VITAKO

aktuell

04|2019

Regionalausgabe

regio iT

PLATZ 1 FÜR REGIO IT

Award für Kommunale Lösungen

VERNETZTE MOBILITÄT

Neue regio iT-Tochter „Better Mobility“

VERNETZUNG UND INFORMATION

Gemeinsame Hausmesse „interface“

INNOVATIONSWETTBEWERB

QKI-Plattform „PlanQK“

BLOCKCHAIN-REALLABOR

Förderbescheid für Projektkonsortium

DOKUMENTEN-MANAGEMENT

Schwungvolle Zusammenarbeit

CYBERSICHERHEIT

Kommunen in der Pflicht

NICHT KRITIS, ABER KRITISCH

IT-Sicherheit zwischen Empfehlung und Zertifikat

„IT MUSS MASSSTÄBE SETZEN“

Bundesdatenschutzbeauftragter Ulrich Kelber im Gespräch

GENOSSENSCHAFT GOVDIGITAL EG

Digitale Infrastrukturen in öffentlicher Hand

Let's do IT.

Nicole J. (31),
seit zwei Jahren
bei Dataport.

Auf einer Wellenlänge mit 112.

Der Sinn-Faktor kommt in IT-Berufen oft zu kurz. Bei uns ist er sozusagen im Quellcode festgeschrieben. Wir arbeiten stets mit der Gewissheit, der Gesellschaft etwas zu geben. Zum Beispiel modernen BOS-Funk für eine reaktionsbereite Feuerwehr.

www.dataport.de

dataport

GUT FÜR ALLE. GUT FÜR DICH.

▲ Peter Kühne ist Vorsitzender des Vitako-Vorstands.

Liebe Leserinnen und Leser,

Cybersicherheit ist zum Maß aller Dinge geworden. Mit zunehmender Digitalisierung und den Vorteilen, die sie für Bürgerinnen und Bürger auch im Umgang mit der Verwaltung hat, wachsen die Herausforderungen in puncto IT-Sicherheit. Mehr Vernetzung und digitale Services bedeuten auch mehr Angriffsflächen für Hacker. Der „Lagebericht zur IT-Sicherheit in Deutschland“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zeigt alljährlich, dass die Zahl der Angriffe auf öffentliche Netze stetig wächst und dass die Angreifer immer raffinierter werden. Hier hilft nur systematischer Schutz.

Die kommunale Ebene gehört vielleicht nicht zu den Hauptangriffszielen von Hackern, doch auch hier kommt es gelegentlich zu erfolgreichen Attacken. Krankenhäuser und Stadtverwaltungen waren schon betroffen, die Systeme mehrere Tage lahmgelegt. Die kommunalen IT-Dienstleister tun ihr Möglichstes, um effektive Schadenabwehr zu betreiben. Doch IT-Sicherheit kostet, und längst nicht jede Kommune und Verwaltung ist in der Lage, eine aufwändige Sicherheits-Zertifizierung zu betreiben.

Bei Vitako gibt es seit Verbandsgründung eine Facharbeitsgruppe für IT-Sicherheit, in der sich IT-Sicherheitsbeauftragte regelmäßig über die Lage austauschen. Zurzeit engagieren sich unsere Experten gemeinsam mit den Kommunalen Spitzenverbänden für ein auf Kommunen zugeschnittenes Schutzprofil. Die sogenannte „Basis-Absicherung Kommunalverwaltung“ basiert auf dem IT-Grundschutz des BSI und definiert Mindestsicherheitsmaßnahmen, um die IT-Systeme in der Kommunalverwaltung ausreichend zu schützen.

In der deutschen Cybersicherheitsarchitektur wird der kommunale Bereich oft als das letzte Glied betrachtet. Erst wenn in Bürgerämtern das Licht ausgeht, rückt dies ins öffentliche Bewusstsein. Es bedarf einer konkreten Strategie, wie Kommunen besser eingebunden werden können.

Eine angeregte Lektüre wünscht,

Herausgeber:
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e. V.
Charlottenstr. 65
10117 Berlin
Tel. 030/20 63 15 60
E-Mail: aktuell@vitako.de
www.vitako.de

V. i. S. d. P.:
Dr. Ralf Resch

Redaktion und Gestaltung: drei | Medien
Merschmann Mühlke Jaschinski GbR
www.drei-medien.de

Die Redaktion behält sich vor, eingesandte Berichte auch ohne vorherige Absprache zu kürzen. Der Inhalt der Beiträge gibt nicht in jedem Fall die Meinung des Herausgebers wieder.

Korrektorat: Henrike Doerr, Textwelten

Druck: Laserline, Berlin

Erscheinungsweise: 4 Ausgaben im Jahr
Auflage: 5.000; Papier: 115g/m² Profibulk

Autoren und Mitwirkende dieser Ausgabe:
Peter Kühne, Vitako; Dr. Ralf Resch, Vitako; Horst Samsel, Bundesamt für Sicherheit in der Informationstechnik; Miklos Csizmadia, AKDB; Markus Albert, Stadt Frankfurt; Daniel Grimm, Vitako; Dr. Sven Herpig, Stiftung Neue Verantwortung; Kai Wagner, Jolocom; Stefan Cink, TeleTrusT; Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit; Frederik Blachetta, PwC Strategy&; Alexander Handschuh, Deutscher Städte- und Gemeindebund; Gürkan Ünlü TÜV Rheinland Consulting; Dr. Catharina Schmalstieg, Vereinte Dienstleistungsgewerkschaft ver.di; Helmut Merschmann, drei | Medien; Sibylle Mühlke, drei | Medien; Monika Majer, Fraunhofer FOKUS; Hiestermann & Frömchen GmbH;

Bildnachweise:
Titel: Mike Orlov - stock.adobe.com;
S. 4 master1305 - stock.adobe.com;
S. 5 Robert Kneschke – stock.adobe.com;
S. 7 kallejipp / Photocase; S. 7, 25 Porträt Resch: Robert Schlesinger; S. 9 patklik / Photocase;
S. 11 spacejunkie / Photocase; S. 13 nattanan - stock.adobe.com, Porträt Grimm: Anke Illing;
S. 16 vectorfusionart - stock.adobe.com;
S. 19 Javier Sánchez Mingorance - stock.adobe.com; S. 20 – 22 Tobias Koch; S. 27 kallejipp / Photocase; S. 29 alphaspirit - stock.adobe.com;
S. 31 Ben Franske, CC BY 2.5: https://de.wikipedia.org/wiki/System/360#/media/Datei:DM_IBM_S360.jpg.

Hinweis: Vitako aktuell erscheint zusätzlich mit drei Regionalausgaben: krz, Lecos, regio iT. Der Vertrieb erfolgt durch das jeweilige Vitako-Mitglied.

ISSN 2194-1165

Die gesuchte Computerpionierin ist Grace Hopper (1906 – 1992). Nach ihrem Studium war sie zunächst Mathematikdozentin, im Zweiten Weltkrieg meldete sie sich zur Navy. Den ersten Compiler der Technikgeschichte entwickelte sie 1952. Die bis heute eingesetzte Programmiersprache ist COBOL. Ursache des Milleniums-Bug war die damalige Speicherknappheit: Für Jahreszahlen waren nur zwei Stellen vorgesehen, weil niemand damit rechnete, dass die Programme über das Ende des 20. Jahrhunderts hinaus benutzt würden.

Schwerpunkt: Cybersicherheit

Digitale Verwaltung

Netztalk

Nicht KRITIS, aber kritisch

IT-Sicherheit in Kommunen zwischen Empfehlungen und Zertifizierung

Sprockhövel, Neustadt am Rübenberge, zuletzt das Berliner Kammergericht – die „Hacker“-Beispiele zeigen, dass Prozesse, Systeme und Leistungen ohne ein sicheres IT-Management im Zweifel zu einem Totalausfall von Behörden führen können.

Die öffentliche Hand mag hierzulande nicht das vorderste Ziel von Hackern sein. Trotzdem kommt es immer wieder zu minder schweren bis großen Zwischenfällen, die an die Öffentlichkeit gelangen und nicht nur für schlechte Presse und Bürgerschlangen vor dem Rathaus sorgen, sondern auch zum Fiasko bei essenziellen Leistungen der Daseinsvorsorge führen können. Gerade für kleine Kommunen mit wenig Kapazitäten vor Ort wird es immer schwieriger, notwendige IT-Sicherheitsmaßnahmen allein umzusetzen.

Der zunehmende Grad an Komplexität und Vernetzung erfordert entsprechend mehr Anstrengungen und Kompetenz, um die Funktionsfähigkeit der Verwaltung auch bei Störungen von außerhalb zu gewährleisten. Es geht darum, sensible Bürger- und Unternehmensdaten nicht nur vorzuhalten und intern zu verwalten, sondern so effektiv und effizient wie möglich zu schützen.

Für die künftige Informationssicherheit spielt dabei die Ausgestaltung der weiteren digitalen Öffnung der Behörden hin zu Bürgern und Unternehmen eine maßgebliche Rolle. Ob bei Online-Services, städtischen Apps oder beim Aufbau agiler Verwaltungsarbeitsplätze – schon jetzt stellen die kommunalen IT-Dienstleister dafür sichere Infrastrukturen, Systeme und Verfahren zur Verfügung. Nicht nur Gebäude, Hardware und Netze müssen sicher sein. Gerade für die Gesamtbetrachtung sind die Prozesse und die damit einhergehenden Rollen und Qualifikationen sicherheitsentscheidend.

Studie unterstreicht Bedeutung von Zertifikaten

Immer mehr IT-Dienstleister lassen ihre Kompetenz deshalb zertifizieren. Eine Vitako-Umfrage von Oktober 2019 (siehe Seite 33) ergab, dass in der kommunalen IT erhebliche Anstrengungen unternommen werden, um Cybersicherheit zu gewährleisten. Im Vordergrund stehen dabei aktuelle Virenschutzsoftware, Patch-Management und Sicherheitsgateways, um Malware und Viren sowie Phishing-Angriffe als die beiden größten wahrgenommenen Bedrohungen abzuwehren. Die Untersuchung ergab auch: Für 80 Prozent der Teilnehmenden ist eine Sicherheitszertifizierung des Rechenzentrums sehr wichtig oder wichtig. Bei den Zertifikaten ist ISO 27001 deutlich am stärksten verbreitet, gefolgt vom Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Ergebnis der Untersuchung ist aber auch, dass mehr als 40 Prozent der teilnehmenden Verwaltungen beziehungsweise Unternehmen bisher noch nicht zertifiziert sind. Das zeigt: Das Problembewusstsein ist da, aber die konkrete Umsetzung in Form von Zertifikaten benötigt noch Zeit und Geld, was gerade in kleineren Organisationen nicht immer zur Verfügung steht.

Absehbar keine festen Anforderungen

Ende März dieses Jahres gelangte die Referentenvorlage des IT-Sicherheitsgesetzes 2.0 an die Öffentlichkeit. Derzeit ist davon auszugehen, dass ausschließlich der Bereich der Abfallentsorgung zur Gruppe der Kritischen Infrastrukturen (KRITIS) hinzukommt. Für den neu eingeführten Begriff der „Infrastrukturen von besonderem öffentlichen Interesse“ kann – zumindest bislang – ausgeschlossen werden, dass Kommunen oder ihre IT-Dienstleister darunter fallen. Wie eingangs beschrieben, betreiben aber gerade Kommunen wichtige Register und verwalten sensible Bürgerdaten

etwa aus dem Melde- und Sozialwesen. Dennoch unterliegen diese Informationen dem Entwurf zufolge auch künftig keinen festen Anforderungen an die Sicherheit ihrer IT-Systeme.

ISMS aufbauen, BSI-Grundschutz vorbereiten

Auch der IT-Grundschutz hat für Kommunen bislang nur empfehlenden Charakter. Vitako plädiert deswegen für den verstärkten Aufbau von Informationssicherheits-Management-Systemen (ISMS) auf kommunaler Ebene – der erste Schritt in Richtung BSI-Zertifizierung.

Hierfür wurde 2017 gemeinsam mit den Kommunalen Spitzenverbänden die „Handreichung für die Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ veröffentlicht (zum PDF: bit.ly/2CAeO29). Die Publikation soll erste praktikable Hinweise für die Etablierung von ISMS und deren kontinuierlicher Pflege geben. Der IT-Planungsrat empfiehlt schon seit 2015 „ISIS12“ (Informations-Sicherheits-management-System in zwölf Schritten) speziell für den Einsatz in kleinen und mittleren Kommunen. Die Kompatibilität dieser Einstiegsvariante zu IT-Grundschutz und ISO 27001 soll einen späteren Umstieg auf ein umfangreicheres ISMS mit höherem Schutzniveau erleichtern.

Basis-Absicherung Kommunalverwaltung

Gemeinsam mit Vertretern der kommunalen Spitzenverbände und weiteren öffentlichen Akteuren engagieren sich die kommunalen IT-Dienstleister in der Arbeitsgruppe „Modernisierung IT-Grundschutz“. Daraus ist Mitte Oktober das novellierte IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ hervorgegangen. Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und definiert die Mindestsicherheitsmaßnahmen, die umzusetzen sind, um sich in der Kommunalverwaltung ausreichend zu schützen.

IT-Sicherheit ist ein anhaltender Prozess, das machen gerade diese vielen Komponenten und Stufen beim Aufstieg zum IT-Grundschutz deutlich. Selbst wer keine direkte Aussicht auf ISO 27001 und IT-Grundschutz besitzt, kann sich mit kleinen Schritten den höheren Schutzniveaus freiwillig nähern.

Awareness-Prozess forcieren

Aktuell scheinen weder Länder noch Bund daran interessiert, den Kommunen weitere verpflichtende Vorschriften zu machen – das Konnexitätsprinzip würde die „Verursacher“ dazu verpflichten, zusätzliche Kosten selbst zu tragen. Dadurch wird das Niveau der IT-Sicherheit in den einzelnen Kommunen absehbar sehr unterschiedlich bleiben. Deshalb ist es wichtig, gerade kleine Gebietskörperschaften mit Argumenten, Erklärungen und Beispielen zu unterstützen, sich zwar nicht wie KRITIS verhalten zu müssen, sich dennoch als kritisch zu betrachten. Um das zu erreichen, gilt es, den Awareness-Prozess voranzutreiben, zu sensibilisieren und niederschwellige Angebote zu unterbreiten. So engagieren sich die kommunalen Dienstleister dabei, Verwaltungsmitarbeitende vor Ort anzusprechen, Qualitätsmaßstäbe zu formulieren und Standards zu empfehlen. Informationssicherheit als Bestandteil der Daseinsvorsorge bleibt für Vitako ein Top-Thema.

◀ Dr. Ralf Resch ist Vitako-Geschäftsführer.

Kooperativer Ansatz

Bundesamt für Sicherheit in der Informationstechnik baut Zusammenarbeit mit Ländern und Kommunen aus

Die Gestaltung von Cybersicherheit kann nur durch die gemeinsamen Anstrengungen und Aktivitäten aller Akteure in Staat, Wirtschaft und Gesellschaft zum Erfolg geführt werden. Das zeigt der im Oktober vorgelegte Bericht zur „Lage der IT-Sicherheit in Deutschland 2019“ sehr deutlich.

In Zeiten der Digitalisierung kommt kaum ein Bereich ohne zuverlässige und sichere Kommunikationssysteme aus. Auf der anderen Seite wächst die Anzahl der Cyberangriffe kontinuierlich. Zunehmend, und befördert durch konkrete Beispiele, wächst das Bewusstsein dafür, dass derartige Angriffe existenzbedrohend sein oder ganze Infrastrukturen lahmlegen können.

▲ Horst Samsel ist Abteilungsleiter Beratung für Bund, Länder und Kommunen und für Cyber-Sicherheit für Wirtschaft und Gesellschaft im BSI.

Der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist ein jährlicher Gradmesser sowohl für die Risiken als auch für die Chancen der Digitalisierung. Er nennt aktuelle Daten, Fakten und Statistiken, er informiert über die gestiegene Qualität der Cyberbedrohungen, aber er beweist auch, dass die gemeinsame Abwehr nennenswerte Erfolge zeitigt. Im Berichtszeitraum vom 1. Juni 2018 bis zum 31. Mai 2019 hat das BSI rund 114 Millionen neue Schadprogrammvarianten registriert, DDoS-Angriffe mit bis zu 300 Gbit/s Angriffsbandbreite beobachtet und bis zu 110.000 Bot-Infektionen täglich in deutschen Systemen registriert.

Die Zahl der Schadprogrammvarianten ist auf über 900 Millionen angestiegen. Allein durch die Emotet-Kampagne im September 2018 ist die Anzahl der täglichen neuen Varianten von rund 300.000 auf 450.000 angestiegen.

Diese Angriffe haben zu zahlreichen Produktionsausfällen in der Wirtschaft und zu teils erheblichen Beeinträchtigungen in Einrichtungen des Gemeinwesens geführt. So waren mehrere Krankenhäuser, etwa in Rheinland-Pfalz und im Saarland, sowie kommunale Einrichtungen wie Stadtverwaltungen von solchen Angriffen betroffen. Ein Beispiel: Neustadt am Rübenberge, Stadt und selbständige Gemeinde in der Region Hannover, wurde Opfer eines Emotet-Angriffs. Das IT-System der Verwaltung war über eine Woche lang lahmgelegt. Die Kfz-Zulassungsstelle musste geschlossen werden, das Bürgerbüro konnte mündliche Auskünfte erteilen, aber keinerlei Anträge entgegennehmen.

Von Schäden durch die zahlreichen Angriffswellen durch die Schadsoftware Emotet nicht betroffen war die Informationstechnik der Bundesverwaltung, für deren Sicherheit das BSI zuständig ist. In den Regierungsnetzen werden 61 Prozent der Cyberangriffe nur durch eigenentwickelte Lösungen und Signaturen abgewehrt. Auch Betreiber Kritischer Infrastrukturen, die die Sicherheitsanforderungen und Empfehlungen des BSI umgesetzt haben, blieben von den gravierenden Schadensauswirkungen erfolgreicher Cyberangriffe weitgehend verschont.

Der Bericht zur Lage der IT-Sicherheit in Deutschland 2019 steht auf der BSI-Webseite unter www.bsi.bund.de/lageberichte zum Download zur Verfügung und kann auch als Print-Exemplar bestellt werden. Die Informationssicherheitsberatung für Länder und Kommunen ist per E-Mail über Sicherheitsberatung-Regional@bsi.bund.de erreichbar.

Information und Kooperation

An diesen konkreten Beispielen zeigt sich, wie wertvoll die integrierte Wertschöpfungskette der Cybersicherheit des BSI tatsächlich ist. Sie spiegelt sich in den operativen Schutzmaßnahmen für die Regierungsnetze ebenso wider wie in den Zertifizierungs- und Standardisierungsanforderungen des BSI an IT-Produkte und -Services. Aber auch in die Kooperations-, Unterstützungs- und Informationsleistungen für Länder und Kommunen fließt das Know-how des BSI ein.

Übergeordnetes Ziel sollte sein, ein einheitliches Mindestniveau der Informationssicherheit in der Bundesrepublik Deutschland zu schaffen und so die Resilienz zu erhöhen. Dieses Ziel wird angesichts der fortschreitenden Digitalisierung der Verwaltung und einer damit einhergehenden zunehmenden Vernetzung von IT-Strukturen immer wichtiger. Das BSI als Kompetenzzentrum und Cybersicherheitsbehörde des Bundes hat dafür bereits verschiedene Maßnahmen erfolgreich umgesetzt:

- In allen KRITIS-Bereichen (ober- und unterhalb der Schwellwerte) wird mit dem UP KRITIS eine öffentlich-private Kooperation zwischen Betreibern, deren Verbänden und den zuständigen staatlichen Stellen ermöglicht. Ziel ist es, die Versorgung mit kritischen Dienstleistungen auch im Angriffsfall aufrechtzuerhalten. Der UP KRITIS fördert den fachlichen Austausch und bietet den Teilnehmern durch das BSI aufbereitete Informationen zu spezifischen Bedrohungen und zur allgemeinen Cybersicherheitslage. Gerade Kommunen und kommunale Betreiber, die nah an den Schwellwerten liegen, sollten sich einen Beitritt überlegen. Bereits heute kommen knapp 20 Prozent aller Mitglieder aus dem kommunalen Bereich.
- Die Allianz für Cybersicherheit ist eine gute Alternative für alle, die im Nicht-KRITIS-Bereich aktiv sind. Sie stärkt durch Information und Austausch nicht nur das Bewusstsein für die Bedeutung von Cybersicherheit, sondern hilft auch aktiv, das Know-how zum Schutz vor Cyberangriffen zu verbreiten. Mitglieder in der Allianz sind heute etwa 13 Gemeinden, 39 Kreise und 61 Städte.
- Der IT-Grundschutz bietet ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die Standards liefern dabei die bewährte Vorgehensweise, das Kompendium informiert über konkrete Anforderungen. Regelmäßig werden zudem IT-Grundschutztage durchgeführt. Bereits 2018 hat das BSI gemeinsam mit kommunalen Spitzenverbänden das IT-Grundschutzprofil für Kommunen zur Basis-Absicherung veröffentlicht.

Ausbau in der Fläche

Das BSI arbeitet stetig daran, die Zusammenarbeit mit den Bundesländern und den Kommunen auszubauen. Mit den regionalen Verbindungsstellen in Hamburg, Stuttgart, Wiesbaden und Dresden soll die Vernetzung des BSI in der Fläche verstärkt werden. Die Verbindungspersonen sind zentrale Anlaufstellen in den jeweiligen Regionen.

Allerdings können – bedingt durch die hohe Zahl von Kommunen – deren Beratungsanliegen derzeit nur in begrenztem Umfang individuell gelöst werden. Ihre Einbindung in ein ganzheitliches Sicherheitsniveau erfolgt durch die Länder und kommunalen Spitzenverbände als Multiplikatoren. Auch durch Bündelung und Vernetzung mit landeseigenen Strukturen oder durch einen Austausch auf operativer Ebene über den Verwaltungs-CERT-Verbund können die Kommunen partizipieren.

Sicher mit Zertifikat

Erfahrungen aus der Praxis

Viele kommunale IT-Dienstleister stellen sich den Herausforderungen durch die Digitalisierung und setzen bei der IT-Sicherheit auf eine Zertifizierung.

Die Herausforderungen und Chancen der Digitalisierung stehen in unmittelbarem Zusammenhang mit der Informationssicherheit. Für ein öffentlich-rechtliches Unternehmen wie die AKDB hat IT-Sicherheit inzwischen quasi den Status eines Produkts im eigenen Leistungsportfolio erlangt. Aus diesem Grund wurde schon 2013 eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) umgesetzt. Das geschützte Zertifikatssiegel ist in Deutschland und inzwischen sogar europaweit zu einem Gütezeichen für sichere IT-Produkte und IT-Dienstleistungen geworden. Es erfüllt den legitimen Anspruch der Kunden in Zeiten steigender Gefährdungen in der digitalen Welt, mit sicheren Produkten und Dienstleistungen arbeiten zu können.

Wie in vielen Bundesinstitutionen der Fall, ist auch beim BSI der Zertifizierungsprozess sehr stark formalisiert. Das hat den Vorteil, dass die Prozesse dadurch besser vergleichbar und stärker standardisiert sind, als andere Rahmenwerke in diesem Umfeld.

Bayerisches LSI bietet Sicherheitssiegel an

Das seit kurzer Zeit bestehende bayerische Siegel „Kommunale IT-Sicherheit“ eignet sich vor allem für kleinere bayerische Städte, Märkte und Gemeinden und soll den Anforderungen des bayerischen E-Government-Gesetzes gerecht werden. Das Siegel selbst ist kein Informationssicherheits-Management-System und ersetzt auch keinen der gängigen ISMS-Standards. Es ist vielmehr als Vorstufe zu einer Zertifizierung auf Basis einer Selbstauskunft zu betrachten.

Die Unterschiede der BSI-Zertifizierung zu der – besonders in der freien Wirtschaft – bevorzugten ISO-27001-Zertifizierung („Native ISO 27001“) bestehen hauptsächlich in der stärkeren Formalisierung und Anpassung der verwendeten Methodik durch starke Konkretisierung der Vorgaben und Anforderungen der zugrunde liegenden ISO/IEC-27000-Normenreihe.

Diese Vorgaben führen zwangsläufig zu großen Aufwänden und Änderungen im Unternehmen, die nicht unterschätzt werden sollten. Ein gut eingeführtes Change-Management hilft bei der Bewältigung der Aufgaben.

Zunächst müssen wichtige vorbereitende Tätigkeiten durchgeführt werden. Diese betreffen den Aufbau von Know-how zum IT-Grundschutz, das Asset-Management, Dokumentation, Prozesse und Organisation. Alle diese Bereiche müssen analysiert, bewertet und unter Umständen nachjustiert, angepasst und im Zweifelsfall auch neu aufgebaut werden. Daran schließen sich Planungen an zur Informationssicherheitsstrategie, den Sicherheitsprozessen, notwendigen Ressourcen (Hardware, Software, Dienstleistung) und Mitarbeitern, die mit „Best Practice“-Management-Prinzipien das ISMS bilden. Ist das ISMS dann ausgestaltet und definiert, erfolgt die Umsetzung und Implementierung im Unternehmen. So werden etwa Ressourcen beschafft, Mitarbeiter geschult und sensibilisiert sowie Sicherheitsprozesse initiiert, umgesetzt und dokumentiert.

Der formale Vorgang der BSI-Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann beginnen, wenn alle vorbereitenden Tätigkeiten erfolgt sind und das ISMS eingeführt ist. Eine weitere Voraussetzung für die Vergabe eines Zertifikates ist eine Überprüfung des ISMS beziehungsweise des Untersuchungsgegenstandes durch einen vom BSI zertifizierten Auditor für ISO-27001-Audits auf der Basis von IT-Grundschutz. Nach der formalen Antragsstellung beim BSI für die Zertifizierung, die unter anderem Informationen über den Untersuchungsgegenstand (Informationsverbund), einen bereinigten Netzplan, ein Firmenprofil sowie einen Zeitplan für das Audit beinhalten muss, kann nach Prüfung und Bestätigung durch die Zertifizierungsstelle das Audit durchgeführt werden.

Aufwände für Re-Zertifizierung und Überwachungsaudits

Im Rahmen des Audits werden von der Institution erstellte Referenzdokumente gesichtet, eine Vor-Ort-Prüfung durchgeführt und ein Auditbericht erstellt. Für die Vergabe des ISO-27001-Zertifikats auf Basis von IT-Grundschutz wird

dieser Auditbericht von der Zertifizierungsstelle im BSI geprüft. Das Zertifikat ist jeweils für den Zeitraum von drei Jahren gültig und setzt jährliche Überwachungsaudits voraus. Nach Ablauf der Gültigkeit muss eine Re-Zertifizierung erfolgen, die aufwandsmäßig einer Erstzertifizierung entspricht. Üblicherweise dauert ein Audit für eine Erst- beziehungsweise Re-Zertifizierung etwa fünf bis sieben Arbeitstage. Die jährlich durchzuführenden Überwachungsaudits schlagen mit circa drei bis vier Arbeitstagen zu Buche.

Der Auditor erstellt im Nachgang zum Audit einen detaillierten Auditbericht über die geprüften Dokumente sowie die Vor-Ort-Prüfung und führt eventuelle Abweichungen und Empfehlungen zu den geprüften Zielobjekten auf. Der Auditteamleiter legt außerdem in kurzer Form seine Gesamteinschätzung vor, die auf den Ergebnissen der für das Auditverfahren beschriebenen Prüfschritte basiert. Umstände oder Ergebnisse, die die Erteilung beziehungsweise Aufrechterhaltung des Zertifikats besonders positiv oder negativ beeinflussen, können an dieser Stelle herausgestellt werden.

Da sich die Anforderungen des BSI im Laufe der Zeit durch die Ablösung des IT-Grundschutzkataloges mit der Einführung des IT-Grundschutzkompendiums geändert haben, musste die AKDB für die in diesem Jahr durchgeführte Re-Zertifizierung erhebliche Ressourcen einsetzen. Sehr hilfreich bei der Durchführung des Zertifizierungsprozesses war die Nutzung eines ISMS-Dokumentations- und Workflowsystems, das den IT-Grundschutz und die notwendigen Prozessschritte strukturiert abbildet und die Erstellung der umfangreichen Referenzdokumente aus dem System ermöglicht.

Die Entscheidung der AKDB zur Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz war also ein wichtiger und zukunftsweisender Schritt sowie der richtige strategische Ansatz. Gerade in Zeiten hochgradiger digitaler Bedrohungen und gestiegener gesetzlicher Anforderungen zum Datenschutz ist die Bedeutung der Informationssicherheit noch einmal erheblich gewachsen und besonders im Umfeld von IT-Produkten und IT-Dienstleistungen zwingend erforderlich.

▲ Miklos Csizmadia ist IT-Sicherheitsbeauftragter der AKDB.

Cybersicherheit aus kommunaler Perspektive

Modernisierung des IT-Grundschutzes für Kommunen notwendig

Aktuelle Sicherheitsvorfälle bringen die Bedeutung von Cybersicherheitsmaßnahmen in das Bewusstsein von Entscheidern. Eine Vitako-Facharbeitsgruppe hat sich an der Veröffentlichung des IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung Version 2.0“ beteiligt.

Cybersicherheit und Cyberbedrohungen gehören zu den vielfältigen Themen, mit denen sich eine Kommune auseinandersetzen muss. Sicherheit und Schutz im behördlichen Umfeld sind dabei keine Individualleistungen, sondern Teamaufgaben – die Summe aus Erfahrung und Technik. Die ideale Zusammenarbeit sollte sich dabei auf die Verantwortlichen in unterschiedlichen Fachbereichen, den Gebietsrechenzentren sowie in Bundes- und Landesbehörden erstrecken. Je intensiver sich politische und strategische Entscheidungsebenen mit Cybersicherheit auseinandersetzen, desto stärker wird das Thema auch von Mitarbeitern in der Verwaltung wahrgenommen und gelebt. Es braucht also politische Impulse.

Ein wichtiger Impuls zur Verbesserung der Informationssicherheit in deutschen Verwaltungen ist die 2013 verabschiedete und 2018 fortgeschriebene „Leitlinie für Informationssicherheit“ (PDF: bit.ly/2CAeO29) des IT-Planungsrates, deren Umsetzung auch den Kommunen empfohlen wurde. Als Reaktion aus kommunaler Sicht erarbeitete und veröffentlichte Vitako in Kooperation mit den kommunalen Spitzenverbänden im Jahr 2017 die Handreichung „Informationssicherheitsleitlinie in Kommunalverwaltungen“, die erläutert, wie ein kommunales Informationssicherheitsmanagement-System aufgebaut und unterhalten werden kann. Die Handreichung beschreibt, wie eine dahinterstehende Informationssicherheitsleitlinie konzipiert und gestaltet werden kann, und bietet einen Überblick, welche Entscheidungen und Maßnahmen umzusetzen sind.

Anforderungen an kommunale IT-Sicherheit

Mit der zunehmenden Vernetzung und gemeinsamen Nutzung von Daten und Infrastrukturen wächst die Angriffsfläche für Cyberattacken. Teilweise auch überaus erfolgreiche Angriffe auf die deutsche Verwaltungs-IT aller föderalen Ebenen in den vergangenen Jahren lassen das Thema Cybersicherheit mehr und mehr in den Fokus rücken. Wer aber kann das Thema Sicherheit in der öffentlichen Verwaltung speziell in den Kommunen antreiben? Dazu ist es notwendig, zwei Dimensionen des Begriffs Cybersicherheit in Kommunalverwaltungen zu beleuchten. Zum einen müssen aus Sicht der Bürger sowohl Online-Verwaltungsdienste vor Cyberbedrohungen als auch die Daten der Bürger selbst geschützt werden. Zum anderen sollte aus Sicht der Verwaltungsmitarbeiter die Verfügbarkeit der IT-Verfahren und Fachanwendungen oberste Priorität von Sicherheitsmaßnahmen sein.

Prinzipiell geht es also auch in dieser mehrdimensionalen Betrachtungsweise darum, die drei Säulen der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integrität von Daten sicherzustellen. Die Schwierigkeit dieser Aufgabe im Umfeld der Kommunalverwaltung liegt oft auch in den verteilten Verantwortlichkeiten verborgen. Während IT-Dienstleister eher die Verfügbarkeit der IT-Verfahren und Dienste mit ihrer technischen Kompetenz gewährleisten, sorgen Fachabteilungen in den Kommunen und Landkreisen für die inhaltliche Umsetzung der Informationssicherheit und stellen demzufolge die Vertraulichkeit und die Integrität der Daten sicher. Ein systematisches Vorgehen, das sowohl Verantwortlichkeiten als auch organisatorische und technische Maßnahmen aufzeigt, ist zwingend notwendig.

Eine mögliche Systematik wird insbesondere kleineren Kommunen bereits an die Hand gegeben. Über das „Forum der IT-Sicherheitsbeauftragten von Ländern und Kommunen“ (IT-SiBe-Forum http://www.it-sibe-forum.de) wurde bereits Anfang 2016 die kommunale

Arbeitsgruppe „Modernisierung IT-Grundschutz“ initiiert. Als Ergebnis der Arbeitsgruppe wurde im Oktober 2019 das IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung in der Version 2.0 veröffentlicht. Das Profil soll Kommunen den Einstieg in die Informationssicherheit erleichtern und dabei helfen, die gröbsten Schwachstellen aufzudecken und zu beseitigen, um möglichst schnell das Sicherheitsniveau in der Kommunalverwaltung anzuheben.

Systematische Herangehensweise notwendig

Folgende Minimalziele sollten Kommunen, Landkreise und deren Entscheidungsträger im Rahmen einer systematischen Herangehensweise beachten:

- Informationen werden während der gesamten Verarbeitung und Speicherung gegen unbefugten Zugriff geschützt.
- Informationen werden nur an berechtigte Personen oder, wo erlaubt, an andere Fachanwendungen weitergegeben.
- Abhängigkeiten werden transparent dargestellt, Unterstützungsprozesse werden miterfasst.
- Ein Prozess zum Umgang mit Sicherheitslücken wird etabliert.
- Datensicherung und Übungen zur Rekonstruktion werden durchgeführt.
- Zugriffe werden dort, wo notwendig, protokolliert. Die Protokolldateien dienen auch der Fehleranalyse. Es findet eine fortlaufende Entwicklung im Rahmen einer Fehlerkultur und eines Lernens aus Fehlern statt.
- Ausgelagerte Prozesse werden gesteuert und das Zusammenspiel mit den ausgelagerten IT-Ressourcen überprüft. Die Überprüfung kann durch den Dienstleister auch durch eine Zertifizierung nachgewiesen werden.
- IT-Verfahren und Systeme werden mit aktueller Software und Hardware, die zum Zeitpunkt der Installation keine bekannten Sicherheitslücken aufweisen, bereitgestellt und mit Update-Mechanismen ausgestattet.

Neben Systematik und technischer Kompetenz seitens des Dienstleisters benötigt es auch eine in Cybersicherheitsfragen unterstützende Instanz in der Kommune. Ein(e) Informationssicherheitsbeauftragte(r) (ISB) sollte zur Regel werden in Kommunen – leider ist dies noch nicht überall der Fall. Er oder sie unterstützt und berät die Entscheidungsträger der Fachverfahren, der Verwaltung und der Politik auf kommunaler Ebene, um technische Rahmenbedingungen in Abstimmung mit dem Dienstleister zu implementieren. Vitako hat bereits vor mehr als zehn Jahren die Facharbeitsgruppe „IT-Sicherheit und Datenschutz“ ins Leben gerufen, in deren Rahmen sich ISBs und Datenschützer aus den Mitgliedsunternehmen in regelmäßigen Treffen austauschen, um sich auf Bedrohungen vorzubereiten und entsprechende Abwehrmaßnahmen umzusetzen, die im eigenen Wirkungskreis noch nicht aufgetreten sind.

▲ Markus Albert ist IT-Sicherheitsbeauftragter der Stadt Frankfurt.

▲ Daniel Grimm ist Bereichsleiter Informationsmanagement bei Vitako.

Deutschlands Cybersicherheitsarchitektur

Anbindung der Kommunalebene ist ausbaufähig

In den letzten Jahren hat die Anzahl der staatlichen Akteure im Bereich Cybersicherheit massiv zugenommen. Ein Überblick.

Um Zuständigkeiten sinnvoll zu verteilen oder um einen Ansprechpartner zu finden, ist es wichtig, die aktuelle staatliche Cybersicherheitsarchitektur in Deutschland zu kennen. Das beinhaltet sowohl die Bundes- als auch die Länder- und die Kommunalebene. Da Cybersicherheit aber nicht an den Landesgrenzen haltmacht, sollten zunehmend auch internationale Verbindungen, vor allem innerhalb Europas, einbezogen werden.

Den Ausgangspunkt der institutionellen Struktur im Bereich Cybersicherheit Deutschland kann man guten Gewissens auf den 1. Januar 1991 datieren. Dies war die Geburtsstunde des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit seinem heutigen Charakter. Als Dreh- und Angelpunkt der IT-Sicherheit in Deutschland dient es noch heute als zentrale Anlaufstelle. Die Anzahl der staatlichen Akteure auf Bundes- und Landes-, aber auch auf Kommunalebene, die sich mit IT-Sicherheit beschäftigen, ist seitdem jedoch massiv angestiegen. Das liegt unter anderem daran, dass aufgrund neuer Herausforderungen zusätzliche Behörden geschaffen worden sind. So wurde das Cyber-Abwehrzentrum (Cyber-AZ) im BSI zum Beispiel mit der Cybersicherheitsstrategie 2011 eingeführt oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) erstmals in der Cybersicherheitsstrategie 2016 erwähnt und 2017 geschaffen.

Digitalisierung als Treiber

Ein weiterer Grund für den rasanten Anstieg der letzten Jahre in der Teilhabe staatlicher Akteure ist die Digitalisierung selbst. Sicherheit ist ein zentrales Element der Digitalisierung. Wenn weite Teile des Allgemeinwesens digitalisiert werden, bedeutet das, dass auch IT-Sicherheit breiter gedacht werden muss. So diskutiert man auch bei der Gesundheitskarte, bei den Betreibern kritischer Infrastrukturen, aber auch beim vernetzten Kühlschrank und der Smart City von morgen über IT-Sicherheit. Dadurch wurde aus der rein technischen IT-Sicherheit, also dem Erreichen der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, die sogenannte Cybersicherheit. Von vielen wird sie nur als neumodischer Begriff abgetan, aber Cybersicherheit umfasst viel mehr als nur technische Sicherheit.

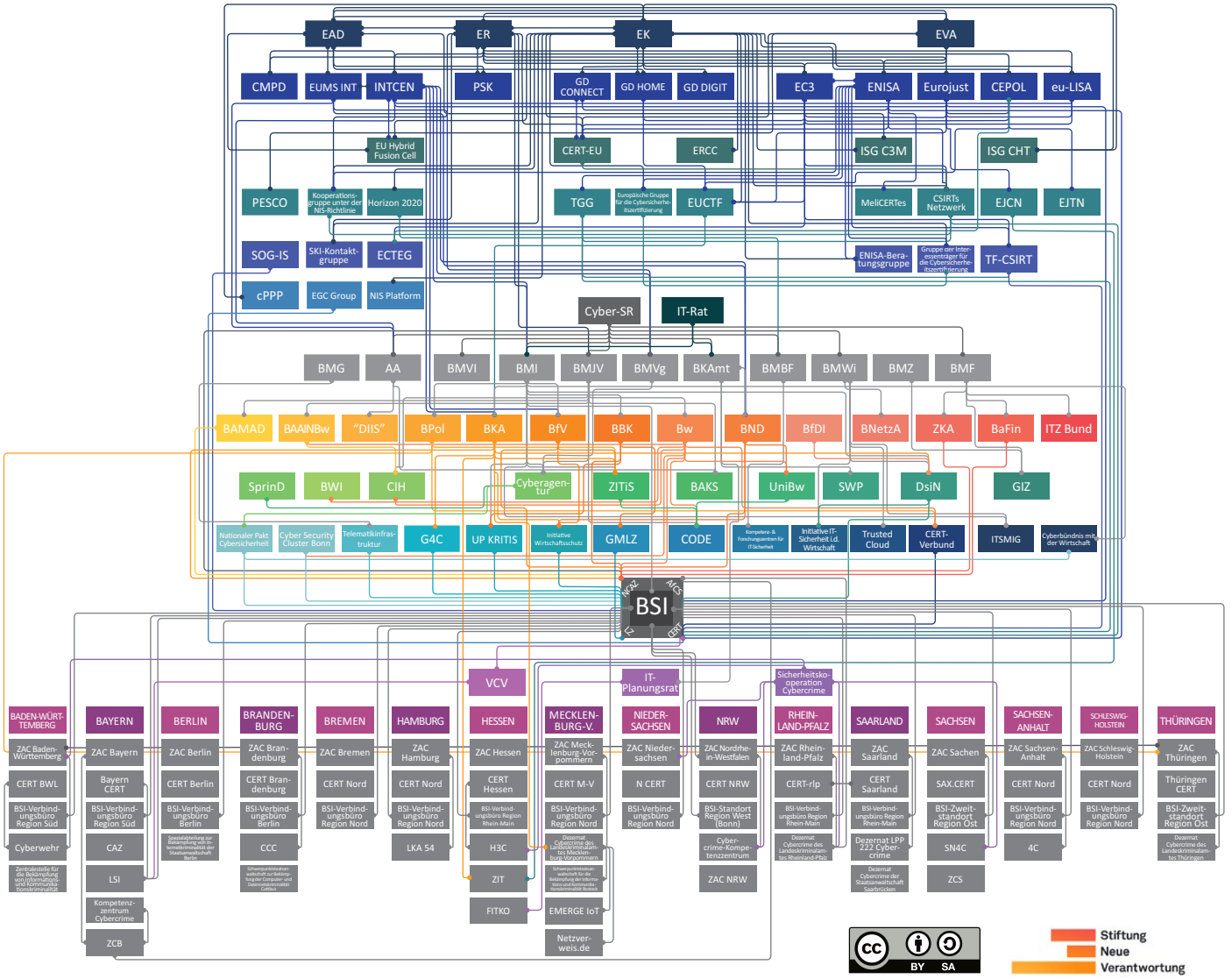
Zusätzlich zur Erreichung der Schutzziele beinhaltet sie auch politische, rechtliche, soziale und kulturelle Dimensionen. Die Digitalisierung – zusammen mit der Evolution von IT-Sicherheit hin zu Cybersicherheit – sorgt nicht nur für neue Behörden, sondern ist auch ein Grund dafür, dass zunehmend Behörden am Cybersicherheitsdiskurs teilnehmen, die vorher keine oder nur wenige Berührungspunkte mit IT-Sicherheit hatten.

Es gibt keinen Masterplan

Die Gesamtheit aller Institutionen, die in Deutschland an Cybersicherheit beteiligt sind, kann man als Cybersicherheitsarchitektur bezeichnen. Diese Architektur ist nicht am Reißbrett geplant worden. Die Entwicklung ähnelt wie beschrieben eher der einer typischen deutschen Stadt: Sie ist über lange Zeit gewachsen und es wurde immer dort etwas gebaut, wo es gerade notwendig war. Während hinter jeder einzelnen Institution in diesem Gebilde sicherlich eine Strategie steckt, gab es für die Architektur als solche keinen Masterplan.

Das ist nicht verwunderlich, denn der institutionelle Aufbau bewegte sich parallel zur Entwicklung des Themas Cybersicherheit. Gewachsene Strukturen führen oft zu Friktionen wie Zuständigkeitsproblemen und Mehraufwand etwa bei der Ressourcenverteilung. Bisher behilft man sich da in Deutschland mit einem einfachen, aber recht wirkungsvollen Trick: Sowohl auf strategischer Ebene als auch auf operativer Ebene gibt es jeweils einen zentralen Akteur („Spinne im Netz“), der viele Institutionen verbindet und den Informationsaustausch und die Koordination gewährleisten soll. Auf strategischer Ebene ist das der Cybersicherheitsrat (Cyber-SR) und auf operativer Ebene ist es das BSI, unter anderem mit seinem Nationalen Cyber-Abwehrzentrum.

STAATLICHE CYBERSICHERHEITSARCHITEKTUR



Leider hinkt die Einbindung der Länder- und vor allem der Kommunalebenen in diesen Strukturen bisher hinterher. Abhilfe soll, zumindest für die Einbindung der Bundesländer, eine Erweiterung des Nationalen Cyber-Abwehrzentrums schaffen. Jedoch handelt es sich hierbei um ein Vorhaben, das über die Jahre vielfach angefangen, aber bisher noch nicht vollendet worden ist.

Gesamtstrategie erarbeiten

Die Entwicklung der deutschen Cybersicherheitsarchitektur ist noch nicht abgeschlossen. Es ist auch nicht verwerflich, dass es bisher dafür kein Gesamtkonzept gab, auch wenn das sicherlich hilfreich gewesen wäre. Da die Digitalisierung jedoch noch nicht abgeschlossen ist und kritische Entwicklungen wie die Vermengung von zivilen und militärischen Aspekten in Deutschland (unter anderem durch die Cyber-Agentur von Innen- und Verteidigungsministerium) zunehmen, sollte man spätestens jetzt systematisch eine konkrete Strategie für die Cybersicherheitsarchitektur in Deutschland erarbeiten.

Mit dem Papier „Zuständigkeiten und Aufgaben in der deutschen Cybersicherheitspolitik“ hat die Stiftung Neue Verantwortung einen nicht abgeschlossenen Erstentwurf zum Status quo der Architektur und der Zuständigkeiten vorgelegt. Weil dort bisher die Kommunalebene fehlt, freuen sich die Autoren auf Ihr Wissen über Cybersicherheitsarchitektur auf der Kommunalebene. Bitte E-Mail an: sherpig@stiftung-nv.de.

▲ Dr. Sven Herpig, Head of International Cyber Security Policy bei der Stiftung Neue Verantwortung. bit.ly/2O1Hs1l

Selbst-souveräne Identität

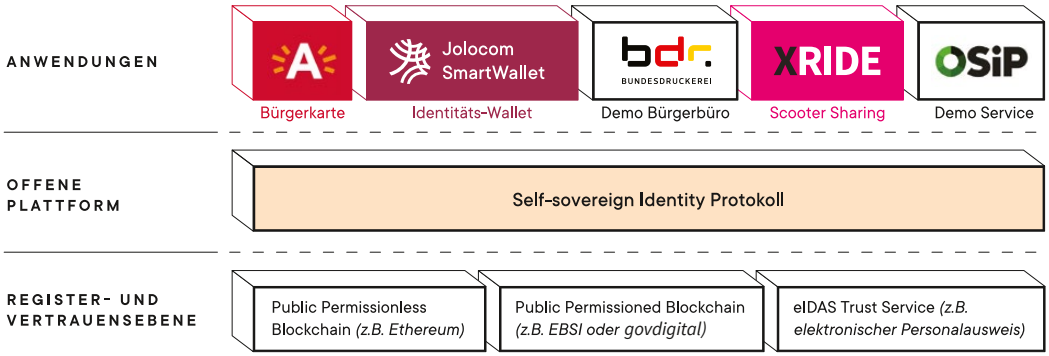
Paradigmenwechsel im Identitätsmanagement

Eine sichere digitale Identität ist die Voraussetzung für zahllose Interaktionen in der heutigen Online-Welt. Selbst-souveräne Identitätslösungen nehmen den Blick der User ein anstatt der Perspektive von Organisationen.

▲ Kai Wagner ist bei Jolocom zuständig für Business Development and Strategy.

Durch die Digitalisierung gewinnen Alternativen zu gedruckten Identifikationsdokumenten zunehmend an Bedeutung. Digitale Identitätslösungen bleiben dabei oft auf einzelne Anwendungsfälle begrenzt. Die Bereitstellung einer einfachen und anwendungsübergreifenden Identitätslösung stellt bisher sowohl für den öffentlichen als auch für den privaten Sektor eine Herausforderung dar. Eine interoperable und dezentral organisierte Identifikationsinfrastruktur, wie sie derzeit entsteht, gibt neue Antworten auf dieses Problem und wird bereits international erprobt.

In der Online-Welt beginnt die überwiegende Mehrheit aller Aktivitäten mit der Erstellung eines Benutzerkontos, auf das im Anschluss mithilfe von Benutzername und Passwort zugegriffen werden kann. Dieses Modell der digitalen Identität wird aus der Perspektive der Organisation bereitgestellt, da lediglich der Zugang zu einem Benutzerprofil oder Kundenkonto verfügbar gemacht wird. Die Speicherung der Daten erfolgt bei der Organisation und kann vom Nutzer nur bedingt nachvollzogen werden. So entsteht ein unübersichtliches Nebeneinander an Benutzerkonten und Log-ins, die den Organisationen dienen, dem Nutzer aber eine hohe Komplexität aufbürden.



◀ Das „Self-sovereign Identity"-Modell ermöglicht die Harmonisierung unterschiedlicher Vertrauensdienste und Identitätsanbieter auf Basis eines Protokolls für den sicheren Austausch der Identitätsdaten. Durch die Datenhaltung im Identitäts-Wallet des Bürgers wird die Nutzung bestätigter Dokumente über unterschiedliche Anwendungen hinweg ermöglicht.

Als Antwort auf diese sogenannten zentralen Identitätslösungen haben sich in den vergangenen Jahren „föderierte" Identitätslösungen herausgebildet. Hierbei tritt ein Akteur als Identitätsdrehscheibe auf, indem er anderen Diensten ermöglicht, auf die von ihm verwalteten Identitäten (Benutzerkonten) zuzugreifen. Für den Bürger bedeuten diese Systeme eine vereinfachte Nutzbarkeit, da nur noch die Zugangsdaten zur Identitätsdrehscheibe erinnert werden müssen.

Organisationen können derartige Identitätsdrehscheiben bei sich einbinden und erhalten so einen vereinfachten Zugang zu ihren Nutzern, ohne selbst eine digitale Identität anbieten zu müssen. Beispiele für Identitätsdrehscheiben sind Google und Facebook, die den Zugang zu weiteren Diensten Dritter ermöglichen, aber auch das Angebot von Verimi aus Deutschland.

Identität aus Sicht des Bürgers

Das Problem der digitalen Identität könnte an dieser Stelle als gelöst betrachtet werden, doch leider ergeben sich aus dem Konzept der Identitätsdrehscheibe neben der verbesserten Nutzbarkeit auch viele Probleme. Um von einer Identitätsdrehscheibe zu profitieren, müssen Bürgerinnen und Bürger ihre Daten in die Hände der Identitätsdrehscheibe geben und sich wiederum darauf verlassen können, dass sie dort sicher verwahrt und nicht für andere Zwecke missbraucht werden. Eine selbstbestimmte Verwaltung der Daten ist nicht möglich. Für Organisationen, die eine Identitätsdrehscheibe nutzen wollen, ergibt sich ein zusätzliches Problem, denn jede Identitätsdrehscheibe stellt ein in sich geschlossenes System dar, welches nur für jene Akteure funktioniert, die sich dem dahinterliegenden Konsortium anschließen und allen damit einhergehenden Nutzungsbedingungen (wie dem Teilen von Nutzungsstatistiken und Kundendaten) zustimmen.

Um für Kunden attraktiv zu sein, bleibt einer Organisation heute oft nur die Möglichkeit, sich einem solchen Konsortium anzuschließen. Dadurch wird die Kontrolle über den Kontakt mit ihren Nutzern in weiten Teilen in die Hände der Identitätsdrehscheibe gegeben. Ein neues Modell digitaler Identität soll hier Abhilfe schaffen: Bei der sogenannten selbst-souveränen Identität wird die Identitätsinfrastruktur vom Bürger aus gedacht, anstatt die Perspektive einer Organisation einzunehmen.

Der Bürger wird dabei selbst zur Identitätsdrehscheibe, denn alle Daten sind lokal in seinem „digitalen Wallet" auf dem Smartphone gespeichert. Vergleichbar mit dem Portemonnaie werden darin alle Dokumente abgelegt, mit denen sich der Bürger ausweisen kann (Führerschein, Bibliotheksausweis, Bankkarte). Die auf offenen Standards basierende sichere Protokollinfrastruktur, das „Self-sovereign Identity"-Protokoll, gewährleistet dabei, dass Dokumente sicher an den Bürger ausgestellt, von ihm gespeichert und bei gleichbleibendem Vertrauensniveau zur Authentifizierung vorgelegt werden können. Das Ganze geschieht anbieterunabhängig, sodass ein Wettbewerb für Vertrauensdienste und Wallet-Anbieter gewährleistet wird.

In der konkreten Anwendung bedeutet dies, dass der Bürger sich von Vertrauensdiensten eine digitale Kopie seiner Dokumente ausstellen lässt und diese in seinem Wallet speichert. Dabei bleibt zu jedem Zeitpunkt transparent, von wem ein Dokument ausgestellt wurde, welches Vertrauensniveau vorliegt und ob das Dokument noch gültig ist oder entzogen wurde.

Während das beschriebene „Self-sovereign Identity"-System auch durch die Anbindung an zentrale Vertrauensdienste ermöglicht werden kann (eIDAS, Video-Ident etc.), gibt es zusätzlich die Möglichkeit, auch dezentrale Netzwerke auf Blockchain-Basis für die Bereitstellung der Register zu nutzen und demgemäß hohe Transparenz und Fälschungssicherheit zu ermöglichen. Ein Beispiel für eine solche Blockchain-Infrastruktur ist die von der Vitako initiierte genossenschaftlich betriebene Blockchain (siehe Seite 24). Mithilfe des „Self-sovereign Identity"-Protokolls können somit alle Bürgerinnen und Bürger von einer anbieterunabhängigen Identitätslösung profitieren, die genauso einfach funktioniert wie ihr analoges Portemonnaie und die darin enthaltenen Ausweis- und Kundenkarten.

Komplizierte Schlüsselmomente

Neue Dienste erleichtern die Einrichtung einer Ende-zu-Ende-Verschlüsselung

Die Frage nach einer sicheren, verschlüsselten E-Mail-Kommunikation ist auf der Agenda vieler Unternehmen und Organisationen. Als größter Hemmschuh der Technologie gilt jedoch nach wie vor das aufwendige Zertifikatmanagement auf den Clients.

S/MIME und PGP gelten als die beiden bekanntesten Verschlüsselungsverfahren. Bei der Frage nach den Unterschieden gibt es hinsichtlich der Informationssicherheit keine nennenswerten Unterschiede. Oftmals kommen sogar dieselben Algorithmen zum Einsatz. Die zwei größten Unterschiede liegen zunächst in der Vertrauenswürdigkeit des Schlüsselmaterials. Während bei S/MIME ein hierarchischer Ansatz dafür sorgt, dass Zertifikate, die unter einer bestimmten Certificate Authority (CA) ausgestellt wurden, immer als vertrauenswürdig eingestuft werden können, muss bei PGP jedem Schlüssel einzeln vertraut werden. Es gibt zwar den Web-of-Trust-Ansatz, dieser ist jedoch zum einen nicht standardisiert und erfordert zum anderen ein hohes Wissen bei allen Beteiligten. Der zweite Unterschied ist die hohe Verfügbarkeit von S/MIME in vielen gängigen E-Mail-Clients wie Outlook, Thunderbird und Co. Bei PGP muss dagegen in jedem Fall zuerst ein Add-in installiert werden.

Vertrauen rückt vor dem Hintergrund des stark angestiegenen Angebots von Cloud-Diensten immer weiter in den Mittelpunkt. Für akkreditierte Trust Center wie D-Trust, SwissSign und GlobalSign ist Vertrauen schon seit Langem die Grundlage ihres Geschäfts. Daneben gibt es mit der European Bridge CA (EBCA) des Bundesverbands IT-Sicherheit e. V. (TeleTrusT) einen Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKI) zu einem PKI-Verbund. Sie ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen. Jeder Teilnehmer stellt dabei sicher, dass seine PKI den Anforderungen der EBCA entspricht und nicht selten auf dem nahezu selben Sicherheitsniveau betrieben wird, wie die akkreditierten Trust Center.

Ende-zu-Ende oder Gateway?

Neben der Auswahl des Verfahrens als solches, gibt es zwei Umsetzungsszenarien. Die sogenannte Ende-zu-Ende-Verschlüsselung (E2E) beschreibt die Umsetzung der Verschlüsselung auf dem Client des Benutzers. Für die Ver- und Entschlüsselung müssen dabei dem E-Mail-Client alle benötigten Zertifikate zur Verfügung stehen. Beim Einsatz von mobilen Geräten stellt dies mitunter eine nur schwer lösbare Aufgabe dar. Der Vorteil bei E2E ist die etwas höhere Informationssicherheit, da die E-Mail in verschlüsselter Form im Postfach des Benutzers liegt. Dies ist zugleich auch ein Nachteil, da der Aufwand beispielsweise bei der Stellvertretereinrichtung enorm ansteigt. Der Stellvertreter muss ebenfalls im Besitz des richtigen Schlüsselmaterials sein. Der mobile Zugriff, Archivierung und automatische Weiterleitungen sind entweder herausfordernd oder gar unmöglich.

Zentrale Verschlüsselungs-Gateways automatisieren die Verwaltung des Schlüsselmaterials und übernehmen darüber hinaus vollständig transparent die Verschlüsselung, Entschlüsselung, Signatur und die Prüfung der Signatur. In der Praxis bedeutet das, dass der Endanwender überhaupt nicht mehr manuell in den Prozess eingreifen muss – und auch der zuständige Administrator nachhaltig entlastet wird.

Platin für die kommunalen Lösungen der regio iT

Die Leserinnen und Leser der Fachzeitschrift „E-Government Computing“ haben entschieden: Die regio iT ist das beste E-Government Unternehmen Deutschlands in der Kategorie „Kommunale Lösungen“. Dirk Schweikart, Centerleiter Kommunale Digitalisierungslösungen der regio iT, nahm die Platin-Auszeichnung bei der festlichen Galaveranstaltung im Berliner Hotel de Rome am 2. Oktober entgegen.

Der Anruf mit der Nachricht zu der Auszeichnung war für den Centerleiter eine freudige Überraschung. „Wir freuen uns sehr, dass wir aus Sicht der Leserinnen und Leser von E-Government Computing einen wesentlichen Beitrag zur kommunalen Digitalisierung leisten“, erklärte Schweikart. Das Serviceportal der regio iT dient als Datendrehscheibe und ist sowohl Rahmen als auch Herz der flächendeckenden Umsetzung des E-Government. Neben dem modularen Aufbau überzeugt offenkundig auch der Service der regio iT.

Der bundesweite Digitalisierungsprozess nahm durch das 2017 beschlossene Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) Fahrt auf. Die daraus entstandene Zielsetzung, bis 2022 jegliche Verwaltungsdienstleistungen auch digital über Verwaltungsportale zur Verfügung zu stellen und diese Portale zu einem Verbund zu verknüpfen, unterstreicht die Bedeutung zusätzlich.

Bereits zum vierten Mal wurde der E-Government-Award verliehen, der unter der Schirmherrschaft von Staatssekretär Klaus Vitt, dem Beauftragten der Bundesregierung für Informationstechnik, steht. Neben ihm erschienen auch die Staatssekretärin und CIO des Landes Berlin, Sabine Smentek, der Staatsrat und CIO des Landes Bremen, Henning Lühr, sowie der Staatssekretär und CIO des Landes Thüringen, Dr. Hartmut Schubert. „Solche Auszeichnungen sind Bestätigung und Ansporn zugleich“, betonte Schweikart nach der Preisverleihung.

▲ Dirk Schweikart nahm die Auszeichnung in Berlin entgegen.

Ausgezeichnet wurden die Finalisten der Leserumfrage der „E-Government Computing“ in insgesamt zehn Kategorien. Namhafte Unternehmen waren nominiert. Umso erfreulicher für die regio iT, es in der Kategorie „Kommunale Lösungen“ nicht nur unter die Finalisten geschafft zu haben, sondern von den Lesern mehrheitlich auf den ersten Platz (Platin) gesetzt zu werden.

regio iT-Tochter ermöglicht Mobilität für alle, jederzeit und überall

Die regio iT hat eine neue Tochter: Anfang Oktober startete die „Better Mobility“ – die gemeinsame Gesellschaft von regio iT und dem Aachener ÖPNV-Anbieter ASEAG – ins Unternehmensleben. Das jüngste Kind der IT-Experten aus Aachen und Gütersloh will Mobilität für alle, jederzeit und überall ermöglichen.

Die Mission des Teams rund um Geschäftsführer Jörg Röhlen ist es, alle Mobilitätsangebote einer Stadt digital zu vernetzen und so das eigene Auto verzichtbar zu machen. Mit dem „Mobility Broker“ bietet die Better Mobility dazu eine Plattform für Bürger und Unternehmen. „Es geht um mehr, als nur Fahrpläne und Fahrscheine auf eine App zu transformieren“, beschreibt Röhlen seine Vision einer gelungenen Mobilitätswende, zu der die Better Mobility beitragen will. Das Team arbeitet beispielsweise auch an Mobilitätsflatrates und innovativen Jobtickets sowie an verschiedenen Modulen, um Unternehmensflotten besser auszulasten.

Für Bürger erleichtert der Mobility Broker vor allem die alltägliche Mobilität: Wissen, wann der Bus fährt und Online-Tickets kaufen. Das Fahrrad oder Carsharing passend dazu buchen oder einmal Ride-Sharing ausprobieren? Außerdem die volle Kostenkontrolle behalten durch eine integrierte Rechnung am Monatsende!

All das ist drin in der Whitelabel-App, die etwa in Aachen seit dem 18.10.2019 unter dem Namen „movA“ verfügbar ist und von der ASEAG betrieben wird. Weitere Informationen unter: **www.bettermobility.de**

Hausmesse „interface“ ein voller Erfolg

Wörtlich nahmen die Gastgeber das Motto der „interface“: Als Kommunikationsschnittstelle konzipierten die drei kommunalen IT-Dienstleister civitec, kdvz Rhein-Erft-Rur und regio iT die erste gemeinsame Hausmesse.

Mit vollem Erfolg, wie die mehr als 300 Vertreterinnen und Vertreter aus Kommunalverwaltungen und anderen öffentlichen Institutionen nach der Veranstaltung am 18. September im MEDIO.RHEIN.ERFT in Bergheim verdeutlichten.

Das Konzept kam gut an. Eine Ausstellung rund um die Digitalisierung der öffentlichen Hand flankierte die 40 Fachvorträge zu Themen wie „Digitalisierung in Schulen“, „Prozessoptimierung im kommunalen Finanzwesen“ oder „Intelligenter Posteingang“. Zwischen den Vorträgen wurden die Kommunikationsinseln in der Ausstellung für den direkten Austausch zwischen Kunden, IT-Dienstleistern und Lieferanten rege genutzt.

Entsprechend positiv fällt das Fazit der Veranstalter aus: Die „interface“ als gemeinsame, kundennahe Veranstaltung, die alle Prozessbeteiligten rund um die Digitalisierung der Verwaltung und kommunalen Einrichtungen zusammenbringt, ist ein Format mit Zukunft. Wiederholung ausdrücklich erwünscht!

PlanQK siegt beim Innovationswettbewerb

PlanQK verbindet künstliche Intelligenz und Quantencomputing – eine Plattform für innovative Anwendungen

Diese Projektidee – an PlanQK beteiligen sich neben der regio iT Partner aus Forschung und Industrie – konnte sich unter insgesamt 130 Konsortien beim Innovationswettbewerb „Künstliche Intelligenz als Treiber für volkswirtschaftlich relevante Ökosysteme“ des Bundesministeriums für Wirtschaft und Energie durchsetzen. Das Gesamtvorhaben hat ein Volumen von 19 Mio. Euro. Künstliche Intelligenz (KI) fördert die Technologie – wirft aber auch neue Fragen auf. Deren Lösung erfordert eine Rechenleistung, die aktuelle Computer nicht bieten können. Daher die Idee, KI mit Quantencomputing zu verbinden und eine offene Plattform für quantenunterstützte künstliche Intelligenz (QKI) zu entwickeln. Hier setzt das Teilprojekt der regio iT an: Die PlanQK-Plattform liefert die technische Basis für den Aufbau einer Community, in der QKI auf aktuelle Anforderungen der kommunalen Verwaltung angewendet wird. Anhand von vier Anwendungsfällen bei vier Verwaltungen will die regio iT Nutzen und Übertragbarkeit der PlanQK-Plattform für die öffentliche Verwaltung verifizieren.

Reallabor im Rheinischen Revier

Der NRW-Wirtschafts- und Digitalminister Andreas Pinkwart will die Blockchain-Nutzung vorantreiben

Am 2. September übergab der Minister dem Konsortium des Projektes „Blockchain Reallabor im Rheinischen Revier“ den Förderbescheid zum Aufbau des BR 3-Reallabors. Zum Projektkonsortium gehören neben der regio iT die Fraunhofer-Gesellschaft sowie die Hochschulen aus Aachen, Bochum und Gelsenkirchen. Der Fokus liegt auf der Daseinsvorsorge und dem Energiesektor, aber auch Anwendungen aus den Bereichen Logistik, Industrie und Finanzwirtschaft sollen erprobt werden. Der Minister sieht in dem BR 3-Projekt das „ideale Umfeld, um Anwendungen zu testen, etwa bei der kommunalen Wasserversorgung oder der intelligenten Abrechnung von Energieverbrauch“. Auch die heimische Wirtschaft werde profitieren, so Pinkwart. Zudem mache das Projekt Nordrhein-Westfalen zum bundesweiten Vorreiter beim Aufbau des Internets der Werte. Fördergelder in Höhe von 1,2 Mio. Euro stellt die NRW-Landesregierung bereit. Starten sollen die Praxisprojekte 2020.

▲ Minister Andreas Pinkwart übergibt Dieter Rehfeld, Vorsitzender der regio iT-Geschäftsführung, den Förderbescheid.

▶ Hier gehts zum govchain-Blog von Dieter Rehfeld: **https://govchain-blog.de**

Totale Begeisterung bei regio iT und Stadt Wassenberg

Gerade mal hundert Tage ist es her, dass sich beide Seiten förmlich in Lobeshymnen überboten. Grund für so viel Euphorie: Die Stadt Wassenberg setzt auf das Dokumenten-Management-System (DMS) enaio® von Optimal Systems – die regio iT war verantwortlich für dessen Einführung.

▲ Jürgen Justen, regio iT (links), Annika Schmitz, Stadt Wassenberg (rechts)

„Wir sind total begeistert vom Projekt und der zügigen Umsetzung“, lobt Annika Schmitz, als Fachbereichsleiterin der Stadt Wassenberg verantwortlich für Verwaltungsmanagement und Ratsangelegenheiten. Binnen vier Monaten wurde das Rathaus auf die datenbankgestützte Verwaltung und Archivierung von Dokumenten umgestellt.

Das Kompliment kam prompt zurück: „Ohne Kunden auf der anderen Seite, die so auf Zack sind, kann das nicht so zügig gehen“, schwärmt Jürgen Justen, Leiter der regio iT-Geschäftsstelle in Heinsberg. Schließlich sorgte zunächst der IT-Verantwortliche der Stadt für die passende Leitung zur regio iT – in deren hochsicheren Rechenzentren die Daten und Dokumente liegen – und schon konnte es losgehen. Die regio iT installierte die passende Testumgebung und in kürzester Zeit füllten sich die digitalen Ordner. Die Liveschaltung konnte zügig erfolgen. „Wir fühlen uns super betreut“, betonte Annika Schmitz beim Besuch des Vorsitzenden der regio iT-Geschäftsführung, Dieter Rehfeld, kurz nach der Umstellung.

Die Euphorie hat sich bis heute nicht gelegt: „Das Programm läuft störungsfrei und fließend“, lobt Annika Schmitz, die die laufende Projektbetreuung „sehr gut“ findet. Dazu gehört auch die Schulung der Mitarbeiterinnen und Mitarbeiter im Rathaus. „Das hat super funktioniert“, ist die 31-Jährige auch Wochen später noch angetan. Inzwischen weisen sich die Mitarbeiterinnen und Mitarbeiter untereinander in das DMS ein und profitieren von der Umstellung. „Man merkt es bei der täglichen Arbeit, wie schnell das System läuft und wie flott man die Akten findet“, berichtet die Fachbereichsleiterin von ihren eigenen Erfahrungen und gibt mächtig Gas in Richtung Verwaltung 4.0.

„Datensicherheit und mobiles Arbeiten sind wichtige Zukunftsthemen“, erläutert die Verwaltungsexpertin. Dementsprechend hat sie gemeinsam mit dem Bürgermeister der Stadt, Manfred Winkens, und den Verantwortlichen der regio iT weitere Projekte angestoßen: das Outsourcing der gesamten IT sowie die Einführung einer Virtuellen Desktop Infrastruktur (VDI). Mit den Aufgaben der Verwaltung wächst auch die IT-Infrastruktur, die stets auf dem neuesten Stand und vor Eingriffen von außen geschützt sein muss. Die regio iT verfügt über zertifizierte hochsichere Rechenzentren für das Hosting des Verwaltungsgeschäftes. Und über ausgezeichnete IT-Fachleute, die die Betreuung der Infrastruktur gerne übernehmen ...

Die Einführung des VDI gehört ebenfalls zu dem Paket, das in naher Zukunft den politischen Gremien zur Entscheidung vorgelegt wird. Künftig könnte jede Mitarbeiterin, jeder Mitarbeiter, jederzeit von überall mit jedem internetfähigen Endgerät auf seinen Arbeitsplatz zugreifen – modernes Arbeiten in einer modernen Verwaltung mit Unterstützung der regio iT.

Impressum . . . . .

regio iT gesellschaft für informationstechnologie mbh

Lombardenstraße 24
52070 Aachen
Telefon: 0241 - 413 59 0
E-Mail: medien@regioit.de

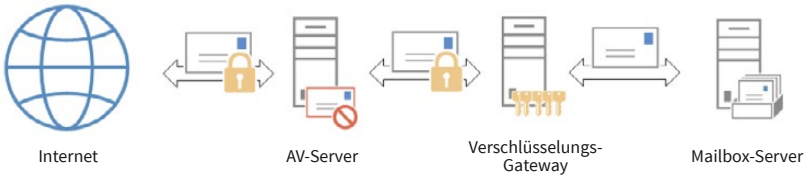
Langer Weg 7a
33332 Gütersloh
Telefon: 05241 - 2113 0
www.regioit.de

V.i.S.d.P.: Dieter Rehfeld, Redaktion: Birgit Becker
Vertrieb: Jürgen Kouhl, vertrieb@regioit.de
Autoren dieser Ausgabe: Carola Adenauer, Melanie Fraedrich

Nachteilig ist, dass die E-Mail unverschlüsselt im Postfach des Benutzers liegt. In diesem Fall gilt es, das Postfach mit möglichst engen Zugriffsberechtigungen und durchgängiger Transportverschlüsselung bestmöglich zu schützen. In den allermeisten E-Mail-Server-Infrastrukturen stellt dies heute jedoch keine Hürde mehr dar.

Ein weiterer, äußerst wichtiger Punkt ist die Betriebssicherheit. Bei E2E kann der Inhalt einer E-Mail erst am E-Mail-Client auf Spam- und Virengehalt geprüft werden. In der Regel stehen dort dann nicht mehr dieselben Filter und Werkzeuge zur Verfügung wie am Gateway. Benutzer, die E2E nutzen, müssen demzufolge nicht nur hinsichtlich der Verschlüsselung gut geschult werden, sondern auch besonders wachsam im Umgang mit Anhängen und URLs in E-Mails sein.

Der Datenschützer des jeweiligen Unternehmens muss daher im Einklang mit der IT-Security-Abteilung festlegen, welche Form der Umsetzung für welche Benutzer oder Anwendungsfälle zu wählen ist. Dabei ist zu berücksichtigen, dass die E2E-Verschlüsselung nicht, wie fälschlicherweise häufig angenommen wird, durch die Datenschutzgrundverordnung vorgeschrieben ist! Oft entscheiden sich Unternehmen für einen hybriden Einsatz. E2E kommt nur bei Personen mit besonders hohem Schutzbedarf (Geschäftsführer, Betriebsarzt) zum Einsatz, während der überwiegende Teil der E-Mail-Kommunikation durch ein Gateway abgesichert wird.



▲ Ein typisches Konfigurationsszenario für die Gateway-basierte Verschlüsselung

Tools für Verschlüsselung

Neben den Verschlüsselungs-Gateways gibt es schon seit einiger Zeit unterschiedliche Tools, die die E2E-Verschlüsselung erleichtern sollen. Mailvelope gehört zu den bekannteren Tools und ist unlängst im Rahmen eines vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geförderten Projekts nutzerfreundlicher gestaltet worden. Dabei handelt es sich um eine reine Browser-Erweiterung, die auf Basis von PGP arbeitet. Die Verwendung auf mobilen Clients ist nicht möglich, es sei denn, man exportiert das private Schlüsselmaterial und verwendet es mit einem PGP-fähigen E-Mail-Client auf dem mobilen Gerät. Die Einrichtung von Mailvelope ist schnell und einfach. Wie bei jeder E2E-basierten Verschlüsselung muss der Verwender sich jedoch auch hier selbst um die Sicherung und Wiederherstellung des privaten Schlüsselmaterials kümmern. Für technisch unbedarfte Benutzer endet das nicht selten im Verlust von E-Mail-Inhalten, weil die E-Mail aufgrund von verlorengegangenen Schlüsseln nicht mehr entschlüsselt werden kann.

▲ Stefan Cink ist Mitglied im Lenkungsgremium der TeleTrusT European Bridge CA und ist Spezialist für E-Mail-Sicherheit bei Net at Work GmbH.

„IT muss Maßstäbe setzen“

Der Bundesdatenschutzbeauftragte Ulrich Kelber über die Datenschutzgrundverordnung als „Goldstandard“, Datenethik und die Rolle der kommunalen IT-Dienstleister

Herr Kelber, vor etwa eineinhalb Jahren wurde die europäische Datenschutzgrundverordnung (DSGVO) eingeführt. Wie zufrieden sind Sie mit dem Umsetzungsstand bis heute?

Die DSGVO ist definitiv ein voller Erfolg. Sehr viele Unternehmen, für die Datenschutz früher ein Fremdwort war, haben sich aufgrund der DSGVO mit dem Thema auseinandergesetzt. Vor allem aber sehen wir, dass die DSGVO sich auch international zu einer Art Goldstandard entwickelt hat, an dem sich neue Datenschutzgesetze weltweit orientieren.

Gegenwärtig wird die digitale Souveränität des Staates und die Abhängigkeit von Marktmonopolisten auch in der kommunalen IT diskutiert. Welche Schwierigkeiten sehen Sie aus datenschutzrechtlicher Perspektive?

Wir befinden uns hier oft in einer faktischen Abhängigkeit zu einigen Anbietern, die niemals gut sein kann. Insbesondere dann, wenn die in Rede stehenden Produkte nicht hinreichende Datenschutzstandards gewährleisten, weil zum Beispiel nicht beeinflussbare Datenübermittlungen stattfinden. Wir sollten daher noch stärker an der Entwicklung europäischer Alternativen arbeiten, bei denen Datenschutz bereits „ab Werk“ ein wesentliches Unterscheidungsmerkmal darstellt.

Sie haben sich unlängst für eine stärkere Inpflichtnahme Irlands ausgesprochen. Die dortige Datenschutzbehörde ist zuständig für die Datenschutzverstöße etwa von Facebook, geht aber ausgesprochen lax mit der Durchsetzung der DSGVO um.

Hier geht es um Glaubwürdigkeit der Europäischen Union. Wir können nicht auf der einen Seite die DSGVO als das Gesetz loben, vor dem sich auch die global operierenden IT-Konzerne nicht mehr verstecken können, und dann auf der anderen Seite auch nach über 500 Tagen Anwendbarkeit noch keine einzige Entscheidung in den vielen anhängigen Verfahren vorweisen. Die Kollegen in Irland haben mit einem komplizierten nationalen Verwaltungsrecht zu kämpfen. Daher sollten wir bei der anstehenden Evaluierung der DSGVO sicherlich überlegen, ob und wie man hier eine Verfahrensbeschleunigung erreichen könnte.

Auch Deutschland hat sich bislang nicht durch konsequentes Vorgehen gegen Datenschutzverstöße hervorgetan. Derzeit wird von Bund und Ländern ein Bußgeldkatalog erarbeitet. Können Sie uns erläutern, was genau geplant ist?

Bei dem aktuell von der Datenschutzkonferenz veröffentlichten Konzept handelt es sich nicht um einen klassischen Bußgeldkatalog wie zum Beispiel im Straßenverkehrsrecht, sondern um eine Art Leitfaden, an dem sich die deutschen Aufsichtsbehörden bei der Bemessung von Geldbußen orientieren werden, bis einheitliche europaweite Leitlinien vorliegen. Wir werden auch in Deutschland höhere Bußgelder sehen.

▶ Vitako-Geschäftsführer Dr. Ralf Resch im Gespräch mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Ulrich Kelber (im Bild rechts)
Fotos: Tobias Koch

Seitens Wirtschaft und Industrie wird der Datenschutz häufig als Hürde und Innovationshemmnis empfunden. Wie begegnen Sie solchen Vorbehalten?

Mit Unverständnis. Wir sehen gerade, dass amerikanische Unternehmen wie Apple Millionenbeträge in Werbung investieren, mit der ausschließlich innovative Datenschutzfeatures ihrer Produkte herausgestellt werden. Dies passiert, weil es einen immer größeren Markt für entsprechende Angebote gibt. Wieso nutzen deutsche Unternehmen dies nicht und schaffen sich mit datenschutzfreundlichen und innovativen Angeboten einen Wettbewerbsvorteil?

Wie lassen sich Datenschutz und Informationsfreiheit bei künstlicher Intelligenz und Big Data so einbinden, dass sie den Interessen von Wirtschaft und Gesellschaft gerecht werden?

Meines Erachtens schließen sich Datenschutz und künstliche Intelligenz (KI) oder Big Data keineswegs aus. Gerade KI muss nicht nur innovativ, sondern auch transparent und fair sein. Wie auch die Datenethikkommission in ihrem gerade veröffentlichten Abschlussbericht eindrucksvoll klargestellt hat, kann der Datenschutz hierfür ein wesentlicher Garant sein.

Mit dem Once-only-Prinzip ändern sich Rechtsvorschriften bei internen Verwaltungsverfahren. Inwieweit ist der Datenschutz hiervon betroffen und wie kann Once-Only datenschutzkonform ermöglicht werden?

Hier stehen mehrere datenschutzrechtliche Fragen im Raum. Im Wesentlichen muss aber zum einen sichergestellt werden, dass wir nicht zu einer übergreifenden Personenkennziffer kommen, unter der das komplette Leben der betroffenen Person erfasst und nachverfolgbar wird. Zum anderen müssen die Bürgerinnen und Bürger weiterhin den Überblick und die Kontrolle über ihre Daten behalten. In diesem Zusammenhang werden Lösungen wie beispielsweise das Datencockpit diskutiert.

Die Bundesregierung hat ihre Blockchain-Strategie vorgelegt. Darin geht ein Abschnitt dezidiert auf die Potenziale für die Verwaltung ein. Befasst sich Ihre Behörde auch mit dieser Technologie – welche Chancen, welche Hürden sehen Sie?

Die Blockchain-Technologie ist ein sehr spannendes Thema, dessen Bedeutung in der Zukunft noch weiter zunehmen könnte. Allerdings stehen wir aus datenschutzrechtlicher Sicht noch relativ am Anfang einer hochkomplexen Materie. Vor allem wird es darum gehen, wie bei einer solchen dezentralen und revisionssicheren Datenverarbeitung die Rechte zum Beispiel auf Löschung, Korrektur oder Auskunft umgesetzt werden können.

Welche Rolle spielen für Sie die öffentlichen IT-Dienstleister, wenn es darum geht, die Rechte und den Datenschutz der Bürger in einer immer digitalisierten Welt und einem entsprechenden Staatswesen zu gewährleisten?

Eine sehr große Rolle, da große Mengen sensibler personenbezogener Daten in der öffentlichen Verwaltung verarbeitet werden. Die hier eingesetzte IT muss in Sachen Datenschutz und Datensicherheit Maßstäbe setzen. Ich freue mich daher sehr, dass sich Vitako als Schnittstelle und Sprachrohr zu seinen Mitgliedern für das Thema Datenschutz starkmacht.

▲ MdB Elvan Korkmaz (SPD), Bundesdatenschutzbeauftragter Ulrich Kelber und Vitako-Vorstand Dr. Johann Bizer beim Vitako-Herbstempfang im Reichstag (von links) Fotos: Tobias Koch

Weniger Abhängigkeit

Vitako-Herbstempfang: Digitale Souveränität erfordert einen gemeinsamen europäischen Ansatz

Nachdem die Niederlande mit einer Datenschutzfolgenabschätzung zu Windows 10 und Office 365 die Debatte um Telemetrie-Daten ins Rollen gebracht hatten, konnte der Datenschutz für die niederländischen Regierungsbehörden verbessert werden. Erneute Datenschutzfolgenabschätzungen ermöglichen den Niederlanden nun den Einsatz von Windows 10 und Office 365 ProPlus. Für Office Online und die mobilen Office-Apps gibt es aber bisher keine Entwarnung. Das niederländische Justizministerium und der europäische Datenschutzbeauftragte luden Vertreter europäischer Regierungs- und EU-Behörden sowie internationaler Organisationen zu einer Tagung nach Den Haag. Auch Vitako war vor Ort. Es wurde deutlich, dass die niederländische Lösung nur der erste Schritt sein kann und dass es eines gemeinsamen Ansatzes bedarf, um sich gegenüber den großen Software-Herstellern zu positionieren.

Der Bund wird aktiv

In Deutschland wurden die mit Microsoft bestehenden Verträge Anfang des Jahres verlängert. Für die Zeit danach sucht das Bundesinnenministerium (BMI) aber nach Alternativen und hat auch aufgrund der von ihm beauftragten Studie (siehe Beitrag auf der gegenüberliegenden Seite) bekannt gegeben, diese Abhängigkeit verringern zu wollen und sich bei der Suche nach Alternativen mit den Ländern und der Europäischen Union abzustimmen.

Beim Vitako-Herbstempfang stand das Thema ebenfalls im Mittelpunkt. Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit, Ulrich Kelber, betonte in seinem Vortrag, dass die digitale Souveränität des Staates Voraussetzung ist für die informationelle Selbstbestimmung der Bürger. Vitako-Vorstand Johann Bizer warnte eindringlich vor der hohen Abhängigkeit von einzelnen Software-Herstellern und besonders vor der Verlagerung sensibler Daten zu außereuropäischen Cloud-Anbietern. Die Bundestagsabgeordnete Elvan Korkmaz (SPD) bezeichnete Vitako als den „zentralen Ansprechpartner in allen Fragen des Einsatzes von Informationstechnik im kommunalen Sektor“.

Alternative Open Source

Immer häufiger wird über Open-Source-Lösungen für die Verwaltung nachgedacht. Die Diskussion, wie die breitere Nutzung von Open-Source-Software vorangebracht werden kann, ist inzwischen auf allen Ebenen angelaufen. In der der Vitako-Facharbeitsgruppe „Windows 10“ berichtete Thomas Bönig, IT-Referent der Stadt München, von den Erfahrungen bei der Umstellung auf Open-Source-Software. Zwar wurde das Projekt vor einigen Jahren wegen verschiedener Schwierigkeiten beendet, dennoch sind noch immer viele Open-Source-Lösungen in Verwendung. Thomas Bönig warnte davor, einen vollständigen Umstieg als einzelne Kommune zu stemmen, und plädierte stattdessen für Initiativen auf Bundes- oder europäischer Ebene.

Föderale und europäische Zusammenarbeit

Entscheidend ist nun, dass konkrete Ziele formuliert und mit deren Umsetzung begonnen wird. Der Prozess, um die beschriebenen Abhängigkeiten zu lösen, wird mehrere Jahre andauern – insbesondere, wenn eigene Lösungen entwickelt werden sollen. Dabei müssen alle föderalen Ebenen zusammenarbeiten, auch der Austausch mit anderen europäischen Ländern ist wichtig. Die kommunalen IT-Dienstleister werden diesen Prozess weiter mit ihrem Fachwissen begleiten.

Der Autor Daniel Sieberath ist Referent für Informationsmanagement bei Vitako.

Koordiniertes Auftreten

Eine Studie zeigt Wege zu mehr digitaler Souveränität

Angesichts der Digitalisierung setzen sich Behörden zunehmend mit ihrer digitalen Souveränität auseinander. Welche Abhängigkeiten zu Technologieanbietern und Probleme mit Vernetzung und Datenaustausch bestehen?

Eine strategische Marktanalyse von Strategy& im Auftrag des Bundesministeriums des Innern, für Bau und Heimat ergab, dass die Bundesverwaltung in allen Schichten des Software-Stacks stark von wenigen Software-Anbietern abhängig ist. Diese Abhängigkeit resultiert in kritischen Schmerzpunkten, insbesondere in den Bereichen Informationssicherheit und Datenschutz.

Um die strategischen IT-Ziele des Bundes zu erreichen, müssen die in der Studie aufgezeigten Schmerzpunkte entlastet werden. Die Analyse identifiziert vier führende Strategien, die auch parallel verfolgt werden können.

1. Ein wichtiger Ansatzpunkt für die digitale Souveränität ist die Schaffung von Rahmenbedingungen. So können beispielsweise Architekturrichtlinien Vorgaben für die weitere Entwicklung der Software-Landschaft bilden und eine Verstärkung von Abhängigkeiten verhindern.

2. Eine weitere Strategie ist das Verhandeln mit Anbietern. Schmerzpunkte können potenziell durch Zugeständnisse reduziert werden, die zugrunde liegende Abhängigkeit bleibt jedoch bestehen.

3. Zusätzlichen Spielraum bietet die Möglichkeit der Diversifizierung mit proprietärer Software. Problematisch hierbei ist jedoch, dass entweder bewusst eine Abhängigkeit mit einem weiteren Anbieter eingegangen wird oder in der Eigenentwicklung erhebliche Investitionen notwendig sind.

4. Als vierte strategische Option wurden der Aufbau und Einsatz von OSS-Alternativen identifiziert. Die Analyse vergleichbarer Vorhaben fand viele Beispiele zur Machbarkeit solcher Lösungen, sofern gewisse Erfolgsfaktoren berücksichtigt werden. Behörden können auf bestehende OSS-Anwendungen mit umfangreichen Funktionalitäten zurückgreifen, die notwendigen Wartungs- und Anpassungsaufgaben müssen entweder durch die IT-Dienstleister selbst oder die Steuerung externer Dienstleister durch diese übernommen werden. In vielen Fällen ist hierfür eine Anpassung von Strukturen und der Aufbau zusätzlicher Kompetenzen notwendig.

Die Übertragbarkeit der Ergebnisse auf die kommunale Ebene ist im Einzelfall zu prüfen. Hierzu müssten zunächst individuell Toleranzen festgelegt werden, um in der Folge einzelne Abhängigkeiten sowie ihre Kritikalität als Ausgangslage zu analysieren. Gegebenenfalls müssten darauf aufbauend Handlungsfelder und Maßnahmen erarbeitet werden, um die eigene digitale Souveränität sicherzustellen. Der Austausch über alle Verwaltungsebenen ist hierbei wichtig, um von Erfahrungen zu lernen sowie ein koordiniertes gemeinsames Auftreten zu ermöglichen.

◀ Frederik Blachetta ist Director bei Strategy&, der Strategieberatung von PwC, und berät Klienten aus dem öffentlichen Sektor zu digitaler Transformation und IT-Strategie.

Die von der PwC Strategy& im Auftrag des BMI durchgeführte „Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern“ kann hier heruntergeladen werden: https://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2019/20190919_strategische_marktanalyse.html

Genossenschaft govdigital gründet sich

Öffentliche IT-Infrastrukturen für neue Technologien und digitale Daseinsvorsorge

Am 12. Dezember 2019 wird sich in Berlin die durch kommunale und öffentliche IT-Dienstleister getragene Genossenschaft govdigital gründen. Sie will neue Technogien auf Basis digitaler Infrastrukturen in öffentlicher Hand vorantreiben – und anderen Gebietskörperschaften zur Verfügung stellen.

Einer der Arbeitsschwerpunkte der govdigital eG ist, das Potenzial der Blockchain-Technologie für die Zusammenarbeit von Verwaltungs- und Identifikationsvorgängen auszuloten. In der Vergangenheit war deshalb häufiger von einer „Blockchain-Genossenschaft“ beziehungsweise von „govchain“ die Rede. Der Ansatz der Genossenschaft ist jedoch breiter und technologieoffener – das spiegelt sich auch im neuen Namen govdigital. Die Genossenschaft wird neue Entwicklungen aufgreifen und für Kommunen, Länder und Bund nutzbar machen. Im Sinne einer digitalen Daseinsvorsorge für öffentliche Verwaltungen und andere öffentliche Institutionen wird eine sichere und verbindliche bundesweite Kommunikation gewährleistet werden.

Idee zur Reife gebracht

An der konzeptionellen Vorbereitung der govdigital eG hat etwa ein Dutzend kommunale IT-Dienstleister mitgewirkt. Die zunächst lockere Idee wurde im Kreis interessierter Vitako-Mitglieder weitergedacht und in den vergangenen Monaten konkretisiert. In kleiner Runde konnten komplexe Themen zügig vorangebracht und in einen passenden institutionellen Rahmen gegossen werden. Das Modell einer Genossenschaft ist dafür ideal: Die Mitglieder begegnen sich auf Augenhöhe, gleichzeitig können neue Interessenten jederzeit hinzustoßen – bei geringem bürokratischen und finanziellen Aufwand.

Neun Gründungsmitglieder

Zu den bisherigen Gründungsmitgliedern (mit Genossenschaftsanteilen) zählen nach aktuellem Stand zum Redaktionsschluss Mitte November die AKDB, Dataport, ekom21, regio iT, SIT, krz Lemgo, KDO, Governikus sowie die vom Bund getragene Bundesdruckerei. Die Genossenschaft ist damit gleichermaßen kommunal und öffentlich geprägt – weitere kommunale Akteure befinden sich noch in der Entscheidungsphase. Für die Zukunft wird mit weiteren Interessenten gerechnet.

Geschäftsräume in Berlin

Vitako hat diesen Prozess von Beginn an begleitet und wird mit der neuen Genossenschaft eng verbunden sein. Auch räumlich: die govdigital bezieht am 12. Dezember ein Büro in der Vitako-Geschäftsstelle in Berlin-Mitte und nimmt dort ihre Geschäftstätigkeit auf. Auf diese Weise können gerade in der Gründungsphase Ressourcen geteilt und Synergien erzielt werden.

Blockchain-Strategie der Bundesregierung

Die Bundesregierung hebt in ihrer „Blockchain-Strategie“ das bisherige kommunale Engagement zur Entwicklung der Blockchain für die öffentliche Hand hervor. Die kommunalen IT-Dienstleister freuen sich, mit der künftigen Genossenschaft den Auf- und Ausbau einer öffentlichen Infrastruktur voranzutreiben und die Zukunftstech-

Blockchain – eine Distributed-Ledger-Technologie

Blockchain ist eine der bekanntesten Distributed-Ledger-Technologien. Im Grundsatz werden damit beliebig viele gleichgestellte Kopien des Ledgers (etwa: Kassenbuch, Konto, Register) von unterschiedlichen Parteien dezentral unterhalten. Neu hinzugefügte Transaktionen werden in alle Kopien des Ledgers übernommen. Notwendig dafür ist eine Übereinkunft über den jeweils aktuellen Stand des Ledgers, den eben nur alle beteiligten Konten beziehungsweise Rechenzentren des Netzwerks gemeinsam geben können. Abweichungen fallen sofort auf und Manipulationen können erkannt und analysiert werden.

nologie für die Verwaltung zu entwickeln. Vitako bietet der Bundesregierung Erfahrungsaustausch und die weitere Beteiligung bei der Umsetzung ihrer Strategie an. Die Anerkennung der bisherigen Anstrengungen sollte künftig durch konkrete Fördermaßnahmen der Bundesebene unterlegt werden.

Sicheres Umfeld für Produkte und Aufgaben der Daseinsvorsorge

Die öffentliche Hand soll die Blockchain und weitere Technologien in einem sicheren Umfeld für Produkte und Aufgaben in der Daseinsvorsorge nutzen – so lässt sich der Zweck des govdigital-Modells zusammenfassen. Die notwendige Infrastruktur wie Server und Datenbanken soll in zertifizierten Rechenzentren zur Verfügung gestellt und betrieben werden. Auf Basis dieser Infrastruktur sollen dann auch Landes- und Bundeseinrichtungen Anwendungen für die öffentliche Hand entwickeln und anbieten können.

Blockchain(-Infrastruktur) as a Service

Konkret richtet sich das Angebot der govchain eG an Kommunen, Ämter und öffentliche Unternehmen. Applikationen bieten Behörden etwa die Möglichkeit, Echtheitsnachweise, Bescheinigungen und Abrechnungen einfacher und kostengünstiger durchzuführen. Mögliche konkrete Nutzungen sind die Validierung von Zeugnissen und Führerscheinen, Nachbarschaftsstrom-Verträgen oder rechtssichere Nachweise von Entsorgungswegen. Die Genossenschaft ist darauf ausgerichtet, verschiedene Services bereitzustellen. Das kann „Blockchain as a Service“ (BaaS) sein, ebenso wie die Durchführung von Transaktionen (Validierung) oder die Nutzung der Blockchain-Infrastruktur „Blockchain-Infrastruktur as a Service“ (BIaaS) für den Betrieb von Applikationen.

Für Anwendungen im öffentlichen Sektor ist es sinnvoll, dass die Distributed Ledger Technology nicht in einer allgemein verfügbaren Blockchain wie etwa Bitcoin oder Ethereum betrieben wird – sondern dass eine sichere Eigentümergemeinschaft existiert, sich also die Rechenknoten („Nodes“) im Besitz und der Verfügungsgewalt der öffentlichen Hand befinden. Im Rahmen dieser „Private Infrastructure“ können dann Anwendungen entwickelt und sicher betrieben werden. Wir halten Sie über die Gründung und die Arbeit der govdigital eG auf dem Laufenden!

GOVDIGITAL

◀ Dr. Ralf Resch ist Vitako-Geschäftsführer.

Gemeinsam smart

Kommunale Angebote verbessern sich zu langsam

Wie steht es um Smart Citys in Deutschland? Der Innovators Club des Deutschen Städte- und Gemeindebundes und der TÜV Rheinland führten unter den 500 größten deutschen Städten einen „Smart City Readiness Check“ durch.

▲ Alexander Handschuh ist Sprecher des Deutschen Städte- und Gemeindebundes.

▲ Gürkan Ünlü ist Senior Vice President von TÜV Rheinland Consulting.

Das Fundament hat Lücken

Leistungsstarke Breitbandverbindungen sind der Schlüssel zur Wettbewerbsfähigkeit von Städten und Gemeinden. Gerade mit Blick auf den Umbauprozess zu digitalen Städten und Regionen werden bereits in wenigen Jahren Breitbandgeschwindigkeiten im Gigabit-Bereich zwingend notwendig sein. Derzeit fehlt es allerdings in vielen Kommunen noch an einer flächendeckenden, leistungsstarken Infrastruktur. Jede fünfte der im Rahmen des „Smart City Readiness Check“ befragten Kommunen weist noch Lücken in der Versorgung auf. Zudem fehlt in mehr als der Hälfte der Städte ein flächendeckendes WLAN-Netz. Obwohl offenkundig noch immenser Ausbaubedarf besteht, gab jede dritte Kommune an, sich nicht am Bundesförderprogramm für den Breitbandausbau zu beteiligen. Dies zeigt, dass Ausrichtung und Abwicklung der Förderprogramme noch Optimierungspotenzial aufweisen. Vielfach sind Städte und Gemeinden auf qualifizierte Beratung angewiesen, um Förderprogramme nutzen zu können.

Lebensqualität statt Stau

Besonders im Bereich der Mobilität können digitale Lösungen dazu beitragen, den Verkehr in den Kommunen zu reduzieren, Schadstoffbelastungen zu vermeiden und somit die Lebensqualität zu verbessern. Gerade die Vermeidung des Parkplatzsuchverkehrs kann die Verkehrsbelastung deutlich reduzieren. Allerdings setzen nach den Ergebnissen des „Smart City Readiness Check“ bislang lediglich 14 Prozent der befragten Kommunen Apps ein, die freie Parkplätze im Stadtgebiet anzeigen. Auch Angebote zum Online-Erwerb von Fahrscheinen für den öffentlichen Personennahverkehr sind bislang bei lediglich 60 Prozent der Kommunen verfügbar. In nur rund einem Drittel der Kommunen werden digitale Lösungen zur Verkehrssteuerung eingesetzt. Positiv ist hingegen, dass das Thema „Sharing“ in den Kommunen angekommen ist. In mehr als 70 Prozent der Städte stehen Car-Sharing-Angebote zur Verfügung, rund ein Drittel bietet Bike-Sharing-Angebote an und in immerhin jeder zehnten Kommunen werden gemeinsame Fahrten über Ride-Sharing-Angebote organisiert.

Effizienter Bürgerservice

Heute erwarten Bürgerinnen, Bürger und Gewerbetreibende von ihrer Stadt oder Gemeinde ähnliche Online-Serviceangebote wie es sie in anderen Bereichen im Netz bereits gibt. Wer Flüge online bucht oder über Kontinente hinweg Videotelefonate führt, hat wenig Verständnis für eine Verwaltung auf dem Stand vor 50 Jahren. Digitale Verwaltungsdienstleistungen sind daher ein wichtiger Baustein einer digitalen Stadt oder Gemeinde. Der „Smart City Readiness Check“ zeigt gerade in diesem Bereich Nachholbedarf. Rund 30 Prozent der befragten Städte und Gemeinden bieten bislang wenig oder gar keine Online-Services für ihre Bürgerinnen und Bürger an. Noch schlechter sieht es bei den Unternehmensdienstleistungen aus. Hier halten mehr als die Hälfte der befragten Kommunen keine Angebote vor. Auch die Kommunikation innerhalb der Verwaltungen hat den Sprung ins digitale Zeitalter noch nicht vollzogen. Intern sind E-Mails und Telefon die favorisierten Kommunikationsmittel. Nur knapp jede zweite Kommune nutzt bereits Cloud-Lösungen, um Daten zentral abzulegen. Schließlich ist es auch um die Fortbildungsangebote für Mitarbeiterinnen

und Mitarbeiter noch nicht gut bestellt. Rund 75 Prozent aller Kommunen bieten Fortbildungen im Bereich Digitalisierung unregelmäßig oder gar nicht an. Für die Kommunen ist also im Bereich E-Governance noch einiges zu tun.

Smarte Gebäude und Vernetzung

Auch bei Energieerzeugung und -verbrauch können digitale Technologien einen wichtigen Beitrag dazu leisten, Kommunen fit für die Zukunft zu machen. Das Energiesystem der Zukunft setzt auf regenerative Energieträger. Um diese sinnvoll zu nutzen und eine sichere Versorgung zu gewährleisten, ist eine intelligente Vernetzung von Erzeugung und Verbrauch ebenso notwendig wie ein Ausbau der Netze und eine Steigerung der Energieeffizienz.

Besonders beim Einsatz von digitalen Technologien für mehr Energieeffizienz sind die Kommunen bereits heute vergleichsweise gut aufgestellt. Mehr als 30 Prozent der kommunalen Gebäude verfügen bereits über smarte Technologien, etwa intelligente Steuerungstechnik oder Instrumente zur Erfassung und Auswertung des Energieverbrauchs. Auch der Einsatz (meist) smarter LED-Technologien schreitet schnell voran: Knapp die Hälfte der Straßenbeleuchtung in den befragten Kommunen ist bereits heute damit ausgestattet.

Geschwindigkeit und Vernetzung fehlen

Die Ergebnisse des „Smart City Readiness Check“ in den ausgewählten Sektoren zeigen, dass auf dem Weg zu digitalen Städten und Regionen allenfalls ein erster Schritt gemacht wurde. Die Kommunen müssen die Digitalisierung mit mehr Entschlossenheit und mehr Geschwindigkeit angehen, um Schritt zu halten.

Der „Smart City Readiness Check“ erfasst die digitalen Fortschritte innerhalb einzelner Sektoren und bezogen auf Einzelmaßnahmen. Wirkliche Mehrwerte für Bürgerinnen, Bürger und Unternehmen entfalten digitale Städte und Regionen allerdings erst dann, wenn es gelingt, bislang getrennt voneinander agierende Sektoren einer Stadt miteinander digital zu vernetzen. Dazu bedarf es vor allem der Mitwirkung aller Akteure der Stadtgesellschaft. Neben dem öffentlichen Sektor sind auch Wirtschaft und Zivilgesellschaft gefragt, an dem Zukunftsprojekt Smart City mitzuwirken.

Die Basis digitaler Städte und Regionen ist die intelligente Vernetzung von Daten aus Sektoren, die zuvor getrennt agierten. Das Herzstück solcher Konzepte bildet eine Datenplattform, auf der die Informationen zusammenlaufen und miteinander verknüpft werden können. In dieser Konzeption sind die unterschiedlichen Akteure vor Ort von entscheidender Bedeutung. Erst wenn es gelingt, Daten aus der öffentlichen Verwaltung, den kommunalen Unternehmen, der Privatwirtschaft und der Zivilgesellschaft verfügbar zu machen und miteinander zu neuen Anwendungen und Lösungen zu verknüpfen, können echte Mehrwerte entstehen. Dabei geht es nicht um personalisierte Daten oder Informationen, die einer Person zugeordnet werden können. Interessant sind aber beispielsweise die Daten, die im Bereich der Energieeffizienz oder des Energieverbrauchs gewonnen werden. Sie können einen Beitrag zu einem intelligenten Energiesystem der Zukunft leisten. Der Fortschritt auf dem Weg zu „Smart Citys“ wird derzeit in einer Neuauflage der Befragung erhoben.

Serie: ARBEITSMARKT UND QUALIFIZIERUNG IN DER KOMMUNALEN IT
Teil 1: Qualifizierter Nachwuchs – Blick auf die Hochschulen
Teil 2: Aus- und Weiterbildung in der kommunalen IT
Teil 3: Neue Wege beim Recruiting
Teil 4: Blick in die Zukunft – Qualifikationen 2029

Die Public Sector IT braucht kompetente Köpfe, die Lösungen entwickeln und umsetzen. In der Jahresserie geht Vitako aktuell der Frage nach, wie Verwaltungen und IT-Dienstleister ihren Fachkräftebedarf gegenwärtig und in der Zukunft sichern. Die Arbeits- und Wirtschaftssoziologin Dr. Catharina Schmalstieg über die Aufgaben der Verwaltung in zehn Jahren – und wie man sich heute darauf vorbereiten sollte.

Weichenstellung

Gezielte Qualifizierung für die Verwaltung von morgen

Wie könnte die öffentliche Verwaltung 2029 aussehen? Vielleicht so: Vieles wird online erledigt und Termine für persönliche Beratungen werden telefonisch oder per Mail vereinbart. Beschäftigte, die früher viel Zeit auf die manuelle Eingabe von Daten verwenden mussten, haben nun mehr Zeit für die Beratung. Digitale Kommunikationstechnologien haben die Potenziale des Gemeinwesens erweitert und es gibt neue digitale Angebote. Kommunale IT-Dienstleister und Landesrechenzentren bieten Bürgerinnen und Bürgern eigene Cloud-Spaces und -Dienste an. Dank digitaler Souveränität können diese mit Datensicherheit und Datenschutz punkten.

Zurück im heute – 2019: Die Versprechen der Digitalisierung, öffentliche Dienstleistungen für Bürgerinnen und Bürger einfacher verfügbar zu machen und zugleich die Arbeitsprozesse für Beschäftigte einfacher und besser zu gestalten, sind noch nicht eingelöst. Öffentliche Dienstleistungen digital anzubieten, erfordert das Mitwirken der Beschäftigten. Die im Onlinezugangsgesetz (OZG) und andernorts gesteckten Ziele können nur erreicht werden, wenn Beschäftigten eine Perspektive geboten wird, sie beteiligt werden und ihr Know-how in den Veränderungsprozess einbringen können. Denn man verfolgt ein Ziel am ehesten motiviert, wenn man selbst beteiligt ist und die eigene Handlungsfähigkeit erhalten bleibt.

Weiterbildung für die Zukunft

Die Automatisierung von Verwaltungsverfahren und der Einsatz von künstlicher Intelligenz verändern Arbeitsabläufe und -inhalte der öffentlichen Verwaltung. Viele Tätigkeiten sind vollständig oder teilweise automatisierbar. Bisherige Aufgaben werden wegfallen, neue Tätigkeiten und Qualifikationsprofile werden entstehen. Beschäftigte fragen sich, wie sie durch diesen Wandel kommen. Hier stehen wir gemeinsam vor der großen Aufgabe, Angebote für die Qualifizierung, Fortbildung und auch Umschulung und Zweitausbildung zu entwickeln. Eine gewaltige Herausforderung, weil aktuell niemand genau sagen kann, welche Qualifikationen gefordert sein werden. Die öffentlichen Arbeitgeber müssen diesen Wandel besser vorbereiten und begleiten, damit sich alle auf den Weg zu einem Öffentlichen Dienst der Zukunft machen können und es am Ende keine Digitalisierungsverlierer gibt. Im Oktober hat die stellvertretende ver.di-Vorsitzende Christine Behle bei der Sitzung des IT-Planungsrats vorgestellt, wie ein Tarifvertrag die anstehenden Veränderungen begleiten und absichern könnte.

IT-Fachkräfte sind von diesen Entwicklungen in besonderer Weise betroffen. Sie schreiben Code für Schnittstellen, Programme für Online-Verfahren, sie richten Netzwerke ein und managen sie, setzen Blockchains auf, sorgen für IT-Sicherheit und Controlling, setzen neue Verfahren um und unterstützen Anwenderinnen und Anwender. Ihre Aufgaben befinden sich im Wandel – dazu kommt als weitere Herausforderung der anhaltende Fachkräftemangel, der sich künftig zuspitzen wird, da viele in den Ruhestand eintreten werden.

Anforderungen an IT-Fachkräfte wachsen

Für IT-Fachleute werden das Arbeitsvolumen und die Arbeitsanforderungen zunehmen. Neben dem unabdingbaren IT-Grundwissen werden weitere Kenntnisse gefragt sein, etwa Projektmanagement, Planungs-Know-how, Beratungs- und Betreuungskompetenzen. Für die Bereitstellung der digitalen Daseinsvorsorge brauchen IT-Fachleute auch ethische, juristische und politische Urteilskraft. Darauf muss die Aus- und Weiterbildung abgestellt werden. Bei der Entwicklung von Software müssen die Nutzergruppe der Bürgerinnen und Bürger, aber auch die kommunalen Beschäftigten als Gruppe von Anwenderinnen und Anwender berücksichtigt werden. Dabei sind Software-Ergonomie, Arbeitnehmerdatenschutz und Wahrung von Persönlichkeitsrechten als Kriterien zu benennen, die gute digitale Arbeit und damit auch gute Erfahrungen in der Anwendung der Programme und Fachverfahren ermöglichen.

Dem Fachkräftemangel im IT-Bereich versuchen die kommunalen Arbeitgeber auf unterschiedlichen Wegen zu begegnen. Sie setzen weiter auf Ausbildung im eigenen Haus: Klassisch als Ausbildung im kommunalen IT-Betrieb, in einigen Stadtverwaltungen wird seit Kurzem auch der duale Studiengang Verwaltungsinformatik angeboten. Darüber hinaus bieten einige kommunale IT-Dienstleiter in Kooperation mit Fachhochschulen berufsbegleitende Studiengänge an, in denen sich die Beschäftigten weiterbilden oder Verwaltungsfachangestellte einen weiteren Berufsabschluss erwerben können. Die individuelle Qualifizierung beeinflusst wesentlich Zukunftschancen, berufliche Mobilität und berufliche Perspektiven der Mitarbeiterinnen und Mitarbeiter. Berufsbegleitende Weiterbildungen und Inhouse-Schulungen können auch geeignete Angebote für die Qualifizierung von Quereinsteigerinnen sein.

Der genaue Qualifizierungsbedarf ist noch unklar

Derzeit liegen für den öffentlichen Dienst keine Forschungsergebnisse vor, die über eine Beschreibung der Umbrüche hinausgehen. Konkret fehlen Analysen, die Grundaussagen zu Qualifikationsanforderungen für die Arbeit im öffentlichen Dienst der Zukunft vornehmen. Es ist zu begrüßen, dass der amtierende Vorsitzende des IT-Planungsrats, Henning Lühr, eine Qualifizierungsoffensive fordert und der IT-Planungsrat erste Weichen für eine wissenschaftliche Untersuchung der Veränderungen von Arbeit und Qualifikation gestellt hat. Der Weg in einen modernen öffentlichen Dienst kann nur gelingen, wenn die Auswirkungen von Automatisierung auf Arbeitsorganisation und -abläufe bekannt sind und gestaltet werden können.

Dr. Catharina Schmalstieg leitet den Bereich Kommunalpolitik und Digitalisierung öffentlicher Dienst beim Bundesvorstand der Vereinten Dienstleistungsgewerkschaft – ver.di.

Was macht eigentlich … die IBM 360/30?

Die Zentraleinheit hatte einen Hauptspeicher von 32 Kilobyte, hinzu kamen drei Platteneinheiten, ein Lochkartenleser, der immerhin mit 30.000 Karten pro Stunde fertig wurde, ein Lochkartenstanzer und ein Lochstreifenleser sowie Drucker, Steuereinheiten und Konsolenschreibmaschinen, nicht zu vergessen die Sortiermaschine. So sah anno 1968 eines der modernsten kommunalen Rechenzentren der Bundesrepublik aus, es stand in Moers. Der Rechner, ein IBM System 360/30, war mit seinen 80.000 Instruktionen pro Sekunde für seine Zeit rasend schnell. Auch VW in Wolfsburg setzte das System für die elektronischen Datenverarbeitung ein.

IBM beherrschte damals den Computermarkt und stellte mit der Baureihe S/360 erstmals ein einheitliches und leicht erweiterbares System vor. Die Entwicklungskosten betrugen über fünf Milliarden Dollar, den zweifachen Jahresumsatz von IBM aus 1962. Doch sie sollten sich rechnen: das S/360 entwickelte sich zum Dauerbrenner, noch in den achtziger Jahren machte es die Hälfte des Firmenumsatzes aus. Eingesetzt wurde es im kommunalen Bereich vor allem, um Steuern und Abgaben zu berechnen. Einen Markt für kommunale Software gab es damals noch nicht, sodass diese meist in den Programmiersprachen COBOL oder FORTRAN selbst geschrieben werden musste. Aber dann ratterte die S/360 los. Ein originales Exemplar dieses Rechen-Dinosauriers steht heute im Deutschen Technikmuseum München.

Helmut Merschmann

Branchenticker

Der wöchentliche Newsletter mit aktuellen Branchenmeldungen. Jeden Freitag frisch vom Vitako-Redaktionsteam. Hier abonnieren: **www.vitako.de/abonnements**

Nationaler Pakt

Auf dem Digitalgipfel in Dortmund ist Ende Oktober der „Nationale Pakt Cybersicherheit“ offiziell gestartet. Das Vorhaben soll den Rahmen bilden für eine bundesweit bessere Vernetzung der Akteure aus dem Bereich der Cybersicherheit. Zudem sollen gute Lösungen und Angebote für mehr Cybersicherheit in Deutschland im Sinne von Best Practice einer breiten Öffentlichkeit zugänglich gemacht werden. In der ersten Projektphase des Nationalen Paktes werden möglichst alle Beteiligten und ihre Beiträge auf der Basis einer systematischen Erhebung erfasst. Ziel ist es, die Ergebnisse in ein Gesamtbild der IT-Sicherheitsaktivitäten münden zu lassen – in ein „Online-Kompendium Cybersicherheit“.
https://bit.ly/34tw0SU

Föderale Digitalisierungsarchitektur

Vitako hat im Rahmen seiner OZG-Task-Force ein Positionspapier zur föderalen Digitalisierungsarchitektur veröffentlicht, das eine Übersicht zum faktischen Stand der föderalen IT-Architektur bietet. Das Papier unterstreicht die Bedeutung höchstmöglicher Standardisierung und die Festlegung von Architekturelementen bei der Umsetzung des Online-Zugangsgesetzes (OZG). Microservices und Container-Technologien sind dabei vorgesehen. Dabei bedarf es vor allem Interoperabilität und einer Vereinheitlichung von Schnittstellen unter Beibehaltung vorhandener Lösungen. Das Positionspapier skizziert den Phasenplan „föderale kommunale Digitalisierungsarchitektur“ und fordert dafür kommunale Governance ein.
https://bit.ly/36wbAdS

Jahresbericht vorgelegt

Der Nationale Normenkontrollrat (NKR) hat seinem Jahresbericht 2019 zehn Kernbotschaften vorangestellt. Darin äußert sich das Gremium auch zum Online-Zugangsgesetz (OZG). Das OZG werde nur Erfolg haben, wenn Online-Leistungen gut ankommen und die Nutzerzahlen steigen. Notwendig sei die Klärung der Datenschutzfrage bis Ende des Jahres, da davon viele weitere Schritte abhängen. Auch die Nachnutzung sei noch nicht geklärt. Während die Bereitschaft zur Zusammenarbeit zwischen Bund und Ländern sich ständig ausweite, sei ein Erfolg des OZG noch nicht garantiert. Die strukturellen Defizite, die Deutschland bei der Digitalisierung seiner Verwaltung über Jahre hinweg aufgebaut habe, seien groß.
https://bit.ly/33qShQU (PDF)

Köpfe & Technik

In unserer Rätselreihe beschreiben wir jeweils eine Person, die für (mindestens) eine bedeutende technische Neuerung verantwortlich ist. **Erraten Sie, um wen es diesmal geht?**

Sie war von Jugend an technikbegeistert, studierte Mathematik und Physik in Vassar und Yale, erschuf wichtige Meilensteine der Computergeschichte und war so unentbehrlich, dass die US-Marine sie zwei Mal (!) aus dem Ruhestand holte und erst mit 80 Jahren im Rang eines Flottillenadmirals entließ. Anekdotische Bekanntheit verschafften ihr allerdings nicht ihre bedeutenden Erfindungen, sondern ausgerechnet zwei Bugs, was bekanntlich „Programmfehler“ oder „Insekt“ bedeuten kann. Der erste Bug findet sich im Logbuch ihrer Forschungsgruppe: Ein Klebstreifen fixiert eine Motte, die den Ausfall eines Computerrelais verursachte. Begleitnotiz: „Ersten tatsächlichen Bug gefunden.“ Sie trug zur Bedienungsfreundlichkeit von Computern bei, indem sie den ersten Compiler entwarf, der englische, französische oder deutsche Anweisungen verstand und daraus ein lauffähiges Programm erzeugte. Sie wirkte maßgeblich an der Entwicklung einer Programmiersprache mit, die an die natürliche Sprache angelehnt und bis heute in Gebrauch ist. Diese Arbeit war Ursache des zweiten (weitaus bekannteren) Bug ihrer Karriere: den Millennium-Bug, aufgrund dessen für den Jahreswechsel 1999/2000 eine globale Technik-Apokalypse befürchtet wurde – die jedoch ausblieb.

Wer war’s?

Die Auflösung finden Sie unter dem Impressum auf Seite 4.

▲ Sibylle Mühlke ist freiberufliche Texterin und Autorin u. a. für IT-Themen.

Vitako intern

Vitako intern ist unser E-Magazin, das über aktuelle IT- und E-Government-Themen informiert – aus der Binnenperspektive der kommunalen IT-Dienstleister. Unser PDF-Magazin erscheint alle zwei Monate und präsentiert spannende Berichte aus der Welt der kommunalen IT. Das E-Magazin ist im E-Mail-Abonnement frei erhältlich.
www.vitako.de/vitakointern

In den letzten Wochen ging es Schlag auf Schlag. Vitako intern lässt Veranstaltungen, Berichte, Programme und die Statements aus der Politik Revue passieren. Vitako und seine Mitglieder beschäftigen sich bereits seit 2017 mit der Blockchain-Technologie – und begrüßen die nun veröffentlichte Blockchain-Strategie der Bundesregierung. Mitte Oktober veranstaltete Vitako einen Abendempfang und debattierte mit Entscheidern aus Politik, Wirtschaft und Verbänden. Das Bundesinnenministerium (BMI) will das wichtige Thema digitale Souveränität in den kommenden Jahren zu einem Schwerpunkt machen. Außerdem lesen Sie einen Bericht vom 2. Creative Bureaucracy Festival in Berlin, bei dem Vertreter von Behörden, Verbänden und Unternehmen über künftiges Verwaltungshandeln diskutierten. Der vom Deutschen Städte- und Gemeindebund initiierte „Innovators Club“ befasst sich mit strategischen – auch digitalen – Zukunftsthemen und traf sich zum 22. Deutschlandforum. Außerdem erfahren Sie mehr über die Interface, die gemeinsame Hausmesse der kommunalen IT-Dienstleister civitec, kdvz-Rhein-Erft-Rur und regio iT in Bergheim und außerdem stellen die Vitako-Mitglieder AKDB, dataport, citeq, ekom21, GovConnect, Governikus, krz und regio iT einige ihrer Leistungen vor.

AUSGABE 05 | 2019

BLOCKCHAIN-STRATEGIE
Kommunale Beteiligung

VITAKO-HERBSTEMPFANG
Zu Gast: Ulrich Kelber

DIGITALE SOUVERÄNITÄT
Gegen Abhängigkeiten

„DAS IST NETZPOLITIK“
Zur Rolle des Digitalkabinetts

OKTOBER-EVENTS
Smart Country & NEGZ

KOMMUNALE 2019
Nürnberg lockt Mitte Oktober

Die Bedeutung von interaktiven Tools und mobilen Anwendungen im E-Government nimmt ständig zu. Vitako stellt in jeder Ausgabe eine App für Bürgerinnen und Bürger vor und bewertet diese in verschiedenen Kategorien.

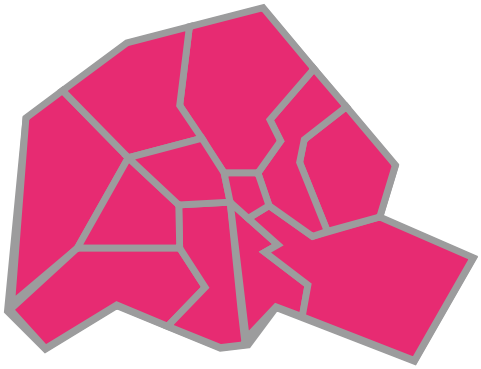
Bürgerapp „Mietenwatch“

Berliner Mietmarkt endlich greifbar

Nach immer lauter und breiter werdenden Protesten steht es nun fest: Die rot-rot-grüne Landesregierung in Berlin wird den Mietendeckel einführen. Das vom Bundesministerium für Bildung und Forschung und dem Prototype Fund geförderte Projekt „Mietenwatch“ versucht den Berliner Mietmarkt durch Datenauswertung und –visualisierung greifbarer zu machen.

Zweck

„Mietenwatch“ hat dafür seit April 2018 circa 80.000 Online-Wohnungsinserate mit Angaben unter anderem zu Nettokaltmieten, Nebenkosten sowie Ausstattung und Lage gesichtet. In drei Themenblöcken „Leistbarkeit“, „Wohnen als Ware“ sowie „Antworten“ werden die Bürgerinnen und Bürgern beispielsweise informiert, in welchem Bezirk sie sich mit ihrem Nettoeinkommen eine Wohnung leisten können oder wie sich die Einführung eines Mietendeckels oder die Vergesellschaftung privater Immobilienkonzerne auswirkt. Die Web-App analysiert dabei den Angebotsmietmarkt und nicht die Situation im Wohnungsbestand. Alte, bestehende Mietverträge sind nicht Teil der Datengrundlage.



Gestaltung/Bedienkomfort

„Mietenwatch“ lädt mit einem modernen Web-Design zum weiteren Stöbern ein. Die Navigation ist intuitiv gestaltet. Zudem bieten die interaktiven Karten einen schnellen Einstieg in die Materie und motivieren die Benutzerinnen und Benutzer zur weiteren Interaktion. Die sensiblen, individuell einstellbaren Daten wie etwa die eigene Nettoeinkommenshöhe werden mit großer Sorgfalt behandelt und nicht gespeichert. Nur die IP-Adresse wird vom Hoster maximal 30 Tage aufbewahrt.

Anwendbarkeit

„Mietenwatch“ trifft den Nerv der Zeit. Neben einfachen Datenvisualisierungen gibt es viele interaktive Karten. Eine Karte misst den Veränderungsdruck in den einzelnen Kiezen. Je höher der Anteil prekär lebender Bürgerinnen und Bürger ist und das Niveau der Angebotsmieten, desto höher ist laut „Mietenwatch“ der Verdrängungsdruck. Zudem liefert „Mietenwatch“ Informationen zu den größten Akteuren auf dem Berliner Mietmarkt und wie diese mit Wohnraum handeln.

Kompatibilität und Kosten

„Mietenwatch“ ist kostenlos und funktioniert derzeit als Web-App. Erreichbar ist sie unter **https://mietenwatch.de**

Nutzen	
Innovationsgrad	**5** • • • • •
Einbindung in den Verwaltungsprozess	-
Gestaltung	
Niedrigschwelliger Zugang	**5** • • • • •
Intuitive Bedienbarkeit	**5** • • • • •
Ansprechendes Design	**5** • • • • •
Mehrere Sprachen	**1** •
Fehlerfreie Bedienung	**5** • • • • •
Inhalte	
Informationsgehalt	**4** • • • •
Zielgruppenorientierung	**5** • • • • •
Partizipationsmöglichkeiten	**1** •
Aktualität und Pflege	**5** • • • • •
Kompatibilität und Kosten	
Verschiedene Betriebssysteme	–
Nutzung via Browser	**5** • • • • •
Kosten	**5** • • • • •
Open Source	**1** •

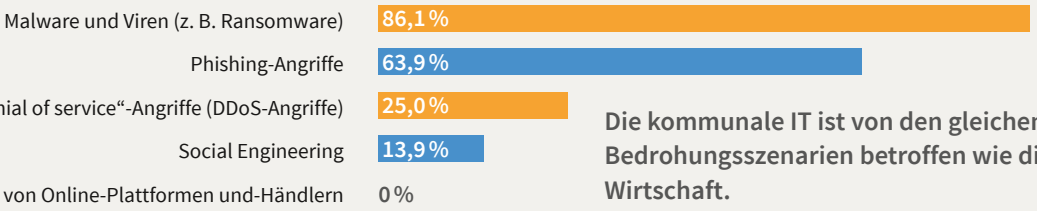
Notenstufen von 1 (schlecht) bis 5 (am besten)

◀ Monika Majer ist Mitarbeiterin des Fraunhofer-Instituts für Offene Kommunikationssysteme (FOKUS).

Vielfältige Anstrengungen

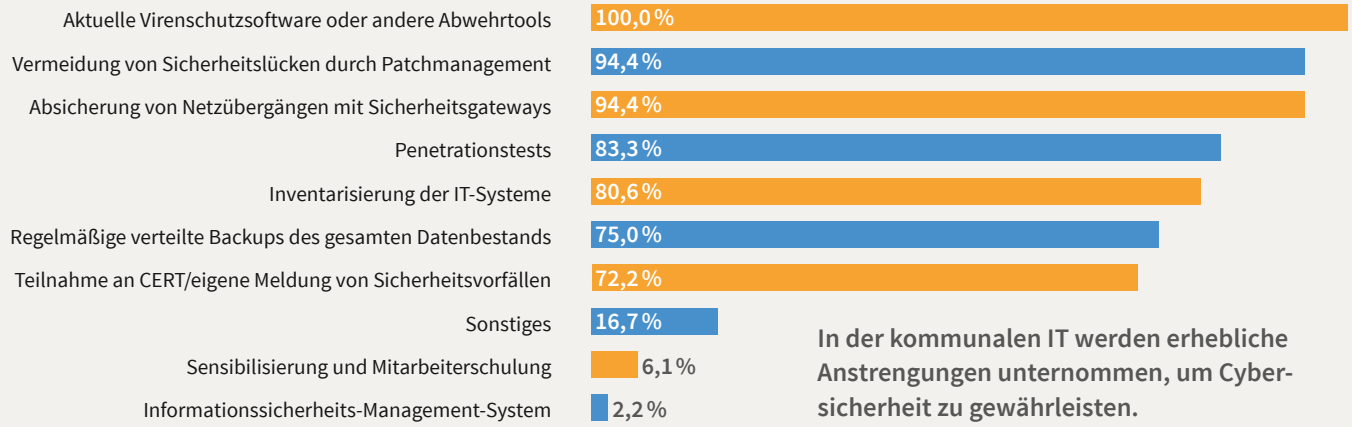
Cybersicherheit steht ganz oben auf der Agenda in der kommunalen IT. Wie beurteilen die Entscheider die aktuelle Situation und welche Schutzmaßnahmen werden getroffen?

1. Welches sind aktuell die beiden größten zu beobachtenden Bedrohungen in der kommunalen IT?



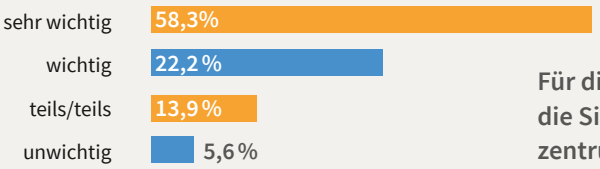
Die kommunale IT ist von den gleichen Bedrohungsszenarien betroffen wie die Wirtschaft.

2. Welche der folgenden Maßnahmen werden in Ihrem Unternehmen/Ihrer Verwaltung bereits umgesetzt, um die Cybersicherheit herzustellen bzw. aufrechtzuerhalten?



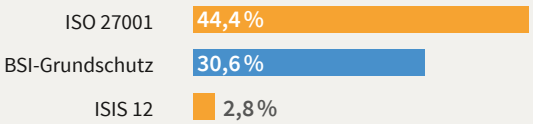
In der kommunalen IT werden erhebliche Anstrengungen unternommen, um Cybersicherheit zu gewährleisten.

3. Wie wichtig ist aus Ihrer Sicht die Sicherheitszertifizierung des Rechenzentrums (des eigenen bzw. des Rechenzentrums, in dem Ihre Daten gespeichert sind)?



Für die große Mehrheit der Befragten ist die Sicherheitszertifizierung des Rechenzentrums sehr wichtig oder wichtig.

4. Nach welchen der folgenden Standards ist Ihr Unternehmen/Ihre Verwaltung zertifiziert?



Über 40 Prozent der teilnehmenden Verwaltungen/Unternehmen sind bisher nicht zertifiziert. Bei den Zertifikaten ist ISO 27001 deutlich am stärkten verbreitet, gefolgt vom BSI-Grundschutz.

Vitako: Spotlight

„Datensouveränität ist höchstes Gebot“ – diese Überschrift stand mehrere Tage auf der offiziellen Internetpräsenz der Bundeskanzlerin. Ähnlich beim Bundeswirtschaftsministerium: „Wir brauchen eine eigene europäische Dateninfrastruktur!“ Beides signalisiert eines: Das Thema digitale Souveränität ist auf höchster Ebene angekommen. Die Frage dominierte Ende Oktober nicht nur den Digitalgipfel der Bundesregierung, sondern bestimmt aktuell ebenso zahlreiche Digitaldebatten. „Endlich!“, möchte man aus Sicht der kommunalen IT-Dienstleister erfreut ausrufen, um sogleich nachzulegen: Nun muss es auch an die Arbeit gehen. Es geht darum, die aktuelle Lage nicht nur richtig zu analysieren, sondern aktiv und vor allem gemeinsam vorzugehen, um Bürgern, Staat und Unternehmen tatsächlich mehr Möglichkeiten souveränen Handelns im Netz zu schaffen. Vitako und seine Mitglieder sind damit seit Langem befasst. Wir freuen uns über jegliche Mitstreiter, die sich diesem Ziel nun ebenso verpflichtet sehen – ausdrücklich dürfen sich auch Kommunen und Länder angesprochen fühlen.

ITKalender

5. Dezember 2019, Oldenburg – Plenum 2019 zum OZG

5. Dezember 2019, Berlin – KI-Camp

9. Dezember 2019, Frankfurt a. M. – IT-Tage 2019

25. – 26. März 2020, Halle/Saale –
8. Fachkongress des IT-Planungsrates

Mehr Informationen und Termine finden Sie im Vitako-ITKalender: www.itkalender.de

Die nächste „Vitako aktuell“ erscheint im März 2020.

HELDEN DER VERWALTUNG

№ 41

Immer einen Schritt voraus. Dank DIGITAL.Consulting

Smart City, Smart Region, Open Data. Die Digitalisierung wirft immer neue Fragen auf. Was ist Priorität Nummer eins? Was setze ich als Kommune um? Und wie? Zum Glück gibt es DIGITAL.Consulting! Das neue Beratungsangebot der AKDB.
Für Verwaltungshelden, die die Zukunft im Blick behalten.

Wer hat eigentlich gesagt, Verwaltung sei langweilig?

Mehr Helden auf www.akdb.de/helden

AKDB