Cyberdelikte verhindern
Wegleitung für Gemeinden

Inhaltsverzeichnis

1 Was Cyberkriminalität mit Ihrer Gemeinde zu tun hat 3

2 Wie Kriminelle Ihrer Gemeinde schaden können 4
2.1 Methoden von Betrügerinnen/Betrügern 4
2.2 Varianten von Erpressung und Diebstahl 5

3 Wie Sie Ihre Gemeinde schützen können 7
3.1 Organisatorische Schutzmassnahmen 7
3.2 Technische Schutzmassnahmen 10

4 Was Sie bei der Auslagerung der IKT-Leistungen beachten sollten 11

5 Was Sie im Schadensfall tun müssen 13

6 Wie Sie zur Ermittlung der Täterschaft beitragen können 14
6.1 Keine falsche Scheu vor einer Meldung 14
6.2 Vorfälle umgehend melden 14

Checklisten
> Tipps für Gemeindekader zum Schutz vor Cyberangriffen
> Tipps für Mitarbeitende von Gemeinden, um Cyberdelikte zu verhindern
> Wie gut ist Ihre Gemeinde vor Cyberangriffen geschützt?
> Empfohlene Standards und Leitfäden im IKT-Bereich

1 Was Cyberkriminalität mit Ihrer Gemeinde zu tun hat

Mehr Bürgernähe, bessere Tourismus- und Wirtschaftsförderung, medienübergreifende, schnelle Dienste: Die Digitalisierung bietet Gemeinden viele neue Möglichkeiten. Zugleich erfordert sie neue Prozesse und führt zu einer grösseren Abhängigkeit von funktionierender Informations- und Kommunikationstechnik (IKT) sowie von den damit verbundenen Dienstleistungsunternehmen. Diese Vernetzungen und Abhängigkeiten nutzen Kriminelle aus.

Der Nachrichtendienst des Bundes hält in seinem Lagebericht von 2019[1] fest, dass auch die öffentliche Verwaltung Ziel von Cyberangriffen sei. Von der Gemeindeverwaltung bis hin zur Stromversorgung – es kann alle treffen. Dabei kann zum Beispiel die Website offline gehen, aber auch das gesamte Netzwerk betroffen sein. Nebst finanziellen Schäden gelangen in manchen Fällen vertrauliche Informationen in falsche Hände – dies mit gravierenden Folgen: Verlust von Daten, Ausfall von Systemen, haftpflichtrechtliche Ansprüche aufgrund einer Datenschutzverletzung oder Reputationsschaden sind einige Beispiele.

Cyberangriffe können das Vertrauen der Bevölkerung in die Verwaltung nachhaltig zerstören.

Mit dem vorliegenden Informationsmaterial geben wir kleineren und mittelgrossen Gemeinden konkrete Empfehlungen zum Schutz vor Cyberkriminalität und zeigen auf, wie nach einem Angriff reagiert werden kann. Damit wird auch ein Beitrag zur Implementierung der Massnahmen der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022» geleistet, die den Schutz der Schweiz im Cyberbereich als gemeinschaftliche Aufgabe von allen Staatsebenen und weiteren Partnern zum Ziel hat.[2]

Zudem wollen wir Sie ermutigen, relevante Vorfälle der Polizei zu melden. Denn nur durch eine Zusammenarbeit von Strafverfolgungsbehörden und Betroffenen können Täter/-innen ermittelt und verurteilt werden, wodurch Cyberkriminalität nachhaltig bekämpft werden kann.

1 Nachrichtendienst des Bundes (2019). Sicherheit Schweiz 2019. Lagebericht des Nachrichtendienstes des Bundes. www.vbs.admin.ch
2 Bundesrat (2018). Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022, www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html

2 Wie Kriminelle Ihrer Gemeinde schaden können

Mit der Drohung, sensible Daten zu publizieren oder Dienste lahmzulegen, insbesondere im Bereich der Versorgungssicherheit, erpressen und bestehlen Cyberkriminelle die Gemeinden.

2.1 Methoden von Betrügerinnen/Betrügern

Durch Täuschung bringt die Täterschaft die Zielperson dazu, gegen deren eigentlichen Willen eine Handlung vorzunehmen. In den meisten Fällen geht es darum, die Zielperson zu verleiten, einen E-Mail-Anhang zu öffnen, einen Link anzuklicken, persönliche Daten wie Passwörter anzugeben oder eine Zahlung vorzunehmen.

Eine häufige Methode heisst Social Engineering. Dabei informiert sich die Täterschaft im Vorfeld vielfach über die Verwaltungs-, Organisations- oder Unternehmensstruktur. Dies geschieht durch öffentlich zugängliche Informationen, zum Beispiel auf der Website der Gemeindeverwaltung oder in sozialen Netzwerken. Daraufhin wird eine Zielperson ausgesucht und diese mit einem auf sie zugeschnittenen Szenario konfrontiert. Die Täterschaft versucht beispielsweise, an Benutzernamen und Passwörter zu gelangen, indem sie sich am Telefon als Mitarbeiter/-in eines Softwareunternehmens ausgibt. Durch Vorgeben akuter Computerprobleme und Vortäuschen von Betriebskenntnissen wird die Zielperson so lange verunsichert, bis sie die gewünschten Informationen preisgibt. Kriminelle missbrauchen in ihren E-Mails oder Anrufen manchmal auch die Namen von Verwaltungseinheiten, wie beispielsweise der Steuerverwaltung, oder von Energieversorgern.

Manipulationsarten

Hierarchie	Die Täterschaft nutzt die hierarchische Organisationsstruktur aus und erzeugt einen gewissen Handlungsdruck. Meist täuscht sie eine Identität vor und fordert Mitarbeitende im Namen einer vorgesetzten Person auf, sensible Informationen freizugeben oder eine Geldüberweisung vorzunehmen.
Zeitdruck	Der Zielperson wird vorgegaukelt, unter Zeitdruck handeln zu müssen.
Gier/Neugier	Der Zielperson wird ein Gewinn oder eine Überraschung versprochen, wenn die Datei geöffnet wird oder auf den Link geklickt wird.
Angst/Wut	Es wird mit Konsequenzen gedroht, falls der Aufforderung nicht nachgekommen wird, oder es werden offensichtlich falsche Aussagen gemacht, die man mit einem Klick auf einen schädlichen Link bereinigen soll.
Anteilnahme	Das präsentierte Thema spricht die Zielperson emotional an. Die Zielperson soll sich zum Beispiel beteiligen, um Missstände zu beseitigen.

2.2 Varianten von Erpressung und Diebstahl

Kriminelle verschaffen sich Zugang zu Ihrem Gemeindenetzwerk durch gestohlene Zugangsdaten, Schadsoftware oder schlecht gesicherte Systeme. Finden die Kriminellen wertvolle Daten, verschlüsseln sie diese oder sie drohen, sie zu veröffentlichen oder zu löschen, falls kein Lösegeld bezahlt wird. Manchmal werden Daten auch kopiert und an Dritte verkauft oder im E-Banking Zahlungen ausgelöst.

Häufige Vorgehensweisen

Ransomware	Schädlinge werden grossflächig verschickt, zum Beispiel per E-Mail. Die mit dieser Methode gefundenen Opfer werden im Anschluss gezielt ausgespäht, und es werden Informationen gesammelt. Hat die Täterschaft Erfolg, übernimmt sie die Kontrolle und beginnt, Daten zu verschlüsseln. Gegebenenfalls werden auch Daten gestohlen. Die Erpresser/-innen fordern für die Entschlüsselung der Daten Lösegeld (engl. ransom).
E-Banking-Trojaner	Neben der Erpressung steht vor allem die Manipulation von Zahlungsaufträgen im Visier von Cyberkriminellen. Dabei setzen sie E-Banking-Trojaner ein. E-Banking-Trojaner sind Programme, welche den Angreifenden Zugang zum E-Banking-Konto eines Opfers ermöglichen. Trojaner werden oft per E-Mail versandt (zum Beispiel getarnt als Rechnung oder Bewerbung).
Phishing	Potenzielle Opfer werden per E-Mail, Website, Internettelefonie oder Kurznachricht darauf hingewiesen, dass bestimmte Zugangsdaten nicht mehr sicher oder aktuell seien. Sie werden zeitgleich aufgefordert, diese unter dem aufgeführten Link zu ändern, welcher jedoch auf eine gefälschte Website führt. Loggt sich die angeschriebene Person auf der Website ein, erhält die Täterschaft die Zugangsdaten, beispielsweise Angaben zu Kreditkarten oder Passwörter für E-Mails oder einen anderen Account.
DDoS (Überlastattacken)	DDoS steht für Distributed Denial of Services. Bei einem solchen Angriff werden die Dienste, zum Beispiel der Internetauftritt, der Mailservice oder die digitale Telefonanlage, durch sehr viele Anfragen überlastet. Dadurch fallen Systeme aus, und die Verwaltung oder das Unternehmen können ihre eigentliche Aufgabe nicht mehr wahrnehmen. Damit der Angriff gestoppt wird, soll ein Lösegeld bezahlt werden. Kriminelle setzen DDoS-Attacken teilweise auch ein, um vom eigentlichen «digitalen Überfall» mit zuvor gestohlenen Zugangsdaten abzulenken.
Remote Access (Fernzugriff)	Remote Access dient dazu, von ausserhalb auf einen Computer oder ein Netzwerk zuzugreifen, beispielsweise im Homeoffice oder für die Fernwartung durch Supportmitarbeitende. Auch Kriminelle nutzen diesen Fernzugang, um auf Verwaltungs- und Unternehmensnetze zu gelangen, zum Beispiel mittels Phishing-Versuchen oder Angriffen auf Passwörter, auf ungesicherte oder auf veraltete Netzwerkkomponenten.

3 Wie Sie Ihre Gemeinde schützen können

Um sich gegen Cyberangriffe zu schützen, braucht es diverse technische und organisatorische Massnahmen. Einige können von den Gemeindekadern selbst umgesetzt, andere müssen mit den internen oder externen IKT-Verantwortlichen besprochen werden. Eine Zusammenfassung der hier aufgeführten Schutzmassnahmen finden Sie als Checklisten im hinteren Teil dieses Dokuments.

3.1 Organisatorische Schutzmassnahmen

> **Regeln Sie die Verantwortlichkeiten**
Benennen Sie in Ihrer Verwaltung Verantwortliche für die Erfüllung der jeweiligen Aufgaben im Zusammenhang mit der Sicherheit von IKT-Systemen. Klären Sie auch die Rollen und die Verantwortlichkeiten bezüglich Notfall- und Krisenorganisation sowie die entsprechenden Kompetenzen. Schnittstellen zu Partnern müssen im Vorfeld identifiziert und die Prozesse aufeinander abgestimmt werden. Klären Sie mit Ihrer/Ihrem IKT-Verantwortlichen, über welche Sicherheitsvorfälle Sie zwingend informiert werden müssen. Dies gilt für Vorfälle, welche Ihre eigene Infrastruktur betreffen, sowie diejenigen des IKT-Dienstleistungsunternehmens.

> **Erfassen Sie Ihre IKT-Umgebung**
Dokumentieren Sie Ihre IKT-Infrastruktur in einer möglichst detaillierten Inventarliste. Nur wenn Sie Ihre IKT-Infrastruktur, Ihre Services, Rechner, User usw. kennen, wissen Sie auch, was Sie schützen und überwachen müssen.

> **Sorgen Sie vor**
Eine gute Strategie gegen Cyberangriffe beginnt vor dem eigentlichen Vorfall: Eingespielte Prozesse und Eskalationspfade sind unabdingbar, um die Kontrolle zu behalten.

Definieren Sie, welche Logdateien (Ereignisprotokolldateien) gespeichert werden und wie lange. Am besten geschieht dies an einem zentralen Ort. Umfangreiche Logdaten helfen, den Ursprung eines Angriffs zu erkennen, Informationen über infizierte Systeme im eigenen Netzwerk zu erhalten und geeignete Gegenmassnahmen zu ergreifen. Aufgrund ihrer Wichtigkeit keineswegs zu vernachlässigen sind bei Logdateien auch die datenschutzrechtlichen Aspekte. Klären Sie Fragen zu Logdateien und zur Detektion von Angriffen mit Ihrer/Ihrem IKT-Verantwortlichen.

Vorabstrategie für den Fall einer Notsituation

> Kommunikations- und Krisenkonzept auf Grösse der Gemeinde angepasst und mit dem Dienstleistungsunternehmen abgestimmt.

> Kontaktlisten (interne und externe Stellen, Dienstleistungsunternehmen).

> Überlegungen
  > zum Totalverlust der IKT-Landschaft (Wiederbeschaffung, Wiederaufnahme Betrieb, Datenverlust usw.);
  > zu den Kommunikationsmitteln, die eingesetzt werden, wenn die IKT-Systeme nicht mehr verfügbar sind.

> IKT-Notfallszenarien, Übungen und Überprüfung der IKT-Infrastruktur auf Angreifbarkeit.

> **Regeln Sie den Umgang mit Informationen und schützenswerten Daten**
Führen Sie eine Daten- und Informationsinventur durch und definieren Sie besonders schützenswerte Elemente. Erstellen Sie ein Schutzkonzept für diese Elemente. Für kantonale und kommunale Datenschutzbestimmungen konsultieren Sie die Webauftritte Ihres Kantons und Ihres Gemeindeverbandes (siehe auch Kapitel 4: «Holen Sie sich Unterstützung»).

Überlegen Sie genau, welche Informationen Sie auf der eigenen Website oder in sozialen Medien offenlegen, denn diese werden von Kriminellen gesammelt. Insbesondere die für die Finanzgeschäfte zuständige Person in der Verwaltung, die Zugriff auf das E-Banking hat, sollte nicht auf der Website aufgeführt sein. Über unpersönliche Kanäle, zum Beispiel Telefon oder E-Mail, sollten grundsätzlich keine vertraulichen Informationen und Daten weitergegeben werden. Vertrauliche Informationen sollten konsequent verschlüsselt oder mit Briefpost an externe Stellen gesendet werden.

Seien Sie vorsichtig bei der Verwendung von Clouddiensten. Diese werden von vielen Programmen genutzt. Überlegen Sie sich, welche Daten lokal und welche in der Cloud gespeichert werden sollen. Legen Sie sensible Daten nie unverschlüsselt in einer Cloud ab. Lesen Sie vor der Nutzung eines Clouddienstes die Allgemeinen Geschäftsbedingungen (AGB) des anbietenden Unternehmens und achten Sie auf die Datenschutzbestimmungen. Daten dürfen nicht weitergegeben werden, zum Beispiel für wirtschaftliche Zwecke. Fragen Sie bei Ihrer Datenschutzaufsichtsstelle nach. Hilfsmittel zum Datenschutz und eine Auflistung der jeweiligen Aufsichtsstellen finden Sie auf der Website der Konferenz der schweizerischen Datenschutzbeauftragten, privatim, www.privatim.ch

> **Verwenden Sie sichere Passwörter**
Definieren Sie verbindliche Passwortregeln und setzen Sie diese auch gegenüber Mitarbeitenden konsequent durch. Die Mindestlänge eines Passwortes sollte bei zwölf Zeichen liegen und das Passwort sowohl aus grossen und kleinen Buchstaben, Zahlen wie auch Sonderzeichen bestehen. Idealerweise ist es zufällig generiert und bezieht sich nicht auf persönliche Informationen, zum Beispiel Namen oder Geburtsdatum. Zusätzlichen Schutz bietet eine Zwei-Faktor-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung von gleichen Passwörtern! Wenn es schwierig ist, sich mehrere Passwörter zu merken, sollten Sie einen Passwortmanager benutzen.

Befolgen Sie diese Regeln, ist eine zyklische Passwortänderung nicht zwingend. Passwörter müssen aber spätestens dann gewechselt werden, wenn sie Dritten bekannt sein könnten oder wenn Mitarbeitende nicht mehr bei der Gemeinde tätig sind.

> **Sensibilisieren Sie die Mitarbeitenden und die Miliztätigen**[3]
Beim Schutz vor Cyberangriffen ist das Gemeindekader in der Pflicht. Dazu gehört auch die Sensibilisierung von Mitarbeitenden. Gemeindeschreiber/-innen tragen innerhalb der Gemeindeverwaltung viel Verantwortung und müssen zunehmend auch Entscheide zu IKT-Fragen treffen. Es empfiehlt sich, die Gemeindeschreiber/-innen auf diesem Gebiet speziell zu schulen und allgemein in Security Awareness Trainings für Mitarbeitende und Miliztätige zu investieren. Organisieren Sie dies zusammen mit anderen Gemeinden oder den kantonalen Gemeindeorganisationen. Das kann helfen, Aufwand und Kosten zu reduzieren. In der Checkliste «Tipps für Mitarbeitende von Gemeinden, um Cyberdelikte zu verhindern» finden Sie Informationen für Mitarbeitende.

3 Politiker/-innen, Externe usw.

> **Seien Sie vorsichtig im Umgang mit E-Mails**
Häufig gelangen elektronische Schädlinge durch E-Mail-Anhänge, getarnt als angebliche Rechnungen oder Bewerbungen, auf Ihren Computer. Blockieren Sie den Empfang von gefährlichen E-Mail-Anhängen. Eine ausführliche, aktualisierte Liste solch gefährlicher Anhänge finden Sie auf der Website des GovCERT[4]. Stellen Sie sicher, dass keine Makros in Office-Dokumenten unsicherer Herkunft ausgeführt werden können. Besprechen Sie dies mit Ihrer/Ihrem IKT-Verantwortlichen. Definieren Sie Kommunikationswege, wie Mitarbeitende verdächtige Vorkommnisse (E-Mail, Computer, Telefonanrufe usw.) melden können, und aktivieren Sie, falls möglich, eine Funktion für die Meldung von dubiosen E-Mails.

Kommunizieren Sie auch achtsam mit Bürgerinnen und Bürgern. Versenden Sie E-Mails nur im Textformat und gehen Sie mit Anhängen sparsam um. Vermeiden Sie Office-Dokumente mit Makros und benutzen Sie stattdessen PDF-Dokumente. Legen Sie Links offen und verlinken Sie nicht auf Websites, die Benutzername, Passwort oder andere Daten verlangen. Betrügerische E-Mails sind mehrheitlich unpersönlich angeschrieben; schreiben Sie Bürgerinnen und Bürger möglichst mit Vor- und Nachnamen an.

Wer seine Einfallstore kennt, kann sie für Cyberkriminelle geschlossen halten.

> **Schützen Sie Ihr Onlinebankkonto**
Verwenden Sie für Zahlungen einen separaten Computer, auf welchem Sie nicht im Internet surfen oder E-Mails empfangen. Sprechen Sie mit Ihrer/Ihrem IKT-Verantwortlichen über die Möglichkeit, Ihre Onlinezahlungen in einem von den restlichen Anwendungen abgegrenzten Bereich (Sandboxing) oder in einem dedizierten, besonders geschützten virtualisierten System zu tätigen.

Klären Sie sämtliche Prozesse, welche den Zahlungsverkehr betreffen. Diese müssen von den Mitarbeitenden in allen Fällen eingehalten werden, zum Beispiel mit dem Vier-Augen-Prinzip und/oder einer Kollektivunterschrift: Hier müssen Zahlungen vor der Auslösung zusätzlich von einem oder einer anderen E-Banking-Nutzer/-in visiert werden. Dies gilt insbesondere, wenn mehrere Mitarbeitende zahlungsberechtigt sind. Sprechen Sie mit Ihrer Bank über mögliche Sicherheitsmassnahmen.

4 www.govcert.ch/downloads/blocked-filetypes.txt

3.2 Technische Schutzmassnahmen

> **Sichern Sie Ihre Daten**
Definieren Sie einen Prozess, der die regelmässige Datensicherung (Back-up) regelt, und halten Sie diesen konsequent ein. Überlegen Sie sich, wie viele Tage Datenverlust Sie verkraften können, und lagern Sie eine zusätzliche Kopie Ihres Back-ups getrennt (offline) und ausser Haus (offsite) aus. Üben Sie und Ihre Stellvertretung von Zeit zu Zeit das Einspielen von Back-ups, sodass Sie im Ernstfall mit dem Prozess vertraut sind. Bewahren Sie Vorgängerversionen des Back-ups über einen mehrmonatigen Zeitraum auf.

> **Nehmen Sie Sicherheitsupdates vor**
Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Stellen Sie sicher, dass Ihre Systeme auf dem aktuellsten Stand sind. Dies gilt auch für das Content Management System (CMS), also das Websiteverwaltungssystem Ihres Webauftritts. Die meisten CMS bieten eine einfach zu aktivierende, automatische Update-Funktion an.

> **Installieren Sie einen Virenschutz**
Installieren Sie auf jedem Computer einen Virenschutz und aktivieren Sie den Echtzeitschutz. Sorgen Sie dafür, dass dieser sich regelmässig aktualisiert und täglich einen vollständigen Systemscan durchführt.

> **Sichern Sie Ihren Fernzugriff**
Schützen Sie Fernzugriffe auf Ihr Netzwerk keinesfalls mit einer einfachen Authentisierung (Benutzername und Passwort). Nutzen Sie mindestens eine Zwei-Faktor-Authentisierung oder setzen Sie eine sichere Verbindung über ein virtuelles privates Netzwerk (VPN) ein. Dies gilt auch für den Zugriff von externen IKT-Verantwortlichen.

4 Was Sie bei einer Auslagerung der IKT-Leistungen beachten sollten

Falls Sie Ihre IKT-Infrastruktur auslagern und Ihre IKT durch eine oder mehrere externe Firmen betrieben wird, finden Sie nachfolgend einige Tipps. In der Checkliste «Wie gut ist Ihre Gemeinde vor Cyberangriffen geschützt?» finden Sie weitere Anforderungen, die im Dienstleistungskatalog und im Vertrag mit dem IKT-Dienstleistungsunternehmen abgedeckt sein sollten. Beachten Sie, dass die Verantwortung nicht ausgelagert oder delegiert werden kann. Bei einem Vorfall kann die Gemeinde am Ende der Haftungskette stehen.

Die Verantwortung liegt beim Gemeindekader.

- **Orientieren Sie sich an den Mindestanforderungen**
  Bereits bei der Abnahme integrierter IKT-Systeme sind Sicherheitsprüfungen durchzuführen. Informieren Sie sich bei der jeweiligen Stelle für IKT in Ihrem Kanton oder bei Gemeindeverbänden über relevante AGB und Vorgaben bei Inanspruchnahmen von Informatikleistungen. Diese Vorgaben sollten Bestandteil der Vertragsverhältnisse zwischen Ihnen und den externen IKT-Dienstleistungsunternehmen sein. Die gesetzlichen Geheimhaltungspflichten für Wartung und Betreuung von IKT-Systemen durch Dritte sind zu regeln und unnötiger Zugang zu besonders schützenswerten Personendaten ist nicht zu gestatten. Abklärungen und Vereinbarungen sind auch mit dem jeweiligen Unternehmen für die Datenspeicherung (Cloudunternehmen) vorzunehmen und zu treffen.

- **Wählen Sie ein qualifiziertes IKT-Dienstleistungsunternehmen**
  Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Kontrollberichte von unabhängigen Dritten können bei der Auswahl des Unternehmens behilflich sein (siehe Checkliste «Empfohlene Standards und Leitfäden im IKT-Bereich»). Sie müssen nicht zwingend zertifizierte Partner auswählen. Empfehlenswert ist es, wenn IKT-Dienstleistungsunternehmen aufzeigen können, dass sie Ihren gestellten Anforderungen entsprechen sowie die von Ihnen geforderte Verfügbarkeit und Sicherheit gewährleisten können. Lassen Sie dies durch eine unabhängige Stelle prüfen oder bestätigen.

- **Führen Sie Sicherheitsaudits durch**
  Die Umsetzung der im Vertrag festgehaltenen Leistungen muss periodisch nach anerkannten Auditstandards, beispielsweise auf Basis COBIT (Control Objectives for Information and Related Technology) der Information Systems Audit and Control Association (ISACA), kontrolliert werden. Nehmen Sie dafür die Dienste unabhängiger Prüfstellen in Anspruch. Das IKT-Dienstleistungsunternehmen kann auch ein sogenanntes ISAE 3402 Type 2 (International Standard on Assurance Engagements) machen lassen – auch bekannt als SOC-2-Bericht (Service Organization Control). Die Prüfstelle bewertet Aspekte von Sicherheit, Verfügbarkeit, Integrität und Vertraulichkeit.

- **Schliessen Sie sich mit anderen Gemeinden zusammen**
  Ist Ihre Gemeindeverwaltung finanziell nicht in der Lage, erweiterte Dienstleistungen von einem IKT-Dienstleistungsunternehmen einzukaufen, schliessen Sie sich mit anderen interessierten Gemeinden zusammen. Dies erlaubt bessere Einkaufskonditionen und reduziert den Beschaffungsaufwand. Eine andere Option ist die Auslagerung dieser Aufgabe an eine grössere Gemeinde.

> **Holen Sie sich Unterstützung**
Diverse amtliche Stellen, Verbände und Organisationen bieten relevante Informationen zur Auslagerung von IKT-Leistungen und Hilfsmittel wie Leitfäden, Merkblätter und Vertragsmuster für die Zusammenarbeit mit IKT-Dienstleistungsunternehmen an.

Beispiele von amtlichen Stellen, Verbänden und Organisationen:

Informations- und Kommunikationstechnik (IKT)

> Die kantonalen Stellen für IKT verfügen über Leitfäden und Hilfsmittel, zum Beispiel das Amt für Informatik und Organisation des Kantons Bern (KAIO), www.be.ch/kaio
> Auch Gemeindeverbände können Unterstützung bieten. Eine Liste der Gemeindeverbände finden Sie unter www.chgemeinden.ch
> Beim Bundesamt für wirtschaftliche Landesversorgung (BWL) finden Sie die Minimalstandards für IKT, www.bwl.admin.ch
> Das Nationale Zentrum für Cybersicherheit[5] (NCSC), www.ncsc.ch, verfügt über nachrichtendienstliche Informationen und Wissen von Computer Emergency Response Teams (CERT) anderer Länder sowie über präventive Massnahmen. Sollte Ihr IKT-Dienstleistungsunternehmen noch nicht Mitglied sein, dann wenden Sie sich an outreach@ncsc.ch
> Die AGB der Schweizerischen Informatikkonferenz (SIK) eignen sich für IKT-Geschäfte der öffentlichen Verwaltung. Zu den AGB der SIK gibt es auch Vertragsvorlagen, https://sik.swiss
> Das Label cyber-safe.ch wurde vom Schweizer Verband für das Cybersecurity-Gütesiegel entwickelt. Es definiert minimale Anforderungen spezifisch für Gemeinden und KMU. Mittels Onlinefragebogen können die Cyberrisiken von Gemeinden und KMU ermittelt werden, www.cyber-safe.ch

Beschaffungen

> Einen Überblick über die Seiten der Verwaltungen des Bundes, der Kantone und der grösseren Städte zum Beschaffungswesen erhalten Sie auf den Websites von eGovernment Schweiz, www.egovernment.ch, und dem Verein simap.ch, www.simap.ch

Datenschutz

> Hilfsmittel zum Datenschutz und eine Auflistung der jeweiligen Datenschutzaufsichtsstellen finden Sie auf der Website der Konferenz der schweizerischen Datenschutzbeauftragten, privatim, www.privatim.ch
> Für das Datenbearbeiten durch Private und durch Bundesorgane ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zuständig, www.edoeb.admin.ch

5 Seit dem 1. Januar 2020 werden diverse Bundesaufgaben im Cyberbereich unter dem Dach des Nationalen Zentrums für Cybersicherheit (NCSC) zusammengeführt. Dies betrifft auch die Melde- und Analysestelle Informationssicherung (MELANI).

5 Was Sie im Schadensfall tun müssen

Erste Hilfe bei einem Cyberangriff

Isolieren
> Trennen Sie alle Systeme umgehend vom Netzwerk. Vergessen Sie nicht, das WLAN auszuschalten.

Kontaktieren
> Kontaktieren Sie Ihre IKT-Verantwortliche oder Ihren IKT-Verantwortlichen sowie alle Ansprechpersonen in der Organisation, die Sie zur Bewältigung des Angriffs benötigen.
> Prüfen Sie die Kontaktaufnahme zur Polizei und die Erstattung einer Anzeige. Warten Sie mit dem Wiederaufsetzen der Systeme, bis die Polizei die Spuren gesichert hat. Spezialisierte Mitarbeitende der Polizei beraten und unterstützen Sie im Vorgehen, sichern Spuren und ermitteln. Auf www.suisse-epolice.ch finden Sie die Telefonnummer eines Polizeipostens in Ihrer Nähe.

Melden
> Melden Sie den Angriff zusätzlich beim NCSC, www.ncsc.ch. Auch Ihr Gemeindeverband sollte über den Vorfall informiert werden, da eventuell mehrere Gemeinden betroffen sind.
> Beachten Sie die Meldepflichten, zum Beispiel bezüglich des Datenschutzes.

Die Verantwortlichen für Ihre IKT oder andere spezialisierte Personen helfen Ihnen, Ihre Infrastruktur zu reparieren und gegebenenfalls wiederherzustellen.

Nach dem Angriff ist vor dem Angriff. Binden Sie die erworbenen Erkenntnisse in die Qualitätsverbesserung, die internen Prozesse, in Dokumentationen, Übungen sowie in die Unternehmensführung und -kultur ein.

6 Wie Sie zur Ermittlung der Täterschaft beitragen können

6.1 Keine falsche Scheu vor einer Meldung

Die Erfahrung zeigt, dass viele Straftaten im Cyberbereich zusammenhängen und Gemeinsamkeiten haben. Jede Anzeige und jede Meldung kann den entscheidenden Hinweis zu einer Täterschaft liefern.

Die Polizei ist nicht an Ihren Verwaltungsgeheimnissen interessiert und wirkt nicht auf Ihre Infrastruktur ein. Sie sucht bei einem Angriff nur nach Informationen und Spuren, die für die Aufklärung der Straftat relevant sind. Die Untersuchung unterliegt dem Amtsgeheimnis. Ausserdem sind Datenschutzbestimmungen auch in den Untersuchungen zu respektieren. Befürchtungen über negative Auswirkungen bei der Erstattung einer Anzeige, wie beispielsweise die Sicherstellung von Rechnern über eine längere Zeit oder die Veröffentlichung eines Falles, sind unbegründet. Die Polizei nimmt Sie sehr ernst und spricht in der Regel Strafverfolgungsmassnahmen zuerst mit Ihnen ab. Sie können jederzeit auch Ihren rechtlichen Fachbeistand einbeziehen. In den meisten Fällen kann eine Vorgehensweise gefunden werden, welche für beide Seiten funktioniert.

Schnelles Handeln kann bei einem Cybervorfall den Schaden reduzieren.

6.2 Vorfälle umgehend melden

Melden Sie strafrechtlich relevante Vorfälle, beispielsweise das unbefugte Eindringen in ein Datenverarbeitungssystem, möglichst schnell der Polizei oder der Staatsanwaltschaft. Besonders dann, wenn ein Schaden entstanden ist. Je länger Sie warten, umso grösser ist die Wahrscheinlichkeit, dass wertvolle Spuren verwischt werden. Ausserdem kann jede Einwirkung dazu führen, dass Spuren nicht mehr verwendet werden können oder gelöscht werden. Jeder Polizeiposten nimmt eine Strafanzeige entgegen. Auf dem Onlineportal Suisse ePolice (www.suisse-epolice.ch) finden Sie die Telefonnummer eines Polizeipostens in Ihrer Nähe.

Prüfen Sie zusätzlich eine freiwillige Meldung an die Strafverfolgungsbehörden oder an das NCSC bei Ereignissen, die keinen Schaden verursacht haben oder die bereits im Versuchsstadium entdeckt wurden. Hinweise an das NCSC können jedoch nicht für eine Anklage respektive in einem Gerichtsverfahren verwendet werden.

Tipps für Gemeindekader zum Schutz vor Cyberangriffen

Ein Cyberangriff kann jede Gemeinde treffen. Mit einigen Vorsichtsmassnahmen können Sie Ihre Gemeinde jedoch besser schützen.

Klären Sie die Verantwortlichkeiten und sorgen Sie vor

> Regeln Sie die Verantwortlichkeiten rund um die IKT-Sicherheit sowie die Schnittstellen zu Ihren Partnern. Eingespielte Prozesse und Eskalationspfade sind unabdingbar, um die Kontrolle zu behalten.

Schützen Sie Ihre Daten

> Regeln Sie den Umgang mit Informationen und Daten. Über unpersönliche Kanäle sollten keine vertraulichen Informationen weitergegeben werden.
> Seien Sie vorsichtig bei der Verwendung von Clouddiensten. Lesen Sie vor der Nutzung eines Cloudunternehmens die Allgemeinen Geschäftsbedingungen und achten Sie auf die Datenschutzbestimmungen. Sensible Daten sollten nie unverschlüsselt in der Cloud abgelegt werden.
> Definieren Sie einen Prozess, der die regelmässige Datensicherung (Back-up) regelt. Lagern Sie eine zusätzliche Kopie Ihres Back-ups getrennt (offline) und ausser Haus (offsite) aus.

Verwenden Sie sichere Passwörter

> Die Mindestlänge des Passwortes sollte bei zwölf Zeichen liegen und das Passwort sowohl aus Gross- und Kleinbuchstaben, Zahlen wie auch Sonderzeichen bestehen. Zusätzlichen Schutz bietet eine Zwei-Faktor-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung gleicher Passwörter. Stattdessen benutzen Sie einen Passwortmanager und generieren Sie für jede Anwendung ein eigenes Passwort.

Sensibilisieren Sie Ihre Mitarbeitenden und Miliztätigen (Politiker/-innen und/oder Externe)

> Gemeindeschreiber/-innen tragen innerhalb der Gemeindeverwaltung viel Verantwortung und müssen zunehmend auch Entscheide zu IKT-Fragen treffen. Es empfiehlt sich, die Gemeindeschreiber/-innen auf diesem Gebiet speziell zu schulen und allgemein in Security Awareness Trainings für Mitarbeitende und Miliztätige zu investieren.

Seien Sie vorsichtig im Umgang mit E-Mails

> Blockieren Sie den Empfang gefährlicher E-Mail-Anhänge und stellen Sie sicher, dass keine Makros in Office-Dokumenten unsicherer Herkunft ausgeführt werden können. Definieren Sie Kommunikationswege, über welche die Mitarbeitenden verdächtige Vorkommnisse (E-Mail, Computer, Telefonanrufe usw.) melden können. Aktivieren Sie, falls möglich, eine Funktion für die Meldung dubioser E-Mails.

Seien Sie auf dem neuesten Stand

> Implementieren Sie Antivirensoftware und stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen.

Sichern Sie Ihren Fernzugriff

> Schützen Sie Fernzugriffe auf Ihr Netzwerk mit einer Zwei-Faktor-Authentisierung. Idealerweise setzen Sie eine sichere Verbindung über ein virtuelles privates Netzwerk (VPN) ein.

Achten Sie auf sicheres Onlinebanking

> Schützen Sie Ihr Onlinebankkonto entweder mit einem separaten Computer, mit einem abgegrenzten Bereich (Sandboxing) oder mit einem dedizierten, besonders geschützten virtualisierten System. Regeln Sie die Zahlungsprozesse, zum Beispiel durch ein Vier-Augen-Prinzip und eine Kollektivunterschrift.

Tipps für Mitarbeitende von Gemeinden, um Cyberdelikte zu verhindern

Beim Schutz vor Cyberangriffen ist das Gemeindekader in der Pflicht. In seiner Verantwortung liegt auch die Sensibilisierung von Mitarbeitenden. Folgende Massnahmen sollten Mitarbeitende in ihrem Alltag umsetzen:

Vorsichtiger Umgang mit E-Mails

> Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender/-innen. Seien Sie besonders vorsichtig beim Öffnen von Office-Dokumenten; aktivieren Sie nie Makros. Scheuen Sie sich nicht vor persönlichen Rückfragen, wenn Ihnen bei einer E-Mail etwas ungewöhnlich vorkommt. Dies gilt auch für bekannte Absender/-innen! Vorsicht auch beim «Antworten»-Knopf: Überprüfen Sie, ob die E-Mail wirklich an die richtige Person geht. Idealerweise schreiben Sie die E-Mail-Adresse neu.

Verwenden Sie sichere Passwörter

> Die Mindestlänge des Passwortes sollte bei zwölf Zeichen liegen und das Passwort sowohl aus Gross- und Kleinbuchstaben, Zahlen wie auch Sonderzeichen bestehen. Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon, E-Mail oder über Webformulare mit, welche Sie per Link geöffnet haben.
> Vermeiden Sie unbedingt die Mehrfachverwendung gleicher Passwörter.

Achten Sie auf schützenswerte Daten

> Überlegen Sie genau, welche Informationen Sie in der Öffentlichkeit, zum Beispiel auf der Website und in sozialen Netzwerken, offenlegen oder im öffentlichen Verkehr besprechen.
> Vertrauliche Informationen sollten konsequent verschlüsselt oder mit Briefpost an externe Stellen gesendet werden.

Wie gut ist Ihre Gemeinde vor Cyberangriffen geschützt?

Wie gut ist Ihre Gemeindeverwaltung vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet? Diese Checkliste hilft Ihnen, sich mit den wichtigsten Fragen zu einem minimalen Cyberschutz auseinanderzusetzen. Nehmen Sie bei jedem «Weiss nicht» oder bei einem «Nein» entsprechende Abklärungen vor. Dabei gilt: Massnahmen zum Schutz vor Cyberangriffen lassen sich nicht an Mitarbeitende delegieren, sondern müssen von den Gemeindekadern angegangen und koordiniert werden.

Falls Sie Ihre IKT ausgelagert haben, prüfen Sie, ob die nachstehenden Punkte im Vertrag mit dem Dienstleistungsunternehmen abgedeckt sind.

	Ja	Nein	Weiss nicht
Aufgaben, Kompetenzen, Verantwortlichkeiten			
Ist in Ihrer Gemeindeverwaltung bestimmt, wer für Cybersecurity verantwortlich ist?	○	○	○
Hat die verantwortliche Person das notwendige Wissen und die Fähigkeiten, um mit Cybersecurity umzugehen, und bildet sie sich regelmässig weiter?	○	○	○
Hat die verantwortliche Person die notwendige hierarchische Stellung und entsprechende Kompetenzen, um Cybersecurity-Massnahmen umzusetzen?	○	○	○
Gibt es Richtlinien für den sicheren Umgang mit IKT-Geräten und mit Daten?	○	○	○
Werden diese Richtlinien und Cybersecurity-Massnahmen konsequent und systematisch umgesetzt sowie regelmässig überprüft?	○	○	○
Sensibilisierung von Mitarbeitenden und Miliztätigen			
Existieren für Ihre Mitarbeitenden Richtlinien zum sicheren Umgang mit E-Mails, digitalen Daten und Internet?	○	○	○
Kennen und verstehen die Mitarbeitenden diese Richtlinien?	○	○	○
Setzen die Mitarbeitenden die Richtlinien konsequent und korrekt um?	○	○	○
Werden die Mitarbeitenden regelmässig bezüglich Cybersecurity, zum Beispiel im korrekten Umgang mit E-Mails, geschult bzw. sensibilisiert?	○	○	○
Datenschutzrichtlinien			
Sind Daten auf Ihren Systemen (Datenablagen und -speicher, Endgeräte und Server) verschlüsselt?	○	○	○
Sind Sie sich der gesetzlichen Vorschriften bezüglich Datenspeicherung und -verarbeitung bewusst?	○	○	○
Kennen Sie Ihre Pflichten im Zusammenhang mit den gesetzlichen Vorschriften bezüglich personenbezogener Daten?	○	○	○
Werden die aktuell geltenden Vorschriften zum Datenschutz in Ihrer Gemeindeverwaltung konsequent und korrekt umgesetzt?	○	○	○
Ist in Ihrer Gemeindeverwaltung der physische Zugang zur Rechner-, Server- und Netzwerkinfrastruktur vor dem Zugriff von Dritten zweckmässig geschützt?	○	○	○
Passwortrichtlinien und Benutzeradministration			
Gibt es in Ihrer Gemeindeverwaltung Richtlinien zur Verwendung von Passwörtern?	○	○	○
Gibt es Richtlinien, die definieren, welche Mitarbeitenden auf welche Daten Zugriff haben?	○	○	○
Werden diese Richtlinien konsequent und korrekt umgesetzt?	○	○	○
Aktueller Schutz vor schädlicher Software			
Sind Ihre Geräte gegen bösartige Software geschützt (Antivirusprogramm)?	○	○	○
Konfigurierte und aktualisierte Firewall			
Sind Ihr Netzwerk und Ihre IKT-Systeme durch eine Firewall geschützt?	○	○	○
Wurden spezielle Firewall-Regeln definiert (zum Beispiel geografische Einschränkung)?	○	○	○
Wird Ihre Firewall regelmässig aktualisiert?	○	○	○

	Ja	Nein	Weiss nicht
Netzwerksegmentierung			
Sind die einzelnen Bereiche Ihrer Gemeindeverwaltung, zum Beispiel Personal und Buchhaltung, getrennt?			
Verwenden Sie einen separaten Computer oder ein separates System nur für Onlinebanking?			
Fernzugriff			
Ist in Ihrer Gemeindeverwaltung der externe Zugang zur Rechner-, Server- und Netzwerkinfrastruktur geschützt (VPN, Zwei-Faktor-Authentisierung)?			
Mit dem Internet verbundene Geräte und Systeme aktuell halten			
Nutzen Sie die Möglichkeit der automatischen Software-Aktualisierung?			
Wird bei Geräten und Systemen, deren Software nicht automatisch aktualisiert wird, diese regelmässig auf den neuesten Stand gebracht, beispielsweise durch den Hersteller?			
Werden die im Umfeld der Gemeindeverwaltung verwendeten Mobilgeräte regelmässig aktualisiert?			
Ist Ihr Content Management System für Ihren Webauftritt auf dem neuesten Stand?			
Geschütztes und verschlüsseltes WLAN			
Ist Ihr WLAN verschlüsselt und geschützt?			
Gibt es je ein separates WLAN für Mitarbeitende und Gäste?			
Back-up			
Wenden Sie einen Daten-Back-up-Prozess an?			
Überprüfen Sie regelmässig die Funktionsfähigkeit und die Lesbarkeit des Back-ups?			
Wird eine zusätzliche Kopie des Back-ups getrennt (offline) und ausser Haus (offsite) aufbewahrt?			
Mindestvorkehrung für die Notfallbewältigung			
Sind die Sofortmassnahmen im Falle eines IKT-Vorfalls definiert?			
Sind die verantwortliche Person sowie die Ansprechperson im Falle eines Vorfalls (zum Beispiel Fehlfunktion, Angriff o.Ä.) definiert und verfügbar?			
Gibt es operative Reaktions- und Wiederanlaufpläne?			
Wissen Sie, wie das Monitoring der Systeme und der Eskalationsprozess geregelt sind?			
Ist eigene Forensik möglich? Wenn nein: Wird sie extern gewährleistet?			
Ist der physische Zugriff auf Systeme gewährleistet (für die Forensik)?			
Stehen ausreichend Datenträger als Sicherungsmedien für Beweismittel zur Verfügung?			
Ist die Verpflichtung zu einer Dokumentation aller relevanten Systeme (beispielsweise in einer Configuration Management Database, CMDB) geregelt?			
Vertrag mit dem IKT-Dienstleistungsunternehmen			
Werden die oben genannten Punkte dieses Assessments durch den Vertrag mit dem Dienstleistungsunternehmen abgedeckt?			
Ist die Haftung in einem Schadensfall und sind die Ausschlüsse der Leistungsverpflichtung (beispielsweise höhere Gewalt) vertraglich geregelt?			
Sind die Servicelevel für Regel- und Notbetrieb eindeutig formuliert (dies betrifft die beauftragten Services in den erforderlichen Sicherheitszielen, beispielsweise Verfügbarkeit, Vertraulichkeit oder Integrität)? Sind Begriffe wie Notbetrieb oder kritischer Vorfall definiert?			
Ist die Exit-Strategie durchdacht und vertraglich festgehalten, insbesondere bei Cloudlösungen?			

Die Checkliste basiert auf dem Cybersecurity-Schnelltest für KMU von ICTswitzerland und von weiteren Partnern: www.cybersecurity-check.ch

Empfohlene Standards und Leitfäden im IKT-Bereich

Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Kontrollberichte von unabhängigen Dritten können bei der Auswahl des IKT-Dienstleistungsunternehmens behilflich sein. Sie müssen nicht zwingend zertifizierte Partner auswählen. Empfehlenswert ist es, wenn IKT-Dienstleistungsunternehmen aufzeigen können, dass sie Ihren Anforderungen entsprechen sowie die von Ihnen geforderte Verfügbarkeit und Sicherheit gewährleisten können. Lassen Sie dies durch eine unabhängige Stelle prüfen oder bestätigen.

Es existiert eine Vielzahl unterschiedlicher Standards und Leitfäden. IKT-Dienstleistungsunternehmen sollten mit den Standards ISO 27001, ISO 22301, ISO 9001 und ISO 14001 vertraut und konform sein. Werden andere verwendet, hat das Unternehmen ein Compliance Mapping nachzuweisen. Sollten Sie einen erhöhten Schutzbedarf haben, müssen Sie auch eigene weitergehende Anforderungen formulieren.

Beispiele von Standards und Leitfäden:

Krisenmanagement, Business Continuity, Disaster Recovery
- ISO 22301, Business Continuity Management System
- ISO 27031, IT Service Continuity Management System
- BS 11200, Krisenmanagement-System

Daten- und Informationssicherheit
- ISO 27001, Informationssicherheit
- ISO 27701, Erweiterung von ISO 27001 um Datenschutz
- ISO 30141, Referenzarchitektur für das Internet der Dinge (IoT), Vertraulichkeit der verarbeiteten Daten
- Ausrichtung gemäss Verordnung der EU 2016/679, Datenschutz-Grundverordnung (DSGVO)
- NIST Cybersecurity Framework

Technische Leitfäden
- EN 50173, Verkabelungsstruktur
- EN 50600, Rechenzentren
- ANSI/TIA-942, Rechenzentren

Andere (v.a. für Hardwarelieferanten)
- ISO 9001, Qualitätsmanagement
- ISO 14001, Umweltmanagement

Leitfäden für Auftraggebende
- ISO 22300, Terminologienorm zu Sicherheit und Resilienz
- ISO 22318, Supply Chain Continuity
- ISO 27036, Informationssicherheit im Lieferantenmanagement
- ISO 31010, Risikomanagement

Impressum

Kantonspolizei Bern, Nationales Zentrum für Cybersicherheit (NCSC) und Sicherheitsverbund Schweiz (SVS) für das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK)

Mitwirkende: Amt für Informatik und Organisation des Kantons Bern (KAIO), Verband Bernischer Gemeinden (VBG), Schweizerischer Gemeindeverband (SGV)

Kontakt: Kantonspolizei Zürich, NEDIK, cyc_nedik@kapo.zh.ch

Bilder: iStock

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali