Bild: stock.adobe.com_piyapong01_125340628

In der Not noch immer ein wichtiger Helfer in Organisationen: das Faxgerät

Zurück in die digitale Zukunft, dank Fax

Schnellere Katasterabfragen, offizielle Dokumente per Knopfdruck herunterladen und nie wieder Warteschlangen in Behörden. Diese Träume der Digitalisierung und damit vieler Stadtoberen, von E-Government-Verantwortlichen und letztendlich der Bundespolitik kennen scheinbar keine Grenzen. Spätestens seit der Corona-Pandemie werden die Wünsche und Forderungen nach mehr digitalisierten Verwaltungsprozessen lauter artikuliert. Der Wunsch: Die digitale Daseinsvorsorge vorantreiben – auch mithilfe des Datenmanagements sowie Geoinformationssystemen (GIS). Doch Vorsicht, die Hürden sind hoch und fangen beim föderalen System hierzulande an und hören bei überforderten Stadtverantwortlichen, mangelnden Prozessen und fehlendem Fachpersonal noch nicht auf. Ein gravierender Punkt ist die Anfälligkeit von Behörden und deren IT-Systeme vor Cyber-Angriffen.

Autor: **Andreas Eicher**

„BKA warnt vor Cyber-Angriffen auf öffentliche Verwaltungen“, „Hackerangriff legt Stadtverwaltung lahm“, „Mehr als 100 Behörden erpresst.“ Drei Überschriften, drei Bedrohungsmeldungen, ein Thema: das Hacking der Verwaltung. Ganz gleich, ob Hochschulen, Krankenhäuser oder Rathäuser. Öffentliche Einrichtungen und Verwaltungen befinden sich seit Jahren im Fadenkreuz gezielter Hackerangriffe. Die Tagesschau berichtet im Sommer 2021 von einer Umfrage des „Bayerischen Rundfunks“ und „Zeit Online“, wonach es Tätern in mehr als 100 Fällen gelungen sei, IT-Systeme

von Behörden und öffentlichen Einrichtungen zu verschlüsseln. Und als ob diese Nachricht samt der Zahl nicht schon besorgniserregend genug ist, kommt der Sender zu dem Schluss: „Die Bundesregierung hat über die Fälle keinen Überblick“ [1]. In diesem Kontext äußerste sich Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), im November 2021 in einem Interview mit der Wirtschaftswoche. Demnach habe seine Behörde keine umfassenden Zahlen zu Hackerangriffen auf Landes- und Kommunalebene [2].

Von der Chefsache, den Chefs und dem Föderalismus

Das klingt bedenklich vor dem Hintergrund, dass es bereits seit dem 1. April 2011 das Nationale Cyber-Abwehrzentrum gibt. Auf den betreffenden Seiten des Beauftragten der Bundesregierung für Informationstechnik heißt es hierzu: „Die zunehmende Bedrohung dieser Infrastrukturen durch Cyber-Kriminelle hat dazu geführt, dass die Bundesregierung das Thema IT-Sicherheit zu Chefsache erklärt hat.“ Verantwortlich für die IT-Sicherheit zeichnet das Bundesministerium des Innern und für Heimat. Also kein Aprilscherz, doch damit nicht genug.

Das Cyber-Abwehrzentrum steht „unter der Federführung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und mit direkter Beteiligung des Bundesamts für Verfassungsschutz (BfV) sowie des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK)“ [3]. An den Zuständigkeiten lässt sich einiges ablesen, nämlich, dass zu viele Chefs die Chefsache verwässern. Und die eingangs beschriebenen Meldepflichten gelten zwar für Bundesbehörden, aber nach A. Schönbohms Worten bestehe keine direkte Meldepflicht an das BSI bei IT-Sicherheitsvorfällen in Kommunen. „Die Meldewege in den Bundesländern sind zudem unterschiedlich organisiert“, so der BSI-Präsident. Damit wird das IT-Sicherheitsgesetz ein Stück weit ad absurdum geführt. Es könnte auch heißen: Der Föderalismus lässt grüßen.

Digitale Souveränität und qualifiziertes Personal

In dieser Gemengelage eines Kompetenz- und Länderhoheitsgerangel stehen die Verantwortlichen in den jeweiligen Einrichtungen und Rathäusern zwischen allen Stühlen. Denn auf der einen Seite soll die Digitalisierung Vorfahrt beim weiteren Ausbau der Behördeninfrastruktur haben, um die viel beschworenen Prozesse schneller und schlanker zu gestalten. In diesem Zuge wird Druck aufgebaut – von der Bundespolitik und der Wirtschaft samt Verbände. Wichtig wäre indes, zunächst einmal die digitale Souveränität der Städte und Kommunen zu fördern. Der Deutsche Städtetag bezeichnet die digitale Souveränität als „die Übersetzung des Prinzips der kommunalen Selbstverwaltung in das digitale Zeitalter“. Und weiter heißt es: „Sie zu stärken ist Handlungsauftrag für Bund und Länder, aber auch für die

Kommunen selbst.“ Hinzu kommen nach Ansicht des Städtetags offene Standards und Schnittstellen, gebündelte Expertise und Lösungen, aber auch ein verlässlicher Rechtsrahmen.

Auf der anderen Seite fehlt das Fachpersonal, um Städte und deren Verwaltungen im digitalen Zeitgeist zu trimmen. Das Arbeiten in Behörden war lange nicht en vouge und gewinnt erst seit einigen Jahren wieder an Beliebtheit. „Der Tagesspiegel“ nannte es im letzten Jahr „Staat statt Startup“ und spricht vom „Traumberuf Beamter“. Ob das die Personallücken – auch mit Blick auf IT- und Cyber-Fachkräfte – in den Verwaltungen zwischen Flensburg und Sonthofen qualitativ auffüllen hilft, das bleibt dahingestellt. Mit Blick auf diesen Punkt schreibt der Deutsche Städtetag: „Digitalisierung kostet Geld und braucht qualifiziertes Personal. Kommunen müssen abseits von Förderprogrammen in die Lage versetzt werden, genug Geld für Digitalisierung zu haben“ [4].

Bild: stock.adobe.com_Eigens_246154854

Die Modernisierung der Verwaltung steht vor großen Herausforderungen – auch mit Blick auf Cyber-Attacken

Im Worst Case sämtliche Fachanwendungen betroffen

Leider hilft Geld alleine nicht, um die digitalen Missstände in vielen Behörden zu mindern. Und so kommt es, wie es kommen muss. Regelmäßig kapern Cyber-Kriminelle sensible IT-Infrastrukturen von Verwaltungen und öffentlichen Einrichtungen. Infolgedessen kommt das Datenmanagement samt GIS-Lösungen und damit die digitale Daseinsvorsorge zum Erliegen. Welche Folgen ein solcher Angriff haben kann, das zeigte sich beispielsweise in Schwerin. Dort führte ein Hackerangriff 2021 zum digitalen Stillstand der Verwaltung. „Deutschlandfunk Kultur“ schreibt hierzu, dass durch den Angriff wochen-, ja monatelang kein Zugriff auf die dienstlichen E-Mails und elektronischen Akten möglich sei. „Sozialamt, Baubehörde, Gesundheitsamt, Jugendhilfe, die Kfz-Zulassungsstelle – alles lahmgelegt“, so der Sender [5]. Nach Angaben des IT-Portals „it-daily“ wurden bei dem Cyber-Angriff im Oktober 2021 Server durch eine Schadsoftware teilweise verschlüsselt [6]. Von solchen Attacken sind im Worst Case auch sämtliche Fachanwendungen in den Behörden betroffen.

Umso mehr gilt es, diese digitale Daseinsvorsorge im Sinne der Städte und Kommunen und letztendlich der Bürger zu schützen. Denn nach Ansicht des Deutschen Städtetags haben digitale Technologien ein großes Potenzial, „kommunale Dienstleistungen radikal zu reformieren und dabei bürgerfreundlicher und effizienter zu gestalten“. Mehr noch werden „im Hintergrund (…) städtische Infrastrukturen digitalisiert und Städte wandeln sich zu Smart Cities. Zusammen ist das ‚digitale Daseinsvorsorge‘ “ [7].

Im Umkehrschluss braucht es eine mehr und qualitativ bessere IT-Sicherheitsberatung in den Verwaltungen. Diese sollte nach Möglichkeit von neutraler Stelle erfolgen. Dabei können die Angebote vonseiten der eingangs genannten zentralen Stellen nur lindern, aber nicht verhindern. Zu groß sind die Einfallstore für Kriminelle im digitalen Raum. Weitergedacht heißt das: IT-Sicherheit benötigt einen durchgängigen Ansatz – von der Beratung im Verbund mit den Lösungsanbietern bis zu klaren Verhaltensmaßnahmen aller Mitarbeiter in den Behörden. Denn der viel genannte „Faktor Mensch“ ist auf die Unterstützung in Form von Awareness-Schulungen und Aufklärungskampagnen angewiesen. Solange dies nicht beherzigt wird, haben vorgestrige Geräte noch immer ihre Daseinsberechtigung. Denn die Ironie des Schicksals ist in vielen Fällen, dass längst vergessen geglaubte Technik, wie das Faxgerät, manche Verwaltung bei einem Cyber-Angriff vor dem völligen Kollaps bewahrt. So titelte die „Frankfurter Allgemeine Zeitung“ nach dem Hackerangriff auf die Landkreisverwaltung in Anhalt-Bitterfeld im letzten Jahr: „Das Fax hat uns erst mal gerettet“ [8]. Hoffen wir, dass es half und die Behörde zurück in die digitale Zukunft fand, dank Fax.

Quellen:

[1] www.tagesschau.de/investigativ/br-recherche/ransomware-103.html
[2] www.wiwo.de/technologie/digitalisierung-der-wirtschaft/verletzliche-verwaltungen-diese-bedrohung-muss-jede-kommune-ernst-nehmen/27774646.html
[3] www.cio.bund.de/Web/DE/Strategische-Themen/IT-%20und%20Cybersicherheit/Cyber-Sicherheitsstrategie-fuer-Deutschland/cyber_sicherheitsstrategie_node.html
[4] www.staedtetag.de/positionen/beschluesse/hauptausschuss-diskussionspapier-digitale-souveraenitaet-von-kommunen-staerken-november-2020
[5] www.deutschlandfunkkultur.de/cyberkriminalitaet-angriffe-auf-behoerden-und-unternehmen-100.html
[6] www.it-daily.net/shortnews/30917-cyberattacke-auf-it-dienstleister-der-landeshauptstadt-schwerin?highlight=-Schwerin
[7] www.staedtetag.de/positionen/beschluesse/hauptausschuss-diskussionspapier-digitale-souveraenitaet-von-kommunen-staerken-november-2020
[8] www.faz.net/aktuell/politik/inland/hackerangriff-auf-landkreis-das-fax-hat-uns-erstmal-gerettet-17455380.html