates für alle im Einsatz befindlichen Programme durch.

Hinweise und Empfehlungen:
- Da auch die Entwickler von Schadprogrammen eine gewisse Zeit benötigen, ist eine aktuelle Software ein aktiver Schutz gegen einen Angriff. Wir empfehlen, alle Programme möglichst zeitnah nach Erscheinen eines Updates zu aktualisieren.
- Ein Virenschutzprogramm und eine gute Firewall anzuschaffen ist mittlerweile Standard. Nur durch eine permanente Aktualisierung kann der ursprüngliche und gewünschte Schutz erhalten bleiben. Stellen Sie eine zeitnahe Aktualisierung der Schutzprogramme sicher.
- Teilweise werden Updates nicht durchgeführt, weil man sich des Risikos nicht bewusst ist oder Ressourcen sparen will. Je älter die Version der Software oder des Betriebssystems ist, desto anfälliger ist sie für einen Cyberangriff. Wir empfehlen, die Anwenderinnen und Anwender auf dieses Risiko zu sensibilisieren und auf zeitnahe Aktualisierungen hinzuweisen.

5.3.3 Zugriffschutz, Passwörter

Umgang mit Passwörtern, Systemvorgaben

Feststellungen:
Rund 80 Prozent der Spezialgemeinden haben den Zugriff passwortgeschützt. Es gilt dabei zu unterscheiden, ob die Passwortabfrage für den Zugriff auf den Computer oder für die Anmeldung an ein bestimmtes Programm eingesetzt wird. In rund 20 Prozent der befragten Spezialgemeinden wird auf eine Passwortabfrage verzichtet. Vereinzelt handelt es sich dabei um zugewiesene Einzelgeräte ohne Zugang zum Netzwerk der Spezialgemeinde.

Die Passwörter sind bei der Mehrheit der Spezialgemeinden auf die Anwenderinnen und Anwender personalisiert. Teilweise gibt es ein Passwort für die Anmeldung am Computer oder ein Programm, welches von mehreren Personen genutzt wird. Dies ist vorwiegend bei Alters- und Pflegeheimen der Fall, wo ein Passwort für den Computer von mehreren

Nutzern verwendet wird. Die Anmeldung am entsprechenden Programm hingegen ist personalisiert.

Im Rahmen der Detailprüfung wurde gefragt, ob Vorgaben für die Komplexität des Passworts oder eine periodische Anpassung des Passworts vorgegeben sind. Je nach Grösse der Spezialgemeinde variieren die Vorgaben oder es ist den Anwendern überlassen.

Hinweise und Empfehlungen:
- Mit den Daten der Spezialgemeinde ist vertraulich umzugehen. Auch wenn ein Gerät nur durch eine Nutzerin oder einen Nutzer verwendet wird und bei ihr/ihm zuhause steht, ist der Zugriff mit Passwort zu schützen. Der Zugriff sollte auch vor Familienmitgliedern geschützt sein. Zusätzlich sind die Daten bei einem Diebstahl des Geräts minimal geschützt. Wir empfehlen, je ein individualisiertes Passwort für den Computer und ein davon abweichendes Passwort für die genutzten Programme zu verwenden. Zum erweiterten Schutz ist eine Verschlüsselung der Festplatte (BitLocker) mit Passwortabfrage vorzusehen.
- Es kommt vor, dass das Passwort am Bildschirm mit einem Notizzettel befestigt oder unter der Tastatur aufbewahrt wird. Der Schutz vor fremden Zugriff ist dadurch nicht gegeben. Achten Sie darauf, dass die Anwenderinnen und Anwender die Passwörter sicher aufbewahren.
- Eine sichere Alternative zur Aufbewahrung von Passwörtern sind spezielle Apps auf dem Smartphone. Der grösste Vorteil einer Passwortmanager-App ist, dass nur noch ein Passwort oder die Face-ID für den Zugriff auf alle übrigen Passwörter benötigt wird. Die Apps können bei Android-Geräten im Google Play Store oder bei Apple-Geräten im App Store heruntergeladen werden.
- Je komplexer das Passwort ist, desto schwieriger wird es, sich den Zugriff zu verschaffen. Mit einem periodischen Wechsel des Passworts wird der Schutz zusätzlich erhöht. Falls unbemerkt einmal das Passwort gehackt wurde, kann es nicht weiter durch Unbefugte verwendet werden.

5.4 Kontrolle

Die periodische Überprüfung der IT ist mit zusätzlichem Aufwand verbunden. Entweder sind es Prüfpunkte im IKS oder es wird geprüft, ob die Geräte und die Software noch aktuell sind. Es gibt auch IT-Dienstleister, welche die gesamte IT einem Sicherheitsaudit unterziehen und so objektiv auf Lücken und das Optimierungspotenzial hinweisen. Der Fortschritt im digitalen Bereich ist gross und eine regelmässige Überprüfung unbedingt notwendig.

5.4.1 IKS

Erwähnung im IKS

Feststellungen:
Bei den wenigsten Spezialgemeinden sind IT-Risiken im IKS abgebildet. Viele Spezialgemeinden erkennen die Notwendigkeit nicht, da sie sich aufgrund der Organisationsstruktur (Arbeit mit Einzelgeräten, kein Netzwerk, Selbstverantwortung der Anwender, usw.) der Risiken nicht bewusst sind.

Hinweise und Empfehlungen:

- Die Aufnahme der IT-Risiken im IKS hat den grossen Vorteil, dass sich der Rat mit der Organisation und den dazu notwendigen Kontrollen auseinandersetzt. Es geht nicht darum, komplexe Prüfhandlungen zu implementieren. Ziel ist es, einfache organisatorische Kontrollen zu haben und diese tatsächlich durchzuführen. Erwähnt seien hier die Aktualisierung des Virenschutzes und der Firewall, die sichere und flächendeckende Anwendung und Aufbewahrung von Passwörtern oder die Prüfung der Zugriffsberechtigungen bei einzelnen Programmen (Übersicht kann bei vielen Programmen gedruckt werden). Die Verantwortung der Kontrollmassnahmen ist an die entsprechenden Personen zuzuweisen. Der Rat kontrolliert die Durchführung der Kontrollmassnahmen.

5.4.2 Kontrolltätigkeiten

Prüfung durch Rat, GPK oder Revisionsstelle, externes Sicherheitsaudit

Feststellungen:

Der Grossteil der Spezialgemeinden führt keine periodischen Kontrollen der IT durch. Bei knapp einem Viertel der Teilnehmenden wurden Kontrollen durchgeführt, welche vorwiegend durch die GPK bewerkstelligt wurden. Vereinzelt ist bei Spezialgemeinden die Meinung vorhanden, dass das Amt für Gemeinden und Bürgerrecht bei der aufsichtsrechtlichen Prüfung auch die IT kontrolliert, was nicht der Fall ist.

Einem externen Sicherheitsaudit haben sich bisher rund 20 Prozent der Spezialgemeinden unterzogen. Zu erklären ist diese niedrige Quote unter anderem, dass sehr viele Spezialgemeinden ohne Netzwerk arbeiten und somit das Risiko auf mehrere Einzelgeräte und autonome Anwenderinnen und Anwender verteilt ist.

Hinweise und Empfehlungen:

- Die Sicherstellung einer periodischen Kontrolle der IT liegt in der Verantwortung des Rates. Die GPK als auch die Aufsichtsstellen sind nachgelagerte Prüforgane, die aufgrund ihrer eigenen Risikobeurteilung die IT prüfen. Der GPK empfehlen wir, im Rahmen der Amtsführungsprüfung die Informatikfragen im Arbeitspapier 1 des Amtes für Gemeinden und Bürgerrecht zu stellen. In grösseren Organisationen empfehlen wir der GPK, in Absprache mit dem Rat und der externen Revisionsstelle periodisch ein IT-Sicherheitsaudit durchzuführen.
- Das Risiko der IT wurde auch bereits vom Bund aufgenommen. Der Bund stellt Branchenstandards für die Spezialgemeinden online zur Verfügung. Diese können als Grundlage für eigene Kontrollmassnahmen genutzt werden. Wir empfehlen dem Rat, sich die Branchenstandards anzuschauen. Die Branchenstandards sind unter folgendem Link abrufbar: Branchenstandards (admin.ch).

6 Schlussfolgerung

Soviel Erleichterung die Digitalisierung mit sich bringt, soviel neue Risiken birgt sie. Wo früher ein abgeschlossenes Büro reichte, muss heute zusätzlich der Zugang durch Kommunikationsnetze gesichert werden.

Es ist positiv zu sehen, dass sich die Mehrheit der teilgenommenen Spezialgemeinden und Zweckverbände Gedanken zur IT-Sicherheit gemacht hat und diverse Massnahmen zur Risikominimierung getroffen wurden. Eine generelle Einschätzung, wie gut die vorhandenen Massnahmen sind, gestaltet sich bis auf einige wenige Bereiche schwierig. Bei den teilnehmenden Spezialgemeinden und Zweckverbänden haben wir von Organisationen mit zwei Einzelgeräten bis zu Organisationen mit über 70 Anwenderinnen und Anwendern eine grosse Bandbreite abgedeckt. Die Bedürfnisse von kleinen Ortsgemeinden über Wasserkorporationen bis hin zu Alters- und Pflegeheimen sind sehr unterschiedlich.

Dennoch ist in vielen Bereichen Optimierungspotenzial vorhanden. Jede organisatorische Massnahme, sei es durch Bestimmung einer oder eines IT-Verantwortlichen und Systemadministratorin oder Systemadministrators sowie die Implementation von Virenschutzprogrammen, dient der Sicherheit. Man darf nicht vergessen, dass viele Hackerangriffe durch Unaufmerksamkeit der Anwenderinnen oder Anwender begünstigt werden. Daher ist die Sensibilisierung aller involvierten Personen äusserst wichtig. Den Verwaltungsratsmitgliedern wird empfohlen, in ihrer Organisation die Prävention durch Sensibilisierung der Mitarbeitenden aktiv zu gestalten. Ihre Mitarbeitenden sind nicht nur ein Risiko, sondern auch das beste Warnsignal zur Vermeidung eines Schadens.

Im Sinn einer Qualitätssicherung sollten die bestehende Organisation und die präventiven Schutzmassnahmen periodisch geprüft und angepasst werden. Nur so kann ein optimaler Schutz gewährleistet werden.