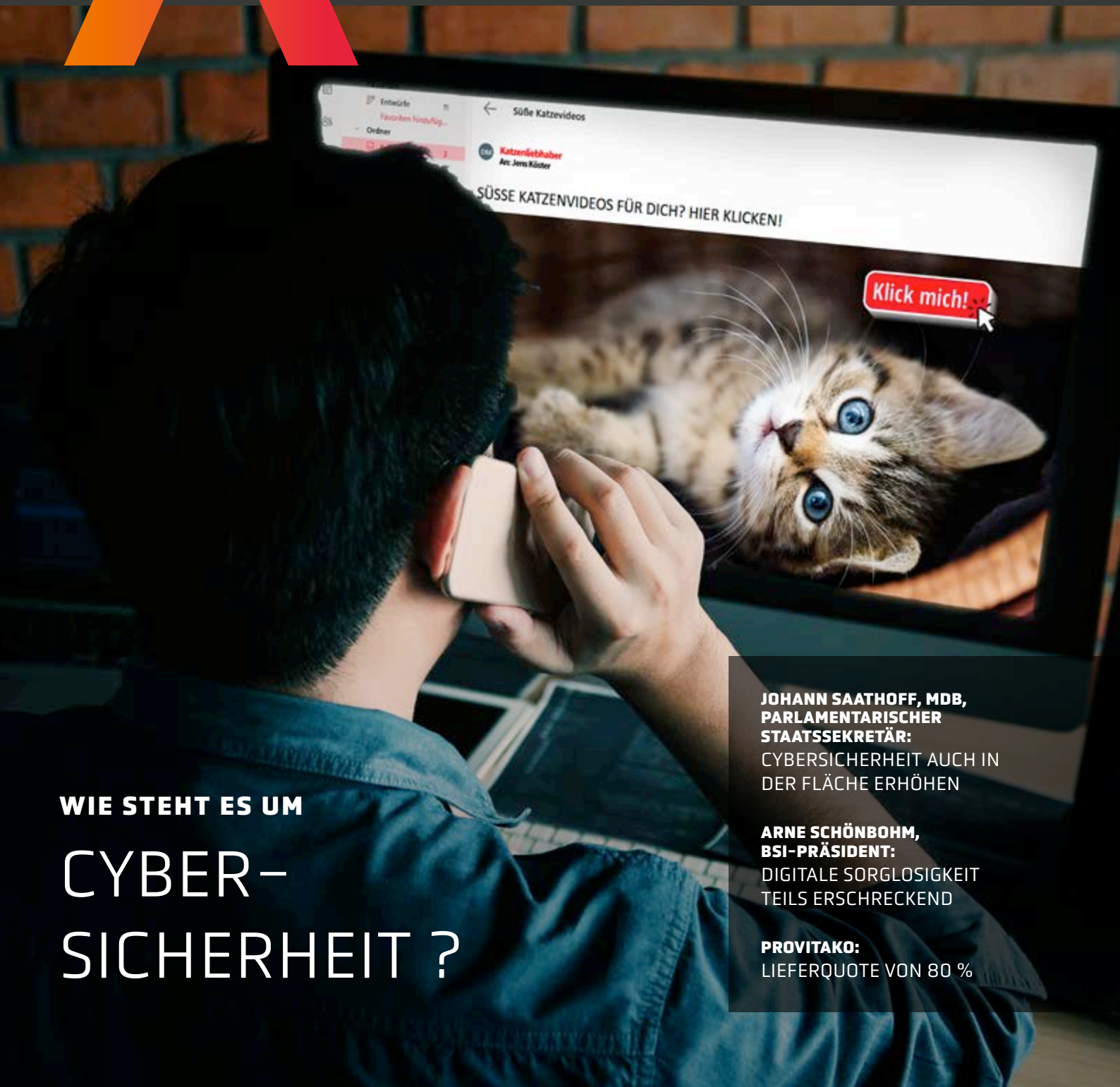
Zeitschrift der Bundes-Arbeitsgemeinschaft
der Kommunalen IT-Dienstleister e. V.

VITAKO AKTUELL

vitako.de

03|2022



WIE STEHT ES UM

CYBER-SICHERHEIT ?

JOHANN SAATHOFF, MDB, PARLAMENTARISCHER STAATSSEKRETÄR:
CYBERSICHERHEIT AUCH IN DER FLÄCHE ERHÖHEN

ARNE SCHÖNBOHM, BSI-PRÄSIDENT:
DIGITALE SORGLOSIGKEIT TEILS ERSCHRECKEND

PROVITAKO:
LIEFERQUOTE VON 80 %

VITAKO-STELLENMARKT

www.vitako.de/karriere

ALLE FREIEN STELLEN IN MITGLIEDSUNTERNEHMEN AN EINEM ORT.

Bei kommunalen IT-Dienstleistern entwickeln Sie die öffentliche IT der Zukunft in einer modernen, mitarbeiterbezogenen Arbeitsatmosphäre.

VON TRAINEE BIS IT-DIREKTOR: ATTRAKTIVE STELLEN IN DER KOMMUNALEN IT.

VITAKO

LIEBE LESERINNEN UND LESER,

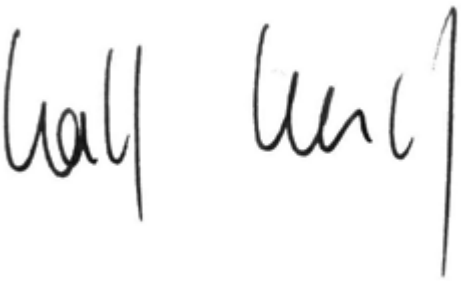
Anfang August 2022 mussten Deutschlands Industrie- und Handelskammern (IHK) ihre Websites vom Netz nehmen. Deutschlandweit. In diesem Moment ist noch unklar, wer die IHK attackiert hat, was das Motiv ist und wie lange es dauern wird, bis die IHK-Verbände ihre wichtigen Leistungen den tausenden Mitgliedsunternehmen wieder zur Verfügung stellen können. Was aber klar ist: Cyberattacken verwunden unsere Volkswirtschaft. Und sie bedrohen uns alle. Insbesondere dann, wenn Kommunen angegriffen werden, persönliche Daten ins Darknet gestellt werden und essenzielle Bürgerdienste schlagartig nicht mehr zur Verfügung stehen.

Es beunruhigt zutiefst, dass Deutschlands Verwaltung die notwendige Cybersicherheit aktuell nicht oder nur ungenügend gewährleisten kann. Dringend müssen strukturelle Themen angegangen werden, Stichworte lauten digitale Verwaltung als Kritische Infrastruktur (KRITIS), Verantwortlichkeit und Standardisierung. Es gibt das leidige Thema der Ressourcen. Mehr Sicherheit ist nicht zum Nulltarif zu haben. Und es gibt den Fakt, dass Cybersicherheit nach wie vor vielerorts auf die leichte Schulter genommen wird: Über 50 Prozent unserer Mitglieder berichten, dass politische Entscheider in den Kommunen Cybergefahren unterschätzen – allen Warnungen zum Trotz.

Mit der neuen VITAKO aktuell wollen wir dem etwas entgegensetzen und die Debatte befeuern. Im Interview beklagt BSI-Präsident Arne Schönbohm eine teils erschreckende Sorglosigkeit in der Verwaltung, wenn es um IT-Sicherheit geht. Johann Saathoff, Parlamentarischer Staatssekretär beim BMI, stellt die Position der Bundesregierung dar. Vom Deutschen Landkreistag betonen der stellvertretende Hauptgeschäftsführer Dr. Kay Ruge sowie der Referent Christian Stuffrein die Notwendigkeit einer ausreichenden Finanzierung, und Manuel Atug, Gründer der AG KRITIS, charakterisiert Cybersicherheit in letzter Konsequenz als Menschenschutz.

Mit diesem Heft wollen wir eine ebenso aktuelle wie facettenreiche Perspektive auf das Thema Cybersicherheit bieten – und das Thema vorantreiben.

Ihr

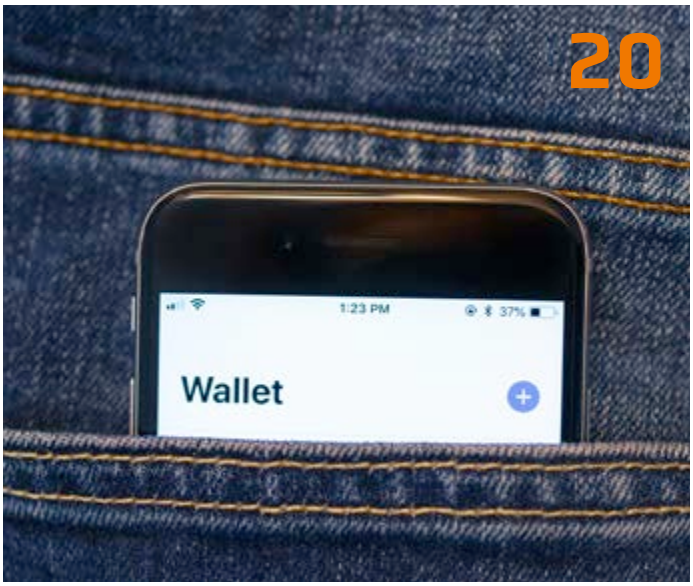


Dr. Ralf Resch ist Geschäftsführer von VITAKO.

SCHWERPUNKT: CYBERSICHERHEIT

6

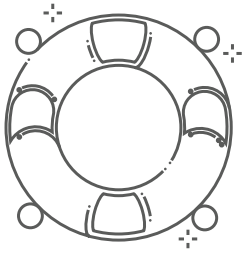

12



CYBERSICHERHEIT: MEHR UNTERSTÜTZUNG UND KOOPERATION NÖTIG

Mit jedem Tag vernetzt sich die Welt stärker. Hacker begreifen jede Verbindung, jede Verkettung als Einladung, in fremde Systeme einzudringen. Dass sie dabei auch vor der öffentlichen Infrastruktur nicht Halt machen, beweisen sowohl die schwerwiegenden Attacken auf den Landkreis Anhalt-Bitterfeld, die Stadt Schwerin und Dutzende andere, als auch die jüngst erfolgte massive Cyberattacke auf die Industrie- und Handelskammern.

Die Politik erkennt die steigenden Gefahren, und der Bund will sich stärker einbringen. Das ist eine gute Sache: Mitte Juli 2022 hat das Bundesinnenministerium (BMI) seine neue Cybersicherheitsagenda veröffentlicht. Allerdings werden Kommunen darin nur ein einziges Mal erwähnt. Dabei sind Kommunen und ihre Dienstleistungen systemrelevant. Sie erbringen über 80 Prozent der Verwaltungsleistungen. Können sie ihrer Aufgabe nicht mehr nachkommen, wird kein Pkw mehr angemeldet, müssen Menschen ohne Wohngeld auskommen, stockt im Ernstfall die Energieversorgung. Dinge, die als selbstverständlich gelten und für das Gemeinwesen von immenser Bedeutung sind. Die Bürgerinnen und Bürger in Anhalt-Bitterfeld etc. haben das direkt erlebt.



CYBERATTACKEN:
IM ZWEIFEL BENÖTIGEN
11.000
KOMMUNEN HILFE – UND ZWAR KURZFRISTIG

KRITIS: AUSGERECHNET KOMMUNEN AUSSEN VOR

Anhand meiner Ausführung möchte ich verdeutlichen, dass die kommunalen Verwaltungen und jene, die sie am Laufen halten – und das sind die kommunalen IT-Dienstleister – eine besonders schützenswerte Infrastruktur darstellen. Dafür gibt es einen Begriff: Kritische Infrastrukturen (KRITIS). Mittlerweile zählen auch „Politik und Verwaltung" zu den neun KRITIS-Sektoren, für die Bund und Behörden massive Unterstützung leisten, um gravierende Störungen abzuwenden. Allerdings: Ausgerechnet die kommunalen Verwaltungen sind außen vor – absurd! Aktuell obliegt es ausschließlich den Ländern, hier für ein angemessenes Maß an Cybersicherheit zu sorgen.

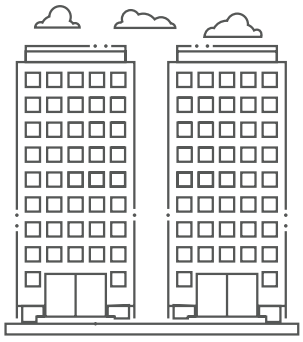
EINE FRAGE DER RESSOURCEN

Warum ich KRITIS erwähne? Ich bin davon überzeugt, dass mit einer entsprechenden Einordnung strukturelle Probleme gelöst werden könnten. Nehmen wir das Thema finanzielle und personelle Ausstattung. Tatsache ist, dass quer durch Deutschland die Ressourcen auf kommunaler Ebene schlicht fehlen, um Cybersicherheit angemessen sicherzustellen. Kommunen bekämen als KRITIS-Sektor die dringend benötigte Unterstützung seitens des Bundes. Siehe die Cybersicherheitsagenda des BMI: In einem eigenen KRITIS-Kapitel werden insbesondere kleinen und mittleren Unternehmen Awareness- und Cyber-Resilienz-Projekte versprochen, und Investitionen in mehr Cybersicherheit sollen finanziell gefördert werden. Warum sollen Kommunen davon nicht in gleicher Weise profitieren?

FÖDERALISMUS IST GUT, ABER...

Wie erwähnt obliegt die Cybersicherheit der Kommunen den Bundesländern. Tatsächlich haben einige Landeshauptstädte in den letzten Monaten Sicherheitsinitiativen gestartet, sei es der neue Warn- und Informationsdienst in Nordrhein-Westfalen, das erweiterte Beratungsangebot in Hessen oder die finanzielle Unterstützung für Cybersicherheitsanalysen

in Niedersachsen. Hinzu kommen auf Landesebene die zahlreichen Cybersicherheitsagenturen, Kompetenzzentren, Bündnisse und vieles mehr. Die Länder machen – in aller Regel unterstützt durch die kommunalen IT-Dienstleister – eine gute Arbeit, und die föderale Struktur trägt zur Cyberresilienz ein Stück weit bei. Gleichzeitig läuft Deutschland allerdings Gefahr, Angreifern einen Cyber-Flickenteppich anzubieten. Auf Dauer kann das nicht gut gehen, so meine feste Überzeugung. Besser wäre es, die kommunale IT als KRITIS einzustufen und relevante Themen bundesweit zu steuern.



SYSTEMRELEVANT:
KOMMUNEN STEMMEN

ÜBER 80 %

DER VERWALTUNGS-LEISTUNGEN

TRAINIEREN, KOORDINIEREN, KOMMUNIZIEREN!

Bis es soweit ist, muss Cybersicherheit über drei Kernthemen gesichert werden. Erstens gilt es, notwendige Kompetenzen systematisch zu trainieren. Mitarbeiterinnen und Mitarbeiter der Kommunen müssen sich der Gefahren etwaiger Cyberattacken und von Datendiebstahl bewusst sein und Alarmzeichen erkennen. Zweitens gilt es, Hilfe besser zu koordinieren. Bei Havarien und Sicherheitsvorfällen brauchen Deutschlands 11.000 Kommunen umgehend Unterstützung. Dafür ist ein deutschlandweit einsatzbereites Cyberhilfswerk aufzubauen. Drittens sind andere Verwaltungen bei Vorfällen konsequent zu warnen. Eine Lösung können sogenannte Computer Emergency Response Teams (CERTs) bieten, die sich auf Bundes- und Länderebene als wichtige Plattformen etabliert haben. Einzelne Initiativen dazu gibt es bereits.

KOMMUNALE IT-DIENSTLEISTER WICHTIGE PARTNER

Es gibt viel zu tun, um die Cybersicherheit um das richtige Maß zu steigern. Immerhin: Die rund 20.000 hoch spezialisierten Mitarbeiterinnen und Mitarbeiter der kommunalen IT-Dienstleister bieten das notwendige Know-how. Wir hinterlegen für unsere Kunden Daten in Hochsicherheitsrechenzentren. Wir implementieren Sicherheitsprozesse, die beim Verdacht eines Cyberangriffs automatisiert und in Bruchteilen von Sekunden ablaufen. Wir führen regelmäßige Schulungen und Workshops durch, um Mitarbeitende bis auf Führungsebene zu sensibilisieren, und wir erarbeiten spezifische Sicherheitsstrategien.

Parallel treiben wir die sicherheitspolitische Debatte voran. Cybersicherheit darf nicht länger eine Frage des Wohnortes sein. Die Einstufung der IT von Kommunen als KRITIS bietet dafür eine entscheidende Möglichkeit. Lassen Sie uns gemeinsam diesen wichtigen Schritt gehen!

Dr. Rolf Beyer ist Vorsitzender des VITAKO-Vorstands.

CYBERSICHERHEIT IN KRITISCHEN INFRASTRUKTUREN

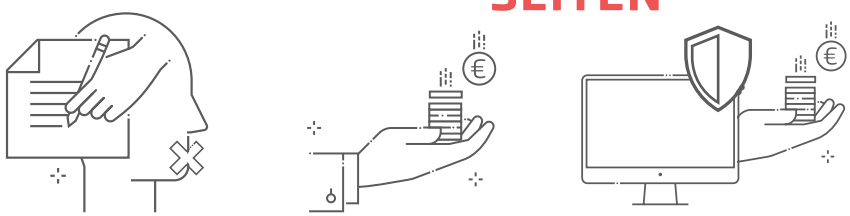
GEMEINSAM MEHR ERREICHEN

In unserer digital vernetzten Welt stehen Cyberangriffe leider inzwischen regelmäßig auf der Tagesordnung. Sei es, dass sensible Informationen oder Unternehmensdaten in erpresserischer Absicht verschlüsselt und damit für die Besitzer unzugänglich gemacht werden, sei es, dass persönliche Accounts von Angreifern übernommen oder Zugangsdaten und Kreditkarteninformationen über Phishing gestohlen und im Darknet verkauft werden. Die Liste an Beispielen immer ausgefeilterer Modi Operandi ließe sich fortsetzen. Anzahl und Intensität der Cyberangriffe hat auch mit der großen Verbreitung von Ransomwareangriffen stark zugenommen. Manche kriminelle Gruppe nutzt oder bietet diese inzwischen an als Geschäftsmodell à la „Ransomware as a service“: Die Namen WannaCry, GoldenEye oder Petya verweisen dann quasi auf besonders verdiente „Mitarbeiter*innen“. Dass hier nicht nur große Konzerne und zahlungskräftige Unternehmen interessante Angriffsziele darstellen, sondern auch öffentliche Verwaltungen in Kommunen, musste 2021 etwa der Landkreis Anhalt-Bitterfeld erleben.

RANSOMWARE/DDOS

+360%

DATEN-LEAK-SEITEN



Schweigegeld-Erpressung | **Lösegeld-Erpressung** | **Schutzgeld-Erpressung**

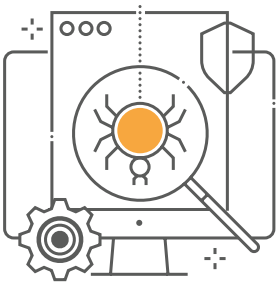
STAATLICH GESTEUERTE ATTACKEN

Neben solch betrügerischen oder erpresserischen Spielarten des Cybercrimes sind auch staatliche oder staatlich gesteuerte Angriffe schon seit längerem Realität. Der russische Angriffskrieg auf die Ukraine hat dies noch verdeutlicht. Fast gleichzeitig mit der russischen Invasion wurde etwa das Satellitenkommunikationssystem des privaten Anbieters ViaSat durch einen Cyberangriff lahmgelegt – das ukrainische Militär war als Kunde dieses Anbieters dadurch zu einem kritischen Zeitpunkt von der Kommunikation abgeschnitten. Aber auch in Deutschland hatte dieser Cyberangriff bekanntlich Folgen, denn die Datenverbindungen des Anbieters wurden auch für Fernwartungszugänge in Windparks genutzt. Zwar war die Stromversorgung nie akut gefährdet, aber der Angriff war so massiv, dass Hardware ausgetauscht

2021

144 MIO.

NEUE SCHADPROGRAMM-VARIANTEN



+22%
gegenüber 2020

werden musste. In Deutschland haben wir die Kollateralschäden dieses und anderer Cyberangriffe nachdrücklich gespürt, und zu befürchten steht, dass dies so bleibt.

KOMPLEXITÄT STEIGT

Neben dem immer schwerer überschaubaren Feld der Akteure im Cyberspace werden auch die Bedrohungen komplexer. Erfolgreiche Angriffe auf IT-Produkte oder Dienstleister als Teil von Lieferketten wie Solarwinds oder Kaseya haben eindrucksvoll demonstriert, dass für eine sichere und funktionsfähige IT vor Ort die Cybersicherheit bereits in der Lieferkette berücksichtigt werden muss.

„Wir müssen alle gemeinsam bemüht sein, die Cybersicherheit auch in der Fläche stetig weiter zu erhöhen."

Hier sei auf das häufige Präventionsdilemma hingewiesen: Sind Maßnahmen erfolgreich und bleiben schwerwiegende schädliche Folgen von Angriffen aus, werden Sinn und Erfordernis der kostspieligen und aufwändigen Maßnahmen mitunter bezweifelt. Führen Angriffe hingegen zu großen Schäden, tritt umgekehrt schnell die Frage auf, warum nicht mehr in die Prävention investiert wurde. Dieses Dilemma wird häufig mit dem Satz „There is no glory in prevention" erfasst.

CYBERSICHERHEIT UND KRITIS

Dieser Umstand ist mit ein Grund dafür, dass für die Cybersicherheit in Kritischen Infrastrukturen (KRITIS) auch staatliche Regulierung nötig ist. Auf Bundesebene sind hier insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und die dazugehörige Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) von Bedeutung. Zwar erfolgt die Bestimmung in der BSI-KritisV, welche Einrichtungen oder Anlagen als KRITIS nach dem BSIG gelten, aus Sicht des Bundes. Dennoch gibt es auch hier Bezüge zur Länder- und Kommunalebene: Beispielsweise gehören viele KRITIS-Betreiber besonders in der Versorgungswirtschaft zu den kommunalen Unternehmen – etwa die Stadtwerke. Trotzdem ist es möglich, dass eine Einrichtung zwar nicht als KRITIS aus Bundessicht im Sinne der BSI-KritisV gilt, jedoch sehr wohl nach Einschätzung von Kommune oder Bundesland eine regionale KRITIS vor Ort darstellt. In diesem Fall sollten natürlich auch diese Einrichtungen durch entsprechende Maßnahmen vor Ort angemessen geschützt werden.

FÖDERALISMUS ALS HERAUSFORDERUNG

Die Probleme des Föderalismus treten somit auch bei der Cybersicherheit zu Tage. Das war absehbar, politische Zuständigkeitsplänkeleien werden bleiben. Es darf aber nicht zum Fallstrick vor allem für kommunale Stakeholder der Cybersicherheit werden, sondern wir müssen alle gemeinsam bemüht sein, die Cybersicherheit auch in der Fläche stetig weiter zu erhöhen. Aus meiner Sicht, jetzt als für Cybersicherheit verantwortlicher Parlamentarischer Staatssekretär, aber auch als ehemaliger Bürgermeister einer niedersächsischen Gemeinde, ist es gerade aktuell besonders wichtig, dass Bund, Länder und Kommunen an einem Strang ziehen und sich gegenseitig unterstützen. Speziell für Länder und Kommunen bietet das BSI hierfür eine eigene Informationssicherheitsberatung an, bei der aktuelle Handreichungen und Empfehlungen gemeinsam mit zahlreichen engagierten Multiplikatoren auf kommunaler Ebene erarbeitet werden. Solche Formate sollten unbedingt unterstützt und ausgebaut werden, denn die Sicherheit im Cyberraum und damit der Schutz Kritischer Infrastrukturen ist eine der dringlichsten gesamtstaatlichen Aufgaben unserer Zeit. In Ostfriesland sagt man: Tosamen schkieren wi dat.

Johann Saathoff, MdB, ist Parlamentarischer Staatssekretär beim Bundesministerium des Innern.

KOMMUNALE CYBERSICHERHEIT: NOTWENDIG – UND VIEL ZU LANGE UNTERSCHÄTZT

Wie in einem Brennglas zeigen die aktuellen Krisenlagen vom Ukrainekrieg mit seinen Auswirkungen auch auf staatliche wie kommunale Institutionen, aber auch der sichere Datenaustausch in einer Pandemie, die Bedeutung der Informationssicherheit auf. Digitalisierung der öffentlichen Verwaltung, damit in Deutschland die Digitalisierung der kommunalen Ebene wie die Erbringung der Daseinsvorsorge (z. B. Schulen, Krankenhäuser) bleiben ohne ausreichende IT-Sicherheit ein Torso! Es geht nicht um Wünschenswertes, nicht primär um Technik. Es geht um eine zwingend zu gewährleistende Voraussetzung digitalen kommunalen Handelns. Es gilt zügig und flächendeckend vor die Lage zu kommen. Die 294 Landkreise, die in den ländlichen Räumen das Rückgrat der Verwaltung darstellen, sind sich der Bedeutung des Themas bewusst und handeln gemeinsam mit ihren IT-Dienstleistern.

STANDARDISIERUNG UND FINANZIERUNG ANGEHEN

Zwei wesentliche Themen, um bei IT-Sicherheit strukturell voranzukommen, lauten Standardisierung und Finanzierung. Aufgrund nach wie vor fehlender verbindlicher Standards ist das IT-Sicherheitsniveau von Kommune zu Kommune vielfach unterschiedlich. Das Präsidium des Deutschen Landkreistages (DLT) tritt seit Längerem dafür ein, den IT-Grundschutz in allen Landkreisen auf dem Niveau der Standardabsicherung oder vergleichbarer Standards aufzubauen. Explizit für die Verwaltungsspitzen wurde in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Papier zur Informationssicherheit für Landrätinnen und Landräte erstellt.

„Kommunen bilden einen wichtigen Baustein der gesamtstaatlichen IT-Sicherheitsarchitektur."

Klar ist, dass die Länder die gemeinsame Zielsetzung – mehr Informationssicherheit auf allen föderalen Ebenen – nicht aus finanziellen Gründen ausbremsen dürfen. Informationssicherheit kostet Geld. Kommunen müssen dafür eine angemessene finanzielle Ausstattung erhalten, aber auch selbst Verantwortung übernehmen. Immer mehr Landkreise beschäftigen beispielsweise neben IT-Sicherheitsbeauftragten bereits Mitarbeiter für das IT-Notfallmanagement. Es bedarf einer Unterlegung der politischen Willenserklärungen zur Steigerung der gesamtstaatlichen Informationssicherheit durch verbindliche Standards. Mögliche Maßnahmen wären beispielsweise die Benennung eines IT-Sicherheitsbeauftragten, Meldepflichten zum Aufbau eines kommunalen Lagebildes der IT-Sicherheit und die Umsetzung des IT-Grundschutzes. Diesbezüglich ist zu diskutieren, ob im Rahmen der nationalen Umsetzung der NIS-2-Richtlinie, über ein dann notwendiges IT-Sicherheitsgesetz 3.0, die Kommunen als kritische Infrastruktur definieren. Die NIS-2.0-Richtlinie subsumiert nach Abschluss der Trilogverhandlungen aktuell unter der öffentlichen Verwaltung nur Bund und Länder. Nichtsdestotrotz haben die Mitgliedstaaten natürlich die Möglichkeit, den Geltungsbereich zu erweitern. Für Deutschland würde sich dabei eine auf Größenklassen basierte Differenzierung anbieten.

BSI ALS ZENTRALSTELLE

Möglichkeiten zur Stärkung der Cyberresilienz können sich auch durch die neu zu schaffende Zentralstelle des BSI ergeben. Dies bedarf allerdings einer Änderung von Art. 87 GG. Eine Bündelung im Bereich der Cybersicherheit vor dem Hintergrund der mangelnden IT-Fachkräfte scheint notwendig. Hier müssten auch die Kommunen partizipieren können. Schon heute besteht auf kommunaler Ebene eine enge Zusammenarbeit mit dem BSI, etwa bei der Erstellung von

IT-Grundschutz-Profilen (z. B. Kommunalverwaltung, Schulen), durch die Verbindungsbüros oder punktuell bei der Unterstützung nach Cyberangriffen.

IDEE DES CYBERHILFSWERKS VORANTREIBEN

Wie sind wir für den Notfall aktuell aufgestellt? Einzelnen Cyberangriffen kann mit den bestehenden Strukturen begegnet werden. Anders bei einem möglichen Flächenbrand, hier wären die bestehenden Ressourcen nicht ausreichend. Analog zum Technischen Hilfswerk wird die Idee eines Cyberhilfswerk diskutiert, das vorwiegend auf ehrenamtliches Engagement gründet. Die Idee des Cyberhilfswerks ist grundsätzlich zu begrüßen. Unmittelbare Zugriffsmöglichkeiten der Landkreise als untere Katastrophenschutzbehörde auf entsprechende Teams wären notwendig. Wir sind davon überzeugt, dass ein Cyberhilfswerk wichtige Ressourcen erschließen kann. Parallel wäre es ratsam, die Kompetenzen der Kommunen und kommunalen IT-Dienstleister weiter aufzubauen. Letztere könnten durch ihr Expertenwissen vor Ort die Koordination übernehmen. Es bedarf auch der Einbindung in die vorhandenen Strukturen des Katastrophenschutzes und die Verknüpfung mit bestehenden Angeboten des BSI und der Länder (CERT, MIRT).

„Länder dürfen mehr Informationssicherheit nicht aus finanziellen Gründen ausbremsen.“

Kommunen bilden einen wichtigen Baustein der gesamtstaatlichen IT-Sicherheitsarchitektur. Die bestehenden Strukturen bieten allerdings keine ausreichende Cyberresilienz. Insbesondere durch Ebenen übergreifende Verfahren und die Vernetzung steigt die Bedeutung der Kommunen für die gesamtstaatliche IT-Sicherheitsarchitektur stetig. In Zeiten von Fachkräftemangel und zunehmender Komplexität bedarf es hierbei einer ausreichenden Finanzausstattung und koordinierter Unterstützung.

DAS TECHNISCHE HILFSWERK HAT RUND

80.000 EHRENAMTLICHE HELFERINNEN UND HELFER

– UND KÖNNTE VORBILD FÜR EIN CYBERHILFSWERK SEIN.

Zum Handlungsleitfaden des Deutschen Landkreistages und des BSI: bit.ly/handleitf

Dr. Kay Ruge ist stellvertretender Hauptgeschäftsführer des Deutschen Landkreistags.

Christian Stuffrein ist Referent für Digitalisierung und IT-Sicherheit beim Deutschen Landkreistag.

DIGITALE SORGLOSIGKEIT ALS ERNSTES PROBLEM

Die Bedrohungslage in Deutschland verschärft sich. Das spüren auch Kommunen. BSI-Präsident Arne Schönbohm erklärt im Interview, wie er die IT-Sicherheit in kommunalen Verwaltungen einschätzt, was verbessert werden kann und welche Unterstützungsangebote das BSI für Kommunen bereithält.

Frage: Wie schätzt das BSI die Bedrohungslage durch Cyberattacken für die deutsche Verwaltung ein?

Arne Schönbohm: Schon im Bericht zur Lage der IT-Sicherheit in Deutschland aus dem Jahr 2021 haben wir für Teilbereiche eindringlich gewarnt. Der Angriffskrieg Russlands gegen die Ukraine hat dies verschärft. Auf kommunaler Ebene sehen wir vor allem zwei Gefahren. Zum einen Ransomware: Dabei geht es um die Erpressung von Lösegeld. Ich denke an die Uniklinik Düsseldorf oder an den Landkreis Anhalt-Bitterfeld. Die Folgewirkungen sind erheblich und langwierig. Ein zweites Thema sind Angriffe auf die IT-Infrastrukturen. Ein bekanntes Beispiel sind die 2021 aufgedeckten Schwachstellen bei Microsoft Exchange, von der mehr als 60.000 Server in Deutschland betroffen waren – größtenteils KMU. Ist etwa der Steuerberater eines IT-Dienstleisters von der Schwachstelle betroffen, kann dies bei vernetztem Arbeiten ein Einfallstor für Cyberangriffe darstellen, die dann auch den Dienstleister und im Ernstfall die betreute Kommune betreffen.

Arne Schönbohm ist Präsident des BSI

Im Oktober stellen wir gemeinsam mit der Bundesinnenministerin den neuen IT-Lagebericht vor. Ich kann vorwegnehmen: Die Lage ist nicht ruhiger geworden.

Wie sind Kommunen bei IT-Sicherheit aktuell aufgestellt?

Das Niveau in Kommunen ist sehr unterschiedlich. Es gibt Landkreise, die das Thema sehr ernst nehmen und sich regelmäßig dazu informieren lassen. Und es gibt andere, die sind weniger aktiv. Teils ist es erschreckend, welch digitale Sorglosigkeit an manchen Stellen herrscht.

Wo liegen die größten Schwachstellen bei kommunalen Verwaltungen?

Die größte Gefahr sehe ich im fehlenden IT-Verständnis, insbesondere auf Führungsebene. IT-Sicherheit wird zu oft als Kostenfaktor gesehen. Die Hinweise und Warnungen von IT-Sicherheitsbeauftragten – so es sie überhaupt gibt – werden häufig ignoriert. Die Folgen dieser strukturellen Schwierigkeiten: Konzepte und Technologien, die eigentlich selbstverständlich sein sollten – wie der BSI-Grundschutz oder Netzwerksegmentierung – kommen nicht zum Tragen. Schulungen von Mitarbeiterinnen und Mitarbeitern in kommunalen Verwaltungen finden nicht so statt, wie das nötig wäre. Hier sehe ich großen Handlungsbedarf.

Welche Maßnahmen könnten helfen, um die Situation zu verbessern?

Zum einen: die kluge Zuteilung von Fördergeldern. Ich denke an das Krankenhauszukunftsgesetz, mit dem der Bund drei Milliarden Euro in die Digitalisierung von Kliniken investiert hat.

„Schulungen von Mitarbeiterinnen und Mitarbeitern in kommunalen Verwaltungen finden nicht so statt, wie das nötig wäre. Hier sehe ich großen Handlungsbedarf“

Arne Schönbohm

Wer an den Mitteln teilhaben wollte, musste 15 Prozent in IT-Sicherheit investieren. Ebenso wichtig: Die Funktion des oder der Sicherheitsbeauftragten muss aufgewertet und direkt an die Landrätin oder den Landrat, an die Bürgermeisterin oder den Bürgermeister angegliedert werden. Und: Wird dessen Rat bewusst ignoriert und es kommt infolgedessen zu einem Sicherheitsvorfall, muss das Konsequenzen haben. Im Brandschutz sind Fragen der Haftung sehr klar geregelt, bei IT-Sicherheit nicht. Am Ende geht es um die Sorgfaltspflicht.

Wie unterstützt das BSI die kommunalen Verwaltungen bei IT-Sicherheit?

Zunächst: Kommunen sind eigenständig. Das heißt: Sie sind selbst verantwortlich für IT-Sicherheit, dies ist keine Aufgabe des BSI. Aber wir bieten zahlreiche Unterstützungsleistungen an. Bei einem Angriff beraten wir – im Fall von Anhalt-Bitterfeld habe ich selbst mit den Landräten noch am Tag des Angriffs telefoniert – oder wir entsenden Hilfsteams. Wichtiger aber ist Prävention. Ein eigenes Referat kümmert sich beim BSI um IT-Sicherheit aus kommunaler Perspektive. Gemeinsam mit den kommunalen Spitzenverbänden haben wir ein BSI-Grundschutzprofil erarbeitet, ein Informationspaket speziell für Kommunen und Stadtverwaltungen. Zudem hospitieren Mitarbeitende des BSI bei Kommunen und Städten, und wir bieten das auch andersherum den kommunalen Mitarbeiterinnen und Mitarbeitern an. Nicht zu vergessen: Mit der Allianz für Cybersicherheit haben wir die größte Cybersicherheitsorganisation Europas aufgebaut. Sie zählt aktuell mehr als 6.500 Teilnehmer und steht auch Kommunen und Stadtverwaltungen offen. Ein kostenloses Angebot zum intensiven Austausch.

13 TAGE

LANG KONNTE EIN UNIVERSITÄTSKLINIKUM NACH EINEM RANSOMWARE-ANGRIFF KEINE NOTFALLPATIENTEN AUFNEHMEN.

Welche Bedeutung haben aus Ihrer Sicht kommunale IT-Dienstleister?

Die IT-Dienstleister spielen eine Schlüsselrolle, weil sie den Kommunen das benötigte Know-how gebündelt zur Verfügung stellen. Die Kernaufgabe von Verwaltung ist ja nicht IT, sondern die Bereitstellung von Bürgerdienstleistungen. Hier können die IT-Dienstleister entlasten. Das BSI arbeitet eng mit den großen kommunalen IT-Dienstleistern zusammen. Es gibt dabei Austauschprogramme, Schulungen und regelmäßige Jours fixes auf Leitungsebene.

Sollten kommunale Verwaltungen und ihre IT-Dienstleister als KRITIS eingestuft werden?

Zwei Richtlinien auf europäischer Ebene streben an, Regierungsinstitutionen und öffentliche Verwaltungen auf Landesebene – nicht auf kommunaler Ebene – als KRITIS einzustufen. Verwaltungen müssen dann bestimmte Kriterien erfüllen und ein Mindestmaß an Cybersicherheit garantieren. Über diesen Hebel hätten sicher auch die Länder ein höheres Interesse, Kommunen bei dem Thema zu unterstützen. Einige Bundesländer machen bereits vor, wie das gehen kann. Das Saarland etwa fördert in seinem kommunalen Digitalisierungsprogramm die Zertifizierung nach dem BSI-Grundschutz. Das ist ein sehr guter Weg. Klar ist: Es geht letzten Endes um starke Resilienz gegen die zunehmenden Bedrohungen im Cyberraum.

IT-KOMPETENZ IN BEHÖRDEN: MANGELHAFT

Cybersicherheit in Kommunen geht jeden etwas an. Schließlich sind es persönliche Daten von Bürgerinnen und Bürgern, die dort verwaltet werden. Als Akteur der Zivilgesellschaft setzt sich Manuel Atug, Gründer und Sprecher der unabhängigen AG KRITIS, dafür ein. Im Interview spricht er über den Zustand von IT-Sicherheit in Kommunen und welche Veränderungen es braucht.

Frage: Herr Atug, wie schätzen Sie den Zustand von Cybersicherheit in deutschen Kommunen aktuell ein?
Manuel Atug: Eher schlecht. Das fängt dabei an, dass Cybersicherheit oft nur wie ein Nebenthema behandelt wird und die Bezahlung der dafür Zuständigen schlecht ist. Hinzu kommen hierarchische Strukturen und eine geringe Bereitschaft, Fehler bei der IT-Sicherheit zuzugeben und diese transparent zu kommunizieren. Das verhindert Fortschritte. Eine veraltete Infrastruktur tut ihr übriges: Mitunter werden 30 Jahre alte Systeme betrieben. Ein Beispiel ist WinFried, der Name sagt schon alles. Das ist ein in vielen Kommunen genutztes System für die Friedhofsverwaltung, es läuft nur auf Windows 98. Das heißt: Viele Kommunen halten uralte Rechner vor mit einem uralten Betriebssystem, auf dem uralte Software läuft.

„Wir haben deutschlandweit schon ein schwieriges Lagebild bei Cybersicherheit – Kommunen gehören sicher zu jenen, die mit am schlechtesten aufgestellt sind."

Das Kernproblem ist allerdings: Es mangelt in Behörden an Digitalisierungs- und IT-Kompetenz – und zwar bei Sachbearbeiterinnen und Sachbearbeitern ebenso wie in den Führungsetagen. Wie wird Software entwickelt? Was ist wesentlich? Warum brauchen wir Open Source? Was ist hilfreich und sicher, und warum brauchen wir das statt glitzernde Blockchains, die nicht funktionieren? Dieses Wissen fehlt – und das auch schon bei denjenigen, die Software für Verwaltungen ausschreiben. Darüber hinaus ist oft nicht klar, dass Digitalisierung kein Produkt ist, das man einfach kaufen kann.

Wir haben deutschlandweit schon ein schwieriges Lagebild bei Cybersicherheit – Kommunen gehören sicher zu jenen, die am schlechtesten aufgestellt sind.

An welchen Punkten würden Sie ansetzen, um diese Probleme rasch anzugehen?
Keine leichte Aufgabe. Die Probleme sind drängend, Ressourcen knapp, und gewachsene Strukturen lassen sich nicht kurzfristig auflösen. Eine Möglichkeit: Der Staat könnte Mitarbeitende und Führungskräfte – und zwar auf allen Arbeitsebenen – systematisch in Sachen Digitalisierung schulen. Dort muss verstanden werden: Digitalisierung heißt nicht, Software zu kaufen und einzusetzen. Denn so landen wir bei absurden Prozessen wie teils in der OZG-Umsetzung. Da füllen Bürger Formulare online aus und laufen dann mit dem unterschriebenen Ausdruck zum Bürgeramt, um diesen in einen Briefkasten zu werfen.

Zugleich müssen wir unbedingt auch in der Bildungspolitik ansetzen. In Ländern wie Dänemark oder Estland gibt es Pflichtfächer wie Informatik, Programmieren oder IT-Sicherheit – dadurch ist die gesamte Bevölkerung einfach deutlich kompetenter als hierzulande. Allerdings ernten wir die Früchte frühestens in 16 Jahren. Daher müssen wir jetzt damit anfangen.

Hilfreich wären auch personelle Konsequenzen, wenn wirklich was schief geht oder erhebliche Lücken in der IT-Sicherheit entdeckt werden. Und zwar sowohl bei leitenden Beamten als auch

„Um seiner Gewährleistungs-verantwortung gerecht zu werden, muss der Staat sichere Fachverfahren bieten. In letzter Konsequenz geht es um Menschenschutz.“

Manuel Atug ist Gründer und Sprecher der unabhängigen AG KRITIS.

bei kommunalen IT-Dienstleistern. Ein Vergleich: Autohersteller machen sich viele Gedanken zur Sicherheit ihrer Fahrzeuge. Warum? Weil sie haften. Eine Kommune, die sich Ransomware einfängt, haftet nicht. Da heißt es dann: Wir sind Opfer einer total fiesen und fähigen Cyberbande geworden, wir konnten nichts dafür. Leider kostet das den Bürger den Verlust seiner Daten, Pech gehabt. Aber wenn Rechner mit Windows 98 genutzt werden, braucht es eben nicht viel Know-how, um diese zu kompromittieren. Das ist schon fast grob fahrlässig.

Bürgerinnen und Bürger haben laut Grundgesetz bestimmte Rechte. Wer einen Personalausweis beantragen will, muss das tun können. Wer zu Sozialleistungen berechtigt ist, muss diese erhalten. Um seiner Gewährleistungsverantwortung gerecht zu werden, muss der Staat sichere Fachverfahren bieten. In letzter Konsequenz geht es um Menschenschutz.

Welche Rolle spielen aus Ihrer Sicht kommunale IT-Dienstleister beim Thema Cybersicherheit?

Da gibt es gute Beispiele – und weniger gute. Das Problem: Wenn man tagtäglich für Behörden arbeitet, läuft man Gefahr, irgendwann auch wie eine zu denken. Begeistert war ich etwa von der Stadt Dortmund mit ihrem Projekt Do-FOSS, das freie Software für Kommunen entwickeln will. Die Verantwortlichen hatten Akteure aus der Zivilgesellschaft und aus NGOs zu einer Diskussion in der Stadt Köln eingeladen, darunter auch mich. Sie wollten das Konzept Open Source verstehen. Zuhörer waren auch Mitglieder der Fraktionen und Vertreter der Parteien. Irgendwann bei meinen Ausführungen hat es bei allen Klick gemacht und die Leute hatten einen Aha-Effekt. Ich würde mir wünschen, es gäbe mehr solcher Initiativen, von denen andere lernen können.

Würde es helfen, kommunale Verwaltungen bzw. ihre IT-Dienstleister als KRITIS einzustufen?

Erstmal: Staat und Verwaltung sind ja bereits KRITIS. Aber: Anders als bei anderen Sektoren wurden vom Gesetzgeber keine konkreten Anforderungen definiert, wie etwa dort IT-Sicherheit umzusetzen ist. Auch gibt es keine externen, unabhängigen Prüfungen. Ebenso keine Meldepflicht für Vorfälle. Aus meiner Sicht ist es überfällig, dass auch Verwaltungen den Zustand ihrer IT-Sicherheit nachweisen und darlegen müssen. Nur so kommen wir beim Thema Cybersicherheit in Behörden wirklich weiter.

PROVITAKO: IT GEMEINSAM BESCHAFFEN – UND KOSTEN SPAREN

ÜBER DIE EINKAUFSGENOSSENSCHAFT PROVITAKO BÜNDELN DIE IT-DIENSTLEISTER IHRE BESTELLUNGEN – FÜR BESSERE PREISE UND MEHR EFFIZIENZ.

Jedes Jahr bestellen öffentliche Vergabestellen in Deutschland Technologie, Software und IT-Dienstleistungen in Milliardenhöhe – Tendenz weiter steigend. Ein Großteil der IT-Beschaffungen wird allerdings nach wie vor in den einzelnen Kommunen abgebildet, obwohl diese in aller Regel Mitglieder bei kommunalen IT-Dienstleistern sind und darüber eine Bündelung erreichen könnten. Diese Aufgabe übernimmt ProVitako. Wesentliche Vorteile im Überblick:

- **Rabatte aushandeln:** Gemeinsam erreichen die Mitglieder von ProVitako große Beschaffungsvolumina. 2022 liegt das Gesamtvolumen voraussichtlich bei gut 135 Millionen Euro. Die Preisskaleneffekte sind beachtlich: Je nach Anzahl und Art des Produktes oder der Dienstleistung sind Rabatte von bis zu 50 Prozent bezogen auf den üblichen Verkaufspreis möglich.

Dr. Ralf Resch ist Geschäftsführer von VITAKO und Vorstand von ProVitako.

- **Aufwand reduzieren:** Kommunale IT-Dienstleister beschaffen Rechner oder Software in der Regel über Ausschreibungen. Damit geht erheblicher Aufwand einher. Unter dem Dach von ProVitako übernimmt die Einkaufsgenossenschaft die entsprechenden organisatorischen Aufgaben – wobei die Mitglieder selbstverständlich ein Mitspracherecht haben und spezifische Anforderungen benennen können.

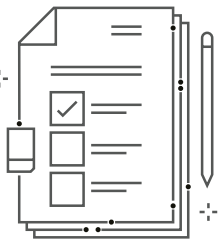
- **Spezialisten gezielt einsetzen:** Ausschreibungen und die darauffolgenden Rahmenverträge müssen juristisch hieb- und stichfest sein. Durch die Bündelung von Ausschreibungsprozessen über ProVitako werden die teuren Vergaberechtsspezialisten effizient eingesetzt – Mitglieder ersparen sich die aufwändige Suche, Kosten werden geteilt.

- **Qualität erhöhen:** Durch die großen Beschaffungsvolumina sind qualitative Kriterien in Ausschreibungen deutlich besser durchsetzbar. Die einheitliche Beschaffung hilft zudem, die technische Ausstattung von kommunalen Verwaltungen zu standardisieren und damit zu verbessern.

ProVitako spielt heute bereits eine wichtige Rolle bei der kommunalen IT-Beschaffung. Vier von fünf VITAKO-Mitgliedern sind bereits dabei. Für mich steht außer Frage, dass ProVitako die Verhandlungsposition der IT-Dienstleister gegenüber internationalen Konzernen weiter steigern wird.

70 %

DER KOMMUNEN WERDEN ÜBER PROVITAKO ERREICHT



ProVitako hat derzeit 42 Mitglieder, die 70 Prozent der Kommunen in Deutschland erreichen. Unser Ziel: Alle Kommunen sollen über ihre kommunalen IT-Dienstleister von ProVitako profitieren.

LENOVO AN PROVITAKO IM JULI 2022:

„Lenovo legt in dieser außergewöhnlichen Situation Prioritäten auf die Aufträge der ProVitako Mitglieder. Die ProVitako ist für Lenovo aktuell der wichtigste Einkaufsverband für das kommunale Geschäft in Deutschland.“

MARKTSITUATION: BEDEUTUNG DES AUFTRAGGEBERS FEDERT ENGPÄSSE AB

DER WELTMARKT LÄSST SICH NICHT ÄNDERN, ABER DIE BEDEUTUNG DES AUFTRAGGEBERS HILFT BEI DER ZUTEILUNG.

Fast täglich kann man den Medien entnehmen, dass die Versorgung mit Gütern nicht mehr in dem Ausmaß gewährleistet werden kann, wie wir es vor der Corona-Pandemie oder dem Ukraine-Krieg kannten. Die wirtschaftlichen Auswirkungen durch den Lieferengpass sind enorm und zeigen eindeutig unsere Abhängigkeit von einer weltweit funktionierenden Produktion und Logistik.

Gerade bei den IT-Infrastruktur-Produkten, die vornehmlich im asiatisch/chinesischen Raum gefertigt werden, wird die Versorgungslücke nicht kleiner. Ob Null-Covid-Strategie oder Abkehr davon, die Auswirkungen sind dieselben: Produktion und Logistik können wegen fehlender MitarbeiterInnen oder bestimmter Rohstoffe und Komponenten nicht sichergestellt werden.

Mit diesen Folgen haben auch die öffentlichen Auftraggeber zu kämpfen. Notebooks, Tablets und Smartphones, also mobile Endgeräte, die durch die Pandemie und die damit einhergehende Home-Office-Tätigkeit in Verwaltungen oder den digitalen Unterricht in Schulen einen geradezu gigantischen Nachfrageschub erhalten haben, sind und bleiben knapp.

Wenn also Lieferengpässe unsere Versorgung bestimmen, dann sind die Bedeutung des Auftraggebers und die über ihn abgebildeten Volumina für die „Zuteilung“ der reduzierten Mengen ausschlaggebend! Genau diese Wechselwirkung konnten wir als ProVitako bei bedeutenden Rahmenverträgen (Notebooks über Bechtle/Lenovo, Tablets und Smartphones über Cancom/Apple) feststellen. Trotz geringer Verfügbarkeit ist die Lieferquote über 80 Prozent!

ÜBER 80 %

LIEFERQUOTE BEI PROVITAKO – TROTZ GERINGER VERFÜGBARKEIT

Allerdings bleibt auch in unseren Rahmenverträgen ein großes Manko: Die Lieferzeit beträgt teilweise 5-6 Monate. Mit Blick auf das zu erwartende Jahresendgeschäft oder auslaufende Förderprogramme ist daher eine Planungsstrategie erforderlich, die den langen Lieferzeitraum berücksichtigt.

In einem abgestimmten Vorgehen mit den Herstellern, den Rahmenvertragspartnern und unseren Mitgliedern bestimmen wir getriggert durch die ProVitako den Forecast für die benötigten IT-Infrastruktur-Produkte und leiten daraus die Bevorratungsgrößen mit den Lieferanten ab, um die Lieferfähigkeit zum Jahresende abbilden zu können.

Damit profitieren alle Mitglieder der ProVitako von der durch die Bedarfsbündelung entstandenen Bedeutung und dem mit Lieferanten und Herstellern abgestimmten Planungsvorgehen.

Gerade in Zeiten wie diesen wird der Nutzen einer großen Einkaufsgenossenschaft deutlich spürbar, denn der Weltmarkt lässt sich nicht ändern, aber die „Zuteilung“ durchaus gestalten!

Jürgen Abelshauser ist CEO von ProVitako.

MARKTPLATZ
für EfA-Leistungen

GOVDIGITAL

MARKTPLATZ FÜR EFA-LEISTUNGEN: BETA-VERSION IST ONLINE

Der Marktplatz für EfA-Leistungen soll vor allem kommunalen IT-Dienstleistern und Kommunen den Einkauf von Online-Services vereinfachen. Die Beta-Version zeigt in einem Schaufenster Leistungen, die nach dem Prinzip „Einer-für-Alle" zentral angeboten und von Behörden und öffentlichen IT-Dienstleistern nachgenutzt werden können.

„Einer für Alle" (EfA) bedeutet, dass ein Bundesland oder mehrere gemeinsam eine digitale Verwaltungsleistung zentral entwickeln und betreiben – üblicherweise durch einen öffentlichen IT-Dienstleister. Andere Bundesländer und Kommunen können diese EfA-Leistung dann mitnutzen.

Govdigital eG übernimmt im Auftrag des IT-Planungsrates den Aufbau des Marktplatzes, der die Nachnutzung von EfA-Leistungen vereinfacht: EfA-Leistungen können dort beworben, bereitgestellt, bestellt und nachgenutzt werden. Auf dem Marktplatz sind Suche, Auswahl und Einkauf möglich, aber auch eine datenschutzkonforme und rechtssichere Nutzung als Inhouse-Vergabe ohne zeitaufwändige Ausschreibungen. Verschiedene Anbieter werden hier ihre „Stände" betreiben: Während Länder über den FITStore der Bund-Länder-Anstalt FITKO inhousefähig „einkaufen" können, richtet sich die govdigital vor allem an die kommunale Ebene. Alle Kommunen und IT-Dienstleister, die direkt oder indirekt Mitglieder der govdigital oder der Pro-Vitako sind, können dort Dienste beziehen. So werden die meisten öffentlichen Gebietskörperschaften in Deutschland erreicht.

Jens Fromm ist Gesamtprojektleiter bei govdigital eG.

„Der Marktplatz ist eine der nötigen Voraussetzungen, um EfA praktisch umsetzen und dauerhaft betreiben zu können." Jörn Riedel

Das neue Schaufenster gibt Besucher*innen einen Eindruck von der Oberfläche und Handhabung des Portals. Erste Pilot-EfA-Leistungen sind verfügbar. Bestellungen sind bereits möglich und laufen zunächst über eine Kontaktaufnahme zum Bereitsteller oder Marktanbieter.

„Wir wollen, dass das EfA-Prinzip für alle Seiten ohne großen Aufwand genutzt werden kann", erklärte Martin Schallbruch, CEO der govdigital. „Der Marktplatz soll der Ort sein, an dem alle Leistungen verfügbar und bestellbar sind."

Die Weiterentwicklung erfolgt bis Jahresende iterativ und in enger Zusammenarbeit mit den Mitgliedern der govdigital und weiteren Partnern, vor allem der FITKO.

„Der Marktplatz ist eine der nötigen Voraussetzungen, um EfA praktisch umsetzen und dauerhaft betreiben zu können. Er strukturiert die Abwicklung zwischen Ländern, Kommunen und ihren Dienstleistern und schafft darüber hinaus Rechtssicherheit", sagt Jörn Riedel, Chief Information Officer der Freien und Hansestadt Hamburg und stellvertretender Aufraggeber des Marktplatzes für den IT-Planungsrat.

www.govdigital.de/marktplatz

KOMMUNE DER ZUKUNFT

UNSERE KINDER WERDEN IN SMARTEN STÄDTEN AUFWACHSEN!

Mit Digitalen Zwillingen und Smarten Services entwickelt die AKDB Systeme für die Smart City. Einblicke von Steffen Kleinmanns, Geschäftsführer der digitalfabriX GmbH, einer Tochterfirma der AKDB.

Wie wirken sich bestimmte Straßensperrungen auf den Verkehr aus? Wo müssen Mülleimer geleert werden? Und wie ist der CO_2-Gehalt im örtlichen Schulgebäude – ist Lüften nötig? Kommunalverwaltungen mussten solche Fragen bisher auf Basis ihrer Erfahrung beantworten oder sie konnten es gar nicht. Steffen Kleinmanns: „Smart-Service-Systeme erweitern Wissen und Handlungsmöglichkeiten der Verwaltungen fundamental – zum Vorteil von Bürgerinnen und Bürgern."

BEISPIEL WINTERDIENST

Ein Beispiel ist der intelligente Winterdienst der AKDB, den zum Beispiel die Kommune Aschheim bereits nutzt: Sensoren im Straßenbelag melden Glatteis und geben an, ob gestreut werden muss.

BEISPIEL: SMARTE MÜLLABFUHR

Vorteile für Kommunen, Bürgerinnen und Bürger:

- Ineffiziente (Leer)fahrten reduzieren
- CO_2-Emissionen senken und Treibstoffkosten senken
- Überfüllte Müllbehälter vermeiden und Sammelstellen sauberer halten
- Ressourcen schonen und Mensch und Maschine entlasten

Gleichzeitig wird der Bedarf an Streusalz ermittelt und mit den Füllständen der Salzsilos abgeglichen – ebenfalls automatisch per Sensoren. Und Winterdienstfahrzeuge melden per Geoposition zurück, wo und wann Schnee geräumt wurde. Wesentliche Informationen bekommt der Einsatzleiter per Push-Benachrichtigung aufs Smartphone. Steffen Kleinmanns: „Winterdienst ist sehr zeitsensibel. Vor allem, wenn die Menschen nicht mit Glatteis rechnen. Smarte Lösungen sind dann sicherheitsrelevant."

DIGITALER ZWILLING MACHT'S MÖGLICH

Eine Schlüsselrolle spielt dabei der Digitale Zwilling realer Objekte. Diese Zwillinge werden mit echten oder simulierten Daten gefüttert, beispielsweise zur Straßenglätte oder CO_2-Konzentration in Räumen. In einem weiteren Schritt lassen sich daraus innovative Services ableiten. „Mit Digitalen Zwillingen und reellen Daten treffen Verwaltungen viel bessere Entscheidungen und sparen Ressourcen", so Steffen Kleinmanns. Im Extremfall retten sie sogar Leben, siehe die Flut im Ahrtal 2021: „Mit einem Zwilling des Flussverlaufs, Echtzeitdaten über den Wasserstand und Informationen über die Einwohnerverteilung wäre eine automatisierte Warnung für die Bevölkerung möglich."

ZUM START: EINFACHE ANWENDUNGEN WÄHLEN

In jedem Fall sollten Kommunen, so Kleinmanns, zunächst mit kleinen, einfachen Anwendungen Erfahrung sammeln. Denn der Aufbau eines umfassenden Smart-City-Systems ist ein mehrjähriger Prozess, zumal viele Stellen einzubinden sind. Mit einem modularen Aufbau kann aber sofort mit einzelnen Anwendungen wie dem Winterdienst produktiv gegangen werden. Immerhin: Mit offenen Standards wäre es möglich, Smart-Service-Systeme auch als EfA-Leistungen zu entwickeln.

Das Potenzial Digitaler Zwillinge und Smarter Services ist riesig. In Steffen Kleinmanns Worten: „Unsere Kinder werden mit smarten Zwillingen in einer smarten Welt aufwachsen." Die AKDB-Unternehmensgruppe arbeitet bereits daran, Memmingen so zu einer Smart City zu machen.

Gesprächspartner war Steffen Kleinmanns, Geschäftsführer der digitalfabriX GmbH, einer Tochterfirma der AKDB.

SERIE

DIGITALE SELBSTBESTIMMTE IDENTITÄTEN

Die ersten beiden Teile der Artikelreihe haben Prinzipien und technische Aspekte erklärt sowie Inhalte und Ziele des BMWK-Projekts IDunion dargestellt. In diesem letzten Teil stellen wir zwei Anwendungsfälle und deren aktuelle Herausforderungen vor, die bei der Stadt Köln prototypisch umgesetzt werden.

REALISIERUNG UND HERAUSFORDERUNGEN KONKRETER ANWENDUNGEN

Im F&E-Projekt IDunion realisiert die Stadt Köln die Anwendungsfälle „Belehrung nach Infektionsschutzgesetz (IfSG)“ und „Fischereischein“ unter anderem mit dem Ziel, eine einfache Übertragung von SSI-Technologien auf andere Leistungen der städtischen Verwaltung zu ermöglichen.

CREDENTIALS STATT PAPIER

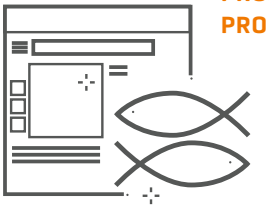
In beiden Fällen soll die behördliche Papierurkunde durch elektronische kryptographische Nachweise (Credentials) ersetzt werden, die der Antragsteller (Holder) in einer Wallet-App empfängt, selbstbestimmt verwaltet und weiternutzen kann. Auch die spätere Prüfung der Credentials durch autorisierte Ordnungsbehörden (Verifier) wird möglich sein. Bei der Einführung sind wissenschaftliche, technische und organisatorische Rahmenbedingungen zu bearbeiten. Insbesondere sind der rechtliche Rahmen zur Gleichstellung von digitaler Repräsentanz und öffentlicher Urkunde zu prüfen und datenschutzrechtliche Anforderungen und Risiken zu klären. Ebenso ist die Akzeptanz der Bürger*innen zur Nutzung einer Wallet zu evaluieren und zu fördern.

BEISPIEL 1: FISCHEREISCHEIN

Für die Ausübung der Fischerei benötigen Bürger*innen entsprechend Landesfischereigesetz unter anderem einen Fischereischein, der die Kommunalverwaltungen (Issuer) ausstellen. Aktuell wird der Fischereischein als Ausweis in Papierform mit einem Passfoto und Meldedaten ausgestellt, wobei eine bestandene Fischerprüfung nachgewiesen werden muss.

Grund für die Wahl des Fischereischeins im IDunion-Projekt ist die Komplexität des Vorgangs. Auf „Issuer“-Seite sind mehrere Voraussetzungen zu prüfen, während auf „Verifier“-Seite verschiedene Behörden aktiv sein können, die aufgrund der häufig abgeschiedenen Lage von Angelgebieten nicht immer von einer Internetverbindung ausgehen können.

9.000
FISCHEREI-PRÜFUNGEN PRO JAHR



BEISPIEL 2: INFEKTIONSSCHUTZ

Der zweite Anwendungsfall ist eine Bescheinigung nach §43 IfSG für Personen, die im lebensmittelherstellenden oder -verarbeitenden Gewerbe oder in der Gastronomie tätig werden und im Rahmen einer (Online-)Schulung über die rechtlichen Voraussetzungen und die gesundheitlichen Risiken im Umgang mit Lebensmitteln belehrt wurden. Dies ist ein Anwendungsfall mit einer einfacheren Datenstruktur, der aber mit 280.000 Fällen im Jahr einen großen Adressatenkreis erreicht und daher für Akzeptanz- und Bedienbarkeitsaspekte aufschlussreich ist.

Die Digitalisierung dieser Vorgänge birgt an sich bereits viele Vorteilen für Behörden und Nutzer. Bearbeitungszeiten reduzieren sich und ein ortsunabhängiger Zugriff auf Vorgänge wird möglich, um nur einige zu nennen. Auf diese Optimierungen fokussiert das Onlinezugangsgesetz (OZG), in dessen Rahmen beide Anwendungsfälle über EfA-Projekte bearbeitet werden – bei der Belehrung durch das Land Niedersachsen und beim Fischerei-

schein durch das Land Schleswig-Holstein. Über die Nachnutzung können Lösungselemente in die Anwendungsfälle einfließen und dabei mit dem SSI-Ansatz kombiniert werden. In enger Abstimmung

280.000

GESUNDHEITSZEUGNISSE PRO JAHR

wird so vom Antrag bis zur behördlichen Prüfung ein vollständig digitaler Prozess designt. Die dabei eingesetzten SSI-Verfahren bringen neue Herausforderungen in organisatorischer, rechtlicher und technischer Hinsicht mit sich.

In organisatorischer Hinsicht ist die heterogene Verifier-Struktur, die sich über unterschiedliche Behörden in unterschiedlichen Bundesländern erstreckt, ein zentrales Thema. Alle Verifier müssen eine App erhalten, die die kryptographische Echtheitsprüfung des vorgezeigten Credentials gegen ein Ledger online durchführen kann. Eine technische Herausforderung ist in diesem Zusammenhang die Offline-Prüfung, die zum Beispiel beim Fischereischein in abgelegen Gegenden nötig sein kann.

Technisch herausfordernd ist auch die Ausstellung und kryptographische SSI-Prüfung eines Lichtbild-Credentials, da die derzeitige eID-Funktion des elektronischen Personalausweises dies nicht beinhaltet. Ob im Anwendungsfall „Fischereischein" das derzeitig genutzte Lichtbild überhaupt als SSI-Credential notwendig ist, wird im Rahmen der aktuellen Spezifikationsarbeit untersucht.

Rechtliche Hürden müssen erkannt, bewertet und gegebenenfalls bearbeitet werden. Teilweise können existierende Experimentierklauseln aus dem Gesetz zur Förderung der elektronischen Verwaltung (EGovG NRW) angewendet werden, an anderen Stellen werden Gesetzesänderungen diskutiert. Bei dieser Thematik hat sich die Unterstützung der DigiSandbox.NRW als sehr hilfreich erwiesen.

Ziel ist die Bearbeitung aller Herausforderungen und die Umsetzung der Anwendungsfälle in einer abgeschlossenen Laborumgebung bis 2023. Dabei werden alle Vorteile der SSI-Technologie realisiert, die im ersten Teil der Artikelreihe ausführlich dargestellt wurden. Insbesondere werden vertrauensvolle, dezentrale Beziehungen zwischen den Akteuren möglich und die vollständige Kontrolle der Nutzer über ihre digitalen Identitätsdaten sichergestellt.

Infos: https://idunion.org/

Markus Batz ist IT-Architekt im Amt für Informationsverarbeitung der Stadt Köln.

Thomas Büttner ist IT-Architekt im Amt für Informationsverarbeitung der Stadt Köln.

LERNPLATTFORMEN UND OPEN SOURCE

Lernplattformen (traditionell Lernmanagementsystem/LMS) organisieren – im Gegensatz zu den üblicherweise diskutierten Cloudlösungen – auch Lerngruppen und Lernvorgänge. Erst dadurch wird zielorientiertes Lernen in hybriden oder e-learning-Umgebungen ermöglicht.

In ihrer aktuellen Studie erfassen Breiter, Müller, Telle und Zeising (2021) die auf Landesebene bereits eingesetzten Lernplattformen. Sie haben erfragt, inwieweit Dienste wie virtuelle Klassenräume, Lerngruppen oder Kollaboration – wobei beispielsweise Dokumente online bearbeitet werden – verfügbar sind. Einige Bundesländer greifen auf den Dienstleister „it's learning" zurück, wobei es sich hier um eine extern betriebene, kommerzielle Standardlösung handelt. Manche Bundesländer setzen selbst betriebene, aber von kommerziellen Anbietern bezogene Standardlösungen wie HPI-Schul-Cloud mit zusätzlicher Open-Source-Komponente ein.

Dr. Christoph Lindner ist Psychologe und wissenschaftlicher Mitarbeiter an der Fakultät für Erziehungswissenschaft der Universität Hamburg sowie am Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik (IPN) in Kiel.

Bernadette Thielen ist Studiendirektorin und Inhaberin der Firma Baldeney IT-Consulting.

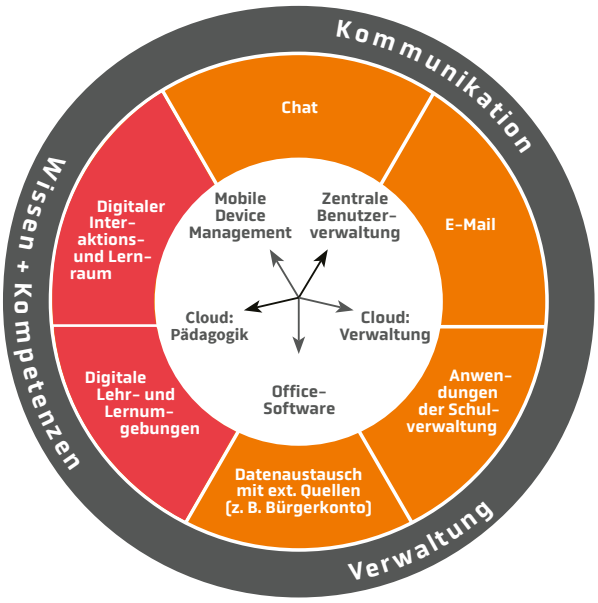
Die meisten Bundesländer haben – zum Teil sehr zügig – ihre bereits vorhandene Lernplattform, basierend auf der Open-Source-Lösung Moodle, massiv ausgebaut oder neu eingeführt. Das ist als sehr positiv hervorzuheben: Abhängig vom Lizensierungsmodell ist Moodle eine kostenlose und frei verfügbare Software mit offenem Quellcode, der individuelle Funktionsanpassungen ermöglicht. Der Betrieb findet meistens als Hosting im eigenen Rechenzentrum statt. Open-Source-Lösungen sind im Sinne der digitalen Souveränität zu befürworten. Auch aus Sicht der empirischen Bildungsforschung und der KMK-Beschlüsse zur individuellen Förderung hat der Einsatz von OSS einen erheblichen Mehrwert: Sie treffen – im Gegensatz zu den meisten kommerziellen Lernplattformen – datengestützte Vorhersagen für das zukünftige Lernverhalten und ermöglichen damit individualisierte digitale Lernförderung.

ENTWICKLUNG FÖRDERN

Sowohl die erwähnte Studie als auch die Praxiserfahrungen in den Bundesländern zeigen: Um Lernplattformen zu verbreiten, sind strukturelle Maßnahmen des Bundes und der Länder überfällig. Konkret:

- Gesetze und Verordnungen zur Lehrmittelfreiheit anpassen, sodass digitale Lernangebote gleichberechtigt neben Printangeboten wie Schulbüchern beschafft werden können.
- Ein Institut für Qualitätsentwicklung in der Digitalen Bildung (IQDB) aufbauen, das Qualitätskriterien für digitale Lernangebote definiert, Lernmodule erprobt, evaluiert und die Entwicklung als (Moodle-)Plugin beauftragt.
- Qualität der Lehrkräftefortbildung für digitales Lernen verbessern und IQBD-Empfehlungen sowie neueste fachdidaktische Erkenntnisse berücksichtigen.

- Moodle-Kurse analog zum Lehrplanbezug des Print-Schulbuchs entwickeln.
- Lehrkräfte durch die Bereitstellung von Funktionsstellen und Ressourcen motivieren
- Performance und Datenschutz der Lernplattformen durch Einbindung der kommunalen IT-Dienstleister beim Hosting sichern und Schulen von Support-Aufgaben durch kommunale Schul- und IT-Verwaltungsassistenzstellen entlasten.



Die Abbildung zeigt, wie die derzeit am Markt angebotenen, teilweise voneinander isolierten technischen Schnittstellen und Anwendungsbereiche zukünftig integriert werden müssten.

Legende:
- **zentrale Softwaremodule für Anwendungen**
- **Anwendungsfelder**
- **Anwendungsbereiche**

EINGESETZTE LERNPLATTFORMEN MIT ENTSPRECHENDEN FUNKTIONSBEREICHEN IN DEN BUNDESLÄNDERN (NACH BREITER, MÜLLER, TELLE UND ZEISING, 2021)

Bundesland	Lernplattform	Datenspeicher	Prüfungen	Kollaboration	Kalender/ Stunden- und Vertretungsplan
Bayern	Moodle*	○	○	☑	☑
Hamburg	Moodle*	○	○	☑	○
Hessen	Moodle*	☑	○	○	○
Nordrhein-Westfalen**	Moodle*	☑	○	☑	○
Rheinland-Pfalz	Moodle*	○	☑	○	☑
Saarland	Moodle*	○	☑	○	☑
Sachsen-Anhalt	Moodle*	○	☑	○	☑
Baden-Württemberg	Moodle* itslearning	☑	☑	☑	☑
Berlin	Moodle* itslearning	☑	☑	☑	☑
Sachsen	Moodle*, LernSax, OPAL Schule	☑	☑	☑	☑
Brandenburg	HPI-Schul-Cloud	☑	○	☑	☑
Niedersachsen	HPI-Schul-Cloud	☑	○	☑	○
Thüringen	HPI-Schul-Cloud	☑	○	☑	☑
Bremen	itslearning	☑	☑	☑	☑
Mecklenburg-Vorpommern	itslearning	☑	☑	☑	☑
Schleswig-Holstein	itslearning, Schul-CommSy SH	☑	☑	☑	☑

Zusätzlich haben Breiter et al. (2021) weitere Kategorien untersucht, die bis auf wenige Ausnahmen in allen Ländern eingesetzt werden: „Klassenraum und Rollenkonzept", „Aufgaben" (nur in Rheinland-Pfalz nicht eingesetzt), „Messenger" (nicht in Bayern und Nordrhein-Westfalen), „Wiki, Blog, Foren" (nicht in Nordrhein-Westfalen), „weitere Dienste" (nicht in Hessen).

*** Auf Moodle-basierende Systeme,**

**** Abweichend für Dortmund, Düsseldorf und Köln;**

Quelle: Breiter, A., Müller, M., Telle, L. & Zeising, A. (2021). Digitalisierungsstrategien im föderalen Schulsystem: Lernmanagementsysteme und ihre Betriebsmodelle. Institut für Informationsmanagement Bremen GmbH (ifib).

SERIE

WAS LERNEN WIR AUS DER KRISE?

Cyberkriminalität steigt enorm. So wurde Mitte Oktober 2021 der Unternehmensverbund SIS|KSM gezielt attackiert – und die digitale Verwaltung in Schwerin sowie im Landkreis Ludwigslust-Parchim lahmgelegt. Matthias Effenberger, Geschäftsführer der SIS und Vorstand der KSM, zu Reaktionszeiten, Notbetrieb und Lehren aus dem Cyberangriff.

RANSOMWARE-ANGRIFF: WENN CYBERKRIMINALITÄT ZUSCHLÄGT

Nach dem Angriff wurden sofort sämtliche IT-Systeme vom Netz getrennt und kontrolliert heruntergefahren. Innerhalb von wenigen Stunden trat unser Krisenstab entsprechend dem Notfallmanagement zusammen. Ein Kommunikationsprozess und eine Verzahnung der Krisenstäbe wurden aufgesetzt. Im Laufe des ersten Tages haben wir spezialisierte Cyber-Forensiker eingebunden, die gemeinsam mit unseren IT-Spezialisten die Untersuchung und Analyse übernommen haben.

NOTBETRIEB IN KÜRZESTER ZEIT

Im Rahmen der Konstituierungsphase wurden binnen weniger Tage besonders wichtige Arbeitsplätze der Verwaltungen/kommunalen Gesellschaften für den Notbetrieb vorbereitet und die Bankenkommunikation sichergestellt. Parallel begann die forensische Untersuchung der Serversysteme sowie der rund 4.000 im Einsatz befindlichen Clients. Unter erhöhten Sicherheitsrestriktionen haben wir in den ersten beiden Wochen die rund 300 wichtigsten Fachanwendungen – darunter Energiehandel, Lohn- und Gehaltszahlungen und Sozialleistungen – im Notbetrieb gewährleistet.

Matthias Effenberger ist Geschäftsführer der Schweriner SIS-IT- und Servicegesellschaft mbH und Vorstand der KSM Kommunalservice Mecklenburg AöR.

So ist es uns gelungen, innerhalb von acht Wochen in einen stabilen Notbetrieb überzugehen – und das bei hohem Digitalisierungsgrad. Ein wesentlicher Teil unseres Erfolgs: Verlässliche und engagierte Mitarbeitende, die sich bis fast zur Erschöpfung in die Arbeit zur Krisenbewältigung „reingehängt" haben. Das ist ein Glücksfall.

AUSGEKLÜGELTES SICHERHEITSNIVEAU

Der Unternehmensverbund SIS|KSM hat eine durchdachte und gut abgesicherte IT-Landschaft. Es sind viele verschiedene IT-Lösungen von globalen Herstellern im Einsatz. Wir arbeiten stetig an der Erhöhung des Sicherheitsniveaus. Hierbei setzen wir auf eine „Zero-Trust-Netzwerkumgebung" – „Vertraue niemanden, verifiziere jeden". Unser seit Jahren bestehendes Cybersicherheitsteam ist darüber hinaus in engem Austausch mit externen Cyberexperten, dem BSI und dem CERT-MV, um die Situation fortlaufend zu bewerten und entsprechende Sicherheitsmaßnahmen zu implementieren. Ein hundertprozentiger Schutz ist allerdings nicht möglich.

WAS GEBEN WIR MIT AUF DEM WEG?

Cybersecurity ist eine Managementaufgabe, denn eine Cyberattacke ist eine essenzielle Gefahr für die Reputation und das Funktionieren vieler Lebensbereiche. Bereits im Vorfeld sollten Verwaltungen/kommunale Unternehmen gemeinsam mit ihren kommunalen IT-Dienstleistern Experten in ihr Notfallmanagement einbinden. Aus unserer Sicht müssen Kompetenzen von kommunalen und Landes-IT-Dienstleistern gebündelt werden – die Einrichtung eines Landes-Cyberhilfswerks M-V wäre eine strategische Lösung.

EURITAS: DIGITALES EUROPA – NUR MIT UNS!

Die EU-Kommission hat die 2020er Jahre als digitale Dekade für Europa deklariert. Entsprechend werden aktuell Schlüsselthemen wie die Cloud-Strategie, die Open-Source-Strategie und die EU-Cybersicherheitsstrategie angegangen – und die Digitalisierung der Verwaltung vorangetrieben. Nun kommt es darauf an, das Praxiswissen aus den Kommunen einzubeziehen, denn: Hier entscheidet sich, ob die Strategien erfolgreich umgesetzt werden. EURITAS, der Verband der kommunalen IT-Dienstleister in Europa, bringt sich entsprechend ein.

ERSTER ANSPRECHPARTNER FÜR DIGITALE SOUVERÄNITÄT

Software-Konzerne wie Microsoft, Google oder Amazon dominieren den europäischen IT- und Cloud-Markt. Auch die öffentlichen Verwaltungen greifen auf ihre Produkte zurück. Ist die Abhängigkeit von einzelnen Anbietern zu groß, verletzt das Europas digitale Souveränität. Weder die Speicherung noch die Verarbeitung von Daten außerhalb der EU sind mit der DSGVO vereinbar. Wie können wir unabhängiger werden?

EURITAS zeigt Wege auf. So bringen wir uns beispielsweise maßgeblich bei der Erstellung einer europäischen Cloud-Strategie für die öffentliche Verwaltung ein und arbeiten gemeinsam an der Vernetzung der nationalen Government-Cloud-Lösungen. Zweites Beispiel ist Open Source: Mit Best-Practice-Beispielen aus europäischen Vorreiterländern wie Italien demonstrieren wir, wie öffentliche Verwaltungen ihre Software-Codes teilen können – Nachahmen ausdrücklich erwünscht.

MEHR AUSTAUSCH ZU CYBERSICHERHEIT

Mit der zunehmenden Digitalisierung von Verwaltungen steigt auch deren Verwundbarkeit durch Cyberattacken. Mit der EU Cybersecurity Strategy for the Digital Decade setzt die EU erste richtige Impulse. Jetzt geht es um die konkreten Schritte: Fachkräfte für das Thema ausbilden und für die Arbeit in Verwaltungen gewinnen, ein Frühwarnsystem für Verwaltungen entwerfen sowie den Austausch zwischen öffentlichen Organisationen verstärken.

Auch dabei geht EURITAS voran. Unsere Mitglieder tauschen sich bereits regelmäßig strukturiert und persönlich über Sicherheitsvorfälle aus. Das intensivieren wir: Wir zeigen etwaige Bedrohungslagen auf, analysieren sie und ermöglichen, über Best-Practice-Beispiele voneinander zu lernen. Unser Wissen teilen wir gerne mit den verantwortlichen Stakeholdern auf EU-Ebene.

EURITAS MEHR GEWICHT VERLEIHEN

All das zeigt: Die grenzüberschreitende Kooperation der IT-Dienstleister stärkt Europa. Dazu zählen auch folgende zwei Themen, die EURITAS mehr Gewicht verleihen:

- **Ausschreibungen:** Über EURITAS sollen sich öffentliche IT-Dienstleister quer durch Europa noch besser bei der Teilnahme an Ausschreibungen zusammenschließen können und damit Aufwand und Kosten reduzieren – was auch gut für ihre kommunalen Auftraggeber ist.
- **EU-Fördergelder:** Wir wollen unsere Mitglieder noch effektiver dabei unterstützen, Fördermittel für wegweisende IT-Projekte im Verwaltungsbereich zu erhalten – und so dazu beitragen, dass wirklich die besten Ideen gefördert werden.

Wir werden unsere Stimme in Brüssel weiter stärken. Nächster Meilenstein: Am 13. und 14. Oktober 2022 bieten wir mit dem EURITAS General Committee Meeting eine Diskussionsplattform mit Stakeholdern aus Exekutive und Legislative. Zudem wollen wir unsere Präsenz in Brüssel verstärken. Als neu gewählter Präsident freue ich mich, den Verband in dieser spannenden Aufbruchszeit führen zu dürfen.

Link zur EU Cybersecurity Strategy: bit.ly/EU-cyber

Dr. Ralf Resch ist Geschäftsführer von VITAKO und Präsident von EURITAS.

DURCHLESEN

Deutscher Städtetag – SMART CITIES NACHHALTIG FÖRDERN

Smart-Citiy-Digitalisierungsprojekte werden in vielen deutschen Kommunen gefördert. Allerdings: Anstatt die Herausforderungen gemeinsam anzugehen, entwickeln die Kommunen zumeist Einzellösungen. Folge ist ein ineffizienter Flickenteppich, so der Deutsche Städtetag in seinem Positionspapier vom Juni 2022. Um die strukturellen Probleme zu lösen, fordert der Spitzenverband fünf Maßnahmen für die nachhaltige Smart-City-Förderung:

- **Plattformansatz:** Bund, Länder und Kommunen müssen sich auf verbindliche Standards einigen und darauf aufbauend einen übergreifenden Plattformansatz verfolgen.
- **Förderung:** Die Förderung von Digitalisierungsprojekten muss gezielt und gleichzeitig flexibel erfolgen. Letzteres beispielsweise durch Abruf- und Prämienförderung.
- **Rahmen:** Maßnahmen müssen rechtlich und fachlich begleitet sowie evaluiert werden. Notwendig sind zudem ein innovationsfreundlicherer Rechtsrahmen sowie förderfähige Experimentierklauseln und Reallaborräume.
- **Vernetzung:** Schon bei der Projektplanung muss auf eine möglichst hohe Vernetzung und Nachnutzung abgezielt werden. Open Source spielt dabei eine wesentliche Rolle.
- **Qualifizierung:** Kommunalverwaltungen sollten mehr Kompetenzen und Wissen aufbauen sowie Erfahrung nachhaltig sichern. Innovationslabs sind stärker zu nutzen.

Zum Positionspapier des Städtetags:
https://bit.ly/smarte_staedte

DURCHSTARTEN

EFFIZIENTER, FAIRER & VALIDER: NEUE APP ERLEICHTERT PERSONALAUSWAHL

Die Auswahl von neuem Personal ist aufwändig und schwierig: Wie können Verantwortliche ihre Bewerberinnen und Bewerber fair und objektiv vergleichen, um die optimale Entscheidung zu treffen? Häufig stützt sich die Entscheidung auf lückenhafte Notizen und ein „Bauchgefühl".

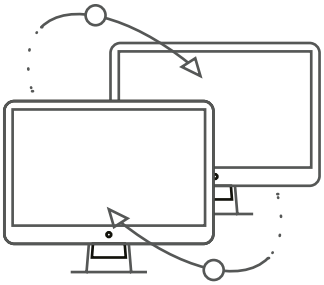
Hier hilft Applysia: Basierend auf dem vorher definierten Anforderungsprofil können Personalverantwortliche Kandidatinnen und Kandidaten in Echtzeit bewerten. Applysia ermöglicht einen grafischen Vergleich der jeweiligen Stärkenprofile und objektiviert die Personalauswahl. Mehrere Kommunen, kommunale Energieversorger und Bundesbehörden setzen die App bereits ein, die sich an spezielle Bedürfnisse anpassen lässt.

Für öffentliche Verwaltung besonders relevant: Applysia läuft nach den Prinzipien „privacy by design" und Datenminimierung, ist natürlich DSGVO-konform und bietet eine verschlüsselte Kommunikation, die über deutsche Rechenzentren mit ISO27001-Zertifizierung läuft.

https://applysia.de/produkt/

DURCHRUFEN

OPEN SOURCE FÜR DIE VERWALTUNG: OPEN CODE AKTIV



Ein weiterer Schritt auf dem Weg zu digitaler Souveränität: Nach erfolgreicher Pilotphase ist die Open-Source-Plattform Open CoDE nun aktiv. Seit Juli 2022 können Bund, Länder und Kommunen auf dem Portal gemeinsam Open-Source-Software entwickeln und rechtssicher austauschen. Das macht es öffentlichen Verwaltungen leichter, entsprechende Produkte einzusetzen. Die ersten Verwaltungsanwendungen gibt es bereits, beispielsweise die Personenstandsdienste der AKDB.

Die Idee zu Open CoDE entstand in einer Arbeitsgruppe aus Vertretern von VITAKO, der Open Source Business Alliance (OSBA) sowie weiteren Expertengremien. Umgesetzt wurde sie vom BMI und den Ländern Nordrhein-Westfalen und Baden-Württemberg. Mittlerweile ist Open CoDE ein Schlüsselprojekt in der Digitalagenda des Bundes, der sie derzeit auch weiterfinanziert.

Die Plattform lebt von der Beteiligung. Sie kann Verwaltungen flexibler, sicherer, unabhängiger und innovativer machen – wenn Entwicklerinnen und Entwickler sowie die zahlreichen Akteurinnen und Akteure Lösungen und Ideen auf ihr austauschen, Anwendungen teilen und gemeinsam weiterentwickeln. Gut genutzt ist sie auch eine enorme Chance, die OZG-Umsetzung voranzutreiben.

Zum Open Source Repository Code: https://opencode.de/

www.vitako.de

VITAKO MIT NEUER WEBSEITE

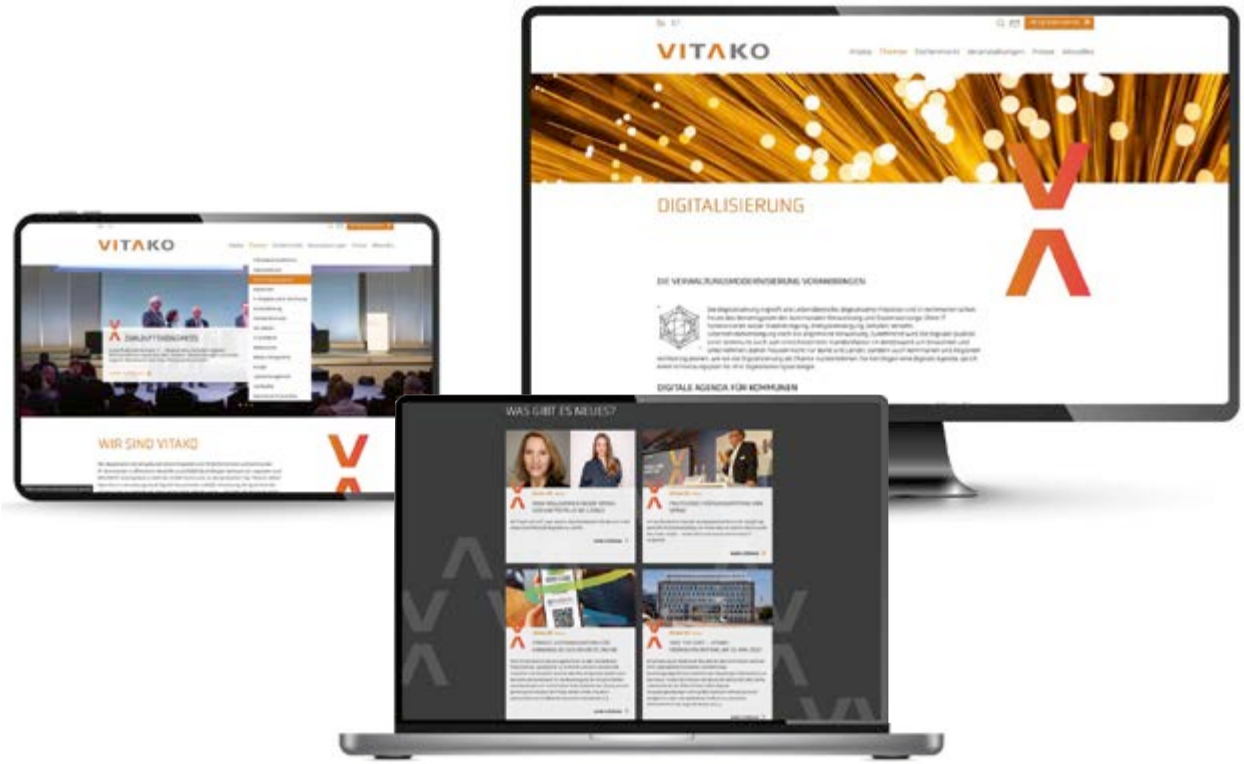
ERSTE ANLAUFSTELLE FÜR DIGITALE VERWALTUNG

Inhaltlich kompetent, voller Tatkraft und transparent. Dafür steht VITAKO. Und das spiegelt seit Juni 2022 auch unser Web-Auftritt. Der Mehrwert für die Nutzerinnen und Nutzer im Überblick:

- **Schnelle Information:** Mit wenigen Klicks erhalten User wesentliche Fakten zu unseren Themen – von IT-Sicherheit bis Open Data.
- **Vertiefende Inhalte:** Unter „Aktuelles" können Besucher unsere Publikationen vom politischen Infobrief bis zum Branchenmagazin „VITAKO aktuell" herunterladen – mehr Hintergrund geht nicht.
- **Immer aktuell:** Neueste Meldungen und Veranstaltungen von VITAKO sowie News aus der Branche publizieren wir auf der Startseite sowie unter „Aktuelles" – stets aktuell.
- **Transparent:** Wer steht eigentlich hinter VITAKO? Neben unseren Mitgliedern stellen wir auch unseren Vorstand und unsere Facharbeitsgruppen vor.
- **Direkter Kontakt:** Wir sind immer für Sie zu erreichen – die Kontaktdaten unserer Mitarbeiterinnen und Mitarbeiter finden Besucher unter „Geschäftsstelle".

Auch das Design spiegelt unsere Werte wider. Modern, dynamisch und mit hohem Wiedererkennungswert.

Alles unter: www.vitako.de



VITAKO HERBSTEMPFANG 2022: CYBERSICHERHEIT

Wir freuen uns, am 20. Oktober 2022 wieder Vertreterinnen und Vertreter aus Politik, Wirtschaft und Journalismus sowie unsere Mitglieder zum VITAKO Herbstempfang einzuladen. Das Thema lautet Cybersicherheit. Damit wollen wir die Schwerpunktsetzung dieser VITAKO aktuell auch im persönlichen Gespräch fortsetzen und weitere Impulse bieten.

Regelmäßig bringen wir Schlüsselakteure zusammen, um Themen wie Cybersicherheit, digitale Souveränität oder die Weiterentwicklung des Onlinezugangsgesetzes zu diskutieren und neue Lösungen anzustoßen.

Im Rahmen des VITAKO Frühjahrsempfangs konnte die Impact-Studie des Instituts der Deutschen Wirtschaft diskutiert werden. Hier: Dr. Ralf Resch, VITAKO-Geschäftsführer, die Moderatorin und ehemalige Bundestagsabgeordnete Elvan Korkmaz-Emre und Dr. Ralf Beyer, VITAKO-Vorstandsvorsitzender (von links nach rechts).

NEUE GESICHTER BEI VITAKO: KATRIN GIEBEL UND ISABELL GROSS

VITAKO erweitert sein Team. Seit 1. Juli 2022 unterstützen Katrin Giebel und Isabell Gross die VITAKO-Geschäftsstelle.

Katrin Giebel treibt als Bereichsleiterin Verwaltungsdigitalisierung die Themen digitale Verwaltung der Zukunft, Green-IT sowie Datenökonomie und KI voran. Sie ist studierte Informationswissenschaftlerin und verfügt als zertifizierte Projektleiterin für Verwaltungsdigitalisierung und Wissensmanagement über umfassende Expertise. Über mehrere Jahre hat sie an der Schnittstelle von Politik, Verwaltung und Behörden gearbeitet – und etwa bei Unternehmen der Bundesverwaltung Digitalisierungsprojekte umgesetzt.

Isabell Gross ist die neue Office-Managerin im Team. Sie verantwortet Empfang, Sekretariat, Buchhaltung und Logistik, behält den Überblick über alle Verwaltungsebenen bei uns und unterstützt Geschäftsführer Dr. Ralf Resch als Assistentin. Zuvor war sie im Sekretariat einer großen Rechtsanwaltskanzlei tätig. Als ehemalige Chef de Rang bringt sie zudem Fähigkeiten aus der System- und Privatgastronomie mit.

Wir freuen uns, mit Katrin Giebel und Isabell Gross zwei erfahrene und kompetente Kolleginnen gewonnen zu haben.

Katrin Giebel ist Bereichsleiterin Verwaltungsdigitalisierung.

Isabell Gross ist Office-Managerin.

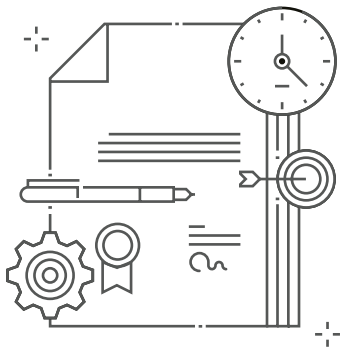
Elena Yorgova-Ramanauskas ist CIO des Saarlandes.

NEUE CIO IM SAARLAND

Elena Yorgova-Ramanauskas ist seit Juni 2022 neue CIO des Saarlandes. Bereits seit April 2022 ist sie Staatssekretärin des saarländischen Ministeriums für Wirtschaft, Innovation, Digitales und Energie. Die parteilose Politikerin hat Betriebswirtschaftslehre und Internationale Wirtschaftsbeziehungen studiert und ist examinierte Wirtschaftsprüferin und Steuerberaterin. Zuletzt war sie bei der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft Dornbach als Geschäftsführerin für den Bereich Abschlussprüfung tätig. Zuvor war sie Direktorin bei der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers. In ihrer Laufbahn hat sie insbesondere große und mittelständische sowie familiengeführte Unternehmen betreut.

DIE DIGITALE BAUGENEHMIGUNG

BAUGENEHMIGUNG KOLLABORATIV UND EFFIZIENT BEANTRAGEN



Wer in Deutschland ein Gebäude errichten möchte, benötigt dafür meist eine Baugenehmigung. Der entsprechende Antrag erreicht schnell einen Umfang von mehreren Aktenordnern und ist in mehrfacher Ausführung einzureichen. Werden weitere Behörden in die Antragsprüfung einbezogen, bedeutet das einen hohen logistischen Aufwand. Circa 220.000 Baugenehmigungen werden jährlich in Deutschland erteilt, wobei jedes Bundesland seine eigene Bauordnung hat.

Mecklenburg-Vorpommern hat im Rahmen des OZG für das vereinfachte Baugenehmigungsverfahren eine vollständig digitale Antragstellung entwickelt, die auf das jeweilige Landesrecht konfiguriert werden kann und seit 2021 eingesetzt wird. Die Referenzimplementierung steht im FIT-Store zur Nachnutzung bereit. Mehrere Bundesländer haben bereits Interesse angemeldet.

GESTALTUNG/BEDIENKOMFORT

Die Vorteile des digitalen Bauantrags liegen vor allem in der Möglichkeit, durch seine Realisierung als Cloud-Lösung mehreren Teilnehmenden gleichzeitig Zugriff auf den Antrag zu geben. Für jeden Antrag wird ein virtueller Vorgangsraum eingerichtet, in dem verschiedene Personen in ihren Rollen als Bauherrin oder Entwurfsverfasser kollaborativ und effizient an der Erstellung arbeiten können. Verzögerungen können so transparent nachvollzogen werden. Ebenso kann daran mitgewirkt werden, diese zu beseitigen.

Erst wenn alle Beteiligten den Antrag freigezeichnet haben, geht er an die Behörde. Postwege und Medienbrüche entfallen. Fehlen den Behörden bei der Bearbeitung Unterlagen, kann über das Portal eine Nachricht an die Antragsstellenden geschickt werden, die dort direkt einen Anhang hochladen können. Der aktuelle Bearbeitungsstand kann jederzeit eingesehen werden. Die Genehmigung selbst kann vom Portal heruntergeladen werden und das Bezahlen der Gebühren erfolgt über E-Payment.

ANWENDBARKEIT

Der Antrag steht nur auf Deutsch zur Verfügung. Es gibt eine Anleitung, die schrittweise durch die Funktionen führt. Für die Barrierefreiheit können individuelle Einstellungen an der Schriftgröße, dem Kontrast und der Darstellungsbreite vorgenommen werden. Eine Hinweisfunktion weist zusätzlich auf noch offen gelassene Stellen hin. Eine feldbasierte Zwischenspeicherung verhindert, dass Daten verloren gehen.

Nutzen	
Innovationsgrad	4 ★★★★
Einbindung in den Verwaltungsprozess	5 ★★★★★
Gestaltung	
Niedrigschwelliger Zugang	4 ★★★★
Intuitive Bedienbarkeit	4 ★★★★
Ansprechendes Design	5 ★★★★★
Mehrere Sprachen	0
Fehlerfreie Bedienung	5 ★★★★★
Inhalte	
Informationsgehalt	5 ★★★★★
Zielgruppenorientierung	5 ★★★★★
Aktualität und Pflege	5 ★★★★★
Barrierefreiheit	
Erklärung zur Barrierefreiheit (erforderlich nach BITV 2.0)	☑
Feedback-Mechanismus	☑

Notenstufen von 1 (schlecht) bis 5 (am besten)
☑ = vorhanden; ☐ = nicht vorhanden

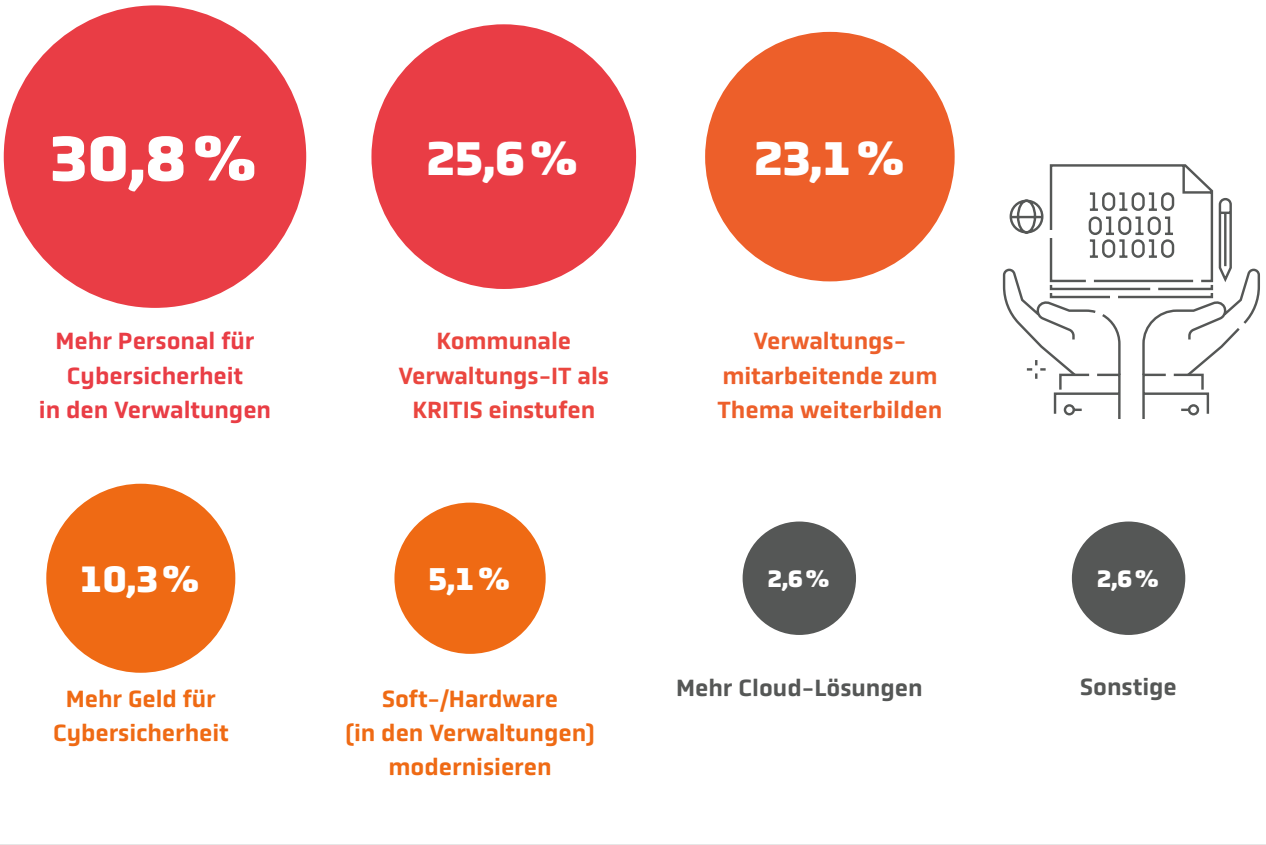
Baugenehmigung digital beantragen:
bit.ly/OZG-Bau

Rosemarie Bähne ist Mitarbeiterin beim Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS).

CYBERSICHERHEIT: NICHT NUR EINE FRAGE DER RESSOURCEN

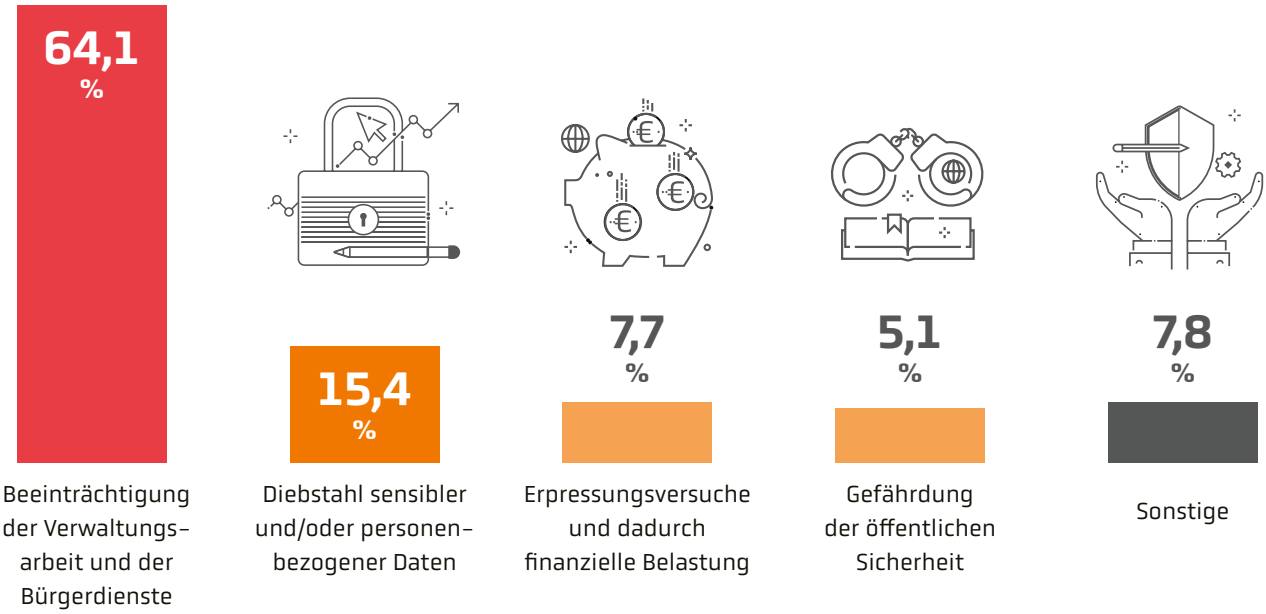
Die kommunalen IT-Dienstleister verfügen zum Thema Cybersicherheit über ein besonderes Erfahrungswissen. Wo sehen sie die größten Risiken – und wie sollten die Kommunen darauf reagieren? Ergebnisse der aktuellen Umfrage unter den VITAKO-Mitgliedern.

Mit welchen Maßnahmen können sich Kommunen am besten gegen Cyberattacken wappnen?

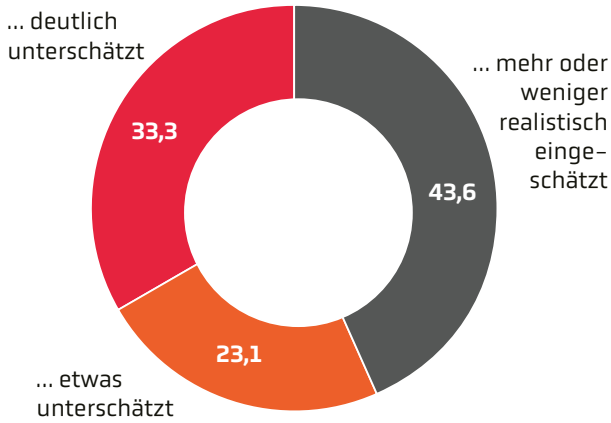


Die Umfrage wurde vom Marktforschungsunternehmen Hiestermann & Frömchen GmbH durchgeführt.

Was sind aktuell die größten IT-Sicherheitsrisiken für die kommunalen Verwaltungen?

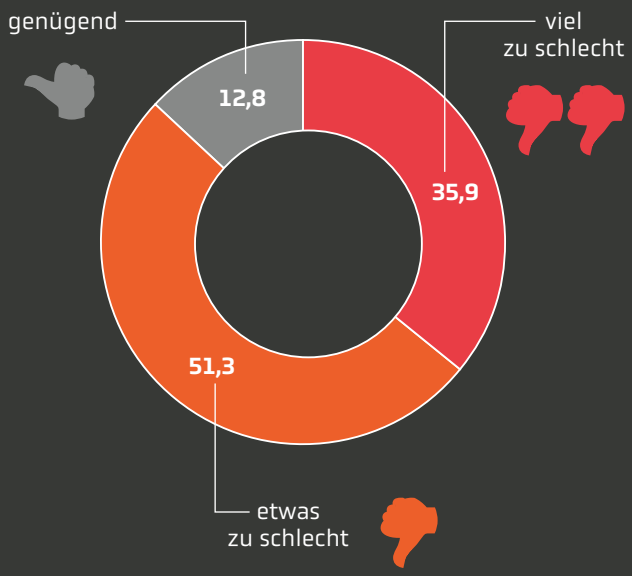


Wie realistisch schätzen die politischen Entscheider in den Kommunen Cyber-gefahren ein? Die Gefahren werden ... .



... deutlich überschätzt = 0 %
... etwas überschätzt = 0 %

Wie sind die Kommunalverwaltungen in Bezug auf das für Cybersicherheit verant-wortliche Personal ausgestattet?



rundungsbedingte Ungenauigkeiten

IMPACT-STUDIE: ALLE ERGEBNISSE ALS BROSCHÜRE AUFBEREITET

Das Institut der Deutschen Wirtschaft (iw) hat im Auftrag von VITAKO im Mai 2022 erstmals den Mehrwert der kommunalen IT-Dienstleister für Deutschland umfassend berechnet. Kernergebnis: Die digitalen Dienste der VITAKO-Mitglieder führen zu Einsparungen von rund 5,1 Milliarden Euro pro Jahr. Dieser Betrag weist den Gegenwert für die zig Millionen Stunden aus, die in Verwaltungen, bei den Unternehmen sowie den Bürgerinnen und Bürgern eingespart werden.

Alle Ergebnisse stehen inzwischen als kompakte Broschüre zur Verfügung. Sie kann unter www.vitako.de/handreichungen heruntergeladen oder in gedruckter Form bestellt werden – eine formlose Mail an Frau Aboli Lion lion@vitako.de genügt.

TERMINE

26. September 2022, Düsseldorf

EIN JAHR EFA-UMSETZUNG ALS ERFOLGSMODELL

https://wsp.mohr-live.de

20. Oktober 2022, Berlin

VITAKO HERBSTEMPFANG

www.vitako.de

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, Gestaltung: Köster Kommunikation

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. Alle Rechte vorbehalten. Nachdruck oder elektronische Verbreitung nur mit Zu stimmung des Herausgebers.

Druck: triggermedien, Berlin

Erscheinungsweise: 4 Ausgaben / Jahr, Auflage: 5.000

Autoren und Mitwirkende dieser Ausgabe:
Jürgen Abelshauser, PoVitako; Manuel Atug, AG KRITIS; Rosemarie Bähne, Fraunhofer-Institut; Markus Batz und Thomas Büttner, Stadt Köln; Dr. Rolf Beyer, KDO; Matthias Effenberger, SIS/KSM; Jens Fromm, govdigital; Steffen Kleinmanns, digitalfabriX; Dr. Christoph Lindner, Universität Hamburg; Dr. Ralf Resch, VITAKO; Dr. Kay Ruge und Christian Stuffrein, DLT; Johann Saathoff, Parlamentarischer Staatssekretär; Arne Schönbohm, BSI; Bernadette Thielen, Baldeney IT-Consulting

Bildnachweise:
Titel: wutzkoh – stock.adobe.com, Julia Naether – stock.adobe.com, smux – stock.adobe.com; S. 4, 7 Andrey Popov – stock.adobe.com, S. 4 Porträt: BSI-Weiler; S. 5, 21 iStock.com/Liyao Xie; S. 5 iStock.com/Drazen Zigic; S. 9 Porträt: Fionn Grosse; S. 11 chayanit – stock.adobe.com; S. 12, 13 Porträts: BSI-Weiler; S. 17 Porträt: atelier-fotogreif@t-online.de; S. 18 Porträt: www.oleheinrich.com; S. 19 Porträt: Philipp Guelland; S. 25 BirgitKorber – stock.adobe.com; S. 28 iStock.com/Helen Datsko; S. 29 dirk hasskarl/fotografie, Porträt links: Leistenschneider; S. 30 Porträt: MWIDE-Oliver Dietze; S. 31 Porträt: Fraunhofer FOKUS

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

ISSN 2194-1165

DIE NÄCHSTE „VITAKO AKTUELL“ ERSCHEINT IM DEZEMBER 2022.

dataport kommunal

Die Kommune der Zukunft ist digital

- und souverän.

Wir unterstützen Sie.

www.dataport-kommunal.de

AKDB Kommunalforum

digital richtung zukunft

Es ist wieder Zeit für das große Treffen der kommunalen Familie.
Endlich wieder gemeinsam vor Ort. In Garching bei München.
Für Experten aus Verwaltung, Politik und Wissenschaft.
Es ist Zeit fürs 5. AKDB Kommunalforum!

20. Oktober 2022
Jetzt anmelden!

www.akdb.de/kommunalforum