2.2 Schutz im digitalen Raum

Die Digitalisierung hat die kommunalpolitische Arbeit grundlegend verändert – in ihren Abläufen ebenso wie in ihrem Wesen. Sie eröffnet neue Möglichkeiten für Austausch und Beteiligung, birgt aber zugleich neue Risiken: Hass, Hetze, Desinformation und digitale Angriffe gehören heute zur Realität von **Bürgermeistern, Ratsmitgliedern** und **Verwaltungsmitarbeitenden.**

Diese Entwicklungen bedrohen nicht nur die persönliche Sicherheit der politischen Akteure, sondern untergraben auch das Vertrauen in demokratische Strukturen vor Ort. Besonders auf kommunaler Ebene, wo Politik erfahrbar und greifbar sein sollte, treffen digitale Überforderung, strukturelle Schwächen und Kommunikationslücken auf immer lautere und schnellere Dynamiken im Netz.

Wer nicht vorbereitet handelt, erzeugt neue Risiken. Doch wer bewusst Strukturen schafft, Prozesse neu denkt und Kommunikation aktiv gestaltet, kann digitale Räume sichern – und Vertrauen stärken. Genau darum geht es: um einen Weg zu mehr Schutz, mehr Souveränität und mehr Gestaltungsfähigkeit im digitalen Raum.

Warum wir uns vor Cyberkriminalität schützen müssen

Ein Anruf: Ein Kollege ist irritiert – ihm wurde eine E-Mail ohne Betreff und mit Link geschickt. Der Absender ist jedoch ein bekannter Gemeinderat. Die IT wird informiert – doch es ist Freitagnachmittag, die Sitzungsvorbereitungen für Montag waren schon fast abgeschlossen.

Cyberkriminalität ist längst in Rathäusern, Sitzungssälen und bei kommunalpolitischen Akteuren angekommen. Sie trifft uns oft in Momenten der Routine, Eile und des Vertrauens.

Dabei zeigt sich: Die Täter arbeiten nicht mit Kapuzenpullis im Keller, sondern im gut ausgebauten Büro. Sie sind Teil einer milliardenschweren Industrie. Professionelle, hochspezialisierte Gruppen mit Zugang zu Tools, Automatisierungen und Manipulationsmethoden sind im Einsatz. Sie agieren systematisch, arbeiten in Schichten. Sie haben Urlaub.

Für sie sind wir keine Gegner/-innen, sondern potenzielle „Kunden" eines kriminellen Geschäftsmodells – und geraten in ein fein verzweigtes System aus Datendiebstahl, Erpressung und Manipulation. Cyberkriminalität folgt dabei einer ökonomischen Logik: Angebot, Nachfrage, Skalierung – und am Ende steht immer der Profit.

Die einen sammeln Daten, andere bieten Verkaufsplattformen, wieder andere nutzen die Informationen für Erpressung – oft mit eingekaufter Software. Die Branche reicht von illegalen bis zu legalen Bereichen. Ein programmierbarer USB-Stick etwa ist an sich legal, kann aber manipuliert Systeme infizieren, sobald er eingesteckt wird. Beim „Cybercrime as a Service" (CaaS) braucht es heute kaum noch eigene Hacking-Kompetenz. Professionelle kriminelle Dienste lassen sich vielmehr schlicht einkaufen.

Die Daten der Kommunen sind viel Geld wert

Kommunen, politische Gremien und Verwaltungen sind dabei keine zufälligen Ziele mehr, sondern lohnende Angriffsflächen, primär aus monetären Gründen. Besonders begehrt sind personenbezogene und sensible Daten – und davon gibt es auf kommunaler Ebene reichlich.

Dabei geht es Angreifenden nur selten um politische Überzeugungen, sondern schlicht um leicht zugängliche Informationen. Wer diese Daten sammelt, handelt nach professionellen Prozessen: Schwachstellen werden systematisch gescannt, E-Mail-Adressen, Logins, Kalender und Notizen gespeichert.

Mit manipulierten E-Mails und Webseiten wird versucht, sensible Daten abzufischen („Phishing"). Unterstützt durch generative KI können heute täuschend echte Fake-Seiten innerhalb von Minuten erstellt werden, zunehmend ohne erkennbare Fehler.

Dabei werden immer seltener Geräte gehackt, sondern Menschen. Der Grund: Es ist günstiger. Schon ein einziger erfolgreicher Versuch in hundert Rathäusern reicht. Algorithmen filtern, kombinieren und priorisieren die gesammelten Daten. Der eigentliche Angriff kann erst Monate oder Jahre später erfolgen – oft ausgelöst durch kleine, unbemerkte Fehler.

Unsere eigentliche Schwachstelle ist daher selten veraltete Software, sondern es sind vielmehr schlechte Prozesse, fehlende Fehlerkultur und mangelnde Meldesysteme. Viele Verwaltungskräfte zweifeln im Verdachtsfall eher an sich selbst, als mögliche Angriffe zu melden.

Wichtig

Es gibt keine Einzelschuld in der IT. Fehler sind vielmehr Ergebnis von Mängeln in der IT-Sicherheitsstruktur – etwa bei ungeschützten E-Mail-Konten von Ratsmitgliedern. Diese Zugangsdaten werden im Darknet wie Aktien gehandelt, sodass ein Zugang zu kommunalen Systemen Tausende Euro wert sein kann.

Und oft bleibt der Angriff zunächst unbemerkt: Nach einer „komischen Sache auf dem Bildschirm" passiert scheinbar nichts – ein gefährlicher Trugschluss, der uns in falscher Sicherheit wiegt. Am eigentlichen Tag des Angriffs hatten Täter den Zugang womöglich schon Monate vorher.

Warum sich die kommunale Ebene so schwer mit Digitalisierung tut

Die kommunale Infrastruktur – vom Sitzungsdienst bis zum Rechnungsprüfungsmodul – ist für Kriminelle ein Netz aus Einstiegspunkten. Am Ende dieser Kette stehen immer Menschen – und hier liegt zunehmend die Schwachstelle.

Was in der Privatwirtschaft Standard ist – Sicherheitsarchitekturen, Monitoringsysteme, Reaktionspläne –, existiert in Kommunen oft nur ansatzweise. Nicht aus Ignoranz, sondern meist aus Ressourcenmangel: Weder Geld noch Zeit stehen in vergleichbarem Maße zur Verfügung.

Das macht die kommunale Ebene zu einem bevorzugten Ziel. Hier trifft hohe Verantwortung auf schwache Schutzmechanismen. Ehrenamtliche Ratsmitglieder mit privaten Geräten oder auch unbesetzte IT-Stellen schaffen eine Angriffsfläche, die leicht zu überwinden ist.

Wenn dann Datenschutz noch als Belastung empfunden wird, Software veraltet ist und hybrides Arbeiten an Papierbergen scheitert, entsteht Frust. Digitalisierung bringt oft nicht sofort Vorteile, sondern zunächst erheblichen Mehraufwand – eine angreifbare Situation, die Cyberkriminellen neue Chancen eröffnet.

Ein Flickenteppich aus (Schein-)Lösungen

Viele digitale Anwendungen bedeuten in der Praxis zunächst Zusatzarbeit: Neue Tools erfordern Schulungen, Abstimmungen und Zeit. Die Folge ist Zurückhaltung – nicht aus Ablehnung, sondern aus Realismus gegenüber der kommunalen Gegenrealität: Ein cloudbasiertes System? Eine gute Idee – doch wer richtet Zugänge ein, sorgt für Support und Datenschutz? In der Praxis entsteht ein digitaler Flickenteppich: einzelne Tools ohne Integration, analoge Abläufe auf digitale Oberflächen verlagert.

Eine häufige Schwachstelle liegt im Versuch, analoge Abläufe einfach digital abzubilden: Eine Word-Datei ersetzt kein Antragssystem, eine Messenger-Gruppe keinen Entscheidungsprozess und eine Beschlussvorlage als PDF auf einem Tablet ist auch noch keine Digitalisierung – sondern eine Papierform mit Internetanschluss.

Zudem erfordern viele Systeme klare Hierarchien und Administration, was offenen kommunalen Strukturen widerspricht. Gerade der politische Bereich lebt vom Austausch, von der Fluktuation, vom Ehrenamt. Selbst wenn daher sichere Systeme angeboten werden, umgehen sie viele in der Praxis – etwa durch private Messenger-Gruppen.

Es fehlt an maßgeschneiderten Lösungen für Kommunen. Viele eingesetzte Tools sind für den unternehmerischen Kontext oder für die private Nutzung und passen daher nur bedingt. Während in Unternehmen etwa KI längst Meetings zusammenfasst, wird im Gemeinderat das Protokoll noch heruntergeladen, wodurch sich wieder Schadsoftware einschleichen kann.

Am Ende wird der kleinste gemeinsame Nenner zum Maßstab: Was alle gerade noch bedienen können, wird genutzt. Digitalisierung verbleibt vielerorts ein notwendiges Übel, das Aufwand bedeutet – eine Zumutung im Gewand der Zukunft.

Vom Bildschirm zur Souveränität: wie wir endlich sicher digital arbeiten können

Was fehlt, ist kein weiteres Update, sondern ein neues Denken.

Nicht die digitale Kopie des Alten, sondern ein Arbeiten, das von Beginn an digital gedacht ist. Digitale Souveränität entsteht nicht durch digitale Ersatzhand-

lungen, sondern durch durchdachte Prozesse – orientiert an den Möglichkeiten der Technik, nicht an Papierformaten. Statt „Wie machen wir das sonst?" sollte die Frage lauten: „Wie könnten wir es besser machen und durch welche digitalen Möglichkeiten?"

Das Ziel ist nicht „papierlos", sondern: reibungsfrei, sicher, nachvollziehbar. Souveränität im Digitalen zeigt sich darin, dass Systeme verständlich, praktisch und sicher zugleich sind. Wer gern und routiniert mit digitalen Tools arbeitet, erkennt Angriffe schneller – weil sie sich nicht im Chaos anderer Baustellen verlieren.

Und wer Prozesse von Grund auf digital denkt, kann sie zugleich absichern. Schauen wir, wie das konkret bei Ratsmitgliedern, Bürgermeistern und Verwaltungsmitarbeitenden aussehen kann.

Fall A) Ratsmitglied – ehrenamtlich, berufstätig, eingebunden: der politische Alltag mit digitaler Struktur

Mariam ist seit vier Jahren im Gemeinderat. Ihre Leidenschaft für Politik ist groß, doch zwischen Beruf, Familie und Ehrenamt bleibt meist nur der späte Abend. Bislang hieß das: Unterlagen in drei Formaten, Chatverläufe, verpasste Anrufe – oft chaotisch, selten effizient.

Mit dem neuen digitalen Ratsportal ändert sich das grundlegend. Es ersetzt nicht nur Papier durch PDF, sondern organisiert politische Arbeit neu: Vorlagen sind mit Projekten verknüpft, Änderungsanträge kommentiert, Aufgabenlisten werden automatisch aktualisiert. Telefonnotizen, Chatverläufe oder spontane Ideen aus Gesprächen mit Fraktionen landen nicht mehr auf Klebezetteln oder in Messenger-Apps, sondern automatisch im System – zugeordnet dem passenden Vorgang im CRM.

Mails weiterleiten, Versionen abgleichen, Dokumente speichern – all das entfällt. Die Plattform ist kein „Add-on", sondern das Rückgrat ihrer politischen Arbeit. Und: Zum ersten Mal fühlt es sich praktikabel, klar und entlastend an.

Warum ist das sicherer?

Das System schützt vor den kleinen Fehlern, die früher große Folgen hatten: etwa beim Öffnen verdächtiger Mails oder versehentlichem Weiterleiten sensibler Inhalte. Die Kommunikation läuft über eine verschlüsselte Plattform mit Multi-Faktor-Authentifizierung. Mariam muss nicht improvisieren – und verringert dadurch automatisch das Risiko, eine Sicherheitslücke zu öffnen.